The Right to an Explanation in Practice: Insights from Case Law for the GDPR and the AI Act

mr. Ljubiša Metikoš, dr. Jef Ausloos[1]

[This is a pre-publication draft paper, forthcoming in *Law, Innovation, and Technology* 17.2, October 2025. The final version is subject to further revisions.]

Abstract

The right to an explanation under the GDPR has been much discussed in legal-doctrinal scholarship. This paper expands upon this academic discourse, by providing insights into what questions the application of the right to an explanation has raised in legal practice. By looking at cases brought before various judicial bodies and data protection authorities across the European Union, we discuss questions regarding the scope, content, and balancing exercise of the right to an explanation. We argue, moreover, that these questions also raise important interpretative issues regarding the right to an explanation under the AI Act. Similar to the GDPR, the AI Act's right to an explanation leaves many legal questions unanswered. Therefore, the insights from the already established case law under the GDPR, can help us to understand better how the AI Act's right to an explanation should be understood in practice.

Keywords: GDPR, AIA, right to an explanation, transparency, AI

[1] The authors would like to thank Thomas Streinz for his thoughtful comments on this paper.

Contents

1. Introduction

It might be an understatement to say that in the past decade, the right to an explanation has sparked debate among legal scholars.[2] Its enigmatic formulation in the EU General Data

[2] Ljubiša Metikoš, 'Explaining and Contesting Judicial Profiling Systems' (2024) 2024 Technology and Regulation 188 Lilian Edwards and Michael Veale, 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?' 15; Paul B de Laat, 'Algorithmic Decision-Making Employing Profiling: Will Trade Secrecy Protection Render the Right to Explanation Toothless?' (2022) 24 Ethics and Information Technology 17; Emre Bayamlıoğlu, 'The Right to Contest Automated Decisions under the General Data Protection Regulation: Beyond the so-Called "Right to Explanation"' (2022) 16 Regulation & Governance 1058; Diana Dimitrova, 'The Right to Explanation under the Right of Access to Personal Data: Legal Foundations in and beyond the GDPR' (2020) 6 European Data Protection Law Review (EDPL) 211; Edwards and Veale; Bryan Casey, Ashkon Farhangi and Roland Vogl, 'Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise' (2019) 34 Berkeley Technology Law Journal 143; Elena Falletti, 'Automated Decisions and Article No. 22 GDPR of the European Union: An Analysis of the Right to an "Explanation"' (27 December 2019) <https://papers.ssrn.com/abstract=3510084> accessed 11 December 2022; Tae Wan Kim and Bryan R Routledge, 'Informational Privacy, A Right to Explanation, and Interpretable AI', *2018 IEEE Symposium on Privacy-Aware Computing (PAC)* (2018); Margot E Kaminski, 'Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability' (2018) 92 Southern California Law Review 1529; Margot E Kaminski, 'The Right to Explanation, Explained' (2019) 34 Berkeley Technology Law Journal 189; Margot E Kaminski and Jennifer M Urban, 'The Right to Contest AI' 121 Colombia Law Review 93; Gianclaudio Malgieri, 'Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations' (2019) 35 Computer Law & Security Review 105327; Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (Social Science Research Network 2017) SSRN Scholarly Paper ID 3088976 <https://papers.ssrn.com/abstract=3088976> accessed 30 October 2021; Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76; Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR' (2017) 31 Harv. JL & Tech. 841; Bryce Goodman and Seth Flaxman, 'EU Regulations on Algorithmic Decision-Making and a "Right to Explanation"', *2016 ICML Workshop on Human Interpretability in Machine Learning* (2015); Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233; Claudio Sarra, 'Put Dialectics into the Machine: Protection against Automatic-Decision-Making through a Deeper Understanding of Contestability by Design' (2020) 20 Global Jurist <https://www.degruyter.com/document/doi/10.1515/gj-2020-0003/html> accessed 28 February 2022; Andrew D Selbst and Solon Barocas, 'The Intuitive Appeal of Explainable Machines' (2018) 87 Fordham Law Review 1085; Tal Z Zarsky, 'Transparent Predictions' (2013) 2013 University of Illinois Law Review 1503; Ljubiša Metikoš, 'Leg het me nog één keer uit: het recht op een uitleg na Uber en Ola. Annotatie bij Hof Amsterdam, 4 april 2023' Privacy & Informatie <https://www.uitgeverijparis.nl/reader_viewer_li/212735/1001688409/abbb98b14677f8a6c1eba0ce9b3f4f86f4027c3d#voetnootnummer8> accessed 29 December 2023; Aviva de Groot, *Care to Explain?: A Critical Epistemic in/Justice Based Analysis of Legal Explanation Obligations and Ideals for 'AI'-Infused Times* (2023); Michael Veale and Lilian Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling' (2018) 34 Computer Law & Security Review 398; Edwards and Veale. Lilian Edwards and Michael Veale, 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?' 15; Paul B de Laat, 'Algorithmic Decision-Making Employing Profiling: Will Trade Secrecy Protection Render the Right to Explanation Toothless?' (2022) 24 Ethics and Information Technology 17; Emre Bayamlıoğlu, 'The Right to Contest Automated Decisions under the General Data Protection Regulation: Beyond the so-Called "Right to Explanation"' (2022) 16 Regulation & Governance 1058; Diana Dimitrova, 'The Right to Explanation under the Right of Access to Personal Data: Legal Foundations in and beyond the GDPR' (2020) 6 European Data Protection Law Review (EDPL) 211; Edwards and Veale; Bryan Casey, Ashkon Farhangi and Roland Vogl, 'Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise' (2019) 34 Berkeley Technology Law Journal 143; Tae Wan Kim and Bryan R Routledge, 'Informational Privacy, A Right to Explanation, and Interpretable AI', *2018 IEEE Symposium on Privacy-Aware Computing (PAC)* (2018); Margot E Kaminski, 'Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability' (2018) 92 Southern California Law Review 1529; Margot E Kaminski, 'The Right to Explanation, Explained' (2019) 34 Berkeley Technology Law Journal 189; Margot E Kaminski and Jennifer M Urban, 'The Right to Contest AI' 121 Colombia Law Review 93; Gianclaudio Malgieri, 'Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations' (2019) 35 Computer Law & Security Review 105327; Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 243; Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76; Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR' (2017) 31 Harv. JL & Tech. 841; Bryce Goodman and Seth Flaxman, 'EU Regulations on Algorithmic Decision-Making and a "Right to Explanation"', *2016 ICML Workshop on Human Interpretability in Machine Learning* (2015); Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233; Claudio Sarra, 'Put Dialectics into the Machine: Protection against Automatic-Decision-Making through a Deeper Understanding of Contestability by Design' (2020) 20; Andrew D Selbst and Solon Barocas, 'The

Protection Regulation (GDPR) has raised many questions regarding how exactly data subjects can exercise this right. Scholars have debated what the scope of the right to an explanation is, what kind of information must be disclosed under it, as well as how we should balance this right vis à vis other rights and interests. Yet, little work has been done on the modest, but growing, number of cases that are starting to emerge on the right to an explanation across the EU,[3] let alone how that case law may affect the new right to an explanation under the upcoming AI Act (AIA).[4]

For the purposes of this paper, we identified relevant cases across several European jurisdictions; Austria, the Netherlands, Sweden, Denmark, Finland, and Germany (see Annex 1). This gradually expanding body of case law is then used to tackle some unresolved questions in existing legal scholarship, with the specific goal of informing the interpretation of the new right to an explanation emerging under the AIA. We start with a short review of how the right to an explanation, lacking a concrete and direct formulation in the GDPR, has taken shape in legal scholarship.

To this end, we provide an analysis of art. 13, 14, 15, and 22 GDPR; showcasing two different methods of deducing the right to an explanation from these provisions. First, one can read art. 22(3) GDPR in light of Recital 71 GDPR. Alternatively, one can also deduce the right to an explanation from art. 13, 14, or 15 GDPR.

Intuitive Appeal of Explainable Machines' (2018) 87 Fordham Law Review 1085; Tal Z Zarsky, 'Transparent Predictions' (2013) 2013 University of Illinois Law Review 1503; Ljubiša Metikoš, 'Leg het me nog één keer uit: het recht op een uitleg na Uber en Ola. Annotatie bij Hof Amsterdam, 4 april 2023' Privacy & Informatie; Aviva de Groot, *Care to Explain?: A Critical Epistemic in/Justice Based Analysis of Legal Explanation Obligations and Ideals for 'AI'-Infused Times* (2023); Michael Veale and Lilian Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling' (2018) 34 Computer Law & Security Review 398; Edwards and Veale.

[3] *Bundesverwaltungsgericht* [2021] Federal Administrative Court, Austria ECLI:AT:BVWG:2021:W211.2234354.1.00, W211 2234354-1; *Datatilsynet* [2020] DPA, Denmark 2019-421-0028; *Datenschutzbehörde* [2020] DPA, Austria ECLI:AT:DSB:2020:2020.0.436.002; *Rechtbank Amsterdam* [2021] District Court, The Netherlands ECLI:NL:RBAMS:2021:1018, C/13/692003 / HA RK 20-302; *SCHUFA* [2023] CJEU ECLI:EU:C:2023:957; *Rechtbank Den Haag* [2020] District Court The Hague, The Netherlands ECLI:NL:RBDHA:2020:1013, C-09-585239-KG ZA 19-1221; *Verwaltungsgericht Wiesbaden* [2021] Administrative Court Wiesbaden, Germany ECLI:DE:VGWIESB:2021:1001.6K788.20.WI.00, 6 K 788/20.WI; *Berliner Beauftragte für Datenschutz und Informationsfreiheit* (DPA Berlin, Germany); *Opinion of Advocate General Pikamäe in the SCHUFA case* [2023] CJEU ECLI:EU:C:2023:220; *Klarna* [2023] Stockholm Administrative Court, Sweden 7679-22; *Rechtbank Gelderland* [2022] District Court Gelderland, The Netherlands ECLI:NL:RBGEL:2022:6145, C/05/404505 / HA RK 22-99. *Bundesverwaltungsgericht* [2021] Federal Administrative Court, Austria ECLI:AT:BVWG:2021:W211.2234354.1.00, W211 2234354-1; *Datatilsynet* [2020] DPA, Denmark 2019-421-0028; *Datenschutzbehörde* [2020] DPA, Austria ECLI:AT:DSB:2020:2020.0.436.002; *Rechtbank Amsterdam* [2021] District Court, The Netherlands ECLI:NL:RBAMS:2021:1018, C/13/692003 / HA RK 20-302; *SCHUFA* [2023] CJEU ECLI:EU:C:2023:957; *Rechtbank Den Haag* [2020] District Court The Hague, The Netherlands ECLI:NL:RBDHA:2020:1013, C-09-585239-KG ZA 19-1221; *Verwaltungsgericht Wiesbaden* [2021] Administrative Court Wiesbaden, Germany ECLI:DE:VGWIESB:2021:1001.6K788.20.WI.00, 6 K 788/20.WI; *Berliner Beauftragte für Datenschutz und Informationsfreiheit*, DPA Berlin, Germany; *Opinion of Advocate General Pikamäe in the SCHUFA case* [2023] CJEU ECLI:EU:C:2023:220; *Klarna* [2023] Stockholm Administrative Court, Sweden 7679-22; *Rechtbank Gelderland* [2022] District Court Gelderland, The Netherlands ECLI:NL:RBGEL:2022:6145, C/05/404505 / HA RK 22-99; *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam,* 200295742/01 [2023] Appeals Court Amsterdam, The Netherlands ECLI:NL:GHAMS:2023:793; *Verwaltungsgerichtshof* [2023] Supreme Administrative Court Austria, ECLI:AT:VWGH:2023:RO2021040010.J09, Ro 2021/04/0010-11; Bundesverwaltungsgericht [2023] Federal Administrative Court Austria ECLI:AT:BVWG:2023:W252.2237416.1.00; Bundesverwaltungsgericht [2023] Federal Administrative Court Austria ECLI:AT:BVWG:2023:W256.2234851.1.00 W256 2234851-1; *Bundesverwaltungsgericht* [2023] Federal Administrative Court ECLI:AT:BVWG:2023:W252.2246581.1.00, W252 2246581-1/6E.

