11 March 2022

EBF_045564

EBF response to the European Data Protection Board's consultation on the draft Guidelines 01/2022 on data subject rights – Right of access

Key points:

- The European Banking Federation (EBF) welcomes the opportunity to provide a response to the European Data Protection Board's (EDPB) consultation on the draft guidelines on data subject rights – right of access.
- The Guidelines should seek to provide additional clarity to the obligations under the GDPR. However, in several sections, the provisions appear to extend the obligations of the GDPR or seem not align with them. We would welcome clarity from the EDPB to ensure data controllers **adhere to their regulatory obligations, meeting the expectations of both local and other DPAs**, including the EDBP, and to ensure that the industry **delivers to data subjects in a manner that is of benefit to them.**
- In many instances, **a prescriptive approach is taken towards how to implement the right of access.** The GDPR itself provides the flexibility to ensure the specific requests of data subjects are addressed, balancing this with the data controller's ability to deliver, keeping in mind their own internal organisational and technical structure. The Guidelines should not take this away.
- The disclosure of certain data relating to credit scoring or anti-money laundering compliance could impact the ability of banks to meet core regulatory and legal requirements, in particular in relation to preventing and detecting financial crime. Moreover, how an institution performs credit scoring is also an element of competition. **Section 6.2 of the guidance should clarify that, where disclosing certain data to the data subject would prejudice a controller's compliance with legal and regulatory obligations, the controller can rely on the exemption in Article 15(4).**

1. Introduction

We welcome the intention of the EDPB to clarify aspects regarding the key area under data subject rights – the right of access. We would like to recall that the purpose of a data request, as per Recital 63 of the GDPR, as part of Article 15, is to assist a data subject with understanding what personal data the controller holds of them "in order to be aware of and verify, the lawfulness of the processing." The existing obligations under the GDPR **clearly define expectations with respect to data requests, whilst also providing appropriate flexibility to ensure the specific request of the data subject is addressed.** This provides the data controller with the ability to deliver upon the specific request, cognisant of its own internal organisational and technical structure.

While comments on specific sections are provided below, we would like to highlight the following points, some of which are a worrying trend throughout the guidelines.

- **Compliance with the boundaries of the GDPR**

We feel that **the guidelines go beyond the GDPR, presenting an expansive interpretation of the right of access**. This approach poses several risks for data controllers, who would face new burdensome obligations that could **interfere with their implementation of the accountability principle within their organisation**. The guidelines also do not sufficiently take into account the **principle of proportionality**, which applies in relation to other obligations that organisations must adhere to, including transparency and notifications to individuals relating to handling of their data by controllers. It should therefore equally apply to an organisations' obligations in response to data subjects' requests.

This is acknowledged in the Guidelines to some extent but not sufficiently. For example, the **layered approach presented** in the guidelines **could be a positive aspect** but the conditions to apply this approach **are very strict and complex.**

- **Acceptance of the company-specific implementation**

In practice, each controller must consider its means and its IT system before implementing internal rules to answer to data subjects' requests. **This conflicts with the lack of flexibility in the prescriptive approach of the guidelines.** For example, almost all of the data disclosed to the data subject needs to be explained in order to be understandable in a "*concise, transparent, intelligible and easily accessible form using clear and plain language*" (cf. 5.2.1. § 126, 5.2.3 §137). If the requested data is stored in hundreds of pages of log files, controllers may need to take additional measures to facilitate the understanding of the log files in addition to just providing the log files. This obligation amounts to a material extension of GDPR Article 15 (which contains no explicit obligation to "explain" personal data).

- **Conflicting legal obligations**

Paragraph 96 lists the types of data to be provided by controllers and includes "*data inferred or other data, rather than directly provided by the data subject (e.g., to **assign a credit score or comply with anti-money laundering rules**…*". Sharing this type of (very sensitive) data poses serious risks to banks: how a bank assesses the creditworthiness of a client while calculating the risks attached to granting a credit facility is not shared. If this was the case, competition among banks would be impeded. Meanwhile, certain aspects of AML compliance are under a duty of secrecy. Divulging information for example on whether a transaction is suspicious or that an institution is investigating it constitutes a breach of AML legislation.

