eLaw
Working Paper Series

No 202ť/00 - ELAW– 202ť

Universiteit Leiden
eLaw

Discover the world at Leiden University

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice

Bart Custers[a,c,*], *Anne-Sophie Heijne*[b,c]

[a] *Law and Data Science at eLaw, the Center for Law and Digital Technologies, Leiden University, the Netherlands*
[b] *Leiden University, the Netherlands*

ARTICLE INFO

Keywords:
Right of access
GDPR
Article 15 GDPR
Profiling
Automated decision-making
Automated decisions
Meaningful information
Trade secrets

ABSTRACT

The right of access in Article 15 of the EU General Data Protection Regulation (GDPR) is essential for empowering data subjects when exercising other data subject rights. In the context of automated decision-making, including profiling, Article 15(1)(h) provides a right to meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. In this research, the notions of 'meaningful information', 'the logic involved', and 'the significance and the envisaged consequences' are analysed. Apart from a legal analysis, empirical research was carried out in 30 countries (27 EU and 3 EFTA EEA Member States), consisting of a survey amongst all Data Protection Authorities (DPAs) and interviews with experts of privacy organisations. Several types of potentially meaningful information that could be in scope of right of access requests were assessed, as well as several types of information on the consequences for data subjects. Even though respondents indicate that most of these types of information should be provided upon access requests, the findings show that most of these types of information are rarely or not at all provided in practice. Providing such information strongly depends on the willingness of data controllers to cooperate, as they may balance this against rights and freedoms of others, including intellectual property and trade secrets. Particularly trade secrets are invoked in practice to block or restrict access requests, despite the GDPR stating that these considerations should not lead to a refusal of the request to provide all information to the data subject.

1. Introduction

The right of access in Article 15 of the EU General Data Protection Regulation (GDPR) is one of the core data subject rights in EU data protection law. The right of access, in conjunction with the right to transparent information in Articles 13 and 14 GDPR, is essential for data subjects when exercising other data subject rights. For instance, a right to rectification (Article 16) or erasure (Article 17) cannot effectively be invoked if data subjects have no knowledge of the data that have been collected or processed.

* Corresponding author.
[c] The authors would like to thank Ela Omersa, Katalin Czászár and Gráinne Murphy for reviews of previous versions of this article.

https://doi.org/10.1016/j.clsr.2022.105727

How the right of access should be implemented in practice is not entirely clear, particularly in the context of data processing that involves algorithms or automated decisions, which is increasingly common in the processing of personal data.[1] Large amounts of personal data are processed by many data controllers, creating a need for automated processing and analysis of those data. Such automated processing can be very sophisticated, using data mining and machine learning tools to discover patterns and relations in large datasets.[2] Profiling tools can categorise and cluster data subjects, predicting and ascribing particular characteristics to them.[3]

The GDPR recognises that these practices carry several risks for data subjects. Some provisions are tailored to provide data subjects with further protection, such as the right to object to automated individual decision-making (Article 21) and the right not to be subject to decisions based solely on automated processing (Article 22). However, effectively invoking these rights is only possible if data subjects are aware of the existence, workings and consequences of these practices. Article 15(1)(h) GDPR explicitly states that when automated decision-making (including profiling) is used, the right of access for data subjects includes access to meaningful information about the logic, significance and envisaged consequences of that processing for the data subject.

Recital 63 GDPR further qualifies this right to meaningful information by stating that it should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property (IP), in particular copyright protection software. In the data economy, distilling knowledge from raw data is the value adding process that is at the core of many business cases. For instance, automated data analyses can extract risks assessments for individuals and groups of people. Such risks assessments can constitute the competitive edge for many companies, such as banks deciding on loans and mortgages, insurance companies deciding insurance premiums, or retailers deciding on dynamic or personalised pricing. The ways in which companies analyse their data, often using sophisticated software specifically developed for these goals, may be part of their trade secrets and covered by IP rights. Given the competitive edge involved, it is unsurprising that companies may be very reluctant to share such information with data subjects, fearful that such disclosures may end up in the hands of competitors.

This raises the question of how to interpret the concept of 'meaningful information' in Article 15(1)(h) GDPR and the extent to which information should be provided regarding 'the logic involved' and the 'significance and the envisaged consequences' for the data subject. From the perspective of empowering data subjects, it is necessary to provide meaningful information on how this works, including its significance and consequences. From the perspective of data controllers, however, it may be essential to protect trade secrets and IP rights, because disclosure may impede their competitive position.

In this empirical research, the practical and legal implementation of Article 15(1)(h) GDPR in 30 European countries is investigated. Through a survey and interviews, different practices are identified and compared and contrasted. This provides more insight into the right of access (empowering data subjects, strengthening their rights) when data processing involves algorithms or automated decisions. The focus is on the concept of meaningful information, information actually useful for data subjects, and how to balance this with competing interests like IP and trade secrets. Therefore, this article addresses the following three research questions:

1) How can 'meaningful information' potentially be defined under Article 15 of the GDPR?
2) When is the information provided useful for data subjects?
3) Which competing interests, like IP and trade secrets, are relevant in this matter and how can they be balanced?

The (geographical) scope of this research concerns all EU Member States (EU-27), as well as European Free Trade Association (EFTA) and European Economic Association (EEA) states (Iceland, Liechtenstein and Norway).[4] In total, 30 countries (27 EU Member States and three EFTA EEA states) were included in this research. The research presented here was carried out between December 2020 and July 2021. Developments that took place during or after July 2021 were not taken into account in this research.

This article is structured as follows. Section 2 provides a description of the methodology used in this research. Section 3 provides a legal analysis of the relevant legislation, with a focus on Article 15 and Recital 63 GDPR. Section 4 focuses on the survey and interviews and the resulting data gathered from different countries. Section 5 provides conclusions and discussed limitations of this research.

2. Methodology

2.1. Data collection

A mixed-method approach was used in this research, consisting of desk research, a survey and interviews. The desk

[1] Hildebrandt, M., and Gutwirth, S. (2008). *Profiling the European citizen: Crossdisciplinary perspectives*. Heidelberg: Springer.; Zarsky, T. Z., 'Mine your own business: Making the case for the implications of the data mining of personal information in the forum of public opinion', *Yale JL & Tech*. 2003, 5, 1.; Schauer, F. (2006). *Profiles, probabilities, and stereotypes*. Harvard University Press.; Custers, B., and Bachlechner, D., 'Advancing the EU data economy: Conditions for realizing the full potential of data reuse', *Information Polity* 2017, *22*(4), pp. 291–309. https://doi.org/10.3233/IP-170419

[2] Zarsky, T. Z., 'Mine your own business: Making the case for the implications of the data mining of personal information in the forum of public opinion', *Yale JL & Tech*. 2003, 5, 1.; Calders, T. and Custers, B.H.M. (2013). What is data mining and how does it work? In: Custers, B.H.M., Calders, T., Schermer, B.W., Zarsky, T.Z. (red.), *Discrimination and Privacy in the Information Society* (nr. 3). Heidelberg: Springer.

[3] Harcourt, B. E. (2007). *Against prediction: Profiling, policing, and punishing in an actuarial age*. University of Chicago Press.; Schauer, F. (2006). *Profiles, probabilities, and stereotypes*. Harvard University Press.;Custers, B. H. M., Calders, T., Schermer, B., and Zarsky, T. (2013). *Discrimination and privacy in the information society: Data mining and profiling in large databases*. Heidelberg: Springer.

[4] Switzerland is an EFTA member, but not an EEA member and was therefore outside the scope.

research entailed literature research, with available literature and online information collected on both technologically and legally relevant information. With regard to technology, the focus was on the workings of algorithms, profiling practices, and automated decision-making processes. With regard to legally relevant information, the focus was on the right of access, the (alleged) right to explanation, the right to object to automated individual decision-making, the right not to be subject to decisions based solely on automated processing, and on trade secrets and IP in the context of algorithms, profiling and automated decisions.

The main goals of the desk research were to collect general background information and to enrich the information collected from the national Data Protection Authorities (DPAs) (via the survey, see below) and experts (via the interviews). The literature research included legislation, policy documents, case-law, parliamentary proceedings, annual reports of DPAs and bodies within the judiciary, and relevant academic publications. The online research primarily focused on the websites of the DPAs (focusing on policy documents and complaints) and the judicial authorities (focusing on case-law) in each of the countries investigated.

A survey was used to better select and organize the information gathered. The survey contained 14 questions in three substantive parts and was completed for each of the countries investigated. The first part (nine questions) focused on the right of access. These were questions on how the right of access in Article 15 GDPR is implemented in national legislation, the extent to which governments and DPAs issued legislation, polices or guidelines to implement the right of access in practice, the availability of case-law, the kinds of information that is/should be provided by data controllers if data subjects invoke their right of access, and the number and nature of complaints DPAs receive related to the right of access. The second part (two questions) focused on algorithms and automated decisions. These were questions on the availability of any policy documents (either from the government or DPAs) that provide guidance on how to apply the GDPR in the context of algorithms, automated decisions or profiling, and on the availability of any policy documents detailing different categories of data that can or should be provided in this context. The third part (three questions) focused on IP and trade secrets, with questions on national legal provisions protecting IP rights or trade secrets in the scope of algorithms and automated decisions, including their scope, and questions on any other competing interests and balancing mechanisms.

The survey was the basis for this research to collect and select information relevant to the understanding of the notion of 'meaningful information' as stated in the GDPR in all EU Member States' and EFTA EEA States' national legislation, and to provide a legal analysis. The first step was to try to complete the survey by desk research as much as possible. The second step was to further complete the survey by distributing it to all national DPAs. The DPAs received an empty version of the survey in order to avoid any bias.

