DIGITALEUROPE

11 MARCH 2022

Balancing rights and obligations for an effective GDPR access right

Executive summary

Access is a cornerstone right in the General Data Protection Regulation (GDPR),[1] whose exercise relies on efficient coordination between the author and the recipient of the access request. For this reason, the right of access should be supported by a well-defined balance between the rights and obligations of both parties.

We urge the European Data Protection Board (EDPB) to take the following points into consideration in the final version of its upcoming Guidelines on the right of access.[2] Notably, the final Guidelines should:

- Clarify that not all types of data are necessarily being requested. The opposite approach would ultimately prove counterproductive for the data subject;
- Encourage the data subject to use the most appropriate or suggested channels. This would avoid misunderstandings between the data subject and the data controller and allow for faster and less costly response;
- Take into account the right to conduct a business, economic interest and proportionality, insofar as they may have a bearing on the controller's assessment of the right of access; and
- Reflect the possible impact from upcoming case law potentially restricting the scope of personal data falling under the access right.

[1] Regulation (EU) 2016/679.

[2] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Table of contents

Finding a balance in the assessment obligations

If the right of access can easily be understood in three parts,[3] the controller's obligations are considerably multiplied. This imbalance results from the data that needs to be provided, the method by which it needs to be provided and how it should be assessed, as explained bellow.

Giving access to *all* personal data

The draft Guidelines recommend that the controller should take it for granted that the disclosure should encompass *all* personal data concerning the data subject,[4] no matter the format in which it is processed.[5]

Depending on the business model and size of the company, finding all possible data, which may also come from various sources, can represent a challenge and will require a high level of internal organisation.

In particular, requiring the controller to search backup systems, which may not be readily or easily accessible, constitutes a disproportionate effort. This was outlined by a German court, which found that restoring the data would involve disproportionate resources, measured against the individual's interest in the information.[6] Proportionality should be applied at all steps of the access right process, including in searching for backup data.[7]

Moreover, the flow of data might also be constantly evolving, depending on the type of processing or its duration. For this reason, it may be hard to identify what data has been collected until the exact time of the reception of the request. The draft Guidelines recognise the risk of an overflow of information.[8] For the right of access to truly serve the data subject's purpose, and to simplify the controller's assessments, the request's scope should first be clear.

Finally, the draft Guidelines take the position that when this includes 'data in a raw format,' which may not be 'directly meaningful' to the reader, the controller should take 'the necessary measures to ensure that the data subject

[3] Para. 3 of the draft Guidelines.

[4] Para. 35, ibid.

[5] Para. 19, ibid.

[6] Judgment of February 6, 2020 – 4 O 6/19.

[7] See 'Proportionality' section, p. 7 below.

[8] Para. 35(b) of the draft Guidelines.

understands the data.'[9] This complex requirement involves considerable effort on the part of controllers goes well beyond what the right of access entails under the GDPR.

Finding the best method for the request

DIGITALEUROPE welcomes the draft Guidelines' support of software tools to facilitate clear access requests. This can be a positive motivation for controllers and data subjects alike to offer and use concrete methods. However, the solution is undermined by the lack of encouragement to the data subject to use them.

Tailoring the processed information to each request would be materially impossible for controllers, who may regularly receive a wide number of requests.[10] The draft Guidelines recognise that the principle of transparent processing already sets obligations,[11] but they should not be further extended for this specific right.

Since a balance ought to be struck between providing sufficient information to ensure transparency and not encumbering data subjects with excessive information, practical and user-friendly provision of information should be favoured. This would be in accordance with the WP29 Guidelines on transparency, which benchmark the presentation of the information at the level of the average member of the 'intended audience.'[12]

The draft Guidelines state that the request does not need to be in any particular form, and can be sent via any communication channel normally used by the controller. At the same time, they do note that the controller 'is not obliged to act on a request sent to a random or incorrect e-mail (or postal) address, not directly provided by the controller, or to a communication channel that is clearly not intended to receive requests regarding data subject rights.'[13]

Several claims received by data protection authorities (DPAs) have already shown that data subjects may have unreasonable expectations as to the channels the controller should use to carry out its obligations.[14]

---

[9] See example at para. 139, ibid.

[10] Para. 111, ibid.

[11] Para. 7, ibid.

[12] Para. 9, WP29 Guidelines on transparency under Regulation 2016/679.

[13] Paras 52–57 of the draft Guidelines.

[14] For example, in Luxembourg's decision D51/2470/2018, the data subject expected that the controller could make an assessment based only on one method. The final Guidelines should further clarify that several methods are in fact possible.

For instance, the UK Information Commissioner's Office has specified what is expected of employees when the request is sent to communication channels normally used by the controller, but not intended to receive request.[15] Similarly, the final Guidelines should further clarify which communication channels the controller would not be obliged to act on.

The final Guidelines should also allow flexibility with regard to the timeframe imposed by Art. 12(3) GDPR when employees are emailed access requests.[16] Such flexibility should take into account normal occurrences such as: the fact that the relevant employees could be on holiday; the email could be marked as spam; or employees could consider the email to be a phishing attack.

Finally, the Guidelines should reflect processes adopted thus far by organisations to implement data subject rights, such as automation systems to respond to data subjects in the appropriate timeframe.

Identifying the request's content

While the draft Guidelines state that the objectives behind the request should never be taken into account,[17] they also state that a request of a malicious intent may be considered excessive.[18] The aim of the request is therefore relevant, if only to identify a malicious intent.