Furthermore, it may **conflict with sectoral regulation and its respective implementations at national level.** We would therefore like to remind that the guidelines state in paragraph 47 that ***"responding to requests shall be exercised by the controller in accordance with sectoral or national rules"*** which by extension **should include anti-money laundering compliance and creditworthiness**

assessment. It should also be noted that sectoral regulation does not fall within the competence of Data Protection Authorities.

Regarding the **right of access and the rights of freedom of others,** the EDPB seems to make a distinction between article 15(4) and article 15 (1) lit. a-h. In the first case, the right of access shall not adversely affect the rights and freedoms of others and in the second case, this limit should not be applicable to the additional information on the processing. We would also suggest that the wording in the summary *"According to Art. 15(4) the right to obtain a copy shall not adversely affect the rights and freedoms of others"* is updated to "*According to Art. 15(4) the right* ***of access*** ~~***to obtain a copy***~~ *shall not adversely affect the rights and freedoms of others*."

- **Identification of the person requesting the information & reasoning of the request**

Non-disclosure of personal data to unauthorised persons is one of the main data protection principles. **How should the guidance be understood when it says that the right of access "*should not be interpreted overly restrictively and may include data that could concern other persons too*" (p.3).** This position seems to run counter to the GDPR itself and does not consider the high risk posed to infringing the rights and freedoms of the other data subject.

When it comes to the **reasoning of the request**, in the opinion of the EDPB, the "*data subject does not have to give reasons for the access request"*. In our view, **the controller needs to have confidence that the particular request in fact is a data subject request**. In practice, banks receive many different requests from clients. Almost all data of natural persons processed by the banks can be considered as personal data, therefore, almost all requests relate to the processing of personal data in one or another aspect. Banks also receive mixed requests, e.g., requests containing a question about some transaction in the account and data recipients.

- **Misuse of the right to information**

Taking into account that access to data is free under the data subject request concept, in practice, data subjects can misuse this possibility and try to access particular data not for the purpose of verifying the legitimacy of their data processing, but, e.g., to provide data to some public institutions or to collect evidence against the responsible body for court proceedings in civil and labour disputes. **A data access request should not be exercised as a fishing expedition.**

In practice, it sometimes is difficult to understand and decide how a particular request should be treated and what would be of most use of to the data subject. **Engaging with the individual to clarify the purpose and reasoning of the request could be very helpful in such cases for both the controller and the data subject.**

2. Section 2: Aim of the right of access, structure of article 15 GDPR and general principles

a. Aim of the right of access (2.1)

Individuals too often consider these rights to be unbounded, which can result in overwhelming organisations with requests. **Some requests are able to disrupt core business activities while not offering the best results to individuals when considering the rationale behind a data subject access request**. With a clearer indication of **what constitutes an abusive request,** organisations could better allocate their resources and not waste them in trying to resolve excessive data subject access

request cases. This would enable a more efficient implementation of data subject access requests for the benefits of the majority of individuals that are exercising their rights in good faith.

Moving to specific points in the guidelines, **Paragraph 13** states that "*the controller should not deny access on the grounds or the suspicion that the requested data could be used by the data subject to defend themselves in court in the event of a dismissal or a commercial dispute with the controller*". However, the Guidelines lack a consideration of the unexpected outcomes this could produce. **A data access request should not be exercised as a fishing expedition** to discover information for a later proceeding or to uncover incriminating or newsworthy evidence.

It should therefore be clarified in the guidelines that the sole purpose of the right to information under data protection law is to **enable the data subject to verify the accuracy of stored data and the permissibility of data processing**. However, if the data subject is pursuing completely different purposes (e.g. collecting evidence against a company in a civil dispute in court), then he or she cannot assert a right to disclosure under Art. 15 GDPR. **Instead, any claims for information by a plaintiff in civil court proceedings must be governed by the rules in the respective civil procedural law in the respective EU member state.**

Finally, more examples are needed from the EDPB regarding exceptions relating to a conflict between employer and employee – which should be of interest to all sectors. There are limits to what an employer must give out, for example material that concern strategy in court proceedings. Such examples must be mentioned as well to give more nuance. One example is not sufficient.

b. Structure of Article 15 GDPR (2.2)

Paragraph 22 states that "*The controller must ensure that the first copy is free of charge, even where it considers the cost of reproduction to be high*". However, this statement goes beyond GDPR Art.12.5(a)(g). Why should a high cost of reproduction not be considered as "constituting a disproportionate effort". Without further substantiation, we would suggest to delete the wording:

*The controller must ensure that the first copy is free of charge, **~~even where it considers the cost of reproduction to be high"~~***.