In the first step, it was possible to complete approximately two-thirds of the survey questions (across all countries). In the second step, completed surveys were received from the DPAs in 21 of the 30 countries, giving a response rate of 70%.[5] In the first and second step, most of the surveys were largely complete. To close the remaining gaps, the third step was to locate and interview experts in specific countries. France, Germany, Ireland and the Netherlands were selected, as these survey results signalled their concrete approach. In these countries, all major privacy organisations were contacted.[6] In total, seven of these organisations put forward experts willing to do an interview. These were relatively evenly distributed: two interviews each for France, Germany, and the Netherlands and one interview for Ireland.[7] interviews were conducted online with experts from privacy organisations in those countries to obtain further understanding of the data subject's perspective. The interviews were semi-structured and took place online. The experts were only asked questions that sought to close the information gaps at that time.

2.2. *Data analysis*

Two analyses were carried out: a legal analysis (based on desk research) and a practical implementation analysis (based on the country survey results), described below in Sections 3 and 4 respectively.

For the legal analysis, the first step was to distil all legal provisions in the GDPR relevant for the right of access in the context of algorithms, automated decisions and profiling. Next, all legal documents (legislation, policy documents, case-law, etc.) collected at national level were analysed in light of the right of access. This was primarily done by searching terms like 'right of access', 'meaningful information', 'automated decision-making', and 'profiling' in the legal documents. Finally, all selected provisions were combined to examine whether they could contribute to a common understanding of the notion of 'meaningful information'.

Research on the practical implementation took place via the survey that was conducted. Per question in the survey the country results were compared and contrasted, revealing different practices across the countries examined. This information was validated by and further enriched with the information distilled from the interviews.

[5] Completed surveys received from the DPAs of: Austria, Bulgaria, Croatia, Czechia, Estonia, France, Germany, Liechtenstein, Hungary, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, the Netherlands, Norway, Poland, Slovakia, Spain and Sweden.

[6] Custers, B.H.M., Dechesne, F., Georgieva, I.N., Sears, A.M., Tani, T., and van der Hof, S. (2019). *EU Personal Data Protection in Policy and Practice* (1st ed. 2019). T.M.C. Asser Press : Imprint: T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-282-8

[7] In France: *Creis Terminal – Centre de Coordination pour la Recherche et l'Enseingement en Informatique et Société* (https://www.lecreis.org) and *Ligue des droits de l'Homme* (https://www.ldh-france.org). In Germany: GDD – *Gesellschaft für Datenschutz und Datensicherheit a.V.* (https://www.gdd.de) and *Stiftung Datenschutz* (https://stiftungdatenschutz.org). In Ireland: *Digital Rights Ireland* (https://www.digitalrights.ie). In The Netherlands: *Bits of Freedom* (https://www.bitsoffreedom.nl) and *Privacy First* (https://www.privacyfirst.nl).

3. Legal analysis

This section focuses on the legal analysis of the right of access in the GDPR. Section 3.1 discusses the Article 15 and Recital 63 of the GDPR. Section 3.2 through 3.5 examine the core concepts in these provisions: "meaningful information" (Section 3.2), "the logic involved" (Section 3.3), "significance and envisaged consequences" (Section 3.4), and "rights and freedoms of others" (Section 3.5).

3.1. *Article 15 and Recital 63 GDPR*

Article 15 GDPR provides data subjects with a right of access. Article 15(1) GDPR introduces the right of access as the right of data subjects to obtain confirmation as to whether or not the data controller is processing their personal data and, if that is the case, access to their processed personal data and to additional information listed under (a) through (h). Article 15(2), which lays beyond the scope of this research, states that the data subject has the right to be informed about the appropriate safeguards taken if personal data are transferred to a third country or to an international organisation. Article 15(3) provides the data subject with the right to obtain a copy of the personal data undergoing processing, which can be subject to a reasonable fee based on administrative costs.[8] According to Article 15(4), this right to obtain a copy shall not adversely affect the rights and freedoms of others.

Recital 63 is the only recital in the GDPR that refers to the right of access,[9] stating that the main goal of the right of access is to enable data subjects 'to be aware of, and verify, the lawfulness of the processing'. In essence, the right of access is about control and empowerment of data subjects. Without the right of access, it is hard for data subjects to exercise other data subject rights. For instance, it is hard to exercise a right to rectification without having access to the actual data – a data subject cannot assess whether data are correct when the data cannot be viewed.

The right of access can be exercised easily and at reasonable intervals. This means that it can be invoked more than once, even regularly, but not disproportionately often. Recital 63 encourages data controllers, where possible, to provide data subjects with remote access to a secure system that enables them to directly access their personal data. Although this is not the only possible implementation, by explicitly mentioning this option, it seems that the GDPR encourages data controllers to provide data subjects with secure remote direct access to their data, for instance, through a personal online environment where they can log-in with a username and password to access their personal data. Recital 63 also offers data controllers of large quantities of information some protection against excessive requests, by stating that data subjects can be asked to specify the information or processing activities to which their request relates.

It is clear that the scope of the right of access reaches beyond the information data subjects themselves previously provided. Recital 63 provides several examples of the information within the scope of the right of access, including data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Typically, these types of information are generated by doctors rather than patients, meaning that inferred data is indeed within the scope of Article 15 GDPR.[10]

Article 15(1)(h) GDPR is the most relevant part of Article 15 for this research, as this article focuses on automated decision-making, including profiling.[11] Where a data controller makes use of automated decision-making or profiling, a data subject has three specific rights:

1) the right to know that automated decision-making or profiling is being used;
2) the right to obtain meaningful information about the logic involved;
3) the right to be informed about the significance and envisaged consequences of such processing.

It is worth first noting that Article 15(1)(h) GDPR refers to Article 22(1) and 22(4) GDPR. These provisions contain some ambiguity, as the article mentions automated individual decision-making in its title and decisions based solely on automated processing in its text. Automated decisions do not always have to be based on automated processing. Also, automated decisions can be partially (rather than solely) based on automated processing. The condition in Article 22(1) GDPR that decisions are based solely on automated processing is therefore a high threshold, requiring that no human is involved in the entire process. In its guidelines on profiling and automated decision-making, the Article 29 Working Party (WP29, the EU data protection advisory body of representatives of national DPAs, the EDPS and the European Commission) took the view that a decision based on solely automated means includes any decision in which a human intervention is not meaningful.[12]

This statement has been confirmed in some national case-law,[13] but it may not be that relevant anyway, as it can be

[8] In 2020 the Dutch Data Protection Authority impose a 830.000 euro fine on a data controller that charged relatively high fees for data subjects requesting access to their data, see https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_bkr_30_juli_2019.pdf

[9] Apart from Recital 63, Recital 64 also mentions the right of access, but not in a substantive way: it requires data controllers to verify the identity of any data subject that invokes the right of access.

[10] Custers, B.H.M., 'Profiling as inferred data: amplifier effects and positive feedback loops', in: E. Bayamlioglu, I. Baraliuc, L. Janssens and M. Hildebrandt (eds.) (2018). *Being Profiled: Cogitas ergo Sum*. Amsterdam University Press, pp. 112-115.; Custers, B. (2006). The risks of epidemiological data mining. In Tavani, H. (Ed.), *Ethics, Computing, and Genomics: Moral controversies in computational genomics*. *Jones and Bartlett Publishers Inc*., pp. 153–155.

[11] The right to transparent information (Articles 13 and 14 GDPR) contain similar provisions in Article 13(2)(f) and Article 14(2)(g), respectively.

[12] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', WP251rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018.

[13] E.g., Court of Amsterdam 11 March 2021, ECLI:NL:RBAMS:2021:1019 (*Ola case*), consideration 4.37

argued that, apart from very advanced forms of AI, humans are usually involved at some point in the data processing and decision-making process. A very strict reading of this would mean that Article 22 GDPR is very rarely applicable. This may affect the extent to which Article 15(1)(h) GDPR can be invoked by data subjects. As Article 15(1)(h) GDPR mentions the existence of automated decision-making (rather than decisions "based solely on automated processing"), the threshold is considerably lower here. Regardless of the interpretation of Article 22 GDPR, it can be argued that a right to meaningful information about the logic involved and the significance and consequences for data subjects can also be invoked where decision-making processes are only partially (rather than completely) automated.

These provisions in the GDPR have triggered heavy debate amongst legal experts.[14] Several scholars have interpreted these provisions (chiefly Article 22 GDPR) as a 'right to explanation', arguing that these provisions effectively create a right for data subjects to ask for an explanation of an algorithmic decision that concerned them.[15] Others have argued that these provisions are actually quite limited,[16] concluding that there is no such right to explanation.[17] Finally, some scholars suggested a more contextual interpretation, suggesting that these provisions can actually provide data subjects with more transparency and accountability.[18] The WP29 also seems to take this latter view in its guidelines on profiling and automated decision-making.[19]

There is some debate as to whether any information that needs to be provided by data controllers (under Articles 13, 14, 15 and 22 GDPR) is *ex ante* or *ex post*.[20] Only Article 13 GDPR explicitly states that it applies 'at the time when personal data are obtained', resulting in an *ex ante* right to information. Articles 14, 15 and 22 do not contain such a phrase and it can be argued that these provisions also apply (and can be invoked by data subjects) at later stages. This distinction is important, particularly for Article 15(1)(h) GDPR, as *ex ante* information is concerned with expectations and predictions, whereas *ex post* information can be much more concrete, particularly when it concerns the significance and envisaged consequences for specific data subjects (see below). Since the right of access in Article 15 can be invoked at any time, it is clear it is not a mere *ex ante* right.

3.2. *Meaningful information*

It appears that the alleged right to explanation does not exist, at least not in a single, neat statutory provision, labelled as such.[21] Unfortunately, the whole debate leaves unanswered the types of information that actually constitute 'meaningful information'. The word meaningful is polysemous, it means both 'intended to show the meaning' (i.e., understandable) and 'serious, important, useful' (i.e., significant).[22] It is unclear which meaning the legislator had in mind, or even, perhaps, both.

Selbst and Powles have provided a more detailed qualification of meaningful information,[23] listing four requirements. First, meaningful information should be interpreted in relation to the data subject.[24] In other words, the information about the logic must be meaningful to the data subject, notably a human and presumably without particular technical knowledge. Second, the term meaningful should be interpreted as meaningful (i.e., useful) in relation to specific rights a data subject wants to exercise, such as those provided in Articles 22 and 23 GDPR. Third, meaningful in this sense involves a minimum threshold for exercising these data subject rights. In other words, the information should be meaningful enough to facilitate a data subject in this. Fourth, the term meaningful

[14] Malgieri, G., 'Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations', *Computer law & security review* 2019, 35(5), p.26. https://doi.org/10.1016/j.clsr.2019.05.002 (viewed 13 April 2021).

[15] Goodman, B., and Flaxman, S., 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"', *AI Magazine* 2017, 38(3), pp. 50-57.https://doi.org/10.1609/aimag.v38i3.2741

[16] See for example, Edwards, L., and Veale, M., 'Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for', *Duke L. & Tech. Rev.* 2017, 16, 18. https://ssrn.com/abstract=2972855 (viewed 13 April 2021).

[17] Wachter, S., Mittelstadt, B., and Floridi, L., 'Why a right to explanation of automated decision-making does not exist in the general data protection regulation', *International Data Privacy Law* 2017, 7(2), pp. 76–99. https://academic.oup.com/idpl/article/7/2/76/3860948 (viewed 13 April 2021).

[18] Selbst, A.D., Powles, J., 'Meaningful information and the right to explanation', *International Data Privacy Law* 2018, Vol. 7, No. 4, pp. 233–242, https://doi.org/10.1093/idpl/ipx022 (viewed 13 April 2021).; Malgieri, G., and Comandé, G., 'Why a right to legibility of automated decision-making exists in the general data protection regulation', *International Data Privacy Law* 2017, Vol. 7, No. 4, pp. 243-265. https://academic.oup.com/idpl/articleabstract/7/4/243/4626991?redirectedFrom=fulltext (viewed 13 April 2021).; Kaminski, M., 'The right to explanation, explained. University of Colorado Law Legal Studies Research Paper No 18-24', *Berkeley Technology Law J* 2018, 34. https://ssrn.com/abstract=3196985 or http://dx.doi.org/10.2139/ssrn.3196985 (viewed 13 April 2021).

[19] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', WP251rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018.

[20] Malgieri and Comandé refer to this as 'architecture' and 'implementation' of automated decisions (Malgieri, G., and Comandé, G., 'Why a right to legibility of automated decision-making exists in the general data protection regulation', *International Data Privacy Law* 2017, Vol. 7, No. 4, pp. 243-265. https://academic.oup.com/idpl/articleabstract/7/4/243/4626991?redirectedFrom=fulltext (viewed 13 April 2021).

[21] Selbst, A.D., Powles, J., 'Meaningful information and the right to explanation', *International Data Privacy Law* 2018, Vol. 7, No. 4, pp. 233–242, https://doi.org/10.1093/idpl/ipx022 (viewed 13 April 2021).

[22] Malgieri and Comandé refer to this as 'architecture' and 'implementation' of automated decisions (Malgieri, G., and Comandé, G., 'Why a right to legibility of automated decision-making exists in the general data protection regulation', *International Data Privacy Law* 2017, Vol. 7, No. 4, pp. 243-265. https://academic.oup.com/idpl/articleabstract/7/4/243/4626991?redirectedFrom=fulltext (viewed 13 April 2021).

[23] Selbst, A.D., Powles, J., 'Meaningful information and the right to explanation', *International Data Privacy Law* 2018, Vol. 7, No. 4, pp. 233–242, https://doi.org/10.1093/idpl/ipx022 (viewed 13 April 2021).

[24] Kamarinou, D., Millard, C., Singh, J., and Leenes, R., 'Machine learning with personal data', *Data protection and privacy: the age of intelligent machines* 2017. Hart Publishing.

should be interpreted flexibly. Specific rules may be too rigid and should be avoided. A flexible approach, guided by functional requirements may best effectuate the right of access while preserving competing rights.

This research adopted this approach, not only focusing on the term 'meaningful information', but also on the term 'useful information'. The former is used in the GDPR and is discussed in this section as a legal concept. The latter is not used in the GDPR, but is discussed in Section 4 as a practical concept, i.e., a practical and functional interpretation on how to implement the legal concept of meaningful information.

The term 'useful information' may not exist in the GDPR, but it does exist in national data protection legislation of EU Member States, providing further support for this distinction. The term 'meaningful information' was translated in the German text of the GDPR with the word '*aussagekräftige Informationen*' (rather than '*bedeutungsvolle Informationen*'). The French text of the GDPR uses the term '*informations utiles*' (rather than '*informations signicatives*'). The Dutch version uses the term '*nuttige informatie*' (rather than '*betekenisvolle informatie*'). The Italian text uses '*signicative*', and the Spanish '*signicitiva*'. These formulations invoke notions of utility, reliability, and understandability.[25]

However useful they may be, these qualifications nevertheless do not provide a concrete answer on the types of information that should be provided when data subjects invoke their right of access. The question of what constitutes useful information is examined in Section 4. But first the two elements are discussed to which the concept of meaningful information applies: meaningful information about the logic involved and (meaningful) information about the significance and consequences envisaged.

3.3. *The logic involved*

With respect to meaningful information about the logic involved, it is important to note that data controllers are not required to provide all of the details about the technologies used for automated decision-making or profiling. There is no requirement to provide the data subject with the software used for the analyses, the algorithms used, or an overview of the categories and profiles in which they are placed. Such information may be helpful in understanding the logic involved, but this may also be achieved in other ways, for instance, by providing descriptive information.[26]

Where the software or algorithms are the object of IP rights, a data controller may not want to provide the code of the software involved and indeed this does not seem to be required. This is in line with restriction that the right of access should not adversely affect the rights or freedoms of others, including trade secrets or IP, in particular the copyright protecting the software (Article 15(4) GDPR and Recital 63 GDPR). Code used for analyses of the data is likely to be subject to IP rights, because the data controller either purchased or developed this software.

The fact that no code has to be provided to data subjects does not provide clarity on the information that has to be provided. The answer to this can be found in the term 'meaningful' in Article 15(1)(h) GDPR. The term meaningful must be understood in the context of meaningful for something or someone. The goal of the right of access, as explained above, is empowerment and control of the data subject. In this context, code may not contribute to empowerment and control of the data subject, as most data subjects will be unable to read and understand the code. At the same time, very general information, such as a notification that data mining, machine learning, or AI technologies are being used is not meaningful information either - the fact that such technologies are being used will not help a data subject to determine whether they consent or should consider invoking additional data subject rights, like the right to object to such data processing. On the contrary, a notification that such tools are being used is likely to raise additional questions for data subjects, such as how these tools are applied and their consequences for the data subject themselves.

Meaningful information about the logic involved is therefore more likely to refer to a description of the technologies used than access to the code or software itself. The description should not be too general (i.e. raising more questions than answers), nor should it be too detailed or technical, impeding a clear answer for the average data subject, without a technological background.[27] Obviously, these examples are oversimplified – in practice, most code and algorithms come with certain explanatory documentation.

Different technologies involve different (types of) logic. A key characteristic distinguishing the major technologies in this field is whether or not they are self-learning. Current technology developments, particularly in machine learning and AI, are increasingly directed at this self-learning. Explaining the logic behind the technology is a complicating factor, however. Technologies that are not self-learning can usually be explained in terms of an input-output process, e.g., these are the input characteristics and some of them weigh in more heavily, and the outcome is that a data subject is categorised as low risk. These technologies yield reproducible output, where the same input always results in the same output. This is not the case for self-learning technologies – the exact same input may result in different output at a later time because the technology has learned to assess the input in a different way.

This self-learning aspect (and the related non-reproducibility) complicates the requirement to provide meaningful information about the logic involved. In fact, the logic involved may not be entirely known to the people who developed the technology, because the technology may have

[25] Selbst, A.D., Powles, J., 'Meaningful information and the right to explanation', *International Data Privacy Law* 2018, Vol. 7, No. 4, pp. 233–242, https://doi.org/10.1093/idpl/ipx022 (viewed 13 April 2021).

[26] Compare this with meaningful information given to patients about medicines. Prescribing a painkiller like Iboprofen could be accompanied with the chemical formula, but this is unlikely to be meaningful information for the patient. Instead, the information should contain a description of the purpose of the medicine, how to use it, its limitations, and possible side effects. Arguably, the chemical formula should be available to DPAs. In the context of data protection, the GDPR does not prescribe that DPAs have access to the code used by data controllers.

[27] Where a data subject has a technological background, more detailed information could obviously be provided and still be meaningful. However, the GDPR does not elaborate on this.

evolved after some time. Due to the issues related to humans no longer understanding the technology (such as loss of control over the technology), a lot of research is being done in the field of explainable AI (XAI).[28] The idea is to develop technologies that are not 'black boxes' where even designers cannot explain why the technologies arrived at a specific decision. Rather, the technology should be explainable, i.e., the results and how they were found should be understood by humans. Obviously, it remains to be seen whether this is realistic – the more advanced AI becomes, the harder it may be to explain to humans. Very sophisticated AI may in the future be well beyond any human understanding.[29]

3.4. *Significance and envisaged consequences*

Aside from meaningful information about the logic involved, data subjects also have a right to be informed of the significance and envisaged consequences of automated data processing if they invoke their right of access. The phrasing is not entirely clear, in that Article 15(1)(h) GDPR does not make it clear whether the word 'meaningful' also applies here or only to the logic behind the automated processing. However, given the entire perspective of the list of data subject rights in the GDPR, it can be assumed that the information about significance and consequences should be meaningful for data subjects. It is hard to imagine how information that is not meaningful could contribute to this specific data subject right and the underlying goals of control and empowerment of data subjects.