[4] European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

Next, we formulate three key interpretive issues of the right to an explanation, which have been raised in scholarly literature and the relevant case law:

- Firstly, we ask what the *scope* is of the right to an explanation. We look for example at whether the right to an explanation only applies to solely automated decision-making or if it also encompasses situations in which automated data processing merely assists a human decision-maker.[5]
- Secondly, we discuss what the right to an explanation encompasses *substantively*; i.e. what kind of information needs to be disclosed. To this end, we also look at whether the right requires explanations of how a particular output or decision was reached, or how the automated decision-making system works in general. In legal scholarship, the difference between these explanations has also been referred to as '*ex post*' and '*ex ante*' explanations, '*Subject-Centric Explanations'* and '*Model-Centric Explanations'*, or '*strong'* and '*weak explanations'*.[6]
- Thirdly, we discuss how one must deal with the issue of *balancing* the right to an explanation, with other interests and rights, such as the right to a fair trial, intellectual property rights,[7] trade secrets, as well as national security interests,[8] and business interests.[9]

Building on the interpretative framework that we develop based on the GDPR's case law, we also explore the AIA's right to an explanation. The new AIA also provides a right to an explanation for specific high-risk AI-systems that inform decision-making in a variety of contexts under art. 86 AIA. This new provision does not amend the right to an explanation under the GDPR, but rather provides an additional right that individual decision-subjects can exercise besides the right to an explanation under the GDPR.

We compare these two different regimes to understand the full scope of the right to an explanation under EU law. From the discussion of the case law on the GDPR, we shall also aim to interpret, and elaborate upon, the AI-Act's right to an explanation, as well as understand what future obstacles the exercise of explainability rights might face.

2. The right to an explanation under the GDPR

Under the GDPR, there is not one provision that explicitly provides a person with a 'right to an explanation'. Rather, legal scholars have proposed two interpretative methods to *deduce* the right to an explanation from a variety of different provisions and Recitals. The first method relies directly on a number of safeguards that are required to be put in place by art. 22 GDPR. The second relies on the right to '*meaningful information about the logic involved'*, present in art. 13, 14, and 15 GDPR.[10] In the following section, we discuss both methods. This shall

[5] *SCHUFA* (n 2); *Rechtbank Amsterdam* (n 2); Wachter, Mittelstadt and Floridi (n 1); Malgieri and Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (n 1). *SCHUFA* (n 3); *Rechtbank Amsterdam* (n 3); Wachter, Mittelstadt and Floridi (n 2); Malgieri and Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (n 2); *Landsgericht Traunstein* [2024] Regional Court Traunstein 6 O 2465/23.

[6] de Laat (n 1); Edwards and Veale (n 1); Wachter, Mittelstadt and Floridi (n 1). de Laat (n 1); Edwards and Veale (n 1); Wachter, Mittelstadt and Floridi (n 1).

[7] de Laat (n 1).

[8] *Rechtbank Den Haag* (n 2).

[9] *Rechtbank Amsterdam* (n 2); de Laat (n 1). *Rechtbank Amsterdam* (n 2); de Laat (n 1).

[10] Kaminski, 'The Right to Explanation, Explained' (n 1).

provide a starting point for the various scholarly questions that have arisen regarding how a right to an explanation would function in practice. These questions, which have their basis in academic literature, are also discussed in the case law that has arisen regarding the right to an explanation. In turn, this shows the wide practical and societal importance of these questions for the use of (semi-)automated decision-making systems in the EU.

2.1. Safeguards listed in art. 22 GDPR and Recital 71

Art. 22 GDPR, while not explicitly mentioning any transparency rights, plays a crucial role in the scholarly discussion on the right to an explanation. This is in part because it formulates a variety of obligations on data controllers regarding the use of automated decision-making systems.

Paragraph (1) of this provision states that a data subject shall not be subject to a decision based solely on automated processing when such a decision produces legal effects or significantly affects the data subject in question. Paragraph (2), subsequently, formulates three exemptions to this general ban:

Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
(b) is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
(c) is based on the data subject's explicit consent.

Finally, paragraph 3 states that in case the decision is taken based on ground (a) or (c), the data controller must implement '*suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision*.'

One might be surprised to see, however, that the right to an explanation is not explicitly mentioned in this list of safeguards. This is in part because art. 22 GDPR is not centrally aimed at providing a right to an explanation, but rather to put a stop to certain kinds of solely automated decision-making. To find the term '*right to an explanation'*, we have to look at Recital 71 GDPR. Here it is stated that the aforementioned safeguards should include '*specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision.'*

Based on this, one could argue that the right to an explanation could be deduced from the list of safeguards mentioned in Recital 71 GDPR. We could then place this list into the safeguards that should be implemented under art. 22(3) GDPR. Wachter et al. problematize this view, however, by stating that Recitals are, in principle, not binding.[11] Indeed, Recitals are meant to set out the reasons for a piece of legislation, and not to provide normative provisions or

[11] Wachter, Mittelstadt and Floridi (n 1).

obligations.[12] On the other hand, Malgieri and Comandé put forward that Recitals can, nevertheless, provide an interpretative guide to reading art. 22 GDPR together with other provisions of the GDPR such as art. 13, 14, and 15 GDPR.[13]

Different scholars have also proposed such a systematic and holistic reading of art. 22 GDPR. We could, for example, interpret the safeguards mentioned in Recital 71, such as the right to an explanation, together with the right to contest, which does feature in art. 22(3) GDPR. Scholars argue that to be able to contest an automated decision, one needs to be able to understand on what grounds a system came to a certain output.[14] This view is also echoed in the WP29 Guidelines on automated decision-making and profiling, stating that: '*The data subject will only be able to challenge a decision or express their view if they fully understand how it has been made and on what basis.*'[15] Moreover, others have also suggested reading art. 22 GDPR in light of fundamental rights and fundamental rights case law to strengthen explainability rights.[16] Especially the right to an effective remedy and the right to a fair trial might prove useful in this regard, considering that a lack of AI transparency can be in breach of these rights according to the CJEU in the PNR case.[17]

However, the safeguards mentioned in art. 22(3) only refer to cases where the automated decision-making is founded on cases (a) or (c). This is problematic, as there are *no* safeguards explicitly mentioned for cases that fall under (b). It is up to the national legislator in such cases, to formulate '*suitable safeguards*'.

In the national law of some EU member states the exception laid down in subparagraph (b) has taken quite broad and vague forms.[18] The GDPR implementation law of the Netherlands (UAVG), for example, provides an exception in art. 40(1) for the ban in art. 22 GDPR, when automated decision-making is necessary to fulfil a legal requirement or a task carried out in the public interest.[19] However, this does not apply to cases of profiling.[20] Nevertheless, art. 40(2) UAVG does reiterate the requirement that there needs to be '*suitable safeguards'*. The UAVG does not specify what these safeguards are, however. Nor does it mention the need to provide

---

[12] European Commission. Legal Service., *Joint Practical Guide of the European Parliament, the Council and the Commission for Persons Involved in the Drafting of European Union Legislation.* (Publications Office 2015) ch 10 <https://data.europa.eu/doi/10.2880/89965> accessed 25 July 2024. European Commission. Legal Service., *Joint Practical Guide of the European Parliament, the Council and the Commission for Persons Involved in the Drafting of European Union Legislation.* (Publications Office 2015) ch 10.

[13] Malgieri and Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (n 1). Malgieri and Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (n 1).

[14] Ljubiša Metikoš, 'Explaining and Contesting Judicial Profiling Systems' (2024) 2024 Technology and Regulation 188; Marco Almada, 'Human Intervention in Automated Decision-Making: Toward the Construction of Contestable Systems', *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law* (Association for Computing Machinery 2019) <https://doi.org/10.1145/3322640.3326699> accessed 11 April 2021; Bayamlıoğlu (n 1); Sarra (n 1). Marco Almada, 'Human Intervention in Automated Decision-Making: Toward the Construction of Contestable Systems', *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law* (Association for Computing Machinery 2019); Bayamlıoğlu (n 2); Sarra (n 2).

[15] EDPB, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018) <https://edpb.europa.eu/our-work-tools/our-documents/guideline/automated-decision-making-and-profiling_en> accessed 18 December 2020.

[16] Dimitrova (n 1).

[17] *Ligue des droits humains ASBL v Conseil des ministres* [2022] ECJ Case C-817/19 [194]. ibid.

[18] Malgieri (n 1).

[19] The wording of this provision is identical to the processing ground present in art. 6 GDPR

[20] It is unclear whether the text of the UAVG implies that profiling can never be legitimated by being based on any Dutch national law or public interest.

an explanation. It simply copies the phrasing of the GDPR in this regard. Other EU Member States. such as France, do provide more detailed implementations of art. 22(3)(b) GDPR.[21] This shows, however, that while the GDPR aims to provide a comprehensive and unified regulatory regime for the EU, the right to an explanation is quite fragmented in the national law of EU member states.

2.2. Notification obligations and data access rights under art. 13, 14, and 15 GDPR

Scholars have also relied upon a different set of provisions to deduce the right to an explanation. Namely: art. 13, 14, and 15 GDPR.[22] Art. 13 and 14 GDPR, first of all, set forth transparency and notification requirements for when personal data is collected directly, or indirectly, about the data subject in question, respectively. These provisions both state in art. 13(2)(f) and art. 14(2)(g) that data controllers must give information concerning: *'the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'*. Art. 15 GDPR too provides a verbatim copy of this text in paragraph (1)(h), but differs in the fact that it provides a direct right for data subjects to request such information *ex post* and individualized to their situation in particular.[23]

In short, various grounds for a '*right to an explanation'*, can be deduced from this analysis. First, we can place the right to an explanation in the list of safeguards required by art. 22(3) GDPR, by reading it in light of Recital 71. Moreover, these safeguards would, in any case, only apply to cases mentioned under subparagraph (a), when the processing is necessary for going into or performing a contractual agreement, or subparagraph (c), when there is explicit consent. For cases under subparagraph (b), when the automated decision-making is authorized by Union or Member State law, only certain Member States explicitly provide a right to an explanation.[24]

Arguably, the obligation to provide meaningful information under art. 13, 14, and 15 GDPR, provides a more secure and well-established right to an explanation. However, the text here too, gives rise to various interpretative questions. In section 4, we delve deeper into the scoping questions that have arisen regarding the GDPR's right to an explanation, to help delineate the area of applicability of the GDPR's right to an explanation. We then ascertain how these questions have arisen in legal practice as well, through an analysis of the relevant case law on the right to an explanation under the GDPR. Moreover, we also compare how these same questions could arise as well under the AIA.

3. The right to an explanation under the AI Act

The AIA is a newly adopted EU regulation that aims to regulate the production, distribution, and use of AI systems. The AIA can be seen as a form of product safety regulation, as it is closely interlinked with the proposed AI liability directive and a set of revisions to other sectoral

[21] Malgieri (n 1).

[22] See, for instance: Selbst and Powles (n 1).

[23] Laurens Naudts, Pierre Dewitte and Jef Ausloos, 'Meaningful Transparency through Data Rights: A Multidimensional Analysis' in Eleni Kosta, Ronald Leenes and Irene Kamara, *Research handbook on EU data protection law* (Edgar Elgar Publishing Ltd 2022).

[24] Malgieri (n 1).

safety regulations such as the Machinery Regulation and the General Product Safety Directive.[25] The fact that the AIA was developed from a product safety perspective, has resulted in a risk-based approach to the regulation of AI.[26] This entails that certain uses of AI are regulated differently, depending on what risk they have to harm citizens' safety, health, and fundamental rights. Under art. 5 AIA, unacceptable risk AI systems are for example banned. However, the brunt of the regulatory requirements of the AIA applies to high-risk AI systems, which are defined in art. 6 AIA and Annex I and III.

Annex I refers to a list of EU product safety legislation, while Annex III lists several different risky uses of AI in certain sectors. The latter includes biometrics (1) critical infrastructure (2), education (3), employment (4), essential private and public services and benefits (5), law enforcement (6), migration (7), and the administration of justice and democratic processes (8).

Within this list, Annex III also provides more detailed and specific examples of high-risk use cases. This includes for example AI systems that are intended to be used as polygraphs by migration officials, under (7)(a) Annex III. However, there exist also several exceptions to this list. For example, whereas AI systems intended to be used to evaluate the creditworthiness of natural persons are classified as high-risk AI ((5)(b) Annex III), AI systems that are used for the purpose of detecting financial fraud are exempted. A number of exemptions to the list of Annex III can also be found within the Recitals of the AIA. Recital 61 for example states that judicial assistance AI systems should not be classified as high risk when they are '*intended for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases, such as pseudonymization of judicial decisions, documents or data, communication between personnel, administrative tasks'*.

While we can thus see a number of specific exceptions throughout the text of the AIA, art. 6(3) AIA contains one very wide and broadly formulated exception. An AI system mentioned in Annex III shall not be considered to be high risk if it does not pose a significant risk of harm to the health, safety, or fundamental rights of natural persons. In this regard, art. 6(3) AIA again focuses on ancillary AI systems, and states that a lack of risk might arise if the system in question does not materially influence the outcome of a decision-making process. This can occur if one or more of the following conditions if fulfilled:

> *'(a) the AI system is intended to perform a narrow procedural task;*
>
> *(b) the AI system is intended to improve the result of a previously completed human activity;*
>
> *(c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or*

[25] Ljubiša Metikoš, 'An Interdisciplinary Toolbox for Researching the AI-Act' [2023] Verfassungsblog <https://verfassungsblog.de/an-interdisciplinary-toolbox-for-researching-the-ai-act/> accessed 11 September 2023; Ljubisa Metikos, 'The AI Act: Weak, Weaker, Weakest' (2024) 3 Ljubiša Metikoš, Mediaforum 73. Nathalie A Smuha and others, 'How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act' (5 August 2021) <https://papers.ssrn.com/abstract=3899991> accessed 14 October 2022.

[26] Marco Almada and Nicolas Petit, 'The EU AI Act: A Medley of Product Safety and Fundamental Rights?' (18 October 2023) <https://papers.ssrn.com/abstract=4308072> accessed 5 August 2024.

(d) the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.'

This list of exceptions is formulated in quite a broad and vague manner.[27] The original proposal for the AIA by the European Commission was already quite unclear in many of its provisions, as it regulates so many widely different sectors.[28] Nevertheless, the version proposed by the European Commission lacked this broad exception, as it was only later added during the legislative process. It is not surprising then that some organizations have described the regime of art. 6(3) AIA as a '*glaring loophole'*, as it gives providers of high-risk AI systems an easy way to exempt themselves from the obligations of the AIA for high-risk AI.[29]

Nevertheless, this regime does not apply to profiling systems. If they are used in any of the use-cases mentioned in Annex III, they are considered to be high risk, according to the last paragraph of art. 6(3) AIA.[30]

All things considered, a quite complex framework has arisen in regard to the scope of what AI systems fall under the right to an explanation of the AIA. The AIA tries to provide, first, a clear and direct list of what is considered to be high-risk AI. It then combines this list, however, with a broad balancing exercise akin to what is in place in the GDPR. This results in a regulatory chimera, that does not provide the legal certainty of directly stating which systems are regulated in a list, nor the broad scope of a balancing exercise that might encompass many different kinds of AI systems.

For those systems that do fall under the category of 'high risk AI', the AIA puts forward various transparency requirements, that address a wide array of different actors and recipients. These include for example the requirement for the provider of an AI system to make the AI system in question intelligible for users so that they might exercise human oversight, under art. 14 AIA.

The AIA also addresses decision-subjects, and explicitly formulates a right to an explanation for individual decision-making in art. 86 AIA under Chapter IX, Section 4 titled '*Remedies'*. The right to an explanation seems to have been quite an afterthought, however. The original proposal of the AIA by the European Commission wholly lacked *any* individual rights. This was criticized in academic scholarship at the time.[31] This stands in contrast with other pieces of AI legislation, such as the proposed Brazilian AI Law, where both a *risk-based* and *rights-based* approach to AI regulation is used.[32] The AIA also contrasts with the GDPR in this regard, as the latter is full of provisions that provide data subjects with different rights to exercise control over their personal data (notably in Chapter III GDPR).

---

[27] Ljubiša Metikoš, 'The AI Act: Weak, Weaker, Weakest' (n 24).

[28] Ljubiša Metikoš, 'An Interdisciplinary Toolbox for Researching the AI-Act' [2023] Verfassungsblog <https://verfassungsblog.de/an-interdisciplinary-toolbox-for-researching-the-ai-act/> accessed 11 September 2023; Ljubisa Metikos, 'The AI Act: Weak, Weaker, Weakest' (2024) 3 Ljubiša Metikoš, Mediaforum 73.

[29] 'The EU AI Act: A Failure for Human Rights, a Victory for Industry and Law Enforcement' (*Access Now*) <https://www.accessnow.org/press-release/ai-act-failure-for-human-rights-victory-for-industry-and-law-enforcement/> accessed 16 April 2024.

[30] Ljubiša Metikoš, 'Explaining and Contesting Judicial Profiling Systems' (2024) 2024 Technology and Regulation 188.

[31] Smuha and others (n 24). .

[32] 'The Road to Regulation of Artificial Intelligence: The Brazilian Experience' (*Internet Policy Review*) <https://policyreview.info/articles/news/road-regulation-artificial-intelligence-brazilian-experience/1737> accessed 10 April 2024.

Art. 86(1) AIA encompasses decisions that are taken based on the output from a high-risk AI system listed in Annex III, which produces legal or similarly significant effects on the health, safety, or fundamental rights of that person. It is up to the individual themselves, however, to assess whether or not they are significantly affected, according to art. 86(1) and Recital 171. If these conditions are fulfilled, the affected person has 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.*' The AIA does not mention any exceptions to this regime. Nevertheless, art. 86(2) does state that the right to an explanation under the AIA does not apply if any exceptions or restrictions are formulated in EU or national laws.

The text of art. 86 AIA seems to provide a big improvement compared to the vague provisions of the GDPR. However, a number of issues still persist. Several questions and criticisms can be raised on the formulation of art. 86 AIA, if we take into consideration the extensive literature and case law that has been building upon the right to an explanation under the GDPR. In the next sections, we discuss three sets of questions in particular: questions of scope, questions of content, and questions on the balancing of rights and interests

4. Questions of scope

One of the most crucial questions regarding the right to an explanation is the extent of its scope. Exactly when can one invoke the right to an explanation? The GDPR and the AIA take quite different approaches in this regard. While the AIA delineates the scope of the right to an explanation to a somewhat pre-determined list of specific AI systems, the GDPR has a more general approach, providing a list of criteria to which a system has to conform to fall under its scope. As we will see in the next few paragraphs, both approaches still raise a number of interpretative questions.

4.1. The General Scope of the GDPR

Before we delve deeper into the scope of art. 22 GDPR, it is important to delineate the scope of the GDPR as a whole. The GDPR only applies to situations in which the personal data of a natural person is processed, according to art. 2(1). In situations where no personal data is processed, the GDPR's right to an explanation is therefore not applicable. In practice, such situations should be quite rare, as the notions of '*processing'* of '*personal data'* are interpreted very widely, including a wide number of different acts and kinds of data.[33]

One would assume that any case of *profiling* would surely fall under the scope of the GDPR. However, in a case before the Department of Administrative Appeals of the Dutch Council of State, the exercise of art. 15 GDPR was hindered as the profiling that took place in that case did not constitute a form of processing of personal data.[34] In this case, a man was classified as high risk for committing fraud by a profiling system used by the Dutch tax authority. The man was classified with '*code 88'*. However, the Court ruled that this was a broad classification that could apply to many different citizens. The man was therefore not identifiable based on this

[33] *Österreichischer Rundfunk and others* [2003] Court of Justice of the European Union Joined Cases C-465/00, C-138/01, C-139/01 [43]; *College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer* [2009] Court of Justice of the European Union C-553/07 [59]; *Peter Nowak v Data Protection Commissioner* [2017] Court of Justice of the European Union C-434/16 [33]; *FF v Österreichische Datenschutzbehörde and CRIF GmbH* [2023] Court of Justice of the European Union Case C-487/21, ECLI:EU:C:2023:369 [23]; *IAB Europe v Gegevensbeschermingsautoriteit* [2024] Court of Justice of the European Union Case C-604/22, ECLI:EU:C:2024:214 [36].

[34] Afdeling bestuursrechtspraak van de Raad van State, Department of Administrative Appeals of the Dutch Council of State 1 February 2023, case no. 202107217/1/A3, ECLI:NL:RVS:2023:394.

classification. Subsequently, the GDPR would not apply to his information request, as there was no processing of personal data.[35]

4.2. The General Scope of the AIA

The AIA is not limited to cases where personal data is processed, as its scope is more directly aimed at addressing AI-based decision-making, rather than regulating the processing of personal data. Still, it is questionable whether the AIA provides a broader scope than the GDPR in this regard. The GDPR addresses any form of solely automated decision-making, besides those taking place in a personal or household activity, foreign policy, or law enforcement, according to art. 2(2)(b)(c) and (d) GDPR, respectively. The AIA, however, can only grant a decision-subject with an explanation regarding high-risk AI systems, which could moreover be excluded through the balancing exercise present in art. 6(3) AIA. Only profiling systems escape this exemption. Nevertheless, profiling still needs to occur in a high-risk context, such as those mentioned in Annex III.

4.3. Three criteria

While the general scope of the GDPR and AIA are somewhat well-defined, their exact application in the context of the right to an explanation has given rise to a number of legal questions. In this section, we discuss how we can better understand the exact scope of the GDPR's and AIA's right to an explanation. To this end, we focus on the criteria formulated in the SCHUFA case. In this case, the Court of Justice of the EU (CJEU) provided a threefold test to assess the scope of art. 22 GDPR, which in turn would limit the scope of the right to an explanation as well.[36] These are:

1. There must be a decision;
2. The decision must be based solely on automated processing, including profiling;
3. The decision must produce legal effects concerning the data subject, or similarly significantly affect them.

In the next paragraphs, we outline how these different elements have been interpreted. Moreover, we also analyse to what extent these elements exist as well under the AIA.

4.3.1. Decision

The concept of decision is not explicitly defined by the GDPR, but is interpreted by the CJEU to have a '*broad scope*'.[37] Still, the wording of art. 22 GDPR focuses on a singular decision moment, ignoring the fact that, in practice, multiple actions can be impactful for the data subject, without being classified as a decision toward that data subject. Binns and Veale point out that decisions taken in a profiling process can be taken by different parties at different times.[38] This was foregrounded in the SCHUFA case, where the SCHUFA company dispensed credit scores of individuals to banks who would use such scores to take decisions about the creditworthiness of the individual concerned. In essence, SCHUFA did not directly take decisions about data subjects' creditworthiness. Nevertheless, these scores were so impactful that banks would not deviate from them in practice.

---

[35] Ibid.

[36] *SCHUFA* (n 2) para 43. *SCHUFA* (n 3) [43].

[37] *SCHUFA* (n 2) para 45.

[38] Reuben Binns and Michael Veale, 'Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR' (2021) 11 International Data Privacy Law 319.

By not including such preparatory tasks under the scope of art. 22 GDPR, there would be a legal lacuna as the data subject could not exercise their right to an explanation under art. 15(1)(h) GDPR before companies such as SCHUFA. Therefore, the CJEU ruled that such preparatory tasks can also fall under the scope of a '*decision'* in the sense of art. 22 GDPR, as long as the final decision '*draws strongly*' on the score assigned by the third party.[39]

In a case before the Regional Court Traunstein in Germany, the criterium from the SCHUFA case that the final decision must draw strongly on a credit score was interpreted quite narrowly. A credit score calculated by a third party can only fall under this criterium if no other information is relied upon by a decision-maker.[40]

The right to an explanation under the AIA also focuses on decisions. However, the term here refers explicitly to the decision taken by a deployer based on the output of a high-risk AI system, according to art. 86(1) AIA. It is then only from the deployer that an individual could request an explanation. Creditworthiness systems fall under the scope of the right to an explanation, according to Annex III point 5(b), and cannot be exempted under article 6(3) as they profile natural persons. Potentially, from an analogue application of the SCHUFA case, companies such as SCHUFA would also be included under the AIA's right to an explanation.

The AIA seems to provide a more cohesive approach in this regard, as it contains explicit provisions that address other actors besides the final decision-maker. For example, art. 13 AIA requires that AI systems be developed in such a way that the system is transparent and interpretable to the deployer. Moreover, under art. 14 AIA, the system needs to be designed in such a way that the deployer can also exercise human oversight over the system. Consequently, deployers are much more likely to have the necessary information regarding an AI-system to provide an explanation.

Under the GDPR, a deployer of an AI system would not be required to *understand* how the AI system functions. Under the AIA, however, articles 13 and 14 AIA make it highly improbable that a deployer would not have the required knowledge to provide an explanation to a decision-subject.

Still, while the deployer is much more likely to understand the AI system in question, it still might be the case that certain crucial aspects of the system's functioning might not be disclosed to them either. It therefore remains important that explanations can be requested along an AI-system's chain of development.

4.3.2. Solely automated processing, including profiling

The GDPR, unfortunately, does not explicitly identify what '*solely*' automated decision-making entails. Various scholars have already pointed out the concern that a token human might be merely involved to circumvent the applicability of art. 22 GDPR.[41] The EDPB guidelines state, in this regard, that human involvement needs to be *meaningful* and not act as a mere token. Moreover, the human overseer must have the '*authority and competence to change the decision'*

[39] *SCHUFA* (n 2) para 61. *SCHUFA* (n 3) [61].

[40] Landsgericht Traunstein (n 3)

[41] Wachter, Mittelstadt and Floridi (n 1); Veale and Edwards (n 1); Edwards and Veale (n 1); Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a Right to Explanationn Is Probably Not the Remedy You Are Looking For' (2017) 18 Duke Law & Technology Review 67; Malgieri (n 1). Wachter, Mittelstadt and Floridi (n 1); Veale and Edwards (n 1); Edwards and Veale (n 1); Edwards and Veale; Malgieri (n 1).

and consider all relevant data.[42] Still, humans might act as a rubber stamp to take up the legal and ethical blame of problematic AI-based decision-making, all the while justifying their use in high-stakes environments.[43] Green for example argues that human oversight measures often fail to properly fix and address the errors of problematic AI.[44]

Assessing the role of the human-in-the-loop in the context of the right to an explanation under the GDPR might seem confusing. Arguably, a right to an explanation can be warranted, even if a human makes a decision based on an algorithmically generated score. The fact that a human overseer has any discretion does not mean that a data subject would not wish to request an explanation of how an important piece of algorithmically generated advice came to be.

The CJEU does not elaborate in the SCHUFA case as to what the role should be of a human overseer. However, Wagner lays down some criteria that could give us some insight into what a 'good' human overseer would constitute in the context of art. 22 GDPR. Wagner identifies several characteristics that could help us assess when a situation of '*quasi-automation'* might arise. These include: the amount of time available to oversee a task, the degree of qualification of the overseer, the degree of liability, the level of support the overseer receives to exercise the task sustainably, the degree to which the system could adapt to the overseer, the ability to access information, and the agency of the overseer.[45]

In the *Uber* case, the District Court of Appeals of Amsterdam ruled that all necessary information must be taken into account by a human reviewer and that a data controller must prove that the reviewers are qualified and knowledgeable. Moreover, in the circumstances of this case, it was also necessary that the data subject was heard by the reviewer before a decision was taken.[46]

Offering to hear the data subject before a final decision has been taken, also played a role in a case regarding a psychological screening system before the District Court of the Hague. Here, the final decision remained in the hands of a human. Moreover, before a final decision was taken, the individual was allowed to provide counter-evidence in the form of an expert report before that human decision-maker. Consequently, the court ruled that there was no 'solely' automated decision-making, even though the screening system provided crucial information to the human decision-maker.[47]

Still, one could argue that the decision-maker does not properly oversee the system and that they did not properly take the data-subject's evidence into account, which would mean that the overseer still is a mere rubber stamp. In practice, it is unclear then how a data controller would be able to prove that the measures that they took to ensure proper human oversight are indeed sufficient. The Supreme Administrative Court of Austria for example ruled that a data controller's '*internal instructions for action'* would not bind a human overseer, especially if

---

[42] EDPB (n 14).

[43] Madeleine Clare Elish, 'Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction' (2019) 5 Engaging Science, Technology, and Society 40.

[44] Ben Green, 'The Flaws of Policies Requiring Human Oversight of Government Algorithms' [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3921216> accessed 10 February 2022.

[45] Ben Wagner, 'Liable, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems' (2019) 11 Policy & Internet 104.

[46] Ljubiša Metikoš (n 1); *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200.295.742/01* (n 2) para 3.24. Ljubiša Metikoš (n 2); *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200.295.742/01* (n 3) [3.24].

[47] *Rechtbank Den Haag* (n 2) para 4.26. *Rechtbank Den Haag* (n 3) [4.26].

there are no verification controls. The court stated that, it could not be ruled out, in that specific case, that a decision would be made exclusively based on the output of profiling system.[48]

A less strict approach to the concept of human intervention also exists in the case law of the GDPR. For example, the District Court of East Brabant in the Netherlands ruled that the mere fact that the text of a decision is written with the help of an automated system, does not constitute solely automated decision-making. This consideration might, moreover, be increasingly relevant when generative AI systems such as ChatGPT are employed in (legal) decision-making procedures, where such systems write (portions of) decisions.[49]

In any case, it might also be difficult to ascertain the exact role of human decision-makers when AI is employed. In a case before the District Court of Gelderland in the Netherlands, a data controller claimed to not take solely automated decisions, even though AI-based technologies may have been used. The data subject contested this, however. The Court ruled that it was up to the data subject requesting a right to an explanation, to provide '*concrete indications*' that there was solely automated decision-making.[50] Consequently, this could place quite a heavy procedural burden on data subjects, however.

Still, a data subject could, potentially, avoid the requirement of meaningful human intervention by invoking art. 15 GDPR. Art. 15(1)(h) states that a data subject has the right to receive information about '*the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved*'. The question arises, however, whether the text '*at least in those cases*', refers to automated decision-making in *general,* or solely automated decision-making in the sense of art. 22(1) and(4) GDPR. In the case of the latter, art. 15(1)(h) would be limited to cases of solely automated decision-making. Here, the case law seems to differ. On one hand, the Amsterdam District Court of Appeals ruled in the cases of *Uber and Ola,* that art. 15(1)(h) is indeed limited to solely automated decision-making,[51] which is in line with the EDPB Guidelines.[52]

However, the Austrian Data Protection Authority ruled that decision-making where automated systems have assisted a decision-maker, *do* fall under the scope of art. 15(1)(h).[53] In an appeal before the Federal Administrative Court of Austria, however, this view was overturned, and art. 15(1)(h) was again restricted to the scope of solely automated decision-making under art. 22 GDPR.[54] It seems, therefore, that art. 15(1)(h) GDPR will most likely have a restricted reading that is limited to solely automated decision-making as defined by art. 22 GDPR.

The requirement that no meaningful human intervention takes place, does not exist for the AIA's right to an explanation, however. The AIA does require that deployers exercise human oversight

---

[48] *Verwaltungsgerichtshof* Supreme Administrative Court Austria, ECLI:AT:VWGH:2023:RO2021040010.J09, Ro 2021/04/0010-11 (n 3).