Meanwhile, we welcome that **paragraph 23** confirms that "*At the same time, the **obligation to provide a copy is not designed to widen the scope of the right of access**: it refers (only) to a copy of the personal data undergoing processing, not necessarily to a reproduction of the original documents (see section 5, para. 150)*". To make this even clearer, we would suggest to add the clarification in bold to provide legal certainty for data controllers:

*"At the same time, the obligation to provide a copy is not designed to widen the scope of the right of access: it refers (only) to a copy of the personal data undergoing processing, not necessarily to a reproduction of the original documents **or a copy of the software where the data is contained."***

Paragraph 26 writes that "*In spite of this broad understanding of a copy, and regarding that it is the main modality by which access should be provided, under some circumstances other modalities could be appropriate. Further explanations on copies and other modalities of providing access are given in section 5, in particular 5.2.2 and 5.2.5".* It is important to emphasize **that the right of access to data pursuant to Art. 15 GDPR should not be confused with the right of access to banking account documents.** Data subjects could confuse "copy of data" as equivalent to "copy of document" that contains personal data, even of an accounting nature. In any case, in the subsequent parts of the document, this difference is confirmed, as already widely done by Data Protection Authorities.

Under **paragraph 28**, Example 2, we welcome that the request referring to the same data and the same period **should be regarded as a request for an additional copy**.

Regarding providing further copies, **paragraph 31** notes that "*In case the controller decides to charge a fee, the controller should indicate the amount of costs it is planning to charge to the data subject in order to give the data subject the possibility to determine whether to maintain or to withdraw the request.*" This brings up the question of, what happens if the data subject does not provide feedback or does not accept the expected cost? We would therefore recommend changing the wording to a recommendation:

*In case the controller decides to charge a fee, the controller, **if possible,** should indicate the amount of costs it is planning to charge to the data subject in order to give the data subject the possibility to determine whether to maintain or to withdraw the request. **In general, the controller shall have no obligation to satisfy the request.**"*

However, the guidelines do not deal with specific copy issuance claims under EU law. Under the revised Payment Services Directive (PSD2), the bank can charge the customer for providing duplicates of account statements. As a lex specialis, this regulation overrules Art. 15 of the GDPR.

c. Completeness of the information (2.3.1)

As a general remark, we would like to remind that in cases where the right to data protection runs up against other fundamental rights, the CJEU has held that it is necessary to **strike a "fair balance"** between the various competing interests. **In other words, a data subject access request should not require the imposition of an "excessive burden" on the data controller**.

- For example, in assessing the data that is to be produced in response to a data subject access request, **data controllers should be able to also have regard to whether or not the data is in a retrievable form** (e.g. offline log-level information stored in a specific system, as opposed to online personal data that is stored on an individual level) and consider the resources and the costs incurred by the data controller in retrieving certain information. In these situations, the data controller should be able to ask the data subject to restrict the request.
- Developments at national level have also begun to acknowledge the need for a balance. For example, in the field of collaboration with the Judicial Authority in Italy, the need to limit the extent of the requests for assessments made to banks has been recognized for a long time. It does not make sense that in terms of the right of access to personal data, such considerations are not taken into account.

Moving to the specific provisions, the first sentence of **paragraph 35** notes that "*Data subjects have the right to obtain, with the exceptions mentioned below, full disclosure of all data relating to them*"; yet not all data can be disclosed depending on where they are held. For example, data held on emails may contain different information, covering several topics or including information about other individuals. It can be very difficult to manually "anonymize" or hide certain information to protect the privacy of other individuals identified in that data (e.g. employees). As a result, it is important that **a case-by-case assessment is undertaken for requests;** this also enables to take into account specificities at national level, such as labour regulation (which can cover access to emails, see in this regard paragraph 168 of the guidelines, or when exceptions of Art. 23 of the GDPR apply, such as the rights of others).

