Przegląd Prawniczy Uniwersytetu im. Adam Mickiewicza | Adam Mickiewicz University Law Review

Vol. 15, 2023
DOI 10.14746/ppuam.2023.15.09

Dominika Kuźnicka-Błaszkowska[1]

The data subject's right to access to information under GDPR and the right of the data controller to protect its know-how

Abstract: The data subject's right to access information on data processing has a very broad meaning. Considering the latest developments in this field (mainly the CJEU ruling on Austrian posts and EDPB guidelines) one can draw the conclusion that the controller's right to protect its confidential information is limited and less valuable than the data subject's rights. However, this may lead to unfair and unequal treatment of companies and data subjects. When looking at this right in a more systematic perspective, it seems that the model of the protection of personal data may go hand in hand with the controllers' business interests. A different interpretation may lead to the discouragement of entrepreneurs, both EU and foreign, from conducting business in the European Union. This is not conducive to the development of the European market and certainly will not attract foreign capital.

Keywords: data access, know-how, confidential information, personal data, GDPR.

Introduction

The main goal of data access right is to ensure that a data subject is aware of whether and how their personal data is processed. This will further allow them to exercise

1 Dominika Kuźnicka-Błaszkowska, Georgia Institute of Technology, School of Public Policy, United States. e-mail: dblaszkowska3@gatech.edu.pl, https://orcid.org/0000-0001-8804-569X.

other rights under the General Data Protection Regulation[2] and the data subject will remain in full control of processing their personal data. Unfortunately, the right to access may conflict with the controller's right to protect confidential information. Considering the latest developments in this field (mainly the CJEU ruling on Austrian posts and EDPB guidelines) one can draw the conclusion that the controller's right to protect its confidential information is limited and less valuable than the data subject's rights. This however may lead to unfair and unequal treatment of companies and data subjects. Further developments in this area, such as the Data Act as well as whistle-blower directive, consequently weaken entrepreneurs' and companies' rights to protect their confidential information. As a consequence, this may lead to discouragement of entrepreneurs, both EU and foreign, from conducting business in the European Union. This is not conducive to the development of the European market and certainly does not attract foreign capital.

The scope of data access right

The right of access to personal data is one of the basic rights of the data subject regulated on the basis of Chapter III of the GDPR. This right was expressly stated already in Directive 95/46 EC,[3] and can also be derived from Art. 8 of the European Convention on Human Rights.[4] This right serves the purpose of guaranteeing the protection of the data subjects' right to privacy and data protection with regard to the processing of data relating to them.[5] The right to data

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

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

4 European Convention on Human Rights, see also judgment of ECtHR of 26 March 1987, *Leander v. Sweden*, 9248/81; judgment of ECtHR of 23 January 1986, *Gaskin v. United Kingdom*, 10454/86; judgment of ECtHR of 28 April 2009, *K.H. and Others v. Slovakia*, 32881/04; judgment of ECtHR of 6 June 2006, *Segerstedt-Wiberg and Others v. Sweden*, 62332/00.

5 See also judgment of CJEU of 20 December 2017, *Nowak v. Data Protection Commissioner*, C-434/16.

access is essential in ensuring that the data subject has control over their data and to exercise their other rights. Without having full knowledge of who processes their data and how, an individual will not be able to identify entities towards which they may exercise further rights. Article 15 of the GDPR governs the rights of data subjects, exercisable against data controllers, to access personal data concerning them which are being processed, as well as a range of information relating, in particular, to the processing of such data.[6]

The exercise of the right of access is realised both in the framework of data protection law, in accordance with the objectives of data protection law, and more specifically, in the framework of 'fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data', as provided by Art. 1(2) GDPR. The right of access is an important element of the whole system.[7] The right of access may facilitate the exercise of the rights flowing from, for example, Art. 16 to 19, 21 to 22 and 82 GDPR. However, the exercise of the right of access is an individual's right and is not conditional upon the exercise of these other rights and the exercise of the other rights does not depend on the exercise of the right of access.[8] The data subject does not have to demonstrate the existence of a legal or factual interest;[9] neither the type of data processed not the form of processing affect the effectiveness of this right.[10] This right can be executed at any time, even if the data is already archived.[11] This does not apply to anonymised data. In situations in which the purposes for which the personal data are processed do not

6 Opinion of Advocate General Pitruzzella delivered on 9 June 2022 (1), *RW v.* Österreichische *Post AG*, C-154/21.

7 European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*, adopted on 18 January 2022.

8 European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*.

9 Also, data subject does not have to demonstrate existence of legitimate interest, decision of Spanish Data Protection Authority of 7 February 2020, no. TD/00318/2019.