The phrasing is also ambiguous in that the adjective 'envisaged' clearly only applies to the consequences, not to the significance. It is clear why the legislator used the term envisaged consequences, as not all consequences may be clear beforehand. However, by using 'significance' rather than 'envisaged significance', the legislator suggest that the significance is in fact clear beforehand.[30] This is hard to understand, as the real significance of automated processing and decision-making for data subjects may only become clear after some time.

In a teleological interpretation, with control and empowerment of data subjects as the underlying goal, it could be argued that a data controller should inform a data subject of both the significance and the consequences to the best of their knowledge. That would imply according to current knowledge and assessment of significance and consequences, as well as any envisaged (prospective) knowledge of significance and consequences.

Selbst and Powles suggest two interpretations of the kind of information this entails.[31] The first is that the significance and envisaged consequences involve information about how the results of automated processing are used. Hence, the 'logic involved' would refer to the technology and the 'significance and envisaged consequences' would refer to the effects the technology causes.[32] The second interpretation is that the phrase 'significance and envisaged consequences' further refines the meaningful information. In other words, meaningful information about the logic involved also encompasses the consequences for data subjects.

This distinction is not entirely clear: both interpretations require that the data controller provides information on the consequences. As a result, these two interpretations do not differ much in terms of the information that needs to be provided. The question of the information to be provided in order to properly inform data subjects about the significance and consequences of automated data processing and decision-making remains. Again, it seems to point to providing useful information, i.e., useful for data subjects in enabling them to properly assess whether they want to exercise their data subject rights. This is examined further in Section 4, which hypothesises ways in which information about significance and consequences can be provided.

3.5. *Rights and freedoms of others*

An important restriction of the right of access is mentioned in Article 15(4) GDPR, which states that the rights and freedoms of others shall not be adversely affected. This exemption explicitly refers to Article 15(3) GDPR, on the right to receive a copy of the personal data undergoing processing. Recital 63 further explains this exemption, stating that the rights and freedoms of others include trade secrets or IP, in particular the copyright protecting the software. Note that this can be either software that the data controller bought off the shelf or developed itself. In practice, trade secrets concern trade secrets of the data controller, not trade secrets of other companies. It also states that the result of these considerations should not be a reason for refusing a request to provide all information to the data subjects. In other words, a balance has to be found

[28] Gunning, D., Stefik, M., Choi, J., Miller, T., Stumpf, S., 'XAI- Explainable artificial intelligence', *Science Robotics* 2019, Vol. 4, No. 37.; Samek, W., Montavon, G., Vedaldi, A., Hansen, L.K., Müller, K.R. (2019). *Explainable AI: Interpreting, Explaining and Visualizing Deep Learning*. Heidelberg: Springer.

[29] A description of the logic involved could also include information on the quality and performance of the technology, including its accuracy, data input quality requirements, effective error rates, convergence of the models, algorithm predictability, etc. Most of these technological details will not constitute meaningful information for the average data subject.

[30] One interpretation of this could be that the legislator intended here that a data subject should be informed of the significance of the role of the automated data processing in the whole process of decision-making, but such an interpretation would not be entirely in line with Article 22, which focuses on fully automated decisions. Nor would it be entirely in line with the end of the provision, that focuses on the [significance for] the data subject. In other words, control and empowerment of the data subject are better served by information on the significance of the consequences for the data subject than by information on the significance of the role of automated data processing in the process.

[31] Selbst, A.D., Powles, J., 'Meaningful information and the right to explanation', *International Data Privacy Law* 2018, Vol. 7, No. 4, pp. 233–242, https://doi.org/10.1093/idpl/ipx022 (viewed 13 April 2021).

[32] Malgieri and Comandé refer to this as 'architecture' and 'implementation' of automated decisions (Malgieri, G., and Comandé, G., 'Why a right to legibility of automated decision-making exists in the general data protection regulation', *International Data Privacy Law* 2017, Vol. 7, No. 4, pp. 243-265. https://academic.oup.com/idpl/articleabstract/7/4/243/4626991?redirectedFrom=fulltext (viewed 13 April 2021).

between protecting data controller interests, such as trade secrets and IP rights, and the data subjects' right to know what is processed about them, and in what way. It is not necessary to provide all the details where this is problematic for data controllers, but at least some information should be provided in response to a right of access request. Section 4 investigates that balance by examining actual practices.

4. Empirical analysis

In order to assess actual practices with regard to the right of access, a survey was sent to all countries within the scope of this research (see details in Section 2). The general impression from the survey results is that many countries did not alter or add to the text of Article 15 when implementing the GDPR. Nor did many countries develop specific policies or guidance on automated decisions and profiling, or any case-law. However, there appear to be differences in how the right of access is implemented in practice. With respect to providing meaningful information on the logic, significance and envisaged consequences of automated decision-making and profiling, there are different views on what types of information are (to be) provided. Different views also exist on how to balance the right of access with the rights and freedoms of others, such as IP rights and trade secrets.

This section provides an overview of the findings. Section 4.1 discusses the legal implementation of Article 15 GDPR in national legislation and any further guidance developed on the right of access. Sections 4.2 through 4.6 discuss practical implementation, complaints, information on consequences, algorithms and automated decisions, and IP and trade secrets respectively.

4.1. *Legal implementation and further guidance*

In implementing Article 15 GDPR, most countries have adopted national legislation (usually a national data protection act). Strictly speaking, the GDPR is binding for all citizens in all EU Member States and national legislation implementing the GDPR is therefore not necessary. However, countries with a dualistic approach to international law (where national and international law are considered separate legal systems) are more inclined to implement international law into national law. Respondents of some countries, such as Lithuania, Slovakia and Austria, indicated that no national legislation was adopted to implement the GDPR.[33]

Countries without national implementation of the GDPR directly apply the text of the Regulation. However, for countries that implemented the GDPR through national legislation, there may be differences in the phrasing of the right of access in Article 15 GDPR. Nine countries (Bulgaria, Croatia, Estonia, France, Hungary, Liechtenstein, Luxemburg,[34] Poland, Sweden) indicated that the phrasing of the right of access in the national data protection act is exactly the same as that of the GDPR.

Typically, some countries have made use of the provision in Article 23 GDPR that allows for further restrictions in the scope of data subject rights, including the right of access. Such restrictions are allowed in the areas of national security, defence, public security, criminal law, general public interest, judicial independence, professional secrecy in regulated professions, the protection of data subject rights and the rights and freedoms of others, and the enforcement of civil law claims. Such provisions can be found in legislation in Ireland (Section 60, amongst other provisions of the Irish Data Protection Act 2018), the Netherlands (Article 41 General Data Protection Regulation Implementation Act), Norway (Article 16–17 Norwegian Data Protection Act), Bulgaria (Article 37a Bulgarian Data Protection Act), and Germany (Sections 24(2), 25(2), 26(2) and 32 of the German Federal Data Protection Act).

In Ireland, the Data Protection Act 2018 provides some specific exceptions to exercising data subject rights. Section 43 of the Act states that data processing for journalistic purposes and for the purposes of academic, artistic or literary expression, is exempt from the provisions on data subject rights where compliance would be incompatible with the relevant stated purposes.

In Luxemburg, the 2018 Data Protection Law made use of Article 85 GDPR to derogate from the rules governing the right of access when it comes to processing for the sole purpose of journalism or academic, artistic or literary expression.

Article 13 of the Spanish Data Protection Act sets out more specific provisions. One of the additions is that the right of access shall be considered granted if the data controller provides the data subject with a remote, direct and secure system for accessing their personal data that guarantees permanent access to the entirety of these data. Recital 63 GDPR mentions this possibility, and Spain elevated it from a recital to an actual legal provision.

The GDPR allows for additional legislation, policies or guidelines detailing how Article 15 GDPR should or could be implemented in practice. According to the survey results, no Member State adopted such additional legislation, nor is there any further government guidance or specific policies. Additional policies exist only in France[35] and Poland.[36] In Austria,[37] there are templates for access requests, along with a standard complaint form that people can use where data controllers do

[33] Malta has implemented the GDPR into national law (Chapter 586 of the Laws of Malta), but not Article 15 GDPR specifically.

[34] In Luxemburg, for example, the 2018 Data Protection Law does not introduce further specifications on the right of access, thus Article 15 GDPR is directly applicable.

[35] CNIL. (n.d.). *Le droit d'accès: connaître les données qu'un organisme détient sur vous*. https://www.cnil.fr/fr/le-droit-dacces-connaitre-les-donnees-quun-organisme-detient-sur-vous; CNIL. '*Professionels: comment répondre à une demande de droit d'accès?'*, 2020, https://www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-dacces.

[36] Urzad Ochrony Danych Osobowych, '*Jak Realizować prawa pacjenta do otrzymania kopii danych osobowych oraz kopii dokumentacji medycznej*.', 2018, UODO. https://uodo.gov.pl/pl/138/440.

[37] Republik Österreich Datenschutz behörde. ‚*Antrag auf AUSKUNFT gemäß Art. 15 DSGVO. Request for Access (Article 15 GDPR)*' [Form]. https://www.dsb.gv.at/dam/jcr:b233fd1e-3c44-4559-8502-28dd85cb9897/Antrag_an_den_Verantwortlichen_Recht_auf_Auskunft_Art_15.pdf.

not comply with access requests.[38] Malta makes a template available on the government intranet, which is accessible to government bodies and entities, but not to data subjects.

Further guidance on how to implement the right of access is provided by some Data Protection Authorities (DPAs). Several countries provide additional guidance on data subject rights in general, such as Liechtenstein, Croatia,[39] Malta,[40] Bulgaria and Estonia.[41] Some countries have more specific guidance on Article 15 GDPR, such as Luxemburg,[42] Norway,[43] Germany[44] and Ireland.[45] No countries have specific guidance on Article 15(1)(h) GDPR, on the right of access in relation to automated decision-making and profiling.