Paragraph 35, point b brings up several considerations:

1. "*In situations where the controller processes a large amount of data concerning the data subject, the controller may have doubts if a request of access, that is expressed in very general terms, really aims at receiving information on all kind of*

data being processed or on all branches of activity of the controller in detail." There are occurrences when **data subjects do not have the contractual right to the documentation of the business relationship**, **but they try to access it via right of access.** As the situation described is critical for this topic, we would recommend stating in the guidelines that **via the right of access the data subject can access *only personal data* and *not documentation regarding the business relationship.***

2. "*The controller shall at the same time give meaningful information about all the processing operations concerning the data subject, like different branches of its activities, different databases etc."* This is excessive and is not contemplated under the GDPR. **Banks have many processing purposes** (e.g. based on legal obligation) that are already summarised in the privacy notice. Should 'meaningful information' be understood as detailed information regarding specific data processing activities? It should be noted that in context where controllers operate in various technical environments (especially established at different times before May 25, 2018) and with many programs and products, this will likely result in an effort similar to the one requested for responding to the generic data access request itself. **In such cases, therefore, controllers should be allowed to share with the data subject a link to their privacy notice, where the data subjects will find sufficient information to submit a more specific request.**

   This approach, while being more pragmatic and efficient by enabling the individual to get the right information at the right **time would not limit the essence of Article 15 to the boundaries of Article 12.** This interpretation is confirmed by a decision of the DPA Germany regarding "Best Practices on Data Subject Rights" dated 08/16/19, which states that, in certain cases, the right to access does not establish an individual right to a copy [of their data], provided a well-structured summary about the processing would satisfy the requirements of Articles 12 and 15. Such a summary would inform about the processing in a precise, transparent and easy to understand manner, allow individuals to submit a subsequent request, a complaint, a claim for damages or lodge a complaint with the DPA, and would minimize the risk of disclosing third party's information while addressing the access request.

3. **We note that good faith communications between the controller and the data subject about the scope of the data being sought are mutually beneficial.** Often, data subjects in fact want specific information, rather than a full record of all personal data, despite lodging a subject access request. If the controller can clarify the specific area of interest of the individual, this will allow the controller to respond more quickly and will save the individual from having to review, store and dispose of large amounts of personal data that is not of interest. Of course, the controller should not pressure or manipulate the individual to narrow a subject access quest.

   We therefore recommend amending the guidance to **state that controllers can communicate with data subjects to clarify the scope of data sought, whether or not there is an exceptional situation, provided this is done in good faith and without placing undue pressure on the individual**. This two-step approach is used in the banking sector and has proved to be beneficial for both the data subject and the controller. Overwhelming the data subject with a lot of information right away does not help with the aim at providing the information in a friendly manner.

4. "*…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***". The last part of the sentence is, in our view, disproportionate. We therefore suggest adding the following qualification:

"*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* ***unless it could constitute disproportionate effort for the controller. If exceptions provided under local law apply, the data controller will not provide access to those data that fall under the exceptions".***

Regarding **paragraph 36** and the correctness of information, it is unclear on what basis of the GDPR the draft guidelines state that the right of access implies an **obligation to give information about data that are inaccurate or about data processing which is no longer lawful**. This interpretation is excessive in our view and sounds like a duty to self-incriminate. This duty to inform makes no sense from two points of view.

- If this controller already knows that data is incorrect or that permission to process data is missing, then this data must be deleted by the controller themselves.
- If it is the data subject who realises that data is incorrect or that the reason for permission has ceased to exist, he or she will inform the controller of this and the controller will delete the data.

The data controller should simply provide access to what falls within the scope of the right of access. This paragraph only adds confusion. We suggest to delete it.