10 Magdalena Abu Gholeh, and Dominika Kuźnicka-Błaszkowska, *Nakładanie administracyjnych kar pieniężnych w rozporządzeniu o ochronie danych osobowych. Aspekty praktyczne*. Warszawa, 2020, 122.

11 Joanna Łuczak, "Article 15" in *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, eds. E. Bielak-Jomaa and D. Lubasz. Warszawa, 2017, 512–513.

or no longer require the identification of a data subject, the controller does not need to maintain identification data for the sole purpose of complying with data subjects' rights, also in light of the principle of data minimisation.[12] On the other hand, if the controller is no longer in possession of personal data because they have transferred the data to third party, the controller is still obliged to comply with data access request.[13]

The right to data access pertains to the data subject and can only be exercised by such. This does not interfere with the right to exercise this right with the help of any legal representative, but this area is subject to national laws.[14] Additionally, controllers are allowed to ask for additional information if they consider that it is 'necessary to confirm the identity of the data subject' if they have 'reasonable doubts' about the identity of natural person making the request.[15] Disclosing information on personal data processed by the controller to the wrong person may further result in a breach of confidentiality, or a data breach, and may interfere with the right to respect for private life of the data subject.[16] If in doubt regarding the identity of data subject, the controller shall ask more questions, rather than leave the request unanswered.[17] As a matter of good practice, the controller shall implement appropriate procedures describing how the data subject's identity can be confirmed (presenting a national ID or passport, providing a unique client code or specific information which is not publicly known).[18] However, the controller who is asking for further information to confirm the identity of the individual raising data access

12 European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*.

13 Decision of Spanish Data Protection Authority of 28 May 2021, no. R/00214/2021.

14 See Gabriela Zanfir-Fortuna, "Article 15. Right of access by the data subject" in *The EU General Data Protection Regulation (GDPR). A commentary*, eds. Ch. Kuner, L. A. Bygrave, and Ch. Docksey. New York, 2020, 461.

15 Judgement of the Berlin Administrative Court of 31 August 2020, no. 1 K 90.19.

16 Zanfir-Fortuna, 460.

17 Decision of Spanish Data Protection Authority of 31 January 2022, no. PD-00099–2022.

18 Paweł Fajgielski, "Article 12" in *Ogólne rozporządzenie o ochronie danych. Komentarz*, ed. P. Fajgielski. Lex, 2018; see also decision of Netherlands Data Protection Authority of 4 August 2021, no. 202006082/1/A3; Article 29 Working Party, *Guidelines on the right to data portability*, adopted on 5 April 2017, WP242 rev.01.

request shall ensure that they are only collecting information which is strictly necessary for the purpose of identifying the data subject and shall use reasonable and proportionate endeavours to obtain such.

The scope of data access consists of three elements:

- confirmation as to whether data about the person is processed or not,
- access to this personal data and
- access to information about the processing, such as the purpose, categories of data and recipients, duration of the processing, data subjects' rights, and appropriate safeguards in the case of third country transfers.[19]

Because the right to access may be executed in different forms and require disclosing various information, it is the data subject who needs to specify what information on data processing they are requesting.[20] However, in general the scope of access shall be limited only to personal data of the data subject or another person on whose behalf the requester acts.[21] If the data subjects require verbatim "information about the data processed in relation to them", the controller should assume that the data subject intends to exercise their full right under Art. 15(1) – (2) GDPR.[22] In the situation when data subject specifically requests e.g. information on data recipients, the controller may provide only a list of recipients or categories of data recipients without providing the other information listed in art 15 (1) GDPR.

The first component of the data access right seems to be relatively straightforward. At the first glance, there are only two possible answers to the question asked by the data subject, namely "is my personal data processed by a specific controller?". The simple answer is "yes" or "no". However, if one reads the definition of "processing" literally, the moment the data controller received a request from the data subject, the "processing" starts. This means that to be

19 European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*.

20 Decision of Spanish Data Protection Authority of 7 February2020, no. E-08210–2021; Judgement of District Court Den Haag of 20 April 2022, no. 20/2732; judgement of the Court of Amsterdam of 11 March 2021, no. C/13/689705/HA RK 20–258.

21 Decision of Finish Data Protection Authority of 18 November 2019, no. 8896/152/2019.

22 European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*.

accurate and fully transparent, the "no" answer shall include information that personal data is not processed for any other purpose rather than answering the data subject request. If the controller does not process the personal data of the data subject, they shall not leave the request unanswered. Providing a false response (either due to not being aware of processing data subject request, human error[23] or maliciously) may entail the data controller is subject to an administrative fine.[24]

The second layer of the data access right guarantees the right to access personal data. The term 'personal' data shall be defined broadly, considering both the definition included in GDPR ("any information relating to an identified or identifiable natural person") as well as practice of various data protection authorities, national courts and CJEU.

EDPB recognizes the following personal data as falling into the scope of the data access right:

- Special categories of personal data as per Art. 9 GDPR;
- Personal data relating to criminal convictions and offences as per Art. 10 GDPR;
- Data knowingly and actively provided by the data subject (e.g. account data submitted via forms, answers to a questionnaire);
- Observed data or raw data provided by the data subject by virtue of the use of the service or the device (data processed by connected objects, transaction history, activity logs, such as access logs, history of website usage, search activities, location data, clicking activity, unique aspects of a person's behaviour such as handwriting, keystrokes, particular way of walking or speaking);
- Data derived from other data, rather than directly provided by the data subject (e.g. credit ratio, classification based on common attributes of data subjects; country of residence derived from postcode);

23 Decision of Spanish Data Protection Authority of 5 January 2021, no. PS/00016/2022.

24 Decision of Norwegian Data Protection Authority of 16 May 2022, no. 20/02875–10 & 20/02875–11.

– Data inferred from other data, rather than directly provided by the data subject (e.g. to assign a credit score or comply with anti-money laundering rules, algorithmic results, results of a health assessment or a personalization or recommendation process);
– Pseudonymised data as opposed to anonymized data.[25]

Apart from the above, there is also other information which may constitute personal data and be accessible by data subjects under art 15 GDPR. In the joint cases C-141/12 and C-372/12[26] the CJEU ruled that the right of access covered personal data contained in minutes, namely the "name, date of birth, nationality, gender, ethnicity, religion and language of the applicant" and, "where relevant, the data in the legal analysis contained in the minute", but not the legal analysis itself. Other attributes which were recognized as personal data and subject to data access right are: written answers submitted by a candidate at a professional examination and any comments of an examiner with respect to those answers,[27] sales calls recording,[28] the number of children conceived as the result of data subject sperm donation,[29] a surveillance report compiled by an insurance company,[30] data of all repairs and services done to the data subject's car while it was in the possession of car repair shop,[31] the original contract with the data subject.[32]

On the other hand, the access right under art. 15 GDPR does not include the general right to inspect the files of the tax authorities,[33] internal correspondence between the complainant and organisational unit in the context of the processing of their asylum application,[34] internal notes and correspondence

25 European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*.
26 Judgment of CJEU of 17 July2014, joined Cases C-141/12 and C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S*.
27 Judgment of CJEU, C-434/16.
28 Decision of Finish Data Protection Authority of 29 April 2022, no. 10587/161/21; decision of Spanish Data Protection Authority of 28 September 2020, no. TD/00129/2020.
29 Decision of Danish Data Protection Authority of 26 November 2021, no. 2020–31–3894.
30 Decision of Danish Data Protection Authority of 6 September 2021, no. 2020–31–3586.
31 Decision of Icelandig Data Protection Authority of 31 October 2022, no. 2021061304.
32 Decision of Cyprus Data Protection Authority of 17 June 2020, no. 11.17.001.008.001.
33 Judgement of the Financial Court of Munich of 3 February2022, no. 15 K 1212/19.
34 Judgement of The District Court of Midden-Nederland of 12 January 2021, no. UTR 20/268.

which can be qualified as personal thoughts from employees intended for internal consultation and deliberation.[35] Additionally, responding to access requests cannot infringe the rights and freedoms of other individuals,[36] which is of a great importance in access request concerning audio or video recordings,[37] especially in the public sphere. In certain situations an overview of the available data suffices and the original documents (or a copy) do not have to be provided.[38]

Right of access to personal data is one of the components of the right to access. The right of access should not be seen in isolation, as it is closely linked with other provisions of the GDPR, in particular with data protection principles including the fairness and lawfulness of processing, the controller´s transparency obligation, and with other data subject rights provided for in Chapter III of the GDPR.[39] This means that right to access shall be exercised in line with general principles of GDPR, most importantly with transparency towards the data subject. Article 15(1) includes the list of details to be provided to the data subject on their request. This list overlaps with the type of information which must be included in the privacy notice according to art. 13 and 14 GDPR.