[49] Philipp Hacker, Andreas Engel and Marco Mauer, 'Regulating ChatGPT and Other Large Generative AI Models', *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery 2023) <https://dl.acm.org/doi/10.1145/3593013.3594067> accessed 20 November 2023; Harry Surden, 'ChatGPT, Artificial Intelligence (AI) Large Language Models, and Law' (31 March 2024) <https://papers.ssrn.com/abstract=4779694> accessed 15 April 2024. Hacker, Engel and Mauer; Harry Surden, 'ChatGPT, Large Language Models, and Law' (2024) 92 Fordham Law Review 1941.

[50] *Rechtbank Gelderland* (n 3) [5.22].

[51] *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200.295.742/01* (n 2). Gerechtshof Amsterdam (n 42).

[52] EDPB (n 14).

[53] *Datenschutzbehörde* (n 2).

[54] *Bundesverwaltungsgericht* [2023] Federal Administartive Court Austria ECLI:AT:BVWG:2023:W256.2234851.1.00 (n 3).

under art. 14 AIA. However, such a requirement is not a condition for the exercise of art. 86 AIA. More explicitly, the list of high-risk AI under Annex III showcases that the EU lawmaker recognizes that many AI systems *assist* and *support* decision-making, and not replace it. Nevertheless, the role that the deployer takes in regard to the AI system, does impact the applicability of the right to an explanation. According to art. 6(3) AIA, an AI system is not classified as high-risk if it does substantially impact the decision-making process.

In this regard the GDPR and the AIA provide two different, but similar, mechanisms to distinguish between AI systems that are, or are not, subject to a right to an explanation.

The GDPR exempts situations from the scope of the right to an explanation, if a human is strongly substantively involved in the decision-making process. We can see this reflected in the fact that the District Court of Appeals of Amsterdam also examines how the oversight is exercised in practice.[55] In this regard, the GDPR aims to delineate its scope to situations where a decision-maker draws strongly on the incontrovertible output of the system, disregarding their own discretion.

However, in the case of the AIA, the EU lawmaker identifies such situations not through the question of whether or not a human is properly involving themselves or not, which is a vague and difficult to answer question as we have seen. Rather, it focuses on the importance of the system *itself,* regardless of how a human interacts with it in practice, providing a more stable scope for the right to an explanation. It is therefore unimportant how a human interacts with the system for the applicability of art. 86 AIA, and the classification of high-risk AI under art. 6 AIA. Nevertheless, the requirements of art. 6 and 86 AIA still share in common with the GDPR, the desire of the EU lawmaker to distinguish between systems that are impactful, and those that are not.

4.3.3. Legal or significant effects

The EDPB has stated that legal effects include any consequence that would affect someone's legal rights, such as the freedom to associate with others, vote in an election, or take legal action. Moreover, this would also include the cancellation of a contract; entitlement to or denial of a particular social benefit granted by law, such as child or housing benefit; or refused admission to a country or denial of citizenship.[56] Significant effects, in turn, would be any circumstance that '*significantly influence the circumstances, behaviour or choices'* of the data subject.[57] The latter, in any case, would include '*automatic refusal of an online credit application or e-recruiting practices without any human intervention'*, according to Recital 71 GDPR. Still, the phrase '*significant effects'* remains a vague concept that has to be determined in the case law of the GDPR.

In the cases of *Uber and Ola,* the Appeals Court of Amsterdam judged that the termination of the account of a ride-sharing driver should be considered as *both* a legal, and a significant effect, as the driver's contract with the platform was terminated, and they also were unable to earn an income anymore from that platform.[58] Moreover, the court added the consideration that certain

[55] Ljubiša Metikoš (n 1); *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200.295.742/01* (n 2). Ljubiša Metikoš (n 2); *Gerechtshof Amsterdam* (n 3).
[56] EDPB (n 14).
[57] ibid.
[58] *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200.295.742/01* (n 2) para 3.18. *Gerechtshof Amsterdam* (n 42) [3.18].

forms of profiling could also lead to criminal prosecution of a data subject.[59]From this case law, it therefore seems that one can *stack* different grounds on which the data subject is impacted. Similarly, according to Advocate-General Pikamäe, SCHUFA's credit score constitutes both a legal and significant impact as well.[60]

Moreover, such effects arguably do not need to take something away from the data subject in a direct sense. In a case before the Supreme Administrative Court of Austria, systems that determine the likelihood that a job applicant would be hired, even if such results are merely used to target the applicant with employment counselling, is considered a significant effect. In part, mere *triage* of a person in a certain group can constitute a significant effect, even though in this case a job councillor had a final say over any decisions made regarding the job applicant.[61] In a case before the Finnish Data Protection Authority, such triage could also lead to a lack of meaningful human intervention. In a medical case, patients who were not chosen by a profiling system, would not receive additional medical attention, significantly impacting them by depriving them of (proactive) healthcare services.[62]

Art. 86 AIA similarly requires that a decision has legal or similarly significant effects which can have an adverse impact on their health, safety, or fundamental rights. However, it is up to the decision-subject *themselves* to assess whether this is the case or not as art. 86(1) AIA states '*that they consider to have an adverse impact*'. This makes the requirement of legal or significant effects to a certain extent pointless, as it is wholly within the discretion of the decision-subject to consider any decision to have a legal or significant impact.

5. Questions of content

Several questions can be raised regarding the content of the right to an explanation. What kind of information must be disclosed and what measures need to be taken to achieve this? In this section, we explore three questions that emerge from the relevant literature what constitutes the content of the right to an explanation. First, how specific must an explanation be? Does a data subject have a right to access the training data of a Machine Learning model, or is a mere description of the system sufficient? And if a mere description suffices, must this explanation be about how a specific output came to be or how the model works in general? Secondly, we ask what the goal is of the right to an explanation and how this goal might impact the kind of explanations that must be provided. Lastly, we also consider how lessons learned from GDPR case law may inform the right to an explanation in the AIA in regard to questions of content that might arise under this regulation.

5.1. How specific must an explanation be?

As alluded to before, the content of the GDPR's right to an explanation under the GDPR can be interpreted in many ways. In the following paragraphs, we first discuss how detailed information, such as the mathematical formula of an automated decision-making system, is excluded from the right to an explanation. Secondly, we discuss whether explanations must be given about the system in general, or how a specific decision came to be. Lastly, we discuss

[59] *Uber* [2021] District Court Amsterdam ECLI:NL:RBAMS:2021:1020 [3.19]. *District Court Amsterdam* (n 3) [3.19].

[60] *Opinion of Advocate General Pikamäe in the SCHUFA case* (n 2).

[61] *Verwaltungsgerichtshof* Supreme Administrative Court Austria, ECLI:AT:VWGH:2023:RO2021040010.J09, Ro 2021/04/0010-11 (n 3).

[62] 'FINLEX ® - Tietosuojavaltuutettu 23.8.2022' <https://finlex.fi/fi/viranomaiset/tsv/2022/20221544> accessed 26 April 2024. *Tietosuojavaltuutettu* [n 3].

various alternative readings of the right to an explanation, that aim to provide guidance to our understanding of this right's contents.

5.1.1. The mathematical formula

The right to an explanation under the GDPR is not to be understood as a right to fully render transparent the underlying system producing the decision. Rather, the right to an explanation has consistently been interpreted as a thorough and relevant *description* (of that underlying system). For example, the EDPB guidelines state that, rather than provide a complex mathematical explanation about how the AI system functions, the data controller must use clear and comprehensive information. The guidelines suggest for example that a data controller could disclose the categories of data that have been used, why these categories are pertinent, the statistics used to build a profile, how a profile is relevant to the decision-making process, and how such a profile is used to make a decision about a data subject.[63] These categories have also been reiterated and applied by the Austrian Federal Administrative Court, who ruled that the '*mathematical formula underlying the automated decision'* does not need to be disclosed.[64] Similarly, in the *Uber* case, the District Court of Appeals of Amsterdam, also ruled that there is no need to disclose the algorithm itself.[65] At the very least, however, a data controller must clearly answer whether or not solely automated decision-making takes place.[66]

5.1.2. General and specific explanations

There has been some confusion on whether explanations ought to be general – i.e. relating to the system as a whole – and/or specific – i.e. relating to the respective decisions being made. Wachter et al. have argued that only descriptions of the entire model need to be disclosed. They argue this on the basis of art. 13(2)f and 14(2)g GDPR being *ex ante* rights. These provisions require the data controller to provide information about the logic involved and expected consequences of the processing to the data subject. Wachter et al. then discard the existence of a right to an explanation of the final decision, simply because the relevant text in the *ex post* right art. 15(1)h is identical to the texts in *ex ante* rights in art. 13(2)f and 14(2)g.[67]

Wachter et al.'s controversial contribution, has stirred discussion on so-called '*Model-Centric Explanations'* and '*Subject-Centric Explanations'*.[68] These have also been described as '*weak*' and '*strong*' explanations, respectively, as explanations of how a specific output came to be would, arguably, be more useful information to a decision subject who wishes to critique and contest that output.[69] Wachter et al.'s argument seems to be largely disproven in the case law, as we can see a number of examples where a data subject was given the right to detailed information about how a specific decision came to be.[70]

---

[63] Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (Wp251rev.01)' (3 October 2017) <https://ec.europa.eu/newsroom/article29/items/612053> accessed 17 July 2021.

[64] ' *Bundesverwaltungsgericht* [2023] Federal Administrative Court ECLI:AT:BVWG:2023:W252.2246581.1.00, W252 2246581-1/6E (n 3).

[65] Ljubiša Metikoš (n 1); *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200.295.742/01* (n 2) para 3.28. Ljubiša Metikoš (n 2); *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200.295.742/01* (n 3) [3.28].

[66] *Datatilsynet* (n 2).

[67] Wachter, Mittelstadt and Floridi (n 1).

[68] Edwards and Veale (n 40).

[69] Metikos, 'Explaining and Contesting Judicial Profiling Systems' (n 13); de Laat (n 1).

[70] *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200.295.742/01* (n 3); *Bundesverwaltungsgericht* [2023] Federal Administrative Court ECLI:AT:BVWG:2023:W252.2246581.1.00, W252 2246581-1/6E (n 3).

In his opinion in the SCHUFA case, AG Pikamäe clarified that '*the controller should provide the data subject with general information, notably on factors taken into account for the decision-making process and on their respective weight on an aggregate level'*.[71] While this statement may suggest that a more general description of the model would suffice, the AG also explains that '*the reasons for a certain result'* must be disclosed as well.