One example of this is where the data requested may be information used to ensure the safety of the controller's anti-fraud systems. Sharing certain pieces of information may compromise the system's safety, or even allow competitors to copy it.

When fraud, identity theft or cybercrime are identified, the final Guidelines should clarify which information needs to be shared with the data subject about the offence. For example, where a fraudster's location could be identified, the Guidelines should specify whether the location data should be shared. It should also be specified how this obligation would be articulated around national legislation.

We welcome the examples and variations illustrating the decision-making process to be followed when further copies are requested.[19] However, they show

[15] See ICO guidance on the right of access, available at https://ico.org.uk/media/for-organisations/documents/2619803/right-of-access-1-0-20210520.pdf.

[16] Para. 57 of the draft Guidelines.

[17] Para. 13, ibid.

[18] Para 188, ibid.

[19] Para. 28, ibid.

that a large degree of interpretation of the request or requests is needed. This interpretation is to be made on a case-by-case basis, as no single clear guiding rule is reflected in the draft Guidelines.

At a minimum, the final Guidelines should clarify what can be considered as a 'reasonable fee' and allow more flexibility in assessing whether an additional copy is being requested.[20]

Identifying the request's content would also be key in satisfying Arts 15(1)(a)-(h), as the draft Guidelines emphasise that certain aspects may vary depending on individual circumstances. There are circumstances where personal data is processed in a standard and predictable way. Here, the privacy policy provided at the time the data was first collected, which was already made to comply with transparency obligations, would constitute an up-to-date and accurate representation.

Missing in the legal framework

Balancing different rights, such as the right to conduct a business

As noted in the Introduction of the draft Guidelines, the right of access originally stems from Art. 8 of the Charter of Fundamental Rights, along with Art. 16, the right to conduct a business. We believe it will be particularly valuable to controllers to receive a more balanced articulation of both rights in the final Guidelines, as the right of access sets direct requirements and obligations that will have a direct impact on their business operations.

The right to run a business could for instance come into play in the controller's assessment of whether a new request is excessive.[21] It could also come into play if a cumulation of requests are made while no new contract is signed and the data is unlikely to have changed. Recognising that such requests should not require the same level of response could considerably simplify and accelerate controller's assessments.

For the same reason, economic interest should be further articulated into the draft Guideline's analysis of Art. 15(4) GDPR. The draft Guidelines give a blanket statement that a company's economic interest does not constitute a right or freedom which could limit the scope of Art. 15(4). However, in the same

[20] Para. 27, ibid.

[21] Para. 28, ibid.

sentence, they recognise that economic interest can contain 'other protected rights.'[22] How the right of access can be articulated around the different protected rights that may constitute an economic interest should be better recognised and developed.

Proportionality

The principle of proportionality,[23] which applies to balancing different fundamental rights, is not applied consistently throughout the draft Guidelines. For instance, on the one hand, controllers are required to prepare themselves 'adequately and proportionately'[24] for requests, but on the other they cannot apply the principle of proportionality to the estimated effort necessary to comply.[25]

The GDPR recognises that providing information can constitute a disproportionate effort for the controller. For instance, Art.14 GDPR excludes the obligation to provide personal data which has not been obtained by the data subject in cases where this would constitute a disproportionate effort. Similarly, the final Guidelines should identify cases in which providing access to information would constitute a disproportionate effort, or at least acknowledge this possibility.

An example of this is provided by the Belgian DPA, who has upheld the refusal by a data controller to provide a data subject with access to 'IT logs.'[26] It found that communication of the logs would create a disproportionately heavy workload for the employer, considering the amount of data to be checked. DPAs can therefore take the burden imposed on a data controller into account and that a proportionality assessment should apply to each stage of the right of access request.

Manifestly unfounded

The draft Guidelines recommend an objective approach to assessing a request. However, the described approach would not allow the controller to presume that

[22] Para. 168, ibid.

[23] Art. 5(4) of the Consolidated version of the Treaty on European Union.

[24] Para.42 of the draft Guidelines.

[25] Page 4 of the executive summary of the draft Guidelines.

[26] Decision 15/2021, of the 9th of February 2021.

the request was manifestly unfounded, even if it includes unobjective or improper language.[27]

The effort on behalf of the author of the request is considerably lower than that of the person receiving and analysing it from the data controller's side. For this reason, the controller is given a disproportionate obligation to analyse and document a request which may be visibly or clearly unfounded.

The final Guidelines should provide an explanation and examples of manifestly unfounded requests, as well as with regard to the investigation necessary on the controller's side to determine whether a request is manifestly unfounded.

Possible restrictions to the scope

If the scope of the right of access does not include a proportionality assessment, the scope of the personal data which can be requested may nevertheless be more limited.

Notably, the CJEU is being asked to decide whether log data is considered as personal data for this specific right.[28] If the CJEU decides that log data is not in the scope of the right of access, this could be an indication that the scope of the data access right can be more restrictive than the general definition of personal data. The consequences of this decision would therefore be important, and the final Guidelines should take them into account.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security Policy

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Béatrice Ericson

Officer for Privacy and Security Policy

beatrice.ericson@digitaleurope.org / +32 490 44 35 66

[27] Para. 178 of the draft Guidelines.

[28] Case C-578/21.

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, Dassault Systèmes, DATEV, Dell, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK