Position Paper

Bitkom views on EDPB Guidelines 1/2022 on data subjects rights – Right of access

11/03/2022

Federal Association
for Information Technology,
Telecommunications and
New Media

Rebekka Weiß, LL.M.
Head of Trust & Security
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

Introduction and Overview

Bitkom welcomes the opportunity to comment on the EDPB Draft Guidelines on the access right under Regulation 2016/679. We believe that more cooperation and exchange between data protection authorities and practitioners is needed to translate the legal text of the GDPR into practice and reduce legal uncertainty.

Although it may not be possible to address specific sector related questions in such broad guidelines, it would be important for regulated sectors, such as the banking sector, to have some specific guidance on how to comply with the right of access without infringing other sectoral legal requirements.

If the EDPB could address some of the constraints that regulated sectors have to comply with, even if only by acknowledging them by outlining a respective example, such as regarding the identification and authentication of data subjects, that would help controllers from these sectors to understand the interplay between sectoral requirements and data privacy requirements.

In general, we recommend that these guidelines be aligned with the needs of practicability and feasibility. Some parts of the current version are missing this perspective (e.g. tailored information according to Art. 15 (1) GDPR, single point of contact), which burdens companies with effort that cannot be considered as proportional according to constitutional law.

1. Aim of the right of access and exceptions (2.1. /13)

The denial of a right to information in the event of legal disputes should remain possible (see also no. 95). The guidelines should be adapted accordingly.

2. Costs for requests (2.2.2.2. / 30 and 38)

The controller is entitled to demand a reasonable fee for the to demand additional copies, Art. 15(3) GDPR. We believe that further concretization is necessary in this regard:

- objective characteristics that serve as a basis
- fee calculation for the data subject
- clarification to what extent the administrative fees of the national authorities apply

The requirement in the Draft Guideline is not comprehensible in its nature and in practice generates considerable administrative effort. Particularly in larger companies a large amount of data is generated that is only available for a short period of time. When a request is received, it is not yet possible to determine what data has been or will be processed and which data must be disclosed accordingly. In some cases, some data will be deleted in the meantime. The position of the EDPB regarding an extension of retention periods is contrary to the principle of data minimization, especially since data records cannot always be attributed only to one data subject. In addition, the period legally granted by law for processing the claims for access would be considerably reduced.

3. Completeness of information (2.3.1. / 35 b) first paragraph)

It is important to acknowledge that the majority of requests of access are expressed in very general terms. This is not the exception rather the rule.

For that reason it is important that the EDPB clarifies how a controller that processes a large amount of data concerning a data subject (such as a bank) can comply with the right of access. The EDPB mentions that this may be possible for example by providing self-service tools in online contexts. If this is not possible the controllers may request the data subject to specify the information or processing to which the request relates before the information is delivered (see Recital 63 GDPR).

Does this mean that a controller that processes a large amount of data, such as a bank, may firstly reply to the data subject request by providing core personal data (such as name, contact details, etc.) and secondly request the data subject to specify which information would the data subject wish to have in addition to that information? It would be very helpful if the EDPB could provide some clarification to this layered approach to the right of access.

The Guidelines seem to provide that a controller cannot request a concretization but must always provide all processed personal data upon request (cf. para. 35): *"If the data subject, who has been asked to specify the scope of its request, confirms to seek all personal data concerning him or her, the controller of course has to provide it in full."*

This interpretation is likely to lead to completely disproportionate efforts in a number of processing scenarios and also opens the door to abuse of the right of access, e.g. in the employment relationship.

The Guidelines should therefore be amended to ensure that in such scenarios there is a "real" right of the controller to concretization, as set out in Recital 63: *"Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates."*

The statements of the BayLDA in the Activity Report 2020 (p. 50 f.) can also be understood in this sense. An obligation to provide information on all data would effectively not be a "concretization" but would remain "general" and not help the data subject in his request.

4. Completeness of the information (2.3.1. / 35 b) second paragraph)

The example of providing information on "different databases" to data subjects seems not to be feasible for several sectors, for instance the banking sector. Banks, as well as other entities, shall not reveal any information on existing databases, for instance due to security reasons. This information is also not useful for the data subject, as they cannot ascertain which database contains data about themselves. We suggest this paragraph be revised by the EDPB.