Meanwhile, under paragraph 38, the following conditions could be difficult to satisfy "*In the case of shorter retention periods than the timeframe to answer imposed by Art. 12(3) GDPR, the timing to answer the request should be adapted to the appropriate retention period in order to facilitate the exercise of the right of access and to avoid the permanent impossibility of providing access to the data processed at the moment of the request*". Organisations may have specific retention policies and it is important that their normal functioning is not disrupted every time there is a right of access request. We would therefore recommend to indicate this as a good practice, rather than a requirement. It should also be clarified that this practice should not mean preservation of the data by the data controller in case the data subject would make an additional request under Art. 18(1)(c).

d. Compliance with security measures (2.3.4)

It would be helpful if the Guidance can clarify that it is acceptable to require a data subject to register (via username and password) for a secure delivery mechanism. For example, in the case where there are large volumes of data, a controller will need to provide access via channels other than encrypted email; registration with a secure portal is an effective way to provide access safely.

3. Section 3: General considerations regarding the assessment of access requests

a. Analysis of the content of the request (3.1.1)

Under paragraph 45, the EDPB states that pseudonymised data should be in the scope of the request. We would welcome a clarification **on how, in practice, such a copy of the data shall be provided to the data subject.** If the controller has pseudonymised data, shall it inform that for the particular purpose, a particular data subject's name and surname is pseudonymised by a code? How would such information help the data subject to reach any conclusions on the lawfulness of processing?

Furthermore, we encourage the EDPB to **provide a balanced approach** on this point so that organizations are not discouraged to implementation of privacy preserving techniques. In the last years, organisations have invested resources in developing and

using meaningful privacy safeguards like pseudonymization, where appropriate, which can make the identification of individuals more difficult. In these cases, and particularly where individuals provide additional information on their identity, Article 11(2) should not be narrowly construed to require companies to undergo further intensive manual diligence in all cases to try to re-identify individuals. **This may have the adverse effect of not rewarding companies that proactively invest in privacy enhancing techniques.**

Also, for organisations to comply in practice with this request they will need to ask to the individual to provide several data elements (like cookie ID, IP address, Bank account number, credit card number, etc.) that will allow the data controller to link to pseudonymised data that they have. By asking for data elements **the data controller will be violating the data minimisation principle set in art. 5(1)c GDPR as well as the principle of integrity and confidentiality (Art. 5(1)f GDPR since it could be impossible for the data controller to identify the data subject based on some data elements**.

We also note that if the reference to pseudonymisation is coupled with the commentary on providing the data in an intelligible format, this could lead to data subjects requesting a reversing of pseudonymisation which would undermine the purpose of pseudonymisation and result in further data processing activity. If pseudonymisation has been adopted to protect the data against unauthorised use, revering pseudonymisation of the batch of data of the data subject will entail security risks.

Under **paragraph 48**, the EDPB writes that "*If the controller has doubts as to which right the data subject wishes to exercise (…….). Such correspondence with the data subject shall not affect the duty of the controller to act **without undue delay***". Flexibility should be introduced regarding the response time, given that the response of the data subject is needed to proceed. In addition, according to the EDPB, "*…, in case of doubts, if the controller asks the data subject for further explanation and receives no response, the **controller should interpret**, bearing in mind the obligation to facilitate the exercise of the person's right of access, **the information contained in the first request and act on its basis***". The guidance to interpret the request first does not seem efficient in our view and could create confusion. The data controller should wait for the data subject's response; as mentioned above, flexibility should be introduced in this case as well as a balance between the data subject's right and the controller's duties.

b. Form of the request (3.1.2)

Paragraph 55 includes the following: "*However, if the data subject sends a request to the controller's employee who deals with the data subject's affairs on a daily basis (single contact of a customer, such as e.g. personal account manager), such contact should not to be considered as a random one and the controller should make all reasonable efforts, to handle such a request so that it can be redirected to the contact point and answered within the time limits provided for by the GDPR.*" Compliance with the response times provided for by the legislation **can be more complicated when requests are dispersed in the context of complex organisations;** this should be recognized in the guidelines.