The GDPR does not prohibit NGOs, privacy interest groups or others to issue guidelines on how to interpret Article 15 GDPR. With the exception of two countries (Germany and Austria), none of the countries have used this option (confirmed during the interviews). Austria has Codes of Conduct, issued by the Chamber of Commerce,[46] while the German Consumer Authority has issued guidance.[47] Both documents, however, offer rather general guidance, not specifically addressing the right of access or automated-decision-making and profiling.

Other clues as to how the right of access is implemented in practice can perhaps be found in case-law. However, the respondents from most countries were unaware of any case-law on the right of access in Article 15 GDPR. This was also confirmed during the interviews. Case-law on Article 15 GDPR exists in Croatia, Norway, Hungary, and Poland, but focuses on Article 15 GDPR in general, not on Article 15(1)(h) in particular. Only the Netherlands [48] and Germany[49] have (limited) case-law on the right of access in the context of automated decision-making and profiling.

4.2. *Practical implementation*

From a practical perspective, the information that should be provided by a data controller when a data subject invokes the right of access is subject to discussion, including how that information should be provided (e.g., format and level of detail). Survey respondents were asked about the types of information generally provided by data controllers when the processing of personal data involves non-deterministic algorithms or automated decisions. Table 1 shows the seven options given. A relatively large number of respondents ($N = 9$, 43%) did not answer this question and several other respondents only partially answered. The DPAs in these countries either had no information or the information was inconclusive.

Nevertheless, some patterns emerge from the findings in Table 1. For most respondents, it is clear that the right of access clearly involves access to data collected (directly) from the data subject. Similarly, none of the respondents think that invoking the right of access involves obtaining code of the algorithms or other data analytics tools used. The interpretation of the phrase 'meaningful information about the logic involved' thus, according to the survey respondents, does not include code or actual algorithms.

For other types of data, the results are more mixed. Even though Recital 63 GDPR states that, where possible, the data controller should be able to provide remote access to a secure system which would provide data subjects with direct access to their personal data, respondents were strongly divided on the need to provide such login details to data subjects: 60% indicated this should be provided, whereas 40% said there is no need. In Spain, Article 13 of the Spanish Data Protection Act states that if a data subject is provided with such login details, the right of access will be considered granted.

Whether the data that should be provided following an access request should include any data other than those collected (directly) from the data subject is also a matter of some controversy. The majority of the respondents (64%, $n = 11$) felt that data not obtained from the data subject should be provided. The GDPR makes a clear distinction between data collected directly from the data subject and data not obtained from the data subject (Article 13 and 14 GDPR). This reasoning is not followed explicitly in Article 15 GDPR and only a small

[38] Datenschutz behörde. (n.d.). *Dokumente*, https://www.dsb.gv.at/download-links/dokumente.html.

[39] Katulić, T., '*Prava Inspitanika prema Općoj Uredbi O Zaštiti Podataka I Zakonu O Provedbi Opće Uredbe O Zaštiti Podataka*'. Agencija za zaštitu osobnih podataka 2021, https://azop.hr/wp-content/uploads/2021/02/Vodic-prava-ispitanika.pdf.

[40] Information and Data Protection Commissioner. (n.d.). *Data Protection for Individuals*, https://idpc.org.mt/for-individuals/your-rights/.

[41] Andmekaitse Inspektsioon. (2019). *Isikuandmete Töötleja Üldjuhend*. https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf.

[42] Commission Nationale pour la Protection des Données., '*The Right of Access*', 2019,. CNPD https://cnpd.public.lu/en/particuliers/vos-droits/droit-acces.html.

[43] Datatilsynet., '*Rett til Innsyn*', 2018, https://www.datatilsynet.no/rettigheter-og-plikter/den-registrertes-rettigheter/rett-til-innsyn/

[44] In Germany, there are several sources: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf; https://www.bfdi.bund.de/DE/Infothek/Transparenz/AccessforoneAccessforall/2020/2020-Arbeitshilfe-Artikel-15-Jobcenter.pdf?__blob=publicationFile&v=1. Also, there are sources at State level, for instance in the state of Hessen: Ronellenfitsch, M., '*Siebenundvierzigster Tätigkeitsbericht zum Datenschutz und Erster Bericht zur Informationsfreiheit*' 2018, AC medienhaus GmbH. https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2018_47_TB.pdf

[45] An Coimisiún um Chosaint Sonraí. (n.d.). *Your Rights under the GDPR*. https://www.dataprotection.ie/en/individuals/know-your-rights/right-access-information.

[46] WKO, '*EU-Datenschutz-Grundverordnung (DSGVO): Auskunftspflicht des Verantwortlichen: Was bei einem Auskunftsantrag zu tun ist*', 2021, https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Auskunftspflicht-des-Vera.html.

[47] Verbraucherzentrale, '*Ihre Daten, Ihre Rechte: die Datenschutzgrundverordnung (DSGVO)*', 2021, https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/ihre-daten-ihre-rechte-die-datenschutzgrundverordnung-dsgvo-25152.

[48] Rb. Noord-Holland 23 May 2019, ECLI:NL:RBNHO:2019:4283, consideration 4.17.; Rb. Amsterdam 20 June 2019, ECLI:NL:RBAMS:2019:4404, consideration 4.11.; Rb. Amsterdam 20 June 2019, ECLI:NL:RBAMS:2019:4418, consideration 4.11.; HR 17 August 2018, ECLI:NL:HR:2018:1316.; RvS 17 May 2017, ECLI:NL:RVS:2017:1259.

[49] Bundesgerichtshof 28 January 2014, VI ZR 156/13, https://openjur.de/u/677956.html.

Table 1 – Types of information provided in access requests involving automated decisions or profiling.

	Type of information	Yes	No	N
A	Login details like username and password[50]	60%	40%	10
B	Personal data collected from the data subject	100%	0%	12
C	Personal data not obtained from the data subject	64%	36%	11
D	Personal data inferred from other available data	67%	33%	12
E	Categories or profiles in which a data subject is placed by a data controller	58%	42%	12
F	Description of the workings or rationale of algorithms or other data analytics tools used	30%	70%	10
G	Code of the algorithms or other data analytics tools used	0%	100%	10

majority of the respondents interpreted Article 15 GDPR as including both types of data in access requests.

Broadly speaking, the same is true for data inferred from other available data. Before discussing inferred data, it is important to clarify the distinction between data not obtained from the data subject and inferred data. Data not obtained from the data subject are data that are indirectly obtained *from* the data subject, for instance, via a data broker. Inferred data are data obtained *on* the data subject, distilled from other available data. Typically, if a person shares her date of birth with data controller A, for this data controller this is personal data (directly) obtained from the data subject (Article 13 GDPR applies). If a data controller A shares the data with data controller B,[51] for the latter this is personal data not obtained (directly) from the data subject, but indirectly, via data controller A. If a data controller A or B infers from the date of birth the current age of the data subject, then this age is inferred personal data. Note that if the data subject had provided her age to data controller A, it would not have been inferred data. In other words, the way in which data is obtained is decisive in this categorisation, not the type of data itself. Having said that, some types of data can only be inferred and never really be provided by a data subject. Typically, personalised statistics and predictions, such as life expectancies and risks to attract particular diseases, can only be distilled from larger datasets. This is not information that data subjects know about themselves.

The percentage of respondents that think inferred data is actually shared with a data subject after a right of access request (66%) is almost the same as for sharing data not obtained from the data subject (64%). This is remarkable, considering that IP rights and trade secrets are explicitly mentioned exceptions in the GDPR with regard to the right of access. Inferred data almost[52] by definition require a data controller to extract new knowledge from available data.[53] For this knowledge discovery process, data analytics tools may be used. Both the tools for analysis and the resulting knowledge may easily fall within the scope of IP, trade secrets or other rights of the data controller deserving protection. By contrast, data not obtained from the data subject often concerns data in datasets that were bought, hired or leased, which to some extent can be considered property,[54] although not IP. Similarly, data not obtained from the data subject hardly qualifies as a trade secret, since the data controller from which it was obtained already had access to these data and it is likely that many other data controllers also have access. Altogether, it is arguably difficult to invoke an exception like IP or trade secrets to the right of access in the case of data not obtained from the data subject.

Another type of information that could be provided are any categories in which a data subject is placed after data analysis. Many data analysis tools, particularly classification tools,[55] distinguish different categories during analysis and then ascribe data subjects to one of those categories. Typically, age can be any value between 0 and around 100, but people are often categorised as minors versus adults, or as young/middle-aged/old. Similarly, after data analysis, people can be categorised into low-risk and high-risk categories for any area. Data subjects are obviously interested in knowing in which

[50] This refers to credentials for accessing a reserved area to view or download the personal data.

[51] This is allowed, for instance, if the purposes are compatible or if the data subject has consented. Ursic, H. and Custers, B.H.M., 'Legal barriers and enablers to big data reuse - a critical assessment of the challenges for the EU law', *European Data Protection Law Review* 2016, Vol. 2, No. 2, pp. 209-221.

[52] Almost, because it may be the case that the extracted knowledge is trivial or at least not novel or unexpected.

[53] Custers, B.H.M., 'Profiling as inferred data: amplifier effects and positive feedback loops', in: E. Bayamlioglu, I. Baraliuc, L. Janssens and M. Hildebrandt (eds.) (2018). *Being Profiled: Cogitas ergo Sum*. Amsterdam University Press, pp. 112-115.

[54] It could be argued that a data controller has a right to process personal data after the data subject consented, or any other legal basis for data processing exists (Article 6 GDPR).

[55] Calders, T. and Custers, B.H.M. (2013). What is data mining and how does it work? In: Custers, B.H.M., Calders, T., Schermer, B.W., Zarsky, T.Z. (red.), *Discrimination and Privacy in the Information Society* (nr. 3). Heidelberg: Springer.

categories they are placed by a data controller, something that is arguably much more important to them then obtaining access to their date-of-birth, address and other data they have themselves previously provided to a data controller. The categories in which people are placed are important to assess their reputation from a data controller's perspective.[56] The importance for data subjects lies in the fact that such information better enables them to assess whether or not they agree with the data processing or perhaps want to object.