5. Compliance with data security requirements (2.3.4. /40)

The EDPB provides that *"In cases where data security requirements would necessitate end-to-end encryption of electronic mails [...]"* in order for controllers to have a standardised approach to the security measures to be applied it would be helpful if the EDPB could concretize in which cases, in the opinion of the EDPB, would end-to-end encryption be necessary. Therefore, the EDPB could provide example cases which would cover this topic.

It should be added that the data subject would have to bear the costs for transfer via registered letter. Considering the amount of DSARS processed by a company it wouldn't be appropriate to make the controller cover these costs.

6. Entry points for data access requests (3.1.1. / 55)

Operationally controllers naturally set up internal processes to address data subject access requests, including by means of appropriate channels for data subjects to submit such requests which are clearly informed to data subjects, for instance in the Privacy Policy. Permitting under this guidance that data subjects address such requests to any official contact point of the controller is thus not feasible for many sectors/stakeholders, creating operational issues in providing a timely reply to the data subject.

In order to comply with the requirements of the GDPR, standardised processes are required to manage extensive data processing, as is common for a bank. Such a standardised process for responding to Art. 15 GDPR requests would no longer be fully possible if each [e.g.] customer agent has to act as a recipient of such a request according to recital 55 of the guidelines. It is not reasonable to expect that controllers can comply with the time limits according to Art. 12 (3) GDPR if a data access request is sent to the non-official contact. However, this would create a high risk for errors and prevent companies from automating processes as much as possible. This would only be possible if companies are authorised to accept data access requests only if they are submitted via a few contact points designated by the company. Clarification in this regard by the EDBP would be useful for the controller's ascertaining of internal procedures.

In addition, the period pursuant to Art. 12 (3) sentence 1 GDPR should not begin until the access request has been initiated in the standardised process, i.e. the request is initiated as per the procedures.

7. Establishing identity of the person making the request (3.2. / 77, 78)

Financial institutions may not process special categories of data (as per Art. 9 GDPR) but may process highly sensitive data such as banking account related information, protected by banking secrecy. In order to clarify authentication procedures within the financial sector the EDPB should clarify if the banking sector and the authentication of banking customers should be understood as a specific circumstance that would allow requesting the ID. Specifically for former customers where it may not be possible to address the request via a secure channel.

In addition, it shall be noted that banking entities are obliged to perform a customer due diligence where an identity document of the customer needs, by law, to be provided by the customer to the bank in order to verify if it is possible to proceed with the bank account opening (the copy of such a document shall then be stored according to banking/AML legal obligations). This means that an identity document and the data contained therein was already provided to the bank in the past and thus shall be an adequate way to verify the data subjects' identity if needed in case of data access request, without having additional data processed by the bank.

We suggest EDPB clarifies this shall not be applicable to specific sectors like the banking sector, for the reasons mentioned above.

We suggest EDPB explains in more detail that controllers are not required to reply to data subject requests by means of third party platforms. It shall be further detailed that it is not operationally feasible to require controllers to reply to data access requests by means of third party platforms. The adhesion to the use of such third party platforms requires, in general, that the controller onboards such third party platform as a service provider. This, in case of several activity sectors, requires a third party risk assessment in light of the sectoral legislation (for instance banking legal and regulatory requirements) and controllers cannot be subject to the burden of being obliged to onboard each and every service provider which provides such a third party platform and is chosen by data subjects to exercise their rights before the controller.

It shall be noted that this would otherwise also conflict with the freedom of contract of controllers, as they would be obliged to accept (or negotiate) contractual terms with such third parties.

Another note is that, if the controller already provides several ways of data subjects exercising their rights - and for which the controller has set up the correspondingly adequate internal procedures - one does not understand why the controller shall be subject to other and external possibilities of data subjects exercising their rights for which operational efforts would need to be changed/reviewed depending on the third party platform chosen by each and every data subject.

It is indeed operationally not feasible to require from the controller to check the security and safe handling of third party platforms to confirm if the reply to such requests can be provided by means of such platforms to the data subjects (even if no adhesion to such a third party platform would be required from the controller).

On a different note, in case a data subject reaches out via a third party platform, identity verification issues are usually triggered, in particular when the data access is required towards sensitive data like banking and financial information of the data subject. In order to confirm the identity of the data subjects in such cases the controllers would once again need to create new internal processes, depending on the third party platform chosen by the data subject - note that the different platforms have different ways of identifying the data subject at stake.