Furthermore, this guidance seems to contrast with the points in paragraphs 54 on the recipients of the access requests. If controllers have to accept and process requests received on the personal mailboxes of employees who are not necessarily responsible for such access requests, the EDPB should clarify that in these very cases it is reasonable that data subjects are not informed about alternative ways to submit the request if the employee is absent. **This is simply because those employees would not be aware that they could be recipients of data access requests.**

In addition to recognizing that response times provided by the legislation can be more complicated when requests are dispersed in the context of complex organisation, we would add in the text that **when the controller has established a dedicated channel for**

submitting requests and has communicated that to its data subjects, e.g. in the privacy notice, data subjects shall submit their requests via those dedicated channels. This is essential due to:

- The limited time to respond to requests: e.g. if a request arrives to an employee of a bank and was not submitted through the official channel, this could mean a struggle to react in time. In big organisations, such a request could get lost or not be understood as an access request.
- The employees that service the established channels are the dedicated experts. Others may not be knowledgeable of how to proceed or not deal with data subject requests every day.

The example following **paragraph 56** is not consistent with paragraph 54 as the controller has provided a specific address for requests intending data subject's rights and the controller is not even entitled to extend the responding period.

Under **paragraph 57**, the EDPB "***considers as good practice*** *for the controllers to confirm receipt of requests in writing, for example by sending e-mails (or information by post, if applicable) to the requesting persons confirming that their requests have been received and that the one-month period runs from day X to day Y.*" While we understand that this is only a "best practice", it could lead to unnecessary complications. It cannot be carried out via an automatic response system since, in practice, communications of various kinds are received at the addresses (in particular email and / or certified e-mail addresses), often not within the competence of the structures supporting the DPO within an organisation.

As a result, in these cases, in the event of an automatic reply, the senders would receive **a message inconsistent with the nature of the request which, in fact, does not fall within those relating to the exercise of rights as regulated by Articles from 15 to 22 of the GDPR.**

In any event, we encourage the EDPB to clarify that giving access to this information - specific timeline to respond to a request - through channels other than emails or post (for example a portal where the data subject can submit and check the status of the request) would meet the same objective.

c. Issues with establishing the identity of the person making the request (3.2)

In general, the guidelines give the impression that controllers are accused of setting too high requirements for the identification of the applicant. This is surprising, because **reliable identification of the applicant is very important in order to avoid providing information to unauthorised persons. The identification procedure which the controller chooses is first and foremost a matter of their responsibility.**

The example below **paragraph 64**, which concerns data processed in connection with the video surveillance of a building, states that *if the requesting person indicates a particular day and time when the cameras may have recorded the event in question, it is likely that the controller will be able to provide such data (Art. 11(2)).* **It also assumes that the requesting person will be the same (and the only person) to request this**. This situation is likely to raise several difficulties; we would therefore suggest removing the example or at least add to the text that:

"it is likely that the controller will be able to provide such data (Art. 11(2)), ***but only if the controller can secure that the identity of the requesting data subject is the same as on the video surveillance."***

d. Proportionality assessment regarding identification of the requesting person (3.3)

Under **paragraph 70,** the text states *"that the controller should implement an authentication (verification of the data subject's identity) procedure in order to be certain of the identity of the persons requesting access to their data, and ensure security of the processing throughout the process of handling an access requests in accordance with Art. 32, including for instance a secure channel for the data subjects to provide additional information."* However, this could give rise **to several risks and inconsistencies.**

- It should be reminded that according to Art. 12(6) GDPR, the controller must authenticate the data subject's identity only if they have reasonable doubt about it.
- The text **does not specify when the data controller / data processor should prepare an "authentication procedure" for the interested party** (and a secure channel for the exchange of information) preparatory to the analysis and processing of requests for access to the personal data.
- In the banking sector, this reading could be further limiting given that, formally, there are authentication procedures linked to Home banking services which, in any case, are not widespread on all customers. See also subsequent paragraphs 71 and 72. It should also be taken into account that **other regulations also require banks to correctly identify a person who is carrying out an operation (e.g., Anti-Money Laundering obligations)** and to keep this information for any subsequent needs that could also be expressed by the competent judicial authority.