In total, 58% of the survey respondents indicated that information on the categories in which data subjects are placed is provided upon an access request. Again, this is remarkable, as it could easily be argued that such information is covered by IP rights or trade secrets. Categorisations, particularly when dealing with credit scores, willingness to pay, payment default risks, customer margins and other economic aspects of individuals, may be highly sensitive information from an economic perspective. In markets with razor-thin margins, this kind of information may well be the competitive edge of companies.

When asked whether a description of the workings or rationale of algorithms or other data analytics tools that are used is provided upon access requests, the majority of the respondents (70%) indicated that this is not the case. The survey question explicitly mentions the context of automated decisions, which means Article 15(1)(h) GDPR applies. This provision prescribes that meaningful information about the logic involved should be provided. This is not optional, but mandatory. However, it seems that this obligation is not routinely complied with.

The final type of information mentioned in the survey was the actual code of the algorithms or other data analytics tools used. None of the respondents indicated that such information is provided when data subjects invoke their right of access. This is perhaps unsurprising, as the GDPR does not prescribe that such information should be provided. In fact, it is often covered by the exception of IP or trade secrets. At the same time, such information may not be very instructive for the average data subject as it may be highly technical and/or complex information, which means that providing such information would be unlikely to meet the criterion of 'meaningful information' in Article 15(1)(h) GDPR.

Apart from the question of actual observable practices (see Section 5.2 for approach limitations), respondents were also asked which of the types of information in Table 1 they consider essential to meet the criterion of 'meaningful information'. This question focuses on what data controllers *should* do rather than on what they are actually doing. A total of five respondents (24%) did not complete this question. This is considerably lower than the previous question, which seems to imply the respondents were more confident answering this question. 44% of the respondents indicated that an account or login details are required, while 88% considered data collected from the data subject essential. For data not obtained from the data subject and inferred data, 81% considered this information essential. The categories in which a data subject is placed is essential, according to 88% of respondents. A description of the workings or rationale of algorithms or other data analytics tools used is essential, according to 69% of the respondents. Only 6% considered the code essential information. The interview results show similar findings: the experts interviewed also considered types B through F important, were mixed about type A, and thought type G non-essential or irrelevant.

There are some clear distinctions between the percentages that describe actual practices and what is regarded as necessary. For the types of information B through F, respondents seem to indicate that such information should be provided more (or perhaps more often) than is currently the case. For the code (type G), respondents agreed that this information does not need to be provided, which is in line with actual practices. For an account or login details, less than half of the respondents believed this is needed, more or less in line with actual practices. The interviews confirmed the gap between what is needed and actual practices for types B through F.

It is interesting to compare these findings with the legal requirements. Type A (an account or login credentials to directly access the personal data) is not mandatory from a legal perspective,[57] although encouraged by the GDPR. This freedom of choice understandably results in a diverse landscape, both in terms of actual implementation and in opinions of DPAs on the need for this. More difficult to understand is that type B (data obtained from the data subject) was not ticked by all respondents. This is the least controversial type of information to be provided during an access request. If the right of access does not cover this type of information, then what does it cover? Types D and E (inferred data and categorisations) are more controversial, as they could be covered by the IP or trade secrets exception. In this light, the percentages of respondents considering this information essential were perhaps quite high. By contrast, type C (data not obtained from the data subject) is much less likely to be covered by these exceptions. As such, the percentage of respondents who considered this essential information during access requests is relatively low. The same applies to type F (the workings or rationale of the tools for analysis). This is a clear legal requirement, but not all respondents indicated that this is essential. It is not clear why some respondents overlooked the connection with Article 15(1)(h) GDPR. During the interviews, the experts stressed the importance of data subjects understanding what is happening with their data, but did not focus on the workings or rationale of algorithms or other data analytics tools used. In other words, the experts did not focus on the specific phrasing of Article 15(1)(h) GDPR, but rather on transparency in a more general way, without qualifying how such transparency should be implemented in practice. Type G (code) shows understandable results: this is not a legal requirement and respondents generally agreed.

[56] Solove, D.J. (2007). *The Future of Reputation: Gossip, rumor, and privacy on the Internet*. Yale University Press.

[57] In Spain, Article 13 of the Spanish Data Protection Act states that if a data subject is provided with such login details, the right of access will be considered granted.

4.3. Complaints

If data subjects invoke their right of access, it is towards a data controller. If the data controller does not comply, data subjects can turn to the national DPA. All DPAs were asked about the numbers and nature of complaints regarding Article 15 GDPR, particularly Article 15(1)(h) GDPR. Although DPAs register and keep track of all complaints, many DPAs (48%, $n = 21$) had no specified statistics on complaints relating to the right of access.[58] However, many others (52%, $n = 21$) had such statistics.[59] Liechtenstein keeps track, but indicated that there were no complaints regarding (non-compliance with) the right of access. Most of the relevant complaints related to delayed or no response from the data controller (procedural non-compliance) or to the contents of the information received (substantive non-compliance).

Of the countries with statistics on Article 15 GDPR-related complaints, only two DPAs mentioned complaints that related to Article 15(1)(h) GDPR (i.e., automated decision-making or profiling). In Malta, one complaint was related to the right of access related to automated decision-making. This case dated from before the introduction of the GDPR (in 2018). No further details were provided. In Spain, one complaint was related to this.[60]

The DPAs were also asked whether data controllers invoke IP rights or trade secrets when data subjects complain about the right of access. Six DPAs (29%) had no information,[61] while four (19%) indicated that this was not the case in the complaints they received.[62] This does not include Liechtenstein, where there were no complaints regarding Article 15 GDPR. Hence, in this one country (5%) the data were inconclusive. Ten DPAs (48%) indicated that data controllers invoke IP rights or trade secrets in these situations.[63] The survey did not ask about frequency, however. In Bulgaria, invoking IP rights or trade secrets is rare. In Germany, this occurs occasionally in Lower Saxony. In Germany, data controllers generally do not invoke IP or trade secrets, except where the algorithm or details of the scoring calculation are affected. In such cases, data controllers usually invoke trade secrets, but not IP rights. In France, the French SA (CNIL) noted that trade secrets are sometimes invoked by data controllers without further explanation justifying how access to the requested data would infringe these trade secrets. As Recital 63 GDPR states that these considerations should not lead to a refusal to provide information to the data subject, the CNIL takes the position that when a data controller decides not to comply with a request for access, it must give reasons for that refusal.

Table 2 – Types of information regarding the consequences for data subjects.

	Type of information	Yes	No	N
A	Are pros and cons listed?	12%	88%	8
B	Are scenarios presented?	22%	78%	9
C	Is significance quantified?	25%	75%	8
D	Are significance and consequences personalised?	50%	50%	8

4.4. Information on consequences

According to Article 15(1)(h) GDPR, data controllers using automated decision-making or profiling should also provide information on the consequences for data subjects when they invoke their right of access. More specifically, information should be provided on the 'significance and envisaged consequences' of this processing. As this can be interpreted in many different ways, the survey suggested some types of information that could be provided and asked respondents about the types of information actually observed in practice (see Table 2).[64] Again, a large number of respondents (57%, $n = 21$) did not complete this question and one respondent only partially completed this question. Many respondents who did not complete the question did not understand the question, did not have any data, or the answer depended on the individual case.

Table 2 shows the majority of respondents (and interviews) stating that most types of information suggested are generally not provided. This is remarkable, as there is a legal obligation to provide information on the 'significance and the envisaged consequences' of the automated decision-making or profiling. Type A (pros and cons) is perhaps the most uncontroversial, but even this type of information is rarely provided in practice. Pros and cons are arguably the minimum information that needs to be provided when discussing consequences for data subjects. Type B is perhaps more controversial, as the GDPR does not explicitly or implicitly mention that scenarios need to be provided. Scenarios could be helpful to inform data subjects about consequences, but are not mandatory. Perhaps, some respondents see data controllers providing scenarios of what could happen as a result of the automated decision-making or profiling.

[58] Austria, Bulgaria, Croatia, Estonia, France, Germany, Hungary, Latvia, the Netherlands, Slovakia and Norway.

[59] Czechia, Ireland, Italy, Malta, Lithuania, Luxemburg, Poland, Spain, Sweden and Liechtenstein.

[60] TD-00157-2020. Resolucion No. R.00623.2020 Vista la reclamación formulado el 15 de mayo de 2020 ante esta Agencia por D.A.A.A., contra Caixabank Payments. The complainant lodged a complaint because he was refused a credit card, requested access to the data, and considered the answer by the financial entity incomplete. The Spanish DPA decision agreed with the complainant and held that he was not provided with information about the logic behind the automated decision-making or that there was an automated system making the decision. The AEPD (the Spanish SA) ordered the bank to give a complete answer. The complainant later lodged complaints against the same financial entity, but on another topic, https://www.aepd.es/es/documento/reposicion-ps-00477-2019.pdf

[61] Austria, Croatia, Hungary, the Netherlands, Sweden and Norway.

[62] Czechia, Ireland, Poland, Spain.

[63] Bulgaria, Estonia, France, Germany, Hungary, Italy, Latvia, Lithuania, Luxemburg, Malta.

[64] These types of information were suggested by the authors.

Although risks for data subjects may be hard to quantify, the word 'significance' in respect of the consequences seems to imply something of a quantification (or at least a further qualification) of these risks. At the very least, it goes beyond a mere description of the nature of the envisaged consequences. However, only two of the eight respondents observed that data controllers provide such quantification or further qualification. During the interviews, none of the experts indicated that any such information is routinely provided. Failing to provide such information could arguably be considered non-compliance.

Whether the size and nature of any consequences should be personalised is another subject of discussion. As automated decision-making and profiling often focus on personalised data analytics, it could easily be argued that the consequences of these types of data processing are not necessarily the same for each data subject. On the contrary, consequences may vary significantly on the basis of the amount of data available on a particular data subject, the nature of these data (for instance, sensitive data), and what the data show (e.g., belonging to a majority or minority group). With different consequences for each data subject, a personalised description of the consequences makes more sense. In fact, a non-personalised description of the consequences might not be considered meaningful information.