Thus, this requirement shall be reviewed by the EDPB and the obligation for data controllers to comply with data access requests which are performed by means of a third party platform shall be in the liberty of the controller to decide whenever the controller provides a clear, structured and compliant way for the data subjects to exercise their rights.

8. Scope of access “notes applications process” (4.1. / 95)

We recommend an adjustment of the wording. The description of the example gives the wrong impression, from our legal point of view, that controllers are obliged to release all personal data collected in the course of an application process in any case, including subjective evaluations, without exceptions being able to intervene. However, such exceptions are certainly possible in accordance with Art. 15 (4) GDPR with regard to the rights of third parties. Thus, there may be constellations in which the personal data of people who provided feedback as part of an application procedure must be protected.

We propose the wording be changed to: Inside the scope of data access requests are summaries of interviews.

Instead of creating a broad obligation for companies to provide any notes taken within an interview it should be defined by the EDPB which information should be provided taking into consideration if such provision would be beneficial to the candidate (a lot of notes taken in interviews are not structures enough to be useful input for the candidate) and more importantly the protection of rights and freedoms of the data subjects providing such notes (the interviewers).

9. Archived personal data (4.2.2. / 107,108)

The EDPB equates data in backup systems with data in live systems. (no. 108) Equating backup systems and live systems means that, by default, a backup system must always be searched, regardless of whether the search in a live system has led to a result. Notwithstanding of the disproportionate effort involved, it must also be taken into account that this requirement not only does not serve the rights and freedoms of the data subjects, but also contradicts the principles of data minimization and storage limitation. If, for example, data has already been deleted from the live system, it is inaccessible to all employees and is also removed from the backup system during the next deletion cycle. This access restriction on data that has actually been deleted from the live system would no longer apply if backup systems also had to be checked regularly.

The same applies in principle to the requirement of the EDPB to provide information about data that is only stored due to a legal obligation (see no. 107). These data are subject to very strict access restrictions and are in principle not accessible. This strict access restriction as an expression of the principles of data minimization and storage limitation would be breached if service employees regularly had to search this data as well for information requests.

Furthermore, the EDPB emphasizes several times that the right of access is not subject to any proportionality restrictions at the company (The right of access is without any general reservation to proportionality with regard to the efforts the controller has to take to comply with the data subject's request).

It is Bitkom´s firm position, that those requirements are too far reaching. Even though the wording of Art. 15 GDPR does not contain any restriction, the GDPR is not without limits. In Recital 4, Sentence 2, for example, the GDPR already stipulates a balancing requirement with other fundamental rights that is actually self-evident. (*"The right to the protection of personal data is not an unrestricted right; it must be seen in the light of its social function and weighed against other*

fundamental rights in compliance with the principle of proportionality."). The same can be found in Recital 63, which also provides for limitations to Art. 15 GDPR *("where possible"* or *"where feasible"*).

Accordingly, this must also be taken into account if companies are required to incur high costs to comply with requests for information, the implementation of which is irrelevant to the rights and freedoms of the data subjects.

10. Scope of a new request for access (4.2.3 /109)

The EDPB does not address whether, in the case of two successive requests for access, it is necessary for transparency, to disclose to the data subject the personal data added between in between the two requests.

In our view, a clarification is necessary whether it must be disclosed which data has been added in the time period between two requests.

11. Scope information provided on data processing (4.3. / 111)

According to Art. 15 (1) GDPR there is to be differentiated between the data access / copy of data which is to be tailored to the data subject on the one hand and the additional information on the data processing which is to explained objectively as far as a requesting category of data subject (e.g. Pre-KYC customer, customer, former customer) is typically concerned on the other hand. Hence Art. 15 (1) GDPR does not require tailored information on the data processing.

12. Scope information provided on data processing / link between processing purposes and processed data per purposes (4.3. /112)

The clear wording of Art. 15 (1) (a), (b) GDPR does not require to provide information to data subjects that directly links between processing purposes and data categories processed.

13. Scope information tailored to data subject (4.3. /113)

According to the wording and purpose of Art. 15 (1) GDPR the requirement of informing on the data processing only requires to inform on which data are typically processed in the context of the processes concerning the data subject.