35 See judgement of the Dutch District Court of Amsterdam of 9 April 2020, no. C/13/673049 / HA RK 19–338.

36 In such a situation, a case-by-case balance test shall be conducted by the data controller, see judgement of the District Court of Central Netherlands of 2 December 2020, no. C/16/501697 / HA RK 20–117.

37 This area was subject to various DPAs decisions and the main outcomes are as follow: the controller does not necessarily need to provide the recording of the conversation, the transcript of such is also acceptable and completes the data subject's request in this regard (decision of Greek Data Protection Authority of 21 February 2020 on Public Power Corporation S.A., no. 2/2020); generally, footage from CCTV may be subject to the data access right (decision of Cyprus Data Protection Authority of 8 July 2020, no. 11.17.001.007.219) but the data controller could deny an access request seeking CCTV evidence in a suit against the police (decision of Danish Data Protection Authority of 22 June 2022, no. 2020–832–0028). In the case of footage from CCTV, controllers can use special techniques to anonymise the images of other individuals to ensure that their right to privacy is protected (decision of Spanish Data Protection Authority of 1 September 2021, no. R/00634/2021).

38 Judgement of the District Court Rotterdam of 22 March 2021, no. ROT 19/4649.

39 European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*.

Access to information about the processing

The last of the components of the data access right is the right to obtain information about the processing. According to article 15 GDPR, the data subject is entitled to receive the following information on data processing from the controller:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR 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;
- the appropriate safeguards pursuant to Art. 46 GDPR relating to the transfer of personal data if the transfer to third country or international organisation occurs.

As was mentioned, part of this information is usually included in a privacy notice which the controller is obliged to provide the data subject with on the basis of articles 13 and 14 GDPR. EDPB states that controllers may carefully use

text modules of their privacy notice as long as they make sure that they are of adequate actuality and preciseness with regards to the request of the data subject.[40]

To comply with a data subject request to provide information on purpose of processing (art. 15 (1) (a)), the controller shall specifically provide the precise purpose(s) in the actual case of the requesting data subject. If the processing is carried out for several purposes, the controller has to clarify which categories of data are processed for which purpose(s), but the controller is not obliged to specify a lawful basis for each specific purpose.

Information on categories of data (Art. 15(1)(b)), in spite of the general nature of those categories and depending on the circumstances of the specific case, may also have to be tailored to the data subject's situation.[41]

The right of access to information about processing includes also the right to obtain information on the data recipient. This particular aspect has recently been analysed by the Court of Justice of European Union.[42] The Austrian Court sought a preliminary ruling on whether the right guaranteed in art 15(1)(c) is limited to information concerning categories of recipient where specific recipients have not yet been determined in the case of planned disclosures, but that right must necessarily also cover recipients of those disclosures in cases where the data [have] already been disclosed. In its assessment, CJEU has stated that art. 15 entails that full transparency shall be provided to the data subject regarding the manner in which personal data are processed and enables that person to exercise the rights laid down in GDPR. Accordingly, the information provided to the data subject pursuant to the right of access provided for in Article 15(1)(c) of the GDPR must be as precise as possible. In particular, that right of access entails the ability of the data subject to obtain from the controller information about the specific recipients to whom the data have been or will be disclosed or, alternatively, to elect merely to request information concerning the categories of the recipient.

40 European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*.
41 European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*.
42 Judgment of CJEU of 12 January2023, *RW v.* Österreichische *Post AG*, C-154/21.

According to Art. 15(1)(d), information has to be given on the envisaged period for which the personal data will be stored, where possible. Otherwise, the criteria used to determine that period have to be provided. The mere reference, for example to "deletion after expiry of the statutory storage periods" is not sufficient.[43]

EDPB also clarifies that "Whereas information on the right to lodge a complaint with a supervisory authority (Art. 15 (1) (f)) is not dependant on the specific circumstances, the data subjects rights mentioned in Art. 15 (1) (e) vary depending on the legal basis underlying the processing. With regard to its obligation to facilitate the exercise of data subject rights pursuant to Art. 12(2), the response by the controller on those rights shall be individually tailored to the case of the data subject and relate to the processing operations concerned. Information on rights that are not applicable for the data subject in the specific situation should be avoided."[44]

Art. 15(1)(h) provides that every data subject should have the right to be informed, in a meaningful way, inter alia, about the existence and underlying logic of automated decision-making including profiling concerning the data subject and about the significance and the envisaged consequences that such processing could have.[45] This may be the most problematic request to comply with, in terms of keeping the know-how of the controller's organisation protected. On the one hand, the data subject has to be informed about the underlying logic of automated decision-making to ensure that he has the right tools to avoid discrimination. On the other hand, disclosing this information may lead to controllers not being able to protect their IP and know how and thus lose the competitive advantage. If the controller spends a lot of time, money and efforts on creating and implementing automated decision-making tools, they most likely would not want to disclose this information to potential competitors.

43 European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*.
44 European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*.
45 Article 29 Working Party Guidelines on transparency under Regulation 2016/679, adopted on 11 April 2018, WP260 rev.01.

Additionally, article 15(2) guarantees that if the personal data have been transferred to a third country or international organisation that has not been recognized as providing adequate protection, the data subject has the right to access information on the safeguards which formed the basis for the data transfer (transfer mechanisms according to art 46). However, it does not seem that controller needs to provide a copy of standard contractual clauses or binding corporate rules (or other documents) to fulfil this obligation. Even though binding corporate rules are usually published by controllers, standard contractual clauses may serve as a part of bigger contract subject in full to confidentiality obligations. Even though the parties are not able to oblige each other to keep the contract confidential, disclosing specific terms (SOP, price, business model) may lead to disclosing the know-how of the controller's organisation.

Even though the scope of data access is relatively broad (and further extended by CJEU and data protection authorities decisions), it does have certain limits. For instance, the CJEU found that the objective of the right of access guaranteed by EU data protection law is to be distinguished from that of the right of access to public documents established by EU and national legislation, the latter aiming at, "the greatest possible transparency of the decision-making process of the public authorities and to promote good administrative practices."[46]

According to EDPB, the data controller is not entitled to ask "why" the data subject is requesting specific information on data processing, but in the practice of interpreting the law DPAs and courts from time to time raise the question of whether the request is in line with the aim of the GDPR.[47] The line of interpretation is not established just yet, hence it may be reasonable to follow EDPB recommendations that the aim of the right of access is not suitable to be analysed as a precondition for the exercise of the right of access by the control-

46 Judgment of CJEU of 17 July 2014, joined cases *YS and Others*, C-141/12 and C-372/12; see also judgement of District Court of Zeeland-West-Brabant of 1 December2021, no. AWB- 20_5521; judgement of the District Court of Central Netherlands of 18 June 2020, no. AWB-20_1431.

47 Judgement of Dutch District Court of Amsterdam, C/13/673049 / HA RK 19–338.

ler as part of its assessment of access requests.[48] However, if the data subject is requesting specific information on how its data is processed or a copy of such data to e.g. defend their rights in the proceedings against data controller, they are entitled to receive such information. The right of access is broadly used by data subjects who are a party of proceedings involving the data controller in the employment law, anticompetition law or antidiscrimination law areas,[49] but also may be used when facing criminal investigation.[50] Nevertheless, the right to access may also be exercised with the aim of discovering the business model of the controller, the results of business initiatives, including the vendors and contractors (serving e.g. as recipients) the controller cooperates with, or even to discover the contractual terms and conditions between controller and other parties. This may lead to controllers not being able to protect their confidential information or know-how, which, in contrast to e.g. trade secrets, are not comprehensively protected in the EU.

