



**Stanford – Vienna
Transatlantic Technology Law Forum**

A joint initiative of
Stanford Law School and the University of Vienna School of Law



European Union Law Working Papers

No. 31

The Meaning of the GDPR Article 22

Emily Pehrsson

2018

European Union Law Working Papers

Editors: Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law Working Paper Series is to share “works in progress”. The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The working papers can be found at <http://tlf.stanford.edu>.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law’s LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, at:

Stanford-Vienna Transatlantic Technology Law Forum
<http://tlf.stanford.edu>

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Emily Pehrsson is a J.D. candidate at Stanford Law School. She earned her bachelor's degree *summa cum laude* in International Relations at the College of William & Mary in 2013. Her main areas of interest include privacy, data protection, and cyber crime. She worked as a summer law clerk in the Criminal Division's Cyber Unit at the U.S. Attorney's Office. Prior to law school, she worked as a Management Consultant with Deloitte's Federal Consulting practice, where she focused on implementing enterprise and innovation strategy for government clients.

General Note about the Content

The opinions expressed in this student paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This European Union Law Working Paper should be cited as:
Emily Pehrsson, The Meaning of the GDPR Article 22, Stanford-Vienna European Union Law Working Paper No. 31, <http://tlf.stanford.edu>.

Copyright

© 2018 Emily Pehrsson

Abstract

This paper proposes an interpretation of several key provisions of the General Data Protection Regulation's (GDPR) Article 22, "Automated Individual Decision-Making, Including Profiling." It analyzes Article 22's text in the context of its legislative history, related EU laws, and stated purposes, to determine the rights that Article 22 creates for EU citizens as well as the obligations imposed on companies operating in the EU. The purpose of this paper is to highlight ambiguous areas of the law and suggest the interpretation that will most likely be upheld by the European Court of Justice (ECJ).

Table of Contents

1. Introduction	1
2. The GDPR's Purpose	3
3. Article 22 Overview	4
4. When Is Article 22 Triggered?	6
4.1 DEFINING PROFILING	7
4.2 BASED SOLELY ON AUTOMATED PROCESSING	9
4.3 LEGAL OR SIMILARLY SIGNIFICANT EFFECTS	12
5. A Prohibition or A Right to Object?	17
6. Article Exceptions	23
7. Safeguards for Exceptions	24
7.1 SUITABLE MEASURES TO SAFEGUARD	24
7.1.1 Right of Explanation	25
7.1.2 Non-Discrimination	29
7.1.3 Correcting Inaccuracies	30
8. Conclusion	31

1. Introduction

Two years ago, the European Union adopted a regulation radically transforming the landscape of data protection and privacy law around the world. The General Data Protection Regulation (GDPR) seeks to strengthen EU citizens' rights against companies that collect and use individuals' data.¹ At the same time, it aims to create consistency in data protection law across the European Union.² The GDPR is unprecedented, not only in Europe, but worldwide. Not only are the requirements imposed on companies strenuous, the consequences of violating GDPR provisions have been dramatically heightened, reaching a possible 2%-4% of annual worldwide turnover in fines per violation.³ Furthermore, the GDPR will reach beyond companies established in the EU.⁴ It will apply to those using EU citizens' data to offer them goods or services or to monitor their behavior.⁵ After a two-year implementation period, the GDPR will come into force on May 25, 2018.⁶ Consequently, companies are investing heavily to understand the impact of the GDPR on their businesses and implement the policies and technologies required to avoid violations.⁷

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, [hereinafter GDPR].

² ALLEN & OVERY, *The EU General Data Protection Regulation*, 2 (2017), <http://www.allenoverly.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf>.

³ GDPR art. 83(4)-(5); ALLEN & OVERY, *supra* note 2, at 5.

⁴ GDPR art. 3; Bryce Goodman and Seth Flaxman, *European Union regulations on algorithmic decision-making and a "right to explanation"*, 2 (Aug. 31, 2016), <https://zdoc.site/european-union-regulations-on-algorithmic-decision-making-an.html>; Kurt Wimmer, *The Long Arm of the European Privacy Regulator: Does the New EU GDPR Reach U.S. Media Companies?*, COMMUNICATIONS LAWYER 16, 17 (Spring 2017), https://www.cov.com/-/media/files/corporate/publications/2017/09/the_long_arm_of_the_european_privacy_regulator_does_the_new_eu_gdpr_reach_us_media_companies.pdf.

⁵ GDPR art. 3(2)(a)-(b); *EU General Data Protection Regulation—Key Changes*, DLA PIPER (Mar. 24, 2018), https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/#wider_territorial_scope.

⁶ GDPR art. 99; Jennifer McCallister, Gabriela Zanfir-Fortuna, and Jennifer Mitchell, *Getting Ready for the EU's Stringent Data Privacy Rule*, JOURNAL OF ACCOUNTANCY (2018), <https://www.journalofaccountancy.com/issues/2018/jan/eu-data-privacy-rule.html>.

⁷ Clint Boulton, *U.S. Companies Spending Millions to Satisfy Europe's GDPR*, CIO (Jan. 26, 2017), <https://www.cio.com/article/3161920/privacy/article.html>.

The GDPR was preceded by the Data Protection Directive (DPD).⁸ The GDPR generally supplants the Directive, in some cases substantially altering the DPD's provisions. The precise requirements of numerous GDPR provisions are open to interpretation. Until the courts arbitrate gray areas in the law, companies must attempt to comply by interpreting the GDPR's legislative history, considering guidance from EU institutions, and analyzing competing analyses by scholars and legal professionals.

This paper proposes an interpretation of several key provisions of Article 22, "Automated Individual Decision-Making, Including Profiling."⁹ It analyzes the rights that it creates for EU citizens as well as the obligations imposed on companies operating in the EU. This paper highlights ambiguous areas, suggesting the interpretation that will most likely be upheld by the European Court of Justice (ECJ).

First, I will analyze the purpose and intent behind the EU passing the GDPR. I will outline the overarching structure of Article 22, explaining how it relates to other provisions in the GDPR and is clarified by a variety of persuasive sources. Next, I will analyze the circumstances under which data processing activities will trigger Article 22 protections. I will assess whether Article 22 imposes a general prohibition of the designated categories of automated decision-making, or alternatively, was intended only to create rights enabling data subjects to challenge decisions once made. Finally, I will analyze the requirements imposed on data controllers to safeguard data subjects' information under specified exceptions.

⁸ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 [hereinafter DPD].

⁹ GDPR art. 22.