The requirement to tailor the information with view to the actual processing that concerns the respective data subject would constitute a disproportionate requirement that the majority of companies concerned will not be able to comply with.

14. Scope information according to Art. 15 (1) (c) GDPR "data recipients" (4.3. /115)

Art. 15 (1) (c) GDPR clearly indicates [by using the word "or"] that a data controller shall have the right to choose whether to provide information on categories of data recipients or concrete data recipients. Hence this section has to be amended accordingly.

Art 15 (1) (c) GDPR is also not subject to a condition whether the information on recipients is already available at the time of an access request. Hence, this differentiation cannot be stipulated additionally by the EDPB under recital 115.

Art. 13 (1) (e) / 14 (1) (e) GDPR and Art.15 (1) c) GDPR contain the same wording *"recipients and categories of recipients"*. Therefore, the same interpretation must always be applied. Therefore, the above differentiation cannot be interpreted in the wording of Art. 15 (1) (c) GDPR, but Art. 13 (1) (e) GDPR / 14 (1) (e) GDPR. But in reality this differentiation is actually not possible in the constellation of Art. 13, 14 GDPR, since at the time of data collection the data cannot already have been transmitted.

This interpretation is also not contradicted by the fact that recital 63 states that controllers must provide information about "data recipients" and that categories of recipients are not mentioned here. However, the wording of recital 63 contradicts the clear wording of Art. 15 (1) (c) GDPR, which, as said, indicates a right of choice of the controller between informing on data recipients or categories of data recipients.

According to the case law of the Court of Justice of the European Union (ECJ), Recitals are irrelevant if they do not comply with the wording of the GDPR.

The ECJ has commented on the legal quality of recitals of Community legal acts, in particular in its decision of June 19, 2014 (Case C-345/13). Accordingly, the recitals do not have any legally binding effect. Literally, the ECJ stated in the aforementioned decision on the legal significance of the recitals: *"[...], it should be noted that the recitals of a Community act are not legally binding and may not be used either to derogate from the provisions of the act in question or to interpret those provisions in a sense which is manifestly contrary to their wording [...]"* It can be concluded from the

aforementioned case law of the ECJ that, when interpreting rules of a Directive, the recitals may in any case not be used to derogate from the provisions of the wording. Therefore, the normative part of the directive is decisive for the interpretation.

Since violations of the GDPR are subject to fines pursuant to Art. 83 GDPR, the constitutional rule of law *"Nullum crimen, nulla poena sine lege stricta"* applies. This prohibits from applying laws more broadly than described and limited by their clear wording. This consequently requires a restrictive application of Art. 15 (1) (c) GDPR, which must be closely oriented to the wording. The wording of Art. 15 (1) (c) GDPR indicates a right of choice of the controller by the word *"or"*. Hence, the additional criterion of differentiating whether the data have already been transmitted may not be applied to Art. 15 (1) (c) GDPR. The requirement to differentiate whether data is already transferred is not mentioned according to Art. 15 (1) (c) GDPR. Hence the EDPB cannot additionally stipulate this as a requirement.

The purpose of Art. 15 GDPR is to provide data subjects an insight into the data processing in order to enable data subjects to assess the lawfulness of the data processing. In some cases, the information on data categories may be sufficient for this purpose, e.g. naming of processors in the EU. This approach is also constitutionally required, since the mildest means of enabling data subjects to assess the lawfulness of data processing can under certain conditions also be the information on categories of recipients.

According to the legal point of view of the European Commission which is indirectly expressed in the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (in the following called: "SCC") data controller can be entitled to only provide information on categories of data recipients as far as this is appropriate in order to provide meaningful information.

According to section 8.2 (a) (iv) SCC data importer are obliged to *"where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7."* Categories of data recipients can provide meaningful information under certain circumstances when detailed information on concrete data recipients is not necessary or required.

Information on concrete data recipients should also not be required in case this information solely or combined with other information would constitute a trade secret.

15. Scope of information according to Art. 15 (1) (d) GDPR "storage periods" (4.3. /116)

According to its clear wording, Art 15 (1) (d) GDPR does not require to provide information that links storage periods, data categories and processing operations.

Applying the requirement of a tailored information acc. to Recital 113, this would mean to provide information that links storage periods and personal data / processing operations tailored to the data subject. This would result in an effort which the majority of companies concerned cannot comply with.