Protecting know-how in the organisation

The right to data access pertains to the data subject, but there is a corresponding obligation pertaining to the controller of the processing. This is the controller being legally responsible for compliance with the right to access.[51] However, it will not always be the controller fulfilling this obligation, as this may flow down to a data processor if it is subject to an agreement between the

48 European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*.

49 See e.g. decision of Bulgarian Data Protection Authority of 28 October 2019, no. ППН-01–116/2019; decision of Data Protection Authority of Brandenburg of 18 October 2021, no. 10 Sa 443/21; judgement of The Court of First Instance of the Central Netherlands of 24 March 2021, no. C/16/502323 / HA RK 20–122. In March 2022 Datatilsynet found the data subject request to access all emails, notes and letters sent or signed by him as excessive, according to Article 12(5)(b) GDPR, since it comprised a very large amount of personal data predominantly connected to his duties and not personal attributes. See decision of Danish Data Protection Authority of 31 March 2022, no. 2021–32–2438.

50 See e.g. judgement of the District Court of Gelderland of 24 August 2020, no. 365592.

51 Zanfir-Fortuna, 461.

data controller and the data processor according to article 28(3)(e) GDPR. In practice it may be the processor who first asks for further information to confirm the requester's identity, but also the one who is communicating with the data subject during the entire process and at the end – responds to the request for data access. Regardless of the contractual means, it is the controller who is ultimately responsible for responding to data the subject's request.[52]

The scope of a data access request may be interpreted broadly, as mentioned before. However, complying with the obligation to provide information may not always be in the best interest of the controller. A broad data access request may result in revealing information perceived as confidential by the controller.

The difficulty which faces the controller when responding to the data subject's request for data access is the fact that there is no binding definition of confidential information or know-how, hence these two values are more difficult to protect. Even though confidential information and know-how is often defined in non-disclosure agreements, these are not binding, neither for the data subject not the data protection authority. 'Confidential information' is often defined as all material, non-public, business-related information, written or oral, whether or not it is marked as such, that is disclosed or made available to the receiving party, directly or indirectly, through any means of communication or observation or which is not intentionally made available to any third party. 'Know-how' is often defined in even more concise way, as "knowledge of how to do something smoothly and efficiently, expertise". Even though the commonly-used definition of 'know-how' is relatively short, there is huge value hidden in information considered as know-how, which often determines the competitive advantage of a particular entity. 'Know-how' is not protected by law in any way, but ensuring that this knowledge is not widely shared is of crucial importance to all companies. Apart from that, not all information which may be part of the data access

52 This is a conclusion from a decision of the Data Protection Authority of Brandenburg, decision from 2019 on unknown company, <https://www.enforcementtracker.com/ETid-271>, access: 9.03.2023.

request is confidential by its nature, but not disclosing such information to the data subject may be important due to e.g. litigations between the controller and the data subject.

Confidential information and know-how is protected by companies in various ways. Even though the law does not protect know-how directly and the protection of confidential information is limited and depends on jurisdiction, companies have developed a set of practices which help them maintain the confidentiality of certain information. First and foremost, confidentiality is protected under non-disclosure agreements which may form a standalone contract between two entities or employer and employee. The obligation to keep certain information secret may also be a part of an employment contract, master service agreement or any other type of contract. There is no need to offer additional compensation for keeping information and know-how confidential. Even if the confidentiality obligation does not form part of the employment contract, in most jurisdictions the employee is obliged by law to keep the information of the employer confidential. Disclosing confidential information against an individual's obligation arising from a contract may be also subject to penalties.

Apart from contractual obligations, companies may also protect confidential information and know-how by ensuring the right level of access designed in the organisation and strictly adhering to the need-to-know principle. This entails storing information separately and implementing 'no printing' or 'clean desk, clean screen' policies. Above all, companies shall ensure that they choose trustworthy partners to cooperate with. However, neither of these measures will play an important role when facing a data access request which may lead to disclosing confidential information.

On the other hand, it is also worth mentioning that if a data subject is requesting access from a controller who is a public entity, the controller may rely on various legal obligations which make them protect information, such as state secrets and other information which the state protects as confidential.

In the public sphere, the right to access information on processing under art 15 GDPR shall not be read as similar or equal to the right to access public information. The purpose and scope of these rights are different, and even though they both consider "access" as a right, the material scope varies.

Additionally, considering various requests from a data subject to obtain access to certain documents or copies, it needs to be emphasized that the right to access information on processing personal data is not equal to the right to receive a copy of personal data. Even though both of the rights are guaranteed under art 15 GDPR and serve similar purpose, their scope is different. Hence, when a data subject is requesting information on processing, this does not mean that the controller is obliged to provide a copy of any documents connected with processing the personal data of the data subject (e.g. a copy of a data processing agreement).

The right to access information on data processing is not absolute. This right must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.[53] The CJEU rightly pointed out that in some circumstances it may not be possible for a controller to provide specific information.[54] However, from the interpretation made by the CJEU, it seems that these circumstances shall have an objective nature. It does not seem that the desire to protect confidential information on the know-how of the controller can serve as 'circumstances' which stop the controller from fully responding to a data subject request in all cases. The Austrian DPA[55] stated that the right to access does not always apply in absolute terms and that it may be restricted by third-party interests such as secrecy obligations. However, in order for such a restriction to apply, a data controller must properly substantiate their arguments for denying the right to access. One of the examples in which controller's rights prevail, is the right to prepare its

53 Judgment of CJEU of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, par. 172.
54 Judgment of CJEU, C-154/21.
55 Decision of Austrian Data Protection Authority of 26 July 2019, no. DSB-D123.921/0005--DSB/2019.

defence in freedom and seclusion.[56] On the other hand, the French DPA has concluded, that 'business secrecy' may be considered as an exception from the data access right only if the data subject is requesting a copy of personal data processed, not information on how the data is processed.[57] The Belgian DPA went further, stating that the data subject does have the right to access an audit report concerning (among others) his work, even though the controller had claimed that the report was confidential in nature and full disclosure may have infringed the IP and privacy rights of others.[58] Protecting confidential information shall not lead to ignoring data access requests. The controller may however anonymise information which he is entitled to protect due to its confidential nature.[59]

Summary

The existing interpretation of the data access right of the CJEU and the EDPB is definitely broadening. Of course, this makes sense from the point of view of the purpose of the GDPR, but it leads to the imposition of new obligations on the controllers, not provided for in the regulation, and the limitation of their rights related to running a business.

There is an important difference between information on data processing and information about the know-how of the controller. It needs to be emphasized that the data subjects' rights under the GDPR are not absolute and shall not lead to limiting controllers' right to protect their confidential information and know-how. Otherwise, this may lead to a weakening of the position of entrepreneurs in disputes, affecting their negotiating position or position on the market, as well as the disclosure of information constituting a business secret, and contribute to actions having the characteristics of acts of unfair competition.

56 Procurator General of the Dutch Supreme Court of 26 August 2022, no. 22/01253.
57 Decision of French Data Protection Authority of 30 November 2022, no .SAN-2022–022.
58 Decision of Belgian Data Protection Authority of 29 July 2020, no. 41/2020.
59 Decision of Hungarian Data Protection Authority of 3 September 2020, no. NAIH/2020/2204/8.

The right balance should be found between guaranteeing the rights of individuals and the rights of entrepreneurs, otherwise excessive restrictions and the inability to protect one's secrets will lead to a weakening of the attractiveness of doing business in the European Union and may contribute to an economic slowdown.

References

Abu Gholeh, Magdalena, and Dominika Kuźnicka-Błaszkowska. *Nakładanie administracyjnych kar pieniężnych w rozporządzeniu o ochronie danych osobowych. Aspekty praktyczne*. Warszawa, 2020.

Łuczak, Joanna. "Article 15." In *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, edited by Edyta Bielak-Jomaa, and Dominik Lubasz. Warszawa, 2017: 507–516.

European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*, Adopted on 18 January 2022.

Fajgielski, Paweł. "Article 12." In *Ogólne rozporządzenie o ochronie danych. Komentarz*. editd by Paweł Fajgielski. Lex, 2018.

Zanfir-Fortuna, Gabriela. "Article 15. Right of access by the data subject." In *The EU General Data Protection Regulation (GDPR). A commentary*, edited by Christopher Kuner, Lee A. Bygrave, and Christopher Docksey. New York, 2020: 449–468.

Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, adopted on 11 April 2018, WP260 rev.01.

Article 29 Working Party, *Guidelines on the right to data portability*, adopted on 5 April 2017, WP242 rev.01.

Decision of Austrian Data Protection Authority of 26 July 2019, no. DSB-D123.921/0005-DSB/2019.

Decision of Belgian Data Protection Authority of 29 July 2020, no. 41/2020.