2. The GDPR's Purpose

A major impetus driving the GDPR's adoption was the substantial increase in the availability and cross-border transfer of EU citizens' personal data.^{10,11} At its most basic level, the Regulation seeks to protect the rights of individuals over their own data and harmonize data protection regulations across the European Union.¹² Advancing the broad principle that "personal data should be designed to serve mankind,"¹³ the GDPR emphasizes the importance of achieving a balance between data protection rights and other considerations. It asserts that "the protection of personal data is not an absolute right," articulating a comprehensive, cross-sector data protection approach that weighs "its function in society . . . balanced against other fundamental rights."¹⁴

Furthermore, with companies increasingly relying on data collection and processing, variation in data protection standards across EU Member States became increasingly problematic. The DPD, enacted in 1995, preceded the GDPR. As a directive, it required, in general, transposition into national law by the Member States before it could be enforced. "The objectives and principles of Directive 95/46/EC remain sound," GDPR Recital 9 explains, but nevertheless, the GDPR was necessary because varying data protection standards across the EU undermined citizens' confidence in their efficacy and hindered economic development and enforcement.¹⁵

¹⁰ *Id.* rec. 5-6.

¹¹ *Id.* art. 4(1). ("[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[.]").

¹² *Id.* rec. 1-13.

¹³ *Id.* rec. 4.

¹⁴ *Id.*

¹⁵ *Id.*

The articulated purpose behind the GDPR serves as an interpretive tool for its provisions.¹⁶ Given the ECJ's purposive approach to legal interpretation, Article 1 and the opening Recitals should inform any analysis of subsequent provisions' meaning. Additionally, Recital 9's emphasis on the stability of the DPD's foundations may support arguments for consistent interpretation of similar provisions in the DPD and GDPR, when the language is ambiguous.

3. Article 22 Overview

GDPR Article 22 outlines data subjects'¹⁷ rights and companies'¹⁸ obligations when personal data is used in a narrow category of automated decision-making. At a general level, Article 22 creates a right not to be subject to certain types of automated decisions,¹⁹ outlines three exceptions to that right,²⁰ and mandates safeguards for the exceptions.^{21,22}

The GDPR was written to be independent of the technological realities of the present day. Instead, it aims to address underlying principles that will remain even with continued innovation

¹⁶ Roberto Baratta, *Complexity of EU Law in the Domestic Implementing Process*, 7 (19th Quality of Legislation Seminar, 2014), http://ec.europa.eu/dgs/legal_service/seminars/20140703_baratta_speech.pdf [hereinafter Baratta].

¹⁷ GDPR art. 4(1) ("Data subject" means "an identified or identifiable natural person.").

¹⁸ For the purposes of this paper, general references to a company or companies should be understood as referencing only those organizations subject to the GDPR's jurisdiction outlined in Article 3.

¹⁹ GDPR art. 22(1) ("The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.").

²⁰ *Id.* art. 22(2)(a)-(c) ("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 authorised 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.").

²¹ *Id.* art. 22(3) ("In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall 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."); *Id.* art. 22(4) ("Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.").

²² Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, WP 251, 19 (Oct. 3, 2017, revised Feb. 6, 2018) [hereinafter Article 29 Guidelines].

in the data sector.²³ As a result, much of the language of Article 22 and related provisions in the GDPR is vague. While this design will likely prolong the GDPR's shelf life, in the short term, it may require substantial interpretation by the courts and EU institutions.

Article 22 cannot be analyzed in isolation. Its terms are defined elsewhere in the GDPR, sometimes explicitly, and other times by implication. As mentioned above, understanding the overall purpose of the GDPR is critical to the analysis of specific provisions. Furthermore, a collection of persuasive, but not legally binding, sources must be considered.

First among these are the Recitals preceding the legally-binding Articles of the GDPR. Recitals in EU law are influential in clarifying ambiguous terms and indicating the legislature's purpose in crafting a particular provision.²⁴ A critical caveat, however, is that Recitals cannot override legally-binding language; if the clear text of a provision contradicts a Recital, then the Recital must give way in the legal analysis.²⁵ In the case of Article 22, Recitals 70, 71, and 73 are of particular importance.

Next, reports and other guidance documents from EU institutions, especially the Commission, are influential.²⁶ For example, the Article 29 Working Party (WP29)²⁷ released guidance further clarifying ambiguous provisions relating to profiling and automated decision-

²³ *Implementing and Interpreting the GDPR, Challenges and Opportunities*, CENTER FOR INFORMATION POLICY LEADERSHIP: HUNTON & WILLIAMS LLP, 3, 7 (2016), <https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/05/CIPL-GDPR-Project-Amsterdam-Workshop-Report.pdf> [hereinafter Hunton & Williams LLP]. See also ALLEN & OVERY, *supra* note 2, at 2 ("There was a growing desire to get the GDPR agreed quickly, even if that meant that some of the detail is left for later.").

²⁴ Baratta, *supra* note 16, at 8. See also Reuben Binns, *How to Comply with GDPR Article 22? Automated Credit Decisions* (Feb. 8, 2017), <http://www.reubenbinns.com/blog/how-to-comply-with-gdpr-article-22-automated-credit-decisions/> [hereinafter Binns].

²⁵ Baratta, *supra* note 16, at 9.

²⁶ *Id.*, at 8.

²⁷ The Article 29 Working Party was created by the 1995 DPD, Article 29 and advises the European Commission on issues relating to data protection in EU law. *European Data Protection Supervisor: Data Protection*, EUROPEAN DATA PROTECTION SUPERVISOR (last visited Mar. 25, 2018) https://edps.europa.eu/data-protection/data-protection/glossary/a_en.

making.²⁸ The GDPR’s interpretation can be influenced by other EU policies. The Digital Market Strategy and ePrivacy Directive overlap with the GDPR in some areas; to the extent possible, the GDPR should be interpreted consistently with other EU data protection and privacy policies.²⁹ Like Recitals, guidance documents and related policies cannot supplant legally-binding text.³⁰

Finally, examining the GDPR’s legislative history can provide additional context for specific wording in the Regulation. In particular, it is informative to analyze similar provisions in the DPD, recommended text from the European Commission in 2012, and proposed changes by the Council and European Parliament prior to the GDPR’s 2016 adoption. Without court cases to clarify the Regulation, these sources are invaluable in discerning the intent of the legislators that crafted and approved the law.

4. When is Article 22 Triggered?

Article 22 applies only in a limited set of circumstances. The baseline requirements are outlined in Article 22(1):

“The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”³¹

²⁸ Article 29 Guidelines, *supra* note 22, at 10.

²⁹ HUNTON & WILLIAMS LLP, *supra* note 23, at 8, 9; *Proposal for an e-Privacy Regulation*, EUROPEAN COMMISSION (last visited Apr. 7, 2018), <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>; *Digital Single Market*, EUROPEAN COMMISSION (last visited Apr. 7, 2018), https://ec.europa.eu/commission/priorities/digital-single-market_en.

³⁰ *Measuring Instruments—Guidance Documents*, EUROPEAN COMMISSION (last visited Apr. 7, 2018), https://ec.europa.eu/growth/single-market/goods/building-blocks/legal-metrology/measuring-instruments/guidance-standards_en.

³¹ GDPR art. 22(1).

This sentence contains several limitations. The data subject's rights apply to *decisions* that are *solely* based on automated processing.³² There are three requirements: First, there must be a decision. Second, the decision has to result from automated processing. Third, the decision must result from a process that includes only automated processing, without human intervention.

Next, the sentence clarifies that “automated processing” can include a practice called “profiling,” further defined below. This phrase neither expands nor limits the extent of the right. Rather, it only clarifies that profiling falls into the larger category of automated processing.

Lastly, even if all of the criteria already mentioned apply, a data subject is only protected under Article 22 if the (1) decision, (2) solely, (3) based on automated processing, (4a) “*produces legal effects concerning him or her*” or (4b) “*similarly significantly affects him or her.*” These terms are not all self-explanatory. The sections below unpack the various requirements for Article 22(1), assessing when a data subject could properly rely on its protection.

4.1 DEFINING “PROFILING”

Article 22(1) includes profiling under the category of “automated processing.” GDPR Article 4(4) defines profiling as:

“[A]ny form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's

³² GDPR art. 4(2) (“[P]rocessing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction[.]”).

performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements[.]”³³

The text defines two major requirements for profiling to exist.³⁴ The first requirement defines *what* the organization must be doing—“any form of automated processing of personal data”³⁵.

The second requirement defines *why* the organization is doing it—“*to evaluate* certain personal aspects relating to a natural person.” What does it mean to evaluate someone’s personal aspects?

The WP29 guidelines adopt a more restrictive view of this phrase, maintaining that it implies an inference must be made—namely, using personal data to judge or predict something about an individual.³⁶ Classifying customers to understand who comprises a customer base would not qualify as profiling.³⁷

The WP29 interpretive guidelines will likely control in subsequent court cases on profiling. WP29 notes that its interpretation is informed by a similar profiling definition in the Council of Europe Recommendations.³⁸ The Council of Europe is an international organization and is thus only persuasive authority. Its interpretation may nevertheless be influential. Absent a strong argument that the text of Article 4(4) contradicts the WP29 guidelines, the guidelines would heavily influence a reviewing court focused on both accurate interpretation and legal predictability. The legislative history, similarly, does not undermine the WP29 interpretation.

³³ GDPR art. 4(4).

³⁴ See Rita Heimes, *Top 10 Operational Impacts of the GDPR: Part 5 – Profiling*, IAPP (Jan. 20, 2016), <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-5-profiling/>.

³⁵ GDPR art. 4(1) (“[P]ersonal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[.]”).

³⁶ Article 29 Guidelines, *supra* note 22, at 7.

³⁷ *Id.*

³⁸ *Id.*; See also *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling*, COUNCIL OF EUROPE COMMITTEE OF MINISTERS, 3 (Nov. 23, 2010), <http://194.242.234.211/documents/10160/10704/Recommendation+2010+13+Profiling.pdf> [hereinafter CM/Rec(2010)13].

The profiling provision was recommended as an addition to the GDPR in the first reading of the European Parliament. The only changes to the provision in the final GDPR text were to reorder “location” and add “interests” and “movements” as aspects to be analyzed and predicted.³⁹

Not every instance of profiling meeting the definition of Article 4(4) would fall under Article 22. For example, the profiling definition only requires “any form of automated processing,”⁴⁰ whereas Article 22 decisions must be “based solely on automated processing.”^{41,42} Additionally, Article 22 requires the decision to produce “legal” or “similarly significant” effects on the data subject.⁴³

4.2 BASED SOLELY ON AUTOMATED PROCESSING

Article 22(1) specifically states that the decision must be based *solely* on automated processing. How strictly will this text be interpreted? Some scholars assert that “even nominal involvement of a human” would exempt a decision from Article 22.⁴⁴ The GDPR’s legislative history since 2012 supports this view. In January 2012, The Commission proposed the following language in Article 20, the earlier version of the final GDPR’s Article 22: “. . . based *solely* on automated processing”⁴⁵ The European Parliament proposed changing the phrase to “solely

³⁹ *Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendations*, Amendment 98, EUROPEAN DATA PROTECTION SUPERVISOR, 1,13 (2015), https://edps.europa.eu/sites/edp/files/publication/15-07-27_gdpr_recommendations_annex_en.pdf [hereinafter Annex].

⁴⁰ GDPR art. 4(4).

⁴¹ GDPR art. 22(1).

⁴² Article 29 Guidelines, *supra* note 22, at 7.

⁴³ GDPR art. 22(1).

⁴⁴ 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*, INTERNATIONAL DATA PRIVACY LAW, 25-26 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469 [hereinafter Wachter].

⁴⁵ (emphasis added) European Commission Proposal 2012/0011, art. 20, 54 COM(2012) 11 final, [http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM\(2012\)0011_EN.pdf](http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf) [hereinafter European Commission Proposal].

and predominantly.”⁴⁶ Consequently, the European Data Protection Supervisor (EDPS) added the word “predominantly” to the provision after receiving amendments from the European Parliament and Council. In the EDPS recommended draft, the same provision read: “Every natural person shall have the right not to be subject to a measure which produces legal effects or significantly affects him or her, and which is based *solely or predominantly* on profiling.”⁴⁷ The word “predominantly” was not included in the version of the GDPR that passed in 2016.⁴⁸ Wachter et al. assert that this legislative history is dispositive, indicating a clear intent by legislators to exclude the word “predominantly” and adopt a narrow interpretation of the word “solely.”⁴⁹

WP29’s guidelines complicate the issue. First, the guidelines appear to reinforce and clarify the strict interpretation, stating, “[“based solely”] . . . means that there is no human involvement in the decision process.”⁵⁰ Following this seemingly unequivocal statement, however, the guidelines qualify the definition of solely, creating a gray area that will likely be litigated. In order to disqualify a decision for containing human involvement, the involvement cannot be “fabricated” and must have an “actual influence on the result.”⁵¹

The guidelines backtrack even further on their initial statement by explaining that “[the decision] . . . should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data.”⁵² This statement adds two new requirements that appear to be at odds with the guidelines’ initial statement about

⁴⁶ European Parliament Legislative Resolution, amendment 115, COM(2012)0011 – C7-0025/2012 (2014), <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN> [hereinafter European Parliament First Reading].

⁴⁷ (emphasis added) Annex, *supra* note 39, at 1, 117.

⁴⁸ GDPR art. 22(1).

⁴⁹ Wachter, *supra* note 44, at 34.

⁵⁰ Article 29 Guidelines, *supra* note 22 at 20. *See also id.* at 8 (“Solely automated decision-making is the ability to make decisions by technological means without human involvement.”).

⁵¹ *Id.*, at 21.

⁵² *Id.*

no human involvement in decision-making. In fact, to avoid Article 22, the guidelines assert that only a person *of sufficient standing and decision-making capacity* can count as “involved.” Further, that person has little discretion in what he or she can consider, being bound to weigh “all the relevant data.”⁵³

These two sentences blur the meaning of “solely.” A court could go two ways on these additional requirements. First, it could find that “solely” is clear in establishing that no human involvement is permitted under Article 22 decisions. If that is the case, then these provisions in the guidelines would necessarily yield to the legally-binding text of the GDPR. Given the legislative history, I predict that the ECJ would uphold the requirement that human intervention not be “fabricated” or “token.”⁵⁴ It would not, however, uphold WP29’s subsequent requirements regarding the person’s authority and the breadth of data considered. These mandates impermissibly strain the meaning of “solely.” Second, the less likely scenario is that the ECJ could determine that “solely” is ambiguous, which would confer greater weight on the legislative history and WP29 guidelines. The guidelines would almost certainly prevail if the court followed this track.

If the court adopts the first approach, an issue around the burden of proof will arise. Human intervention only counts if it is not “fabricated” and if the person could have “an actual influence on the result.” The guidelines do not specify, however, where the burden of proof would lie in showing that human intervention actually influenced, or failed to influence, the outcome of the decision. Pre-clarification, this provision creates a substantial risk for companies relying on predominantly automated decision-making. According to the stand-alone text of Article 22, decisions with any human involvement at all should fall outside of Article 22’s

⁵³ *Id.*

⁵⁴ *Id.*

purview. If a court chose to place the burden on that company to affirmatively show how human intervention influenced a decision, however, the company would face the daunting task of proving after the fact that additional information could have changed the final outcome. Misinterpreting the law up front risks heavy fines under Article 83. Given the legislative history and the guidelines' opening strict interpretation, it seems slightly more likely that the ECJ would place the burden on the complainant to establish that any human involvement played no role in the final decision. Companies may choose, regardless, to follow a risk-averse course until this issue is resolved in litigation.

4.3 LEGAL OR SIMILARLY SIGNIFICANT EFFECTS

The next major qualifier of the rights afforded under Article 22(1) is the requirement that the automated decision produce either a legal, or similarly significant, effect for the data subject. Article 22(1) protects “the right not to be subject to a decision . . . which produces *legal effects* concerning him or her or *similarly significantly affects* him or her.”⁵⁵ This language creates a two-pronged analysis for any decision being considered for Article 22 protection. The decision must yield either a legal effect (Prong 1); or similarly significant effect (Prong 2).

Prong 1

Neither the Recitals nor the legislative history shed additional light on the meaning of “legal effect” under prong 1. The WP29 guidelines, however, attempt to clarify the meaning, while leaving its precise scope ambiguous. The guidelines explain that “only serious impactful events will be covered by Article 22.”⁵⁶ A decision will have a legal effect if it “affects someone’s legal rights,” including changing “a person’s legal status or their rights under a

⁵⁵ GDPR art. 22(1).

⁵⁶ Article 29 Guidelines, *supra* note 22, at 21.

contract.”⁵⁷ This interpretation is consistent with the text of Article 22, and in the absence of additional clarifications from legislative history, the Recitals, or other sources, a court would adhere to this explanation.

The bounds of prong 1, however, are far from clear based on the explanation provided above. As seen in American administrative law, determining when an individual is entitled to a government benefit can be difficult, leaving room for judicial interpretation.⁵⁸ The courts could choose to adopt a narrow interpretation of entitlement, blocking protection for individuals seeking discretionary government benefits. A broader approach to entitlement would allow the court to extend Article 22 to include nearly all recipients of government benefits in any form.

Prong 2

Prong 2’s interpretation was discussed much more in depth than prong 1 by the WP29, the GDPR Recitals, and the legislative history. All three may influence how a court interprets the ambiguous “similarly significant” effect language.

The legislative history illustrates lawmakers’ intention in including the word “similarly” in the phrase “similarly significant” effects. In Article 15 of the DPD, the provision read, “which produces legal effects concerning him or significantly affects him . . .”⁵⁹, notably excluding the word “similarly.”⁶⁰ Neither the 2012 Commission draft of the GDPR⁶¹ nor the Council of Europe recommendations included the word.⁶² It was proposed in the first reading of the European Parliament before being adopted in the final document.⁶³ The legislative history indicates that the decision to restrict “significantly affects” with the word “similarly” was intentional, and should

⁵⁷ *Id.*

⁵⁸ *See, e.g.,* Goldberg v. Kelly, 397 U.S. 254 (1969); Perry v. Sindermann, 408 U.S. 593 (1972); Board of Regents of State Colleges v. Roth, 408 U.S. 564 (1972).

⁵⁹ DPD, *supra* note 8, art. 15(1), at 43.

⁶⁰ Article 29 Guidelines, *supra* note 22, at 21.

⁶¹ European Commission Proposal, *supra* note 44, at 54.

⁶² CM/Rec(2010)13, *supra* note 38, at 6.

⁶³ Annex, *supra* note 39, at 1, 119.

be taken as a real limitation. That analysis, however, leaves open the question of the difference between a “significant effect” and a “similarly significant effect.”

WP29 endeavors to clarify “similarly significant,” emphasizing that a decision that does not change a legal right can fall under Article 22 if the impact is “equivalent.”⁶⁴ The guidance creates a minimum requirement:

“the decision *must* have the potential to:

- Significantly affect the circumstances, behaviour, or choices of the individuals concerned;
- Have a prolonged or permanent impact on the data subject; or
- At its most extreme, lead to the exclusion or discrimination of individuals.”⁶⁵

Notably, the guidance uses the word “must” rather than “may” or “such as.” Unless the decision meets one of the three conditions, it is not a “similarly significant” effect. By contrast, specific areas such as access to financial resources, healthcare, employment opportunities, and education, were listed as potentially significant.⁶⁶ Consequently, a court would likely consider decisions in these areas more seriously, since organizations were warned by the guidance that they could be considered significant.

In the abstract, Recital 71 does not delve deeply into a more precise definition of legal or similarly significant effects, but it does provide two examples of situations in which 22(1) should apply. First, the Recital cites an “automatic refusal of an online credit application.”⁶⁷ It also

⁶⁴ Article 29 Guidelines, *supra* note 22, at 21.

⁶⁵ (emphasis added) *Id.*

⁶⁶ *Id.*, at 22.

⁶⁷ GDPR rec. 71.

highlights “e-recruiting practices without any human intervention” as a secondary application.⁶⁸

In both examples, there would be no legal right or entitlement to the benefit at issue—an approval for extension of credit or a job offer. The Recital, therefore, was addressing prong 2, the “similarly significant effect,” the more ambiguous of the two requirements.

Attempting to extrapolate general principles from the online credit and e-recruiting examples, access to credit can have a large impact on a citizen’s ability to purchase a home, automobile, or pursue educational opportunities. Likewise, employment is a critical component in living and fully participating in modern society. Both employment and credit access have the potential to change someone’s status in society and alter the opportunities they have to support themselves. The extent of the downstream consequences of the decisions could trigger Article 22 protection under prong 2. Examining another angle, credit decisions have historically been fraught with stereotyping and discrimination against protected groups. By including the access to credit example in the Recital, EU legislators could be signaling to a court that it should consider historical abuses in determining whether a decision has a “similarly significant” effect. Other areas of the GDPR and foundational EU principles also address discrimination, lending support for this interpretation of Recital 70’s example.⁶⁹

What other scenarios did the EU intend to include as a similarly significant effect? An analogy from Recital 70’s access to credit and employment examples to university admissions or other educational opportunities is logical. Education is a gateway to future opportunities and a key component of civil participation. Historically, educational access pipelines have been subject to discrimination against vulnerable groups. Educational opportunities were also highlighted as a

⁶⁸ *Id.*

⁶⁹ *Id.* (“Secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect.”).

potential category by the WP29 guidelines. Many of the justifications for including education apply to housing as well, which would support including housing in the same category. Housing was not listed as a WP29 category, however, so may be questioned by reviewing courts.

Up to this point, the legislative history, WP29 guidance, and Recitals have supported an objective analysis of a decision's impact. The WP29 guidance, however, opens up the possibility of a *subjective* analysis, where a court could determine that a decision is "similarly significant" for one individual, but not another.⁷⁰ The subjective analysis approach was only addressed in the context of online advertising, but the guidance does not specifically say that it is inapplicable to other decisions.⁷¹ "[P]rocessing that might have little impact on individuals generally may in fact have a significant effect for certain groups of society, such as minority groups or vulnerable adults."⁷² Certainly in cases pertaining to online advertising, but possibly more generally, this statement could open another door for the courts to examine an individual's background, especially his or her inclusion in a historically disadvantaged group, to determine if a decision has a "similarly significant" effect.

Interpreting prong two subjectively does not conflict with the legally binding text of Article 22, which indicates neither an objective nor subjective approach. Creating such a complex, multi-layered analysis, however, could immerse the courts in a slew of litigation and hurt business across the EU by creating unpredictability in Article 22's application. The articulated goals of the GDPR can be used to argue for or against the subjective analysis method. As discussed above, the GDPR was intended to promote economic growth and foster predictability in data protection law.⁷³ The GDPR also articulates, however, a strong

⁷⁰ Article 29 Guidelines, *supra* note 22, at 22.

⁷¹ *Id.*

⁷² *Id.*

⁷³ GDPR rec. 9.

commitment to preventing discrimination.⁷⁴ Due to the practical difficulties of layering a subjective analysis on an otherwise objective analysis, the court would likely preserve its ability to use a subjective analysis, but only in the narrow context of online advertising.

5. A Prohibition or A Right to Object?

The fundamental question is whether Article 22(1) should be interpreted as a blanket prohibition of all automated data processing that fits the criteria or a more limited right to challenge a decision resulting from such processing. Law firms and companies have speculated about this question since the final language of the law was approved in 2016.⁷⁵ A general prohibition would place the burden of this regulation on organizations, who would be blocked from making certain automated decisions unless they qualified as an exception in GDPR Article 22(2). By contrast, if the section is interpreted as creating a right to challenge the decision after it is made, organizations could maintain most automated decision-making, as long as they had processes in place to address data subjects' concerns when they arose. Organizations could reasonably expect that only a fraction of data subjects would challenge decisions, dramatically truncating Article 22's impact.

Article 22(1) does not clearly distinguish between the competing interpretations.⁷⁶ The WP29 guidelines, however, explicitly state that this section should be interpreted as a prohibition.⁷⁷ Since the guidelines are only persuasive authority, they are not legally binding and

⁷⁴ *Id.*, rec. 14.

⁷⁵ *Profiling and Automated Decision-Taking*, BIRD & BIRD, <https://www.twobirds.com/~media/pdfs/gdpr-pdfs/35--guide-to-the-gdpr--profiling-and-automated-decisiontaking.pdf?la=en>.

⁷⁶ Wachter, *supra* note 44, at 37.

⁷⁷ *Id.*; Article 29 Guidelines, *supra* note 22, at 9 (“A general prohibition on this type of processing exists to reflect the potential risks to individuals’ rights and freedoms.”). *See also id.*, at 19 (“The term ‘right’ in the provision does not mean that Article 22(1) applies only when actively invoked by the data subject. Article 22(1) establishes a general prohibition for decision-making based solely on automated processing. This prohibition applies whether or not the data subject takes an action regarding the processing of their personal data.”).

must yield to the text of the GDPR, if inconsistent. The WP29 claims that Article 22(1)'s phrasing supports its interpretation as a prohibition.⁷⁸ Section 1 states that “[t]he data subject shall have the right *not to be subject* to a decision based solely on automated processing . . .”, implying that no decision-making of this kind should take place from the outset.⁷⁹ WP29 argues that Recital 71 reinforces its conclusion⁸⁰: “However, decision-making based on such processing, including profiling, *should be allowed* where expressly authorised by Union or Member State law . . .”.⁸¹ By stating an exception where the data processing is permitted, the Recital implies that it is disallowed when the exception does not apply.⁸²

Article 22(4) also supports an interpretation of paragraph 1 as a prohibition:

“Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a)⁸³ or (g)⁸⁴ of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.”⁸⁵

Article 9(1) bans processing specific categories of data, such as “racial or ethnic origin, political opinions, [or] philosophical beliefs . . .”.⁸⁶ If Article 22(1) were not intended to be a general prohibition, why would legislators limit the protection for special categories of data provided by paragraph 4 to decisions made under the paragraph 2 exceptions? At a high level, the GDPR

⁷⁸ (emphasis added) Article 29 Guidelines, *supra* note 22, at 20.

⁷⁹ GDPR art. 22.

⁸⁰ (emphasis added) Article 29 Guidelines, *supra* note 22, at 20.

⁸¹ GDPR rec. 71.

⁸² *See* Article 29 Guidelines, *supra* note 22, at 20.

⁸³ GDPR art. 9(2)(a) (“[T]he data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject[.]”).

⁸⁴ *Id.*, art. 9(2)(g) (“[P]rocessing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject[.]”).

⁸⁵ *Id.*, art. 22(4).

⁸⁶ *Id.*, art. 9(1).

seeks to protect data subjects' rights over their data, with a particular emphasis on these sensitive "special categories" of data.⁸⁷ Paragraph 4 only refers to decisions made under paragraph 2, which seems inconsistent with the general purpose of the GDPR, unless paragraph 1 is interpreted as a prohibition.

WP29's interpretation is called into question, however, by the lack of specific language communicating that this section was intended as a prohibition. For example, GDPR Article 9(1) states that "[p]rocessing of personal data revealing racial or ethnic origin . . . *shall be prohibited*."⁸⁸ If EU legislators intended this provision to be a general prohibition, they could have included similar language in Article 22. Instead, they used more ambiguous phraseology: "The data subject shall have the right *not to be subject* to a decision." This language does not indicate whether the right to be free of this type of decision applies *ex ante* or *ex post*. In Article 9, the responsibility is clearly placed on the data processor to completely block the data processing, whereas in Article 22, the language focuses on the data subject—which could imply an intent to create an individualized right to challenge a decision instead of a general prohibition.

The Commission's proposed language in 2012 supported interpreting Article 22 as a prohibition, but the language was amended in the final version of the GDPR.⁸⁹ Deliberately changing the language to read less like a prohibition may indicate that legislators intended Article 22 to be an individual right. The Commission draft stated that "a person may be subjected to a measure of the kind referred to in paragraph 1 [decisions made by automated data processing] *only if* . . ." certain exceptions apply.⁹⁰ By using the phrase "only if," the

⁸⁷ See HUNTON & WILLIAMS, *supra* note 22, at 8.

⁸⁸ (emphasis added) *Id.*, art. 9(1). See Eduardo Ustaran and Victoria Hordern, *Automated Decision-Making Under the GDPR – A Right for Individuals or A Prohibition for Controllers?*, CHRONICLE OF DATA PROTECTION, (Oct. 20, 2017), <https://www.hldataprotection.com/2017/10/articles/international-eu-privacy/automated-decision-making-under-the-gdpr-a-right-for-individuals-or-a-prohibition-for-controllers/>.

⁸⁹ Annex, *supra* note 39, at 1, 119; See also Eduardo Ustaran, *supra* note 86.

⁹⁰ (emphasis added) Annex, *supra* note 39, at 119.

Commission made clear that the provision should block all other instances of automated data processing. This construction was not adopted in the final draft. The European Parliament’s first reading preserved the phrase “only if,” but the Council proposed “Paragraph 1 shall not apply if the decision . . .”⁹¹ In 2016, the final GDPR text followed the Council’s approach, reading “Paragraph 1 shall not apply if the decision . . .” qualifies as an exception. Some legal privacy experts have asserted that this change was a deliberate rejection of the prohibition.⁹² These phrases are not linguistically equivalent. The 2012 draft text specifically states that the measures, meaning the decisions made via automated processing, can only be employed when an exception applies. Therefore, an exception in paragraph 2 is a prerequisite for paragraph 1’s automated decision-making. In the final GDPR text, however, the reference to the “measure” was eliminated. Rather, it refers more generally to paragraph 1, which can be reasonably interpreted as a prohibition or a right to challenge a decision. The meaning changes from restricting the measure itself to restricting the application of the previous paragraph. Further, “[apply] only if” (2012 text) is not equivalent to “shall not apply if” (2016 text). The former explicitly excludes the decision-making in every circumstance except those listed in an exception. The latter, by contrast, is not necessarily exclusive—it indicates three circumstances in which paragraph 1 would not apply, but not to the exclusion of all other circumstances. The legislative history undermines the WP29 interpretation of Article 22 as a general prohibition.

The placement of Article 22 in Chapter III of the GDPR poses an additional challenge to the WP29 interpretation.⁹³ Chapter III, “Rights of the Data Subject,” includes sections such as

⁹¹ *Id.* at 118-119.

⁹² Eduardo Ustaran, *supra* note 88.

⁹³ David Meyer, *Did the WP29 Misinterpret the GDPR on Automated Decision-Making?*, IAPP (Nov. 28, 2017) <https://iapp.org/news/a/did-the-wp29-misinterpret-the-gdpr-on-automated-decision-making/>.

“Right to Erasure,” “Right to Object,” and “Right to Data Portability.”⁹⁴ These sections primarily articulate rights that data subjects can assert under the new data protection regime. By contrast, Chapter IV, “Controller and Processor,” has sections that impose obligations on organizations using data subjects’ information in the course of their operations.⁹⁵ Sections within Chapter IV include “Responsibility of the Controller,” “Security of Processing,” and “Data Protection Impact Assessment.”⁹⁶ Affirmative obligations for companies are generally listed in Chapter IV. Article 22 is placed in the rights-focused Chapter III, implying that EU legislators intended the language to be interpreted as a right that can be asserted by individual data subjects, rather than a prohibition of certain decisions that a company must implement.^{97,98}

Finally, the GDPR was based on the 1995 DPD, Article 15, so Member States previously had the opportunity to interpret a similar provision in order to transpose it into their national laws.⁹⁹ The DPD provision read:

“Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.”¹⁰⁰

⁹⁴ GDPR Chapter III.

⁹⁵ *Id.* Chapter IV.

⁹⁶ *Id.*

⁹⁷ See David Meyer, *supra* note 93.

⁹⁸ Opponents of this view may argue that there are several provisions in Chapter III that simultaneously impose obligations on data controllers and grant rights to data subjects. For example, Article 12 reads, “The controller shall take appropriate measures to provide any information” Similarly, Articles 13 and 14 explain things that the data controller “shall” do.

⁹⁹ Wachter, *supra* note 44, at 38.

¹⁰⁰ DPD, *supra* note 8, art. 15, at 43.

Several Member States interpreted DPD Article 15 as a prohibition, supporting the WP29 interpretation.¹⁰¹ Although there were minor variations among them, Austria, Belgium, Germany, Finland, the Netherlands, Portugal, Sweden, and Ireland interpreted Article 15 as a general prohibition.¹⁰² The UK interpreted the provision differently. There, the law was not considered a prohibition, but rather a right for data subjects to protest an automated decision made about them.¹⁰³

The determination whether Article 22 is a prohibition or a right to challenge automated decision-making will be a close question for the ECJ. The WP29 textual analysis of Article 22, explained by Recital 71, will weigh in favor of interpreting Article 22 as a prohibition. This conclusion is reinforced by the national laws adopted by Member States under the 1995 DPD, interpreting a nearly identical statute as a prohibition. The evolution of GDPR drafts, placement of Article 22 in Chapter III, and contrast with clearer prohibitions in the GDPR (e.g., Article 9) weigh in favor of interpreting Article 22 as a right to be asserted after a decision is made. The ECJ would likely determine that absent a clear articulation of a prohibition in paragraph 1, the burden that would be imposed on companies to comply with such a provision would be unjustifiable. Regardless, until the ECJ definitively resolves this issue, companies risk incurring substantial cost. Either they may cease valuable automated decision-making, fearing fines if the prohibition interpretation prevails, or they may incur massive fines if they gamble by making decisions about data subjects that are later determined to be illegal.¹⁰⁴

¹⁰¹ Douwe Korff, *Data Protection Laws in the EU*, 82, 84 (European Commission, Directorate-General Justice, Freedom and Security, Working Paper No. 2, Jan. 20, 2010) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1638949. *See also* Wachter, *supra* note 44, at 38.

¹⁰² *Id.*

¹⁰³ Douwe Korff, *supra* note 101, at 84.

¹⁰⁴ Violations of Article 22 fall in the higher of the two fine categories. *See* GDPR art. 83(4)-(5). This category permits the EU to fine an entire undertaking a maximum of 4% of the total worldwide annual turnover or 20,000,000 Euros. GDPR art. 83(5)(b).

6. Article 22 Exceptions

Article 22, paragraph 2 outlines three scenarios that are exceptions to paragraph 1's restrictions: execution of a contract, Member State or Union law, and consent. The provision reads:

“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;¹⁰⁵
- (b) is authorised by Union or Member State law¹⁰⁶ 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 consent¹⁰⁷.”¹⁰⁸

The primary interpretive challenges for paragraph 2 are understanding the various restrictions placed on the exceptions by paragraphs 3 and 4 and the Recitals. The following section will assess the meaning of “suitable safeguards” required by paragraph 3, determining in particular whether a right to explanation exists and the extent of the non-discrimination requirement.