The complexity of this requirement is likely to cause errors constantly when companies provide data access. This will put them under a severe risk of fines, which is constitutionally unproportionate.

16. Scope of information according to Art. 15 (1) (e) GDPR "data subject rights"

According to the clear wording of Art. 15 (1) (e) GDPR, it is only required to inform on all data subject rights with no regard to which legal basis applies to the data processing that specifically concerns the data subject. Hence, Art. 15 GDPR does not require that the information on data subjects rights is tailored to whether it may apply in view of the legal basis of the data processing concerning the data subject.

17. Scope of information according to Art. 15 (2) GDPR "safeguards" (4.3. /120)

We suggest that EDPB clarifies that the provision of a copy of the contract/SCCs in place between the data exporter and the data importer is not required, as well as on the level of detail which shall be provided regarding the appropriate safeguards in place

18. Different means to provide access (5.2.2. /133)

The EDPB does not take into account the extent to which a data subject may waive the necessary encryption when transmitting his request for information.

This is supported by the fact that the data subject may determine the processing of his or her personal data and must therefore also be able to waive technical measures (as long as no data of other data subjects is affected).

A clarification in this regard would be helpful in practice to clarify the extent to which a waiver is possible and the details if such a waiver is given.

19. Providing access in a concise, transparent, intelligible and easily accessible form using (5.2.3 / 139)

According to no. 139 of the guideline information provided to the data subject must be *"intelligible"* what means that it should be understood by the intended audience. This shall also and in particular apply e.g. to raw data, codes, activity histories etc. In order to meet this requirement, the controller shall take the necessary measures to ensure that the data subject understands the data, for example by providing an explanatory document that translates the raw format into a user friendly form such as explained abbreviations acronyms etc. In application of the EDPB guidelines, this means that copies must not only be provided to the data subject in accordance with Art. 15 (3) GDPR, but that the content must also be explained. However, Art. 15 (3) GDPR only provides for the right to receive a copy of the personal data being processed. The obligation to provide information in a transparent, comprehensible and easily accessible form using clear and plain language only applies to the information provided pursuant to Art. 15 (1). An obligation to prepare the content of the copies, as apparently demanded by the EDPB, results neither from Art. 12(1) GDPR nor from Art. 15 (3) GDPR.

20. "surprising" processing (5.2.4. / 143)

According to the EDPB's comments, processing that "surprises" the data subject should be highlighted, to the extent that the data controller makes use of the possibility of layered approach.

The EDPB's assumption presumes a breach of the Information Obligations pursuant to Art. 13/14 of the GDPR. Insofar as the data subject was informed about the processing in a GDPR compliant manner, he could not be "surprised" by such processing.

Therefore, the Guidelines should be amended or at least clarified with regard to the term "surprise".

21. Complex requests (5.3 /161/162)

The EDPB Guidelines state that *"The mere fact that complying with the request would require a great effort does not make a request complex."*

The examples/criteria given for the assessment of a complex request are not concrete enough. We believe that further and more detailed clarification and examples are necessary to give practical guidance on the question of the complexity of access requests.

22. Exception to the right of access Art. 15 (4) (6.2./172)

Due to sectoral obligations it may not be possible for a controller to provide information to the data subject on the exact reasons why a right of access request may not be complied with, such as fraud and money-laundering prevention related obligations in the banking sector. Controllers cannot tip the fraudster. Thus it should be included in this recital that the provision of such information should be done without prejudice to any applicable legal obligations that the controller has to comply with and that forbid the controller to provide any information on whether personal data is processed and on the reason why the data access request cannot be complied with, as per Art. 23 (1) d) GDPR.

23. Meaning of manifestly unfounded (6.3.1. / 175-177)

We consider that an additional situation of misuse of Art. 15 GDPR by data subjects shall be added to the guidance provided by the EDPB: sometimes data subjects exercise their Art. 15 GDPR rights before data controllers (i.e. banks) in order to obtain copies of documents issued by public bodies (for instance, certified copies of documentation on garnishments like third-party-declarations). These are situations where data subjects requests copies of such documents where such request shall be directed to the public authorities/bodies who issued such documents but the data subject's effort is smaller when requesting them to controllers (i.e. banks) so as to avoid any bureaucracy (i.e. needing to schedule an appointment at the public authority to get a copy of the relevant document).

Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.