Decision of Bulgarian Data Protection Authority of 28 October 2019, no. ППН-01-116/2019.

Decision of Cyprus Data Protection Authority of 17 June 2020, no. 11.17.001.008.001.

Decision of Cyprus Data Protection Authority of 8 July 2020, no. 11.17.001.007.219.

Decision of Danish Data Protection Authority of 6 September 2021, no. 2020-31-3586.

Decision of Danish Data Protection Authority of 26 November 2021, no. 2020-31-3894.

Decision of Danish Data Protection Authority of 31 March 2022, no. 2021-32-2438.

Decision of Danish Data Protection Authority of 22 June 2022, no. 2020-832-0028.

Decision of Data Protection Authority of Brandenburg of 18 October 2021, no. 10 Sa 443/21.

Decision of Data Protection Authority of Brandenburg of 2019 on unknown company, <https://www.enforcementtracker.com/ETid-271>, access: 9.03.2023.

Decision of Finish Data Protection Authority of 18 November 2019, no. 8896/152/2019.

Decision of Finish Data Protection Authority of 29 April 2022, no. 10587/161/21.

Decision of French Data Protection Authority of 30 November 2022, no. SAN-2022-022.

Decision of Greek Data Protection Authority of 21 February 2020 on Public Power Corporation S.A., no. 2/2020.

Decision of Hungarian Data Protection Authority of 3 September 2020, no. NAIH/2020/2204/8.

Decision of Icelandig Data Protection Authority of 31 October 2022, no. 2021061304.

Decision of Norwegian Data Protection Authority of 16 May 2022, no. 20/02875-10 & 20/02875-11.

Decision of Spanish Data Protection Authority of 7 February 2020, no. E-08210-2021.

Decision of Spanish Data Protection Authority of 7 February 2020, no. TD/00318/2019.

Decision of Spanish Data Protection Authority of 28 September 2020, no. TD/00129/2020.

Decision of Spanish Data Protection Authority of 5 January 2021, no. PS/00016/2022.

Decision of Spanish Data Protection Authority of 28 May 2021, no. R/00214/2021.

Decision of Spanish Data Protection Authority of 1 September 2021, no. R/00634/2021.

Decision of Spanish Data Protection Authority of 31 January 2022, no. PD-00099-2022.

Judgement of Berlin Administrative Court of 31 August 2020, no 1 K 90.19.

Judgment of CJEU of 17 July 2014, joined cases *YS and Others*, C-141/12 and C-372/12.

Judgment of CJEU of 20 December 2017, *Nowak v. Data Protection Commissioner*, C-434/16.

Judgment of CJEU of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18.

Judgment of CJEU of 12 January 2023, *RW v. Österreichische Post AG*, C-154/21.

Judgement of Court of Amsterdam of 11 March 2021, no. C/13/689705/HA RK 20-258.

Judgement of Court of First Instance of the Central Netherlands of 24 March 2021, no. C/16/502323 / HA RK 20-122.

Judgement of District Court Den Haag of 20 April 2022, no. 20/2732.

Judgement of District Court of Central Netherlands of 18 June 2020, no. AWB-20_1431.

Judgement of District Court of Gelderland of 24 September 2020, no. 365592.

Judgement of District Court of Midden-Nederland of 12 January 2021, no. UTR 20/268.

Judgement of District Court Rotterdam of 22 March 2021, no. ROT 19/4649.

Judgement of District Court of Zeeland-West-Brabant of 1 December 2021, no. AWB- 20_5521.

Judgement of District Court of Amsterdam of 9 April 2020, no. C/13/673049 / HA RK 19-338.

Judgment of ECHR of 23 January1986, *Gaskin v. United Kingdom*, 10454/86.

Judgment of ECHR of 26 March 1987, *Leander v. Sweden*, 9248/81.

Judgment of ECHR of 6 June 2006, *Segerstedt-Wiberg and Others v. Sweden*, 62332/00.

Judgment of ECHR of 28 April 2009, *K.H. and Others v. Slovakia*, 32881/04.

Judgement of Financial Court of Munich of 3 February 2022, no. 15 K 1212/19.

Opinion of Advocate General Pitruzzella delivered on 9 June 2022 (1), *RW v. Österreichische Post AG*, C-154/21.

Procurator General of the Dutch Supreme Court of 26 August 2022, no. 22/01253.