¹⁰⁵ The contract exception could be a powerful tool for organizations relying on automated decision-making. Consent is a separate exception, which could indicate that the organization executing the contract in the first exception will determine whether decision-making is “necessary.” While a court could review the decision, this responsibility would give organizations substantial latitude. Wachter, *supra* note 44, at 37. WP29 explains that this authority is limited, however, because a decision would only be “necessary” if no “other effective and less intrusive means to achieve the same goal” were available. Article 29 Guidelines, *supra* note 22, at 23.

¹⁰⁶ This may include the government's efforts to detect fraud and tax evasion. GDPR rec. 71.

¹⁰⁷ GDPR art. 4(11) (“[C]onsent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”).

¹⁰⁸ GDPR art. 22(2).

7. Safeguards for Exceptions

Automated decision-making conducted under the contracting or consent exceptions is subject to the following limitation:

“In the cases referred to in points (a) and (c) of paragraph 2, the data controller *shall 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.”¹⁰⁹

There are two important segments of this provision. First, “the data controller shall implement suitable measures to safeguard the data subject’s rights” establishes a legal obligation for data controllers. Paragraph 3 does not define “suitable measures,” so the interpretation of this term will be key to understanding the burden imposed on organizations.¹¹⁰ Second, the provision sets a mandatory minimum when it states, “at least the right to” (1) “obtain human intervention,”¹¹¹ (2) “to express his or her point of view,” and (3) “to contest the decision.”¹¹²

7.1 SUITABLE MEASURES TO SAFEGUARD

GDPR Article 22(3) requires organizations to develop suitable measures to safeguard data subjects’ information, but a combination of non-binding legal authorities must be used to determine the meaning of this requirement. Most importantly, Recital 71 outlines several

¹⁰⁹ (emphasis added) GDPR art. 22(3).

¹¹⁰ *Id.*

¹¹¹ Article 29 Guidelines, *supra* note 22, at 27 (“Human intervention is a key element. Any review must be carried out by someone who has the appropriate authority and capability to change the decision. The reviewer should undertake a thorough assessment of all the relevant data, including any additional information provided by the data subject.”).

¹¹² GDPR art. 22(3); Wachter, *supra* note 44, at 10.

practices that the organization “should” employ.¹¹³ The language here is critical—the Recital does not present these as absolute requirements, but suggestions or best practices. Lawmakers could have inserted words such as “must” or “at a minimum” in the Recital, but chose not to. A court may choose to incorporate the Recital’s suggestions into the definition of “suitable safeguards,” but lawmakers’ language choice is a strong argument for organizations to challenge the wholesale adoption of Recital 71’s provisions. Similarly, lawmakers could have defined “suitable safeguards” in the legally binding text, but did not. These choices provide organizations an avenue to argue that the definition was meant to be flexible or less stringent than a government enforcement body might maintain.

The following sections address three key areas of ambiguity in the safeguard provision. These areas have the potential to substantially impact companies’ business and pose large risks if interpreted incorrectly.

7.1.1 *Right of Explanation*

Arguably the most critical question arising from this section of Article 22 is whether a right to explanation is conferred on data subjects as a safeguard. Based on the exclusion of the right from the legally binding text and the legislative history of paragraph 3, a court would be most likely to determine that the right to explanation here is strongly encouraged, but not

¹¹³ GDPR rec. 71 (emphasis added) (“In any case, such processing should be subject to suitable safeguards, which *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. . . . In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, *the controller should use* appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect.”).

required. The uncertainty, however, may prompt many companies to implement procedures offering this right to avoid enforcement actions until the law is clarified.

Paragraph 3 lists three minimum safeguards for data subjects—(1) the right to human intervention in the decision; (2) the right to express a point of view; and (3) the right to challenge the decision.¹¹⁴ In Recital 71 these three safeguards are listed again in almost exactly the same way. One additional safeguard is included in the list, however—(4) the right to “obtain an explanation of the decision reached after such assessment.”¹¹⁵ Leaving the fourth factor out of the legally-binding text when so much of the wording is the same indicates lawmakers’ intention to exclude the right to explanation as a legal requirement under Article 22.¹¹⁶ Furthermore, since Recitals are not legally binding, they cannot override the GDPR’s text. Here, there is a strong argument that Recital 71 cannot be interpreted as mandating a right to explanation because it contradicts Article 22(3). Paragraph 3 does not say that companies should implement safeguards, *such as* the right to human intervention, etc. Rather, it establishes a “legal minimum” by using the words “at least” before listing the three examples.¹¹⁷ Therefore, the courts could not appropriately add a fourth requirement to the definition of safeguards to incorporate a right to explanation.

There is an important distinction between a data controller providing *ex ante* descriptions of automated decision-making functionality and *ex post* information on stand-alone decisions made about a data subject.¹¹⁸ Articles 13(2)(f) and 14(2)(g)¹¹⁹ impose an obligation on data controllers to disclose information.¹²⁰ They must notify the data subject of:

¹¹⁴ GDPR art. 22(3).

¹¹⁵ GDPR rec. 71.

¹¹⁶ Wachter, *supra* note 44, at 11.

¹¹⁷ *Id.* at 10.

¹¹⁸ *Id.* at 1, 21-22. *See also* Binns, *supra* note 23 (“One of the significant ambiguities is around whether Articles 13, 14, 15, or 22 give individuals a ‘right to an explanation’, that is, an *ex post* explanation of why a particular

“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.”¹²¹

In Articles 13 and 14, a data subject has a limited right to information about the “logic involved” in the decision-making process. He/she must also be informed of the anticipated consequences of the decision-making process—indicating that this is an *ex ante* right to information before a particular decision is actually made. Article 15(1)(h) is similarly limited in the scope of its required disclosure.¹²² It uses the same language as Articles 13(2)(f) and 14(2)(g) above, but it grants data subjects the right to inquire if their data is being processed and if so, to obtain information about the logic and consequences.¹²³ Articles 13, 14, and 15 create rights to information, but they do not confer a right for a data subject to obtain information about a *particular* decision after the fact.¹²⁴ Recitals 60 and 63 reinforce this conclusion, confirming an *ex ante* right to logic and consequences.¹²⁵ A potential counterargument that may gain traction with a court would highlight the overarching principle of transparency for data processing throughout the GDPR.^{126,127} Another potential counterargument is that the legal minimum

automated decision was made about them.”). For a general description of the distinctions between different “explanation” rights, see Wachter, *supra* note 44, at 6.

¹¹⁹ Article 14(2)(g) imposes the same obligation as Article 13(2)(f). Article 13 applies when data is collected from a data subject. Article 14 applies when data was not collected from the data subject. GDPR arts. 13-14.

¹²⁰ GDPR art. 13(2).

¹²¹ GDPR art. 13(2)(f).

¹²² GDPR art. 15(1)(h).

¹²³ *Id.*

¹²⁴ Wachter, *supra* note 44, at 15.