In the same section, **paragraph 74** notes that "*Taking into account the fact, that many organisations (e.g., hotels, banks, car rentals) request copies of their clients' ID card, it* ***should generally not be considered an appropriate way of authentication****."* Alternative security measures are then proposed. We would like to recall that the GDPR **does not specify what is or is not an "appropriate way of authentication"** and that asking for an ID card by a bank, **given the nature of that data that is to be provided through an access request, can be considered as an appropriate way of authentication.**

- Organisations, based on the accountability principle, are free to decide what are the appropriate ways of authentication, **taking into account their local laws and their other obligations to authenticate the persons** through, for example, the KYC processes. This also applies to considering national laws and practices within different sectors.
- For example, with express reference to banks, the request to attach a copy of the identity document to requests for access to personal data constitutes the main form of authentication of the interested party and of the exact correspondence between the person making the request for access to personal data and the personal data themselves. Furthermore, under paragraph 77, **the EDPB acknowledges that the use of the ID card may be justified in certain contexts,** when special categories of data are processed or in the case of processing of personal data which may pose risks for the data subject (medical or health data). When a financial institution screens its customers against a credit reference database or fraud database, this is likely to result in a high risk for the purposes of GDPR, as outlined by the EDPB in its WP 248. **Therefore, it seems important to be able to continue to ask for a copy of the ID card in the event of an access request**. We would also welcome examples of what technical and organisational measures could be considered appropriate when receiving an ID card via e-mail.

Staying with **paragraph 74,** the following sentence mentions *"Alternatively, the controller may implement a quick and effective security measure to identify a data subject who has been previously authenticated by the controller, e.g. via e-mail or text message*

containing confirmation links, security questions or confirmation codes". Yet this may not be a secure way to proceed. Personal emails and text messages may be hacked and, the wording implies that organisations already have the email addresses and telephone numbers of the data subject.

Moving to **paragraph 76**, the EDPB states that "*to follow the principle of data minimisation the controller* ***should inform the data subject about the information that is not needed and about the possibility to blacken or hide those parts of the ID document****. In such a case, if the data subject does not know how or is not able to blacken such information, it is good practice for the controller to blacken it upon receipt of the document, if this is possible for the controller, taking into account the means available to the controller in the given circumstances*". We have significant reservations on this provision. It is too complex and even impossible to put in place. This would result in each company having to explain to the data subject what data should be redacted in identity documents. Moreover, in the financial sector, where, as we stated before, anti-money laundering legislation obliges the identification of clients, **copies of such IDs need to be kept for evidence and fraud fighting purposes.** Obfuscating the picture is therefore not possible since it contravenes this essential legitimate interest.

It should also be considered that many banks have international clients with different IDs. As a result, it would become even more difficult to tell the data subject which parts of their ID to obscure. We therefore recommend **to delete this paragraph from the guidelines or amend it in such a way that it recognizes that in certain sectors (such as banking) this should not apply.**

We are also concerned about the **example under paragraph 76 relating to the bank branch which asks for a notarised certification of identity.** This is **not a common or practical solution**. We would suggest the EDPB to either provide other solutions or to, alternatively, delete the example.

On **paragraph 78,** the guidelines state that "*taking the above into account, where an ID is requested (and this is both in line with national law and justified and proportionate under the GDPR), the controller must implement safeguards to prevent unlawful processing of the ID. Notwithstanding any applicable national provisions regarding ID verification,* ***this may include not making a copy or deletion of a copy of an ID immediately after the successful verification of the identity of the data subject****."* However, the highlighted provision poses the risk of compromising, at a later stage, a verification of the correct identification of the interested party carried out during the analysis of the access request. The same concern applies to the good practice recommended at the end of the paragraph.

Finally, the EDPB might clarify two additional, general aspects regarding the identification of the data subjects by obtaining a copy of an ID. First, in many instances, this is the *preferred method of authentication for consumers*, despite the possibility to be authenticated in other ways. **The EDPB should clarify that controllers can allow data subjects to identify themselves by providing a copy of an ID if they prefer**, in situations where the controller offers an alternative means of authentication.