The District Court of Appeals of Amsterdam required, similarly to AG Pikamäe's argument, that the weight of parameters on an *aggregate* level must be disclosed as well.[72] This view was also espoused by the Austrian Court of Appeals.[73] The question, remains, however, whether knowing the aggregate weight of certain parameters is enough for a decision subject to contest a decision. Knowing how certain parameters have correlated with each other, as well as their concrete weighting in a particular profile, might be necessary for decision-subjects to have access to an effective remedy to enforce their rights.[74]

In some instances, such an explanation could be given through the use of counterfactuals. Counterfactual explanations, refer to explanations that show what would have happened if a specific situation, or a piece of input data, had been different.[75] However, the question arises how *detailed* such a list of counterfactuals needs to be. In a case against moneylender Klarna, the Administrative Court of Stockholm gave some guidance to data controllers in this regard. It ruled that art. 13(2)(f) and 14(2)(g) GDPR do not require that the data controller needs to disclose every single circumstance in which a negative decision could be reached.[76]

In short, the case law shows that the right to an explanation under the GDPR is not interpreted to constitute only broad descriptions of how the system is generally used. Nevertheless, these explanations do not always give the full amount of detail that a decision-subject could need to effectively check the automated system in question, but have been limited to a certain degree in the case law. Moreover, the case law does not always favour the provision of specific explanations. In a case before the Federal Administrative Court in Austria, a data subject wanted to know how they were associated with a political preference, by a data controller that provided political advertisements. In this case, the Court ruled that it was sufficient that the data subject was informed that the calculation method for the political affiliation was ascertained through 'statistical extrapolation'.[77]

5.2. What is the goal of the right to an explanation?

The right to an explanation has seen a number of more creative interpretations as well, that connect this right together with specific concepts and goals. In this regard, these goals of the

---

[71] *Opinion of Advocate General Pikamäe delivered on 16 March 2023 OQ v Land Hessen Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 22 – Automated individual decision-making – Credit information agencies – Automated establishment of a probability value concerning the ability of a person to meet payment commitments in the future ('scoring') – Use of that probability value by third parties Case C-634/21* (ECJ) [58].

[72] *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200.295.742/01* (n 2) para 3.28. *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200.295.742/01* (n 3) [3.28].

[73] *Bundesverwaltungsgericht* [2023] Federal Administrative Court ECLI:AT:BVWG:2023:W252.2246581.1.00, W252 2246581-1/6E G - W252 2246581-1/6E' (n 3).

[74] Metikos, 'Explaining and Contesting Judicial Profiling Systems' (n 13); Karen Yeung and Adam Harkens, 'How Do "Technical" Design Choices Made When Building Algorithmic Decision-Making Tools for Criminal Justice Authorities Create Constitutional Dangers? (Part I)' (2023) 2023 Public Law 265.

[75] Wachter, Mittelstadt and Russell (n 1).

[76] *Klarna* (n 2).

[77] Verwaltungsgerichtshof [2023] Federal Administrative Court ECLI:AT:BVWG:2023:W252.2237416.1.00 (n 3).

right to an explanation can shape the kind of information that is disclosed. This is because different kinds of information disclosures can be more, or less, well suited to achieve a specific goal.

In a number of cases, data controllers were required by courts to provide a decision-subject with useful information that can help the data subject to *contest* the decision in question.[78] This is in line with the reading of the right to an explanation in light of the right to contest and the right to be heard, present in art. 22(3) and Recital 71.[79] The most extensive reading of the GDPR in this regard, might be present in the work of Sarra, who argues that the right to contest should be interpreted as the '*apex*' of the set of safeguards that are required by art. 22(3). Reading the right to an explanation in this light would impose a high threshold on data controllers to provide detailed information to the decision subject.[80] Moreover, reading the right to an explanation in light of certain fundamental rights such as art. 47 Charter(the right to an effective remedy), could also provide a high standard for the content of explanations. Outside the context of the GDPR, the CJEU has already acknowledged in the PNR case, that the right to an effective remedy can be obstructed by the lack of transparency of certain types of AI systems.[81]

Scholars have also argued that a highly technical explanation is insufficient to properly safeguard contestation. Hildebrandt for example argues that a technical explanation that describes how a system functions is not well suited for most individuals who are affected by a certain AI system. That an algorithm took into account database X and Y might be interesting for a programmer, but it does not necessarily grant a decision-subject with adequate grounds to contest that decision.[82] Therefore, the argument goes, people are rather in need of *justifications.* This dichotomy of explanations vs. justifications can be seen in other scholarly works as well.[83] In this sense, the Berlin Data Protection Authority seems to be the first to explicitly require that data controllers must also '*justify*' the decision that has been created.[84]

5.3. Explanations under the AIA

The AIA provides a similar wording regarding what has to be explained. Art. 86(1) requires that the deployer provide '*clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken'.* At first sight, many of the requirements present in the case law can be read into these requirements as well. Most likely the mathematical formula will also not be disclosed under art. 86 AIA. However, the

---

[78] *Gerechtshof Amsterdam* (n 3). *Berliner Beauftragte für Datenschutz und Informationsfreiheit* (n 2); *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200.295.742/01* (n 2).

[79] Bayamlıoğlu (n 1); Almada (n 13); Sarra (n 1). Bayamlıoğlu (n 1); Almada (n 13); Sarra (n 1).

[80] Sarra (n 1).

[81] *Ligue des droits humains ASBL v Conseil des ministres* (n 16) para 194. *Ligue des droits humains ASBL v Conseil des ministres* (n 17) [194].

[82] Metikos, 'Explaining and Contesting Judicial Profiling Systems' (n 13).

[83] Gianclaudio Malgieri, '"Just" Algorithms: Justification (Beyond Explanation) of Automated Decisions Under the General Data Protection Regulation' (2021) 1 Law and Business 16; Gianclaudio Malgieri and Frank A Pasquale, 'From Transparency to Justification: Toward Ex Ante Accountability for AI' (3 May 2022) <https://papers.ssrn.com/abstract=4099657> accessed 17 July 2023; Clément Henin and Daniel Le Métayer, 'Beyond Explainability: Justifiability and Contestability of Algorithmic Decision Systems' [2021] AI & SOCIETY <https://doi.org/10.1007/s00146-021-01251-8> accessed 15 March 2022; Clément Henin and Daniel Le Métayer, 'A Framework to Contest and Justify Algorithmic Decisions' (2021) 1 AI and Ethics 463; Talia B Gillis and Josh Simons, 'Explanation < Justification: GDPR and the Perils of Privacy' (2019) 2 Journal of Law & Innovation (JLI) 71. Malgieri; Malgieri and Pasquale; Henin and Le Métayer, 'Beyond Explainability'; Henin and Le Métayer, 'A Framework to Contest and Justify Algorithmic Decisions'; Gillis and Simons.

[84] *Berliner Beauftragte für Datenschutz und Informationsfreiheit* (n 2).

information that does have to be disclosed under the AIA seems to be less detailed, and useful, for decision-subjects.

The GDPR's case law, seems to interpret the right to an explanation as specific information pertaining as to how a specific decision came to be. However, the focus of art. 86(1) AIA on the *'role of the AI system'* and the use of the phrase '*main parameters*' can be interpreted as to merely mandate the divulgement of a general explanation of the system. However, it is stronger to argue that art. 86(1) does provide an explanation of the specific decision in question, as it requires that the main elements of the *decision* in question, must be disclosed. Still, as the GDPR does not explicitly require that the weight of specific parameters be disclosed, the AIA will most likely also be interpreted to only divulge the aggregate weight of the main parameters that the system relied upon.

6. Balancing rights and interests

The GDPR provides a number of tools to enable the balancing of different rights and interests within its scope. The same holds true for the right to an explanation as well. In this section, we discuss how the balancing exercise can be understood more broadly within the GDPR, as well as in the specific context of the right to an explanation. Finally, we find that the AIA does not provide a strong balancing exercise, leaving the door open for unreasonable restrictions to the right to an explanation.

6.1. Balancing in the GDPR

The GDPR is fundamentally a balancing framework.[85] The flexibility this entails enables the framework from not breaking under the weight of its notoriously wide scope of application. As such, the GDPR provides for many ways to consider the different rights, freedoms and interests at stake in the context of personal data processing operations. Most notably, perhaps in the legitimate interests lawful ground (art.6(1)f) and corresponding right to object (art.21), explicitly setting of the legitimate interests of data controllers and/or third parties, against data subjects' interests, rights and freedoms. Balancing also features more subtly in other provisions, such as the prohibition on processing sensitive data (art.9(1)), where the GDPR sets stricter conditions for when the balance may exceptionally tip over into favouring the processing of personal data.

When it comes to data subject rights in chapter III of the GDPR, balancing plays an important role as well. Data subjects are bestowed with a number of rights, which they can exercise to gain more insight and control over how their personal data is being processed. Even though these rights are quite elaborate and resolute when compared to similar provisions in different jurisdictions or earlier frameworks, they are not absolute. Data subject rights contain both exceptions and balancing provisions in order to safeguard the interests, rights and freedoms of controllers and third parties controllers. This is also true for the right to an explanation. Yet, because the right does not explicitly feature in Chapter III GDPR and has been construed through case law and scholarship, balancing requirements also do not explicitly feature and have to be derived from different places.

[85] For a detailed explanation, see: Jef Ausloos, *The Right to Erasure in EU Data Protection Law. From Individual Right to Effective Protection* (Oxford University Press 2020) ch 5.

When looking at the operative provisions from which the right to an explanation is derived (i.e. artt. 22 *j* 15(1)h GDPR), the regulator has already tried to pre-empt some balancing by delineating the scope of application to situations where automated decision-making legally or similarly significantly affects data subjects (cf. Section 4 above). Controllers' interests are further protected by how the *content* of the explanation is delineated. Notably, it only requires controllers to give all the information necessary for the data subject to consider challenging the respective automated decision as we discussed in section 5.2.[86] When explanation requests relate to very complex automated decision making processes, controllers' interests are also protected by giving them additional time to respond (art. 12(3)).[87] Data subjects may also be asked to further specify their request in case the controller is processing large amounts of personal data in many different ways.[88] Where controllers are able to demonstrate the explanation request is manifestly unfounded or excessive, they can refuse to act or charge a reasonable fee covering the costs of compliance (art. 12(5)).[89] Moreover, Member States can also lay down exemptions to the (scope or conditions of) the right to an explanation, but only under strict conditions pursuant to articles 23,[90] 85,[91] or 89.[92] Even so, the right to an explanation can never be limited or restricted *contractually* between a data subject and controller.[93]

Article 15(4) puts forward an explicit balancing exercise where accommodating the right to obtain a copy of one's personal data risks adversely affecting the rights and freedoms of others. This might be the case, for example, when a full response to the access request would compromise the privacy, data protection or intellectual property rights of third parties. Importantly, the controller needs to demonstrate that the rights or freedoms of others would be adversely affected in the concrete situation and may not refuse to deliver information

---

[86] Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (Article 29 Working Party 2018) Guidelines WP 251 26–27 <http://ec.europa.eu/justice/article-29/documentation>.

[87] Up to three months if they can provide justificatory reasons for extending beyond the default one-month time limit

[88] Recital 63 and European Data Protection Board, 'Guidelines on Data Subject Rights - Right of Access. Version 2' (EDPB 2023) 01/2022 <https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en>. Recital 63 and European Data Protection Board, 'EDPB Adopts Final Version of Guidelines on Data Subject Rights - Right of Access' (April 2023) <https://edpb.europa.eu/news/news/2023/edpb-adopts-final-version-guidelines-data-subject-rights-right-access_en> accessed 25 April 2023. Recital 63 and European Data Protection Board, 'Guidelines on Data Subject Rights - Right of Access. Version 2'. Recital 63 and European Data Protection Board, 'EDPB Adopts Final Version of Guidelines on Data Subject Rights - Right of Access'.

[89] The burden of proof for this is very high, especially in light of the fact that the exercise of data subject rights such as the right of access and right to an explanation do not hinge on specific motivations. Put differently, data subjects cannot be required to motivate *why* they are exercising their right to an explanation. See in this regard René Mahieu, 'The Right of Access to Personal Data in the EU' (PhD Thesis, Vrije Universiteit Brussel 2023) 174–177; European Data Protection Board, 'Guidelines on Data Subject Rights - Right of Access. Version 2' (n 87) pts 175–195. The burden of proof for this is very high, especially in light of the fact that the exercise of data subject rights such as the right of access and right to an explanation do not hinge on specific motivations. Put differently, data subjects cannot be required to motivate *why* they are exercising their right to an explanation. See in this regard Mahieu 174–177; European Data Protection Board, 'Guidelines on Data Subject Rights - Right of Access. Version 2' (n 87) pts 175–195.

[90] For example, Member States may constrain the applicability or content of the right to an explanation in a national law, when such restriction is deemed necessary and proportionate to safeguard national/public security, defence, criminal investigations, rights and freedoms of third parties, and so on.

[91] When deemed necessary and proportionate to reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information.

[92] In specific situations where the right to an explanation stemming from article 15(1)h is deemed likely to render impossible, or seriously impair scientific or historical research purposes or statistical purposes.

[93] European Data Protection Board, 'EDPB Adopts Final Version of Guidelines on Data Subject Rights - Right of Access' (n 87) para 166. European Data Protection Board, 'EDPB Adopts Final Version of Guidelines on Data Subject Rights - Right of Access' (n 87) [166].

altogether.[94] The way in which the right of access ought to be balanced against the interests, rights and freedoms of others has been discussed by scholars[95] and the EDPB.[96] Crucial for our purposes here, however, is that this balancing provision in article 15(4) does *not* apply to the right to explanation as emerging from art. 15(1)(h) and art. 22 GDPR. Indeed, art. 15(4) explicitly limits the consideration of rights and freedoms of others, to situations where data subjects request a *copy of their personal data undergoing processing* under art. 15(3). *A priori* therefore, the right to an explanation derived from art. 15(1)(h) *cannot* directly be restricted by the rights, freedoms and interests of others, including those of the data controller.

Having said that, there is still space for some level of balancing at a higher level, in light of the GDPR's overall nature as a balancing framework (cf. fairness principle in art. 5(1)(a), as well as the non-absolute character of the right to data protection in Article 8 Charter.[97] Concretely, this means that any potential balancing of countervailing interests to the right to explanation needs to happen at a Charter level. Put differently, whenever (a) the conditions for the right to an explanation as described above are met *and* (b) neither of the exemptions apply (notably, when not deemed manifestly unfounded or excessive), the only way to legally constrain the application of right to an explanation is by demonstrating it would violate a Charter right. This sets a higher standard than mere 'interests', and essentially requires a balancing between the data subject's fundamental right to data protection (and other Charter rights that are pursued by exercising their explanation right)[98] versus the fundamental rights and freedoms of the controller and/or third parties. There is ample scholarship on the balancing of fundamental rights and freedoms, notably also in the context of data protection, which we do not have time to dig into here.[99] That said, the following subsection will take a closer look at the gradually emerging body of European case law that specifically deals with these types of balancing exercises in relation to the right to an explanation.

6.2. Recent case law on balancing explanation rights under the GDPR

In light of the vague guidance on how to balance the right to an explanation, it is useful to look at how judges across Europe have been weighing competing interests, rights and freedoms whenever a right to explanation is exercised. In the available case law so far, we see that there is a wide number of rights and freedoms of the data subject that might underly the exercise of their right to an explanation. This may come as no surprise, as automated decision-making has

---

[94] European Data Protection Board, 'Guidelines on Data Subject Rights - Right of Access. Version 2' (n 87).

[95] Mahieu, Malgieri, Veale, Ausloos, etc.

[96] EDPB access guidelines

[97] Recital 4 GDPR, Article 52(1) Charter, European Data Protection Board, 'Guidelines on Data Subject Rights - Right of Access. Version 2' (n 87) para 173. Recital 4 GDPR, Article 52(1) Charter, European Data Protection Board, 'Guidelines on Data Subject Rights - Right of Access. Version 2' (n 87) [173].

[98] One could think of e.g. respect for private and family life (article 7) because the data subject wishes an explanation of automated decisions regarding their life insurance ratings; or freedom of expression and information (article 11) because the data subject might have their professional content channel automatically removed by a social media platform; right to education (article 14) because the data subject might be automatically rejected from a study program; right to engage in work (article 15) because data subjects might be harmed by the algorithmic systems of a gig-work platform; equality (article 20) and non-discrimination (article 21) because the data subject suspects an automated system has unfairly discriminated them, and so on.

[99] See, for instance: Eleni Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (2015) 21 European Law Journal 657; Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130 <https://academic.oup.com/yel/advance-article/doi/10.1093/yel/yey004/5068688> accessed 13 August 2018; Ausloos (n 83) pt II; David Erdos, *European Data Protection Regulation, Journalism, and Traditional Publishers: Balancing on a Tightrope?* (Oxford University Press 2020); Orla Lynskey, 'Complete and Effective Data Protection' (2023) 76 Current Legal Problems 297 <https://doi.org/10.1093/clp/cuad009> accessed 1 May 2024.

penetrated so many different power dynamics in society: notably in contexts such as work, education, and interactions with the government or financial institutions. At the other end, there is little variation in counterarguments being raised, with controllers most often raising business interests; including trade secrets, legal liability (e.g. when transparency may include other people's personal data), or concerns over reputation or 'gaming the system.' Claims that an explanation would harm business interests has been upheld by the Regional Court of Traunstein in Germany.[100] Moreover, in a recent case brought in the Netherlands, a bank refused to share any information on why it had pre-emptively blocked a client's account under anti-money laundering legislation.[101]

In Austria, the Federal Administrative Court ruled that a data subject's explanation request did not extend to the mathematical formula deployed by the controller in assessing creditworthiness.[102] The controller, a credit ranking agency, had appealed a decision from the Austrian DPA – ordering them to disclose the logic and algorithm used in determining the data subject's creditworthiness – *inter alia* because disclosing the respective algorithms would impair business secrets.[103] The Federal Administrative Court upheld the appeal, though without explicitly acknowledging the controller's business interests and trade secrets claim. Instead, it stated that compliance with the right does not necessitate the ability to 'recalculate' the individual ratings, and the credit agency had appropriately fulfilled its obligation by providing: a) the categories of personal data and why they are relevant to the creation of the profile; b) how the profile is created by automated means, with specific regard to the statistical method(s) used; c) why the profile is relevant for the decision; d) how the profile is actually used in the context of the decision. Not even a month later, the same court also upheld the appeal of a controller who was ordered by the DPA to provide more detailed information under the right to an explanation than they had already shared.[104] In this case, a data subject wished to obtain an explanation of how a mail service provider had inferred and assigned their political preferences for purposes of political targeting. The court essentially said it was sufficient for the controller to share a copy of the data subject's personal data and a simple reference to the use of 'a statistical method' for the respective inferences. Apart from a disconcerting narrowing of the content of explanation rights, these two Austrian cases also signal how the balancing act is inherently tied to how the content of an explanation is given shape.

In 2023, the Amsterdam Court of Appeals ruled on the right to an explanation vis-à-vis platform-work companies Uber and Ola. Across three landmark cases, drivers had requested detailed information and explanations about a variety of algorithmic processes that affected them significantly, such as ratings, drivers' profiles, upfront pricing system, deactivation decisions, fraud probability scores, and more. Uber claimed that accommodating transparency and explanation requests – particularly with regard to its fraud detection systems – would reveal trade secrets. The Court rejected this argument by explaining that the the exemption in light of 'the rights and freedoms of others' (art.15(4)) only applies to the right to obtain a copy of one's personal data in Art.15(3), not regarding the explanation right in Art.15(1)h (see above). Even

---

[100] *Landsgericht Traunstein* (n 3).

[101] Jan-Hein Strop, Sebastiaan Brommersma, Follow the Money, <https://www.ftm.nl/artikelen/bunq-bevriest-bankrekening> accessed 5 August 2024

[102] Verwaltungsgerichtshof [2023] Federal Administrative Court ECLI:AT:BVWG:2023:W252.2237416.1.00 (n 3).

[103] Ibid.

[104] *Bundesverwaltungsgericht* [2023] Federal Administartive Court Austria ECLI:AT:BVWG:2023:W256.2234851.1.00 W256 2234851-1 (n 3).

if additional exemptions may exist in national law (cf. art. 23(1)i),[105] it does not entitle Uber to reject the information requests of drivers in their entirety. The Court explains that a complete rejection of explanation requests would violate proportionality and necessity requirements.[106] With this in mind, the Court emphasizes that Uber is required to at the very least explain on the basis of what factors and what weighting of those factors Uber arrived at its algorithmic decisions such as ride-sharing decisions, the fare decisions and the average ratings, respectively, and also provide additional information necessary to understand the reasons for those decisions.[107] The Court reiterates the EDPB, stating that accommodating the right to an explanation does not necessarily require Uber to expose their entire algorithm(s), and as such deems that the company's interests in its trade secrets are sufficiently safeguarded.

The Amsterdam Court of Appeals also had a chance to explore the balance between drivers' right to an explanation with the privacy and data protection rights of customers. Specifically, Uber and Ola had been asked to provide information about 'reports' per ride and 'individual ratings' per customer, based on passenger feedback reports. The Court explains that the companies acted correctly in anonymizing the statements sent to drivers by default, so that they are not traceable to individual customers. That said, the Court also acknowledged that drivers can still request Uber/Ola to reconsider the anonymisation of concrete reports or ratings in particular instances, when they can motivate why their interests to get complete access supersedes that of the customer's right to protection of personal data.[108]

In short, the argument that a right to an explanation would disproportionally harm business interests, intellectual property rights, trade secrets, or fears that individuals might game the system, are therefore all arguments that will not likely be abused to categorically refuse any kind of explanation in every circumstance. Indeed, these concerns can be circumvented, by providing selective descriptions of the system, rather than showcasing the entirety of its inner workings. However, while this may seem like an understandable interpretation, individuals could still benefit from an explanation that showcases the entirety of the inner workings of an AI system. Arguably, providing a mere description of a system may affect the right to an explanation's functionality for scrutinizing and holding to account algorithmic systems (e.g. for bias).[109]

6.3. Balancing explanations under the AIA

Similarly to the GDPR, the AIA legislator has pre-empted certain balancing by constraining the scope of the right to explanation in art. 86 AIA to high-risk AI systems only. By doing so, the EU legislator chose to mainly safeguard the interests of AI developers and deployers against

---

[105] Transposed in article 41(1)i of the Uitvoeringswet AVG (the Dutch Implementation Law of the GDPR)

[106] *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200295742/01* [2023] Hof Amsterdam ECLI:NL:GHAMS:2023:793 [3.27]; *ECLI:NL:GHAMS:2023:796, Gerechtshof Amsterdam, 200295747/01* [2023] Hof Amsterdam ECLI:NL:GHAMS:2023:796 [3.39]. *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200.295.742/01* para 3.27; *ECLI:NL:GHAMS:2023:796, Gerechtshof Amsterdam, 200.295.747/01* para 3.39.