In the context of personalised consequences, it may be important to consider proportionality: how easy or difficult is it for data controllers to provide personalised information on consequences? On the one hand, it could be argued that this is rather straightforward for a data controller in the business of analysing personal data and making personalised predictions. On the other hand, these business-related data analytics and predictions may be more focused on the organisational goals of a data controller than on this specific GDPR requirement, which requires different kinds of information to be generated. If so, it may actually be (much) more complicated for data controllers to personalise the consequences of the automated decision-making and profiling for each data subject. When this is time-consuming or costly, it may be argued that it is unreasonable to expect personalised information on consequences. The proportionality principle could be useful in assessing reasonableness in this respect (see Section 5.1).

4.5. *Algorithms and automated decisions*

The survey asked about policy documents and further guidance in order to establish the degree of thought behind algorithms and automated decisions in each country. However, most countries (81%) indicated that no such documents exist. In the Netherlands, however, the DPA is developing guidance aimed at algorithms, automated decisions, and profiling, but this was not yet published during this research. In Estonia, France, Germany, and Luxembourg, there is further guidance, although it does not specifically focus on the right of access.

The survey also asked about any documents detailing different types or categories of data in respect of the right of access. Such typologies might be useful in further refining the typologies in Tables 1 and 2. None of the respondents was aware of any such documentation, however. Only the Croatian DPA provided a document, but this guidance (how to draft a privacy policy) was not focused on the right of access.[65]

4.6. *IP and trade secrets*

The final part of the survey focused on how to balance the right of access with IP and trade secrets. Respondents were asked about national legislation on IP rights and trade secrets, particularly in relation to algorithms and automated decision-making.

None of the respondents was aware of any provisions in IP law addressing Article 15 GDPR or the right of access to personal data in the scope of automated decisions and profiling. The most relevant EU legislation is perhaps EU Directive 2016/943 on the protection of undisclosed know-how and business information (the Trade Secrets Directive),[66] but this Directive does not specifically address algorithms, AI or automated decisions. EU IP legislation is in flux, as the EU is preparing new legislation. Currently, Directive 2019/790 on copyright and related rights in the Digital Single Market, which amends Directives 96/9/EC and 2001/29/EC, is under public consultation.[67] However, this new legislative proposal does not specifically address algorithms, AI, or automated decision-making.

In some countries, national legislation on IP contains provisions that are relevant for the right of access. In Hungary, trade secrets have absolute protection.[68] This is relevant when balancing interests: the right of access is a relative right, so absolute protection of IP rights then is decisive and prevailing. Pricing is considered a trade secret. Pricing and prices can be an important aspect of automated decisions and profiling, as many consumers can be affected by online price discrimination,[69] but trade secrets may prevent them from gaining insight into how this works and affects them.[70] In several countries, such as Germany and Malta, respondents explicitly men-

[65] Awareness raising campaign for SMEs. (n.d.). *Vodič-kako izraditi politiku privatnosti?* ARC. https://arc-rec-project.eu/wp-content/uploads/2021/01/Kako-napraviti-politiku-privatnosti.pdf.

[66] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance), OJ L 157, 15.6.2016, p. 1–18, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943 (viewed 19 July 2021).

[67] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, (Text with EEA relevance), OJ L 130, 17.5.2019, p. 92-125, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0790 (viewed 19 July 2021).

[68] See Article 2:47 of the Hungarian Civil Code.

[69] Different definitions of online price discrimination exist in literature, but here we consider online price discrimination as the practice to charge customers different prices for products or services, even though the costs are the same, based on their willingness to pay for it. The willingness to pay is inferred from available data and can be assessed either at individual or group level.

[70] Townley, C., Morrison, E. and Yeung, K., 'Big Data and personalised price discrimination in EU competition law', *Yearbook of European Law* 2017, Vol. 36, p.2.; Shiller, B., 'Personalised price discrimination using Big Data', *Working Paper Brandeis University* 2016, pp. 1-38.; Zuiderveen Borgesius, F.J. and Poort, J., 'Online price discrimi-

tioned a broad interpretation of rights and freedoms of others in this context. Academic research in this area similarly concludes that IP and trade secrets prevail over data protection rights.[71]

The text of Article 15(4) GDPR explicitly mentions 'the rights and freedoms of others'. These others can be data controllers that wish to protect IP or trade secrets, but some respondents noted that these others can also be other data subjects. This is relevant when personal data relate to more than one natural person. Typically, DNA data may contain information not only relating to the data subject requesting access, but also to her family members. The same may apply in respect of genetic diseases. In the context of automated decisions and profiling, this may be even more relevant as these practices need large amounts of personal data as input before they can yield conclusions and decisions. In other words, processing the personal data of others is always required for this, which means there is a low threshold to invoke the exception of Article 15(4) GDPR.

When asked how to balance the right of access with the rights and freedoms of others, respondents in Bulgaria, Latvia and Malta indicated that this is always done on a case-by-case basis. Other respondents (Austria, Germany, Poland) noted that the principles of proportionality and necessity should be used to balance competing interests.

5. Conclusions

5.1. *Answers to the research questions*

The goal of this research was to gain more insight into the right of access (empowering data subjects, strengthening their rights) when data processing involves algorithms or automated decisions. This is protected in Article 15(1)(h) GDPR, which states that data subjects have a right to know 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**, as well as the **significance and the envisaged consequences** of such processing for the data subject'. Three related research questions were developed and are answered below, in light of the findings.

1) How can 'meaningful information' potentially be defined under Article 15 of the GDPR?

Based on the debate on a 'right to explanation', a contextual interpretation of the term 'meaningful information' makes most sense. This implies that information provided under right of access requests should be meaningful for data subjects in order to enable them to exercise their (other) data subject rights. It should provide data subjects with more transparency and accountability. In other words, 'meaningful information' should have practical value for data subjects. This research took an empirical approach to assess such practical value. To distinguish the legal analysis from the empirical analysis, the research focused not only on the term 'meaningful information', but also on the term 'useful information' (see research question 2, below). 'Meaningful information' is used in the GDPR and was discussed as a legal concept. 'Useful information', while not used in the GDPR, exists in the national data protection legislation of several EU Member States and was discussed as a practical concept (i.e., a practical and functional interpretation of implementing the legal concept of meaningful information).

From a substantive perspective, the term 'meaningful information' includes: (i) information about the logic involved; and (ii) information about the impact and consequences. Information about impact and consequences is primarily relevant for data subjects in respect of *whether* they want to invoke their data subject rights (for instance, invoke their rights because they are concerned about the consequences), while information about the logic involved relates to *how* they want to invoke those rights (for instance, choosing between having the data erased on the basis of Article 17 GDPR, switch to another data controller using the right to data portability in Article 14 GDPR, or object to the processing on the basis of Article 21 GDPR).

From a formal perspective, 'meaningful information' should be understandable for data subjects (i.e., no code or algorithms that the average user is unlikely to understand) and should provide insight without causing confusion or raising more questions than it answers (i.e., no details on purchased software or overly broad categories of technologies). The requirement of clear and understandable language stands as the basis of all data subject rights in the GDPR (Article 12(7) GDPR).

2) When is the information provided useful for data subjects?

The goal of the right of access is to empower data subjects and to strengthen their rights. Therefore, the information provided is useful when it contributes to achieving these goals. For each piece of information provided, the decisive criterion could be whether it contributes to the position of a data subject that wants to exercise her rights. The information should allow a common user to make rational decisions about exercising other data subject rights regarding data processing, including the decision to file a complaint at the data controller or DPA, or to go to court.

Most of the types of information assessed in the survey contribute to this understanding. Creating an account, with login details and a password, where data subjects can directly access their own personal data certainly contributes to this. Spain incorporated this option in its data protection legislation, but this is less common in other countries. The GDPR encourages this practice, but without much effect, suggesting that DPAs might consider further encouragement in this respect.

From a substantive perspective, providing information the data subjects themselves previously provided to the data controller is covered by the right of access, but may not be very informative. Far more informative for data subjects is the other data obtained on them indirectly (e.g., from other data con-

nation and EU data privacy law', *Journal of Consumer Policy* 2017, Vol. 40, pp. 347-366.

[71] Malgieri, G., 'Trade secrets v personal data: a possible solution for balancing rights', *International Data Privacy Law* 2016, Vol. 6, No. 2, pp. 102-116.

trollers), data inferred, and any categories in which they were subsequently placed. These are the kinds of information that are useful (and necessary) for data subjects to make adequate decisions about whether they agree to these kinds of processing of their personal data. Code or algorithms, by contrast, do not significantly contribute to this utility.

Data subjects also have a right to more detailed information on the consequences of data processing, particularly when automated decisions and profiling are involved. At a minimum, data subjects should be informed about the pros and cons of this. But beyond this, it makes sense to outline potential scenarios and quantify risks (even if in broad categories, such as low, medium, or high risk). Given that risks may not be the same for each data subject, it also makes sense to provide such information in personalised ways. In practice, however, this information on the significance and envisaged consequences of data processing is rarely – if ever – provided.

Again, from a formal perspective, information is only useful if it is understandable and provides insight without causing confusion, in line with the Article 12(7) GDPR requirement of clear and understandable language.

3) Which competing interests, like intellectual property and trade secrets, are relevant in this matter and how can they be balanced?

Recital 63 GDPR lists examples of competing interests, namely IP and trade secrets. Member States can opt to lay down further exceptions to the right of access in national law for items listed in Article 23 GDPR. These items typically include personal data related to defence, public security, lawyers, the judiciary, or criminal investigations. Several countries have used this provision to implement exceptions to the right of access. Some countries have implemented further restrictions relating to journalism (Ireland, Italy, Poland), public sector information (Poland, Spain), and literature, arts and academic texts (Ireland, Poland). Competing interests (phrased as 'rights and freedoms of others' in Article 15(4) GDPR) thus go well beyond IP and trade secrets in many countries.

Altogether, the 'rights and freedoms' of others are broadly interpreted in literature (prevalence of trade secrets over data protection),[72] in national legislation (many exceptions implemented, even beyond those in Article 23 GDPR), and in actual practice (DPA interpretations in the survey). As a result, when balancing the right of access with competing interests, the findings suggest that much depends on the willingness of data controllers to cooperate. In practice, data controllers may invoke trade secrets and other interests to deny full or partial right of access to data subjects, although this should not result in a refusal to provide information.[73] They have a legal basis to do this, and indeed the survey results show that data controllers actually do invoke trade secrets in these cases, for instance, in France and Germany. There appears to be little willingness amongst data controllers to provide extensive information in right of access requests.[74] This seems to be not entirely in line with Recital 63 GDPR, which states that the result of those considerations should not be a refusal to provide all information to the data subject.

To better reconcile these competing interests, data controllers could consider addressing access requests on a more personalised basis. Depending on the situation (e.g., characteristics of the data subject, the data, the access request), an assessment could be made of the information that should be provided. A tailored approach could be helpful in providing maximum access without interfering with the rights of other data subjects or IP, and without revealing trade secrets.

DPAs may provide decisions on a case-by-case basis, but are also in a position to develop policies, opinions and guidance in this area. The same is true of governments and privacy organisations. As general guidance, the principles of proportionality and necessity could be used to balance competing interests, as suggested by respondents from Austria, Germany, and Poland. Another way of simplifying this balance is to consider trade secrets 'business privacy'.[75] This would mean that privacy of the company and privacy of the data subject have to be balanced, which are perhaps more comparable than the right of access versus rights and freedoms of others. When comparing privacy of the company with privacy of the data subject, this could be done in a qualitative way, in which at least the language used could be relatively similar and the interests comparable to some extent. It could provide data protection authorities or courts with a clearer picture of the interests that need to be balanced. Comparisons in a more qualitative way may be a stretch, though: even though there is research on quantifying privacy,[76] for instance, based on entropy,[77] it is doubtful whether a quantitative approach would ever work, as a quantitative approach may not enable sufficiently taking into account the interests of the different stakeholders.

5.2. *Limitations of this research*

This research focused on the practical implementation of the right of access, particularly in the context of automated decisions and profiling. Actual practices were identified, together

[72] Ibid.

[73] DPAs could have access to trade secrets to assess GDPR compliance, but the GDPR does not provide specific obligations in this respect, only a general obligation for data controllers to comply with DPAs.

[74] The research findings may be somewhat biased here, as the focus was on contested situations (case-law and cases witnessed by DPAs and privacy organisations). It was not possible to make a comparison with uncontested situations.

[75] Malgieri, G., 'Trade secrets v personal data: a possible solution for balancing rights', *International Data Privacy Law* 2016, Vol. 6, No. 2, pp. 102-116.

[76] Rafiei, M., van der Aalst, W.M.P. (2021, March 31) Towards Quantifying Privacy in Process Mining. In: Leemans, S., Leopold, H. (eds) Process Mining Workshops. ICPM 2020. Lecture Notes in Business Information Processing, vol 406. Heidelberg: Springer. https://doi.org/10.1007/978-3-030-72693-5_29.

[77] Alfalayleh, M., and Brankovic, L. (2014, October). Quantifying privacy: A novel entropy-based measure of disclosure risk. In *International Workshop on Combinatorial Algorithms* (pp. 24-36). Heidelberg: Springer.

with possibilities for further improvement. The approach was based on literature research, a survey and interviews. This section discusses some shortcomings of this approach.

The first limitation is the amount of relevant literature available. This is inevitably an issue in new research areas. Here, the dearth of literature confirms that the topic has not been given a lot of consideration in either academia or practice. However, it also made it difficult to assess the existence of any general consensus on particular issues, such as the types of information that need to be provided upon access requests. Further research and policy development is therefore needed.

The second limitation relates to the survey of DPAs. While the survey results are valuable sources and may have the best available overview of actual practices, it is also likely that they have a biased view - if data controllers do not comply (fully or partially) with right of access requests, DPAs may never know about a case of non-compliance unless the data subject files a complaint. It is reasonable to assume that many data subjects abandon their request when a data controller refuses cooperation; in such cases they are unlikely to notify the DPA. When a data controller provides part of the information, it may also be hard for a data subject to assess if other parts of information are still missing, again making it unlikely that DPAs will be informed. As a result, even though the perspective of DPAs is very informative, it is may not provide the full picture.

The survey was addressed to 30 DPAs, 21 of which responded. These are relatively small numbers, casting doubt on the survey's representativeness of trends across the EU. Several DPAs did not fully complete the survey, further reducing the numbers. While the survey provided sufficient information to answer the research questions, it was not used to distil any trends from these results.

The survey results clearly show a snapshot rather than a comprehensive picture. No information was obtained on how future developments. Trends over time were not investigated. The survey was distributed amongst national DPAs and completed by people who are experts in data protection law, but not necessarily in IP law and trade secrets, making those questions more difficult for them to answer. This may be confirmed by some respondents choosing not to answer the questions on these topics, or noting that they were unable to provide those answers.

A third limitation is related to the interviews. Although the interviews provided valuable qualitative information, seven interviews is a small number. Representatives of privacy organisations were contacted in order to give insight in the right of access from a data subject perspective. However, this raises the question of the extent to which privacy organisations experts represent the average data subject. Much like DPAs were merely a proxy for actual business practices, so too were privacy organisations a proxy for data subjects. Nevertheless, the DPAs and privacy organisations are best placed to indicate what is needed (compared to current practices) than data controllers and data subjects themselves. The findings of the interviews were largely in line with the findings of the survey, suggesting that some level of saturation was achieved and that additional interviews with experts at privacy organisations would be unlikely to yield additional information.

5.3. *The way forward*

Given that the goal of the right of access is to empower data subjects and to strengthen their rights, it can be argued that this goal is not achieved very well. Data subjects meet a lot of barriers when invoking their right of access. Literature shows there are several cognitive barriers (such as awareness of their rights and how to invoke them, understanding the information that is provided, and knowing which information is missing if the information provided is limited).[78] Our findings also show legal barriers, such as limited guidance on what information should be provided and opposition from data controllers that provide only partial or limited access or no access at all. Our research clearly shows that, in case of automated decision-making and profiling, access to many types of information is not provided in practice and that any information on the consequences for data subjects is rarely or never provided.

In essence, these practices are not in compliance with the actual provisions in the GDPR, both from a substantive perspective (Article 15 GDPR putting forward on the right of access, most notably Article 15(1)(h) GDPR) and from a formal perspective (Article 12(7) GDPR putting forward the requirement of clear and understandable language). Information that is provided when data subjects invoke their right of access mostly focuses on personal data they already know, rather than on novel information, such as inferred data or categories in which they are placed via profiling or automated decisions. However, these novel, enriched types of data are much more relevant for data subjects, as they entail more severe consequences.[79] On the basis of these observations, we conclude that the right of access, particularly Article 15(1)(h) GDPR, does not function adequately in practice.

A comply-or-explain approach could work here: if a data controller is unable or unwilling to provide particular (parts of) information upon access requests, the data controller should at least explain in some detail for which reasons (e.g., trade secrets, intellectual property, privacy of others) and substantiate why providing such information would be problematic. Also, if no information or only partial information is provided, the data controller should indicate which information is withheld, so that data subjects have a clearer understanding of what is available even though no actual access is provided. Arguably data subjects already have these rights under Articles 12 through 14 GDPR that regulate the right to information.

[78] See, for instance, Eurobarometer Survey 359 (2011) Attitudes on Data Protection and Electronic Identity in the European Union. Brussels; Dutton, W.H., and G. Blank. (2013) Cultures of the Internet; The Internet in Britain, Oxford Internet Survey 2013. http://oxis.oii.ox.ac.uk/reports.

[79] For instance, very sensitive data that people prefer not to disclose can be inferred, see Kosinski, M., Stillwell, D. and Graepel, T., 'Private traits and attributes are predictable from digital records of human behavior', *Proceedings of the National Academy of Sciences* 2013, 110(15): 5802-5805.; Custers, B.H.M., 'Predicting Data that People Refuse to Disclose; How Data Mining Predictions Challenge Informational Self-Determination', *Privacy Observatory Magazine* 2012, Issue 3. www.privacyobservatory.org/.

Looking at our finding that information on consequences for data subjects is rarely or never provided, makes one wonder whether data controllers sufficiently assess consequences for data subjects. Although the GDPR prescribes mandatory data protection impact assessments in many situations (Article 35 GDPR), there still seems a lack of awareness amongst data controllers when it comes to the consequences of data processing for data subjects. Article 15(1)(h) GDPR is clear about the requirement that information on the consequences should be provided to data subjects in cases of automated decision-making or profiling. Data protection authorities could raise more awareness about this requirement, provide further guidance, and enforce this more strongly.

In line with this, more focus on how the information is provided could also be helpful. Transparency, the right to information and the right of access are not merely about which information is provided, but also in which way such information is provided. Article 12(7) GDPR puts forward a very clear requirement that such information needs to be provided in clear and understandable language. This requirement is often not met, so also here more awareness amongst data controllers, further guidance, and stronger enforcement could be helpful.[80] Asking data controllers for feedback on whether they understand the information provided could be an obvious and concrete first step to achieve this.

Declaration of Competing Interest

For this paper, there are no conflicts of interests to report.

Data availability

The data that has been used is confidential.

[80] The Information Commissioner's Office (ICO), the UK Data Protection Authority, has issued guidelines on how decisions made with AI should be explained, see https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-artificial-intelligence/. Such guidelines can be considered as an example of providing more clarity for data controllers about what is needed.