¹²⁵ GDPR rec. 60 (“the data subject should be informed of the existence of profiling and the consequences of such profiling.”); GDPR rec. 63 (“Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing.”).

¹²⁶ *See*, GDPR rec. 60; GDPR rec. 39; GDPR rec. 59.

requires a right to “contest the decision.” A court may determine that it is not possible for a data subject to contest the decision without specific information about how that decision was made. This point would not be dispositive, however—data controllers have to notify data subjects of the existence of a decision, as articulated above, so that information could form the grounds for a challenge, albeit a less compelling one.

To resolve the tension between the transparency principle, limited rights under Articles 13-15, and exclusion of the right to explanation from the text of Article 22, courts will examine the legislative history of Article 22 to understand the intent of the legislators. The comparable provision in Article 20 of the 2012 GDPR draft did not create a “legal minimum” of safeguarding measures. Instead, the provision was written more ambiguously, leaving more room for interpretation: “where suitable measures to safeguard the data subject’s legitimate interests have been adduced, *such as* the right to obtain human intervention.”¹²⁷ Article 20(5) granted the Commission authority to define “suitable safeguards” in the future.¹²⁹ In the First Reading, the European Parliament proposed: “The suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2 shall include the right to obtain human assessment and an explanation of the decision reached after such assessment.”¹³⁰ This language not only avoided a legal minimum, but also explicitly included the right to explanation in the legally-binding text.

¹²⁷ See also Article 29 Guidelines, *supra* note 22, at 27. The guidelines adopt the view that while there is a “minimum” set of safeguards (human intervention, express point of view, and contest decisions), “*in any case* suitable safeguards should also include” the right to explanation. The analysis above remains the same—the guidelines cannot override the plain text of Article 22. If Article 22 establishes a minimum, then Recital 71 can only clarify ambiguities, not contradict it.

¹²⁸ European Commission Proposal, *supra* note 44, art. 20(2)(a), at 54. See also *id.*, art. 20(2)(c), at 54 (“subject to the conditions laid down in Article 7 and to suitable safeguards.”); *id.*, art. 20(4), at 54 (“In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.”).

¹²⁹ *Id.*, art. 20(5), at 54.

¹³⁰ Annex, *supra* note 39, at 1, 122-123.

The final GDPR provision, however, relegated the right to explanation to Recital 71 and used “at least” rather than “such as.”

Understanding the legislative history and examining Article 22’s text, a court would most likely agree with Wachter, et al. that despite the overarching commitment to transparency, lawmakers deliberately excluded an ex post right to explanation of specific decisions from Article 22.

7.1.2 *Non-Discrimination*

Article 22’s non-discrimination requirements face a similar interpretive challenge as the right to explanation. Like transparency, non-discrimination is a consistent theme throughout the GDPR and EU law more generally. The strongest language around preventing discrimination for Article 22, however, is in Recital 71, rather than the legally-binding text. Recital 71 instructs organizations to “secure personal data in a manner” that will “prevent discriminatory effects” on people for their membership in specific protected categories (e.g., race, political belief, religion).¹³¹ If strictly enforced, this provision has the potential to constitute a substantial burden for companies, who would need to assess the unintended consequences of certain types of automated decision-making.

The analysis for this provision closely parallels that of the right to explanation. In a similar fashion, the European Parliament proposed language that would incorporate non-discrimination requirements directly into Article 22 (then, Article 20).¹³² In the final version of the GDPR, this provision was removed to Recital 71.

¹³¹ GDPR rec. 71.

¹³² Annex, *supra* note 39, at 1, 121. (“Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited. The controller shall implement

Furthermore, WP29 guidance calls data controllers to conduct assessments on their data to identify bias, combat prejudicial influences, and eliminate “overreliance on correlations.”¹³³ It specifically separates out two additional non-discrimination provisions, which it presents as “good practice recommendations.”¹³⁴ These latter two principles are clearly meant to be optional, but could help companies demonstrate good faith in the face of an enforcement action.

Notwithstanding Article 9 and Article 22(4) special category protections, Article 22 does not establish robust non-discrimination protections. The legislative history is highly influential here—EU legislators had the opportunity to embed non-discrimination requirements in Article 22, but made a deliberate decision to remove the suggested text. While auditing algorithms and implementing other measures to reduce discrimination could help companies establish a pattern of positive conduct that may help in an enforcement action, these provisions are not included in the GDPR’s requirements and would therefore be deemed not legally enforceable by a court.

7.1.3 *Correcting Inaccuracies*

Recital 71 maintains that the data controller should “implement technical and organization measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized[.]”¹³⁵ This practice is not mentioned at all in the legally-binding text, and the parameters are not described in the Recital. “Ensure” is strong language, implying that an organization could be penalized for

effective protection against possible discrimination resulting from profiling. Profiling shall not be based solely on the special categories of personal data referred to in Article 9.”).

¹³³ Article 29 Guidelines, *supra* note 22, at 28.

¹³⁴ (1) Conducting quality assessments to identify and eliminate discrimination against people; and (2) Auditing the algorithm, making sure that it does not produce unintended discriminatory effects. *Id.* at 32.

¹³⁵ GDPR rec. 71.

implementing only reasonable measures that may allow some mistakes, rather than more expensive and restrictive measures “ensuring” no inaccuracies.

Examining the purpose of the GDPR, legislators were concerned with appropriately balancing economic health and individuals’ rights over their data. In light of these more general principles, a highly restrictive reading of this provision is unlikely to prevail in court. Furthermore, a less restrictive interpretation is supported by the WP29 guidance. Noting the possible negative consequences of errors in the systems or data needed in automated decision-making, the guidance notes that “[c]ontrollers should introduce appropriate procedures and measures to prevent errors, inaccuracies or discrimination on the basis of special category data.”¹³⁶ The guidance further notes that these safeguards should be used periodically, not simply when the algorithm or system is designed.¹³⁷ As “good practice,” the guidance recommends using systems that regularly assess the decision-making process for mistakes.¹³⁸

A court will have considerable flexibility in interpreting this provision, given the lack of legally-binding language. Given the general purpose of the GDPR and the need to make this law reasonable and implementable for businesses, a court would more closely adhere to the approach articulated by WP29. It would judge organizations’ safeguards to determine if they are “appropriate,” which would almost certainly not require the most stringent process available.

8. Conclusion

The GDPR is unprecedented in the field of privacy and data protection. It is an attempt to secure citizens’ rights over their own data, while avoiding hamstringing the digital economy—and in fact, the goal is that ultimately, consistent standards will enhance economic conditions.

¹³⁶ Article 29 Guidelines, *supra* note 22, at 27-28.

¹³⁷ *Id.*, 28.

¹³⁸ *Id.*

While portions of the GDPR developed from previous legislation, technological advances and ambiguous language in the law have resulted in uncertainty about its provisions. Article 22, in particular, has a wide-ranging potential impact, but key decisions have yet to be made about the specific parameters of the law. While this paper conducted an analysis of the likely legal outcomes of several key interpretive questions in the law, this topic must necessarily be revisited as the inevitable cases make their way through the courts in the EU.