[107] *ECLI:NL:GHAMS:2023:796, Gerechtshof Amsterdam, 200.295.747/01* (n 105) para 3.41; *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200.295.742/01* (n 105) para 3.28. *ECLI:NL:GHAMS:2023:796, Gerechtshof Amsterdam, 200.295.747/01* (n 105) para 3.41; *ECLI:NL:GHAMS:2023:793, Gerechtshof Amsterdam, 200.295.742/01* (n 105) para 3.28.

[108] *ECLI:NL:GHAMS:2023:796, Gerechtshof Amsterdam,* (n 104) para 3.17; *ECLI:NL:GHAMS:2023:804, Gerechtshof Amsterdam* ECLI:NL:GHAMS:2023:804 [3.18]. *ECLI:NL:GHAMS:2023:796, Gerechtshof Amsterdam* (n 104) para 3.17; *ECLI:NL:GHAMS:2023:804, Gerechtshof Amsterdam,* para 3.18.

[109] Cynthia Rudin, 'Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead' (2019) 1 Nature Machine Intelligence 206.

having to accommodate explanation rights for every kind of AI-driven decision-making processes.

Drawing more from the GDPR, art. 86 AIA is also limited to individual decision-making that '*produces legal effects or similarly significantly affects that person'*, with the AIA given further clarification that this covers situations where the person considers the AI system '*to have an adverse impact on their health, safety or fundamental rights*.' This also conceals a balancing act, albeit one that is in the hands of the decision-subject. As we have seen in the guidance and case law on GDPR explanation rights, determining what exactly constitutes a significant effect, or 'adverse impact' on one's health, safety or fundamental rights, might easily end up in a complicated balancing argument. Placing this in the hands of the decision-subject, circumvents such discussions, and provides a higher level of protection to the decision-subject.

However, it is questionable how much art. 86 AIA indeed does provide a higher level of balancing protection to the decision-subject than the GDPR. Like we saw under GDPR, art. 86(2) AIA also foresees the possibility of exceptions or restrictions to the right to explanation which may emerge from Union or national law. E.g. one could imagine legislators installing restrictions to explanation rights in the context of fraud detection mechanisms in financial regulations (e.g. anti-terrorism financing, or anti-money laundering), in an attempt at safeguarding the interests of financial institutions and government policy, at the cost of privacy.

Art. 86(2) AIA therefore prescribes that the right to an explanation cannot be invoked if an exception to this right has been laid down in EU or Member State laws. This provision is unrestricted, however. The AIA wholly lacks any mechanism to balance the interest of a decision-subject to receive an explanation vis à vis the interest that an exception aims to protect. This is even more jarring, considering that the precursor to art. 86(2), in older proposed versions of the AIA, did contain an explicit, albeit still quite vague, balancing exercise.[110] This discarded provision required that the restricting measure in question needs to be proportionate and respect the essence of the fundamental rights of the decision-subject.

Now, however, the balancing between the right to an explanation vis à vis other rights and interests, lies solely in the hands of the EU or Member State legislator. In the absence of a balancing provision in the final AIA, individuals who wish to contest the disproportionate restriction of their right to an explanation, must now search for remedies outside the AIA. Either, they need to contest the appropriateness of an exception within the restricting EU or national law itself, or they need to invoke their fundamental rights under the EU Charter. The AIA, however, cannot offer any remedy for such individuals as it stands now on its own.[111]

7. Conclusion: the new landscape of general explainability rights

The concept of the right to an explanation seems to have undertaken a transformation in both legal scholarship, as well as the recent legislative developments in the EU. From its short mention in the Recitals of the GDPR, to a burst of scholarship, it has been developed into a

[110] Art. 68c, amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

[111] Metikos, 'Explaining and Contesting Judicial Profiling Systems' (n 13).

fully-fledged legal right in the case law of different courts and data protection authorities. Moreover, this right has also become more clearly formulated under the AIA. Still, the vagueness that has plagued the GDPR's right to an explanation, seems to not have been clarified much under the regime of the AIA. We identified a number of the main questions that have arisen in both legal scholarship, and case law regarding the scope, content, and balancing act of the right to an explanation.

Our main findings in this regard are that, first of all, while the GDPR's scope is hindered by a number of obstacles, its formulation still leaves room for its application to be broader than that of the AIA. Secondly, many of the questions of content that plagued the GDPR shall likely also arise with the AIA. Arguably, the phrasing of the AIA as to what information needs to be disclosed, seems to fit relatively well with the case law on what information needs to be disclosed under the GDPR's right to an explanation. Lastly, the balancing exercise between the right to an explanation and other rights and interests is implicitly facilitated through a number of provisions in the GDPR. In contrast, the AIA does not put forward any requirement that there be a balance between the right to an explanation vis à vis any exceptions that arise from EU or member state laws. To engage in a balancing exercise, a decision-subject must therefore invoke remedies outside the AIA itself to protect the right to an explanation from excessive restrictions put on it by the EU or Member State legislator.

In short, a new landscape of general explainability rights has emerged. The AIA does provide decision-subjects with an additional right to an explanation, that could expand the scope of the GDPR's right to an explanation. Nevertheless, GDPR's case law can still be applied in a number of different instances, even though the AIA is worded differently in many aspects. Lastly, our findings also show that the AIA's right to an explanation, while not suffering from the same unclarities and restrictions as the GDPR, does suffer from a number of weaknesses, that could hinder the usefulness of this provision for decision-subjects.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

First author: Mr. Ljubiša Metikoš is a PhD researcher at the Institute for Information Law, the Paul Scholten Centre for Jurisprudence, and the RPA Human(e)AI. His research focuses on the regulation of AI from a legal-doctrinal and legal-philosophical perspective. In particular, he examines how a right to an explanation can help litigants to contest AI tools used by judges in the adjudication of cases, and how the inscrutability of these tools can harm due process and procedural justice.

Twitter: @LjubisaMetikos

https://www.ivir.nl/profile/ljubisametikos/

linkedin.com/in/ljubisa-metikos-939a22137

Co-author: Dr. Jef Ausloos is an assistant-professor at the Institute for Information Law, University of Amsterdam. His work centres around different information law issues - and in particular data rights, transparency, and governance of digital infrastructures - and the broader political economy in which they operate. While working on this article, dr Ausloos received funding from the Dutch Research Council (NWO), under grant agreement No VI.Veni.201R.096.

Twitter: @Jausl00s

https://www.ivir.nl/nl/profile/jefausloos/

https://www.linkedin.com/in/jef-ausloos-3046301b?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_contact_details%3BTWtD9w3vQmqOP7E29pACgQ%3D%3D

Annex

Table 1: Overview of the analysed case law from different EU Member States that address the right to an explanation

Name of public body	Type of public body	Country	Decision date	ECLI number, national case number, case name
Rechtbank Den Haag (District Court The Hague)	Judicial	The Netherlands	11/02/2020	ECLI:NL:RBDHA:2020:1013 C-09-585239-KG ZA 19-1221
Rechtbank Amsterdam (District Court Amsterdam)	Judicial	The Netherlands	11/03/2021	ECLI:NL:RBAMS:2021:1018 C/13/692003
Verwaltungsgericht Wiesbaden (Administrative Court Wiesbaden)	Judicial	Germany	1/10/2021	ECLI:DE:VGWIESB:2021:1001.6K788.20.WI.00, 6 K 788/20.WI
Bundesverwaltungsgericht (Federal Administrative Court)	Judicial	Austria	22/12/2021	ECLI:AT:BVWG:2021:W211.2234354.1.00 W211 2234354-1
Rechtbank Gelderland (District Court Gelderland)	Judicial	The Netherlands	01/11/2022	ECLI:NL:RBGEL:2022:6145 C/05/404505 / HA RK 22-99
Gerechtshof Amsterdam (Appeals Court Amsterdam)	Judicial	The Netherlands	04/04/2023	ECLI:NL:GHAMS:2023:793 200.295.742/01 'Uber and Ola'
Gerechtshof Amsterdam (Appeals Court Amsterdam)	Judicial	The Netherlands	04/04/2023	ECLI:NL:GHAMS:2023:796 200.295.747/01 'Uber and Ola'
Gerechtshof Amsterdam (Appeals Court Amsterdam)	Judicial	The Netherlands	04/04/2023	ECLI:NL:GHAMS:2023:804 200.295.806/01 'Uber and Ola'
Förvaltningsrätten i Stockholm (Administrative Court in Stockholm)	Judicial	Sweden	14/04/2023	7679-22 'Klarna'
Court of Justice of the European Union	Judicial	European Union	07/12/2023	ECLI:EU:C:2023:957 C-634/21 'SCHUFA'
Bundesverwaltungsgericht (Federal Administrative Court Austria)	Judicial	Austria	12/06/2023	ECLI:AT:BVWG:2023:W252.2237416.1.00

Bundesverwaltungsgericht (Federal Administrative Court)	Judicial	Austria	27/09/2023	ECLI:AT:BVWG:2023:W256.2234851.1.00 W256 2234851-1
Bundesverwaltungsgericht (Federal Administrative Court)	Judicial	Austria	29/06/2023	ECLI:AT:BVWG:2023:W252.2246581.1.00 W252 2246581-1/6E
Verwaltungsgerichtshof *(*Supreme Administrative Court Austria*)*	Judicial	Austria	21/12//2023	ECLI:AT:VWGH:2023:RO2021040010.J09, Ro 2021/04/0010-11
Landsgericht Traunstein (Regional Court Traunstein)	Judicial	Germany	22/05/2024	6 O 2465/23
Datenschutzbehörde (Austrian Data Protection Authority)	Data Protection Authority	Austria	08/09/2020	ECLI:AT:DSB:2020:2020.0.436.002
Datatilsynet (The Danish Data Protection Agency)	Data Protection Authority	Denmark	26/02/2020	2019-421-0028
Tietosuojavaltuutetun toimisto (Office of the Data Protection Ombudsman)	Data Protection Authority	Finland	23/08/2022	6482/186/2020
Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin Commissioner for Data Protection and Freedom of Information)	Data Protection Authority	Germany	31/05/2023	N/A