Secondly, we would like to stress that the mere note that an ID was verified is not sufficient for controllers to defend themselves in Court actions. Therefore, the industry needs to be able to retain and safely keep a copy of the ID with which the client has been identified and verified.

e. Requests made via third parties/proxies (3.4)

Paragraph 80 describes the requirements for a third party to make a request on behalf of the data subject. In our view, in order to exercise data subject rights, it is not enough to be generally authorised (**e.g., represent rights in the bank**) **but the authorisation**

to exercise data subject rights shall be specifically formulated in the power of attorney.

The EDPB should also take into account that **the legitimacy of the third-party is highly dependent on national laws** which go beyond the knowledge that any Data Protection Office(er) or dedicated unit might have (i.e. in terms of validity of the power of attorneys). This is an additional burden for large organizations operating in different member states as it requires the analysis of various local requirements and sometimes hire/task experts on the matter. **The EDPB should clarify that in these cases, responses could be considered particularly complex and justify an extension of the deadline**.

Furthermore, section 3.4 seems to assume that data access requests will rarely be lodged by third parties, and that this will be done on a small scale by lawyers, legal guardians and other such individuals. In practice, however, there is **a growing trend towards the use of bulk data subject access requests by litigation and complaints management companies, as a part of pre-complaint or pre-litigation information gathering, or indeed as a part of a 'fishing exercise'** to search for potential avenues for litigation. Some of our members receive 1000s of such data access requests per month. **While legally permitted under GDPR, this practice poses risks for data subjects, including in particular data minimisation risks.** By using data access requests, complaints management firms collect large amounts of personal data not required for the complaint, creating data security risks and temptation to re-use the data.

In some cases, these data subject access requests are speculative, with only a minority relating to genuine customers or former customers of the controller. Nonetheless, the controller needs to conduct a search for the customer across its systems, which can be a complex and lengthy exercise. This creates significant administrative burden for the receiving controller, reducing resources available for responding quickly to more genuine, good faith data subject access requests.

More broadly, there are issues with complaints management firms not being transparent with customers about their intentions and the scope of data they will obtain, when seeking the authorisation to lodge a data subject access request on the individual's behalf.

Finally, we note the extreme case of claims management firms sometimes threatening financial services firms with data access requests. For example, in one instance a claims management firm wrote to a range of banks and asked for information, stating that if the information was not supplied, it would lodge 1000s of subject access requests, already authorised with its clients.

We do not consider that the data access right was intended for use as a pre-litigation tool, or as a means to create leverage over other firms. We therefore recommend clarifying in the guidance that, **when a data controller receives a data subject access request from a third party, it can consider the conduct of the third party when assessing whether the 'excessive' exemption applies.** This is consistent with the approach in the guidance in paragraph 188.

Separately, some of the third-party services that lodge data subject access requests on behalf of others require a controller to register and sign up to their website or service before the request can be fully accessed. In some cases, the controller is instructed to pay a fee in order to access the request in full. The guidance should clarify the controller cannot be compelled to register, sign up or pay a fee and where a third party tries to lodge a request in this manner, the request is not valid.

4. Section 4: Scope of the right of access and the personal data and information to which it refers

a. Definition of personal data (4.1)

We have **significant concerns with paragraph 96** and the **types of data listed to be provided by controllers**, as this list of data is **not consistent with trade secrets or some national laws**. These include the following:

- Special categories of personal data as per Art. 9 GDPR;
- Personal data relating to criminal convictions and offences as per Art. 10 GDPR;
- 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);
- **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);

The list provided by the EDPB implies that a case-by-case approach to such data disclosure would be required and this should be reflected in the Guidelines. **Creating a generalized obligation for controllers to share all the data being listed is concerning** for two main reasons.

1. **Data such as logs, traces, system data that may be tied to a user account are irrelevant for data subjects in most cases.**
2. **Disclosing this type data to individuals (such as for instance internal identifiers) may also have security implications for the organisation and for other individuals**. For example, for personal data relating to criminal convictions and offences as per Art. 10 GDPR, in the case of bank investigations carried out by the competent investigative authority, in many cases a specific obligation of confidentiality applies, the failure of which could result in criminal consequences for the bank's staff when they bring them to the attention of the data subject in the face of a data request.

The categorization of "data inferred from other data" is particularly concerning, mentioning **two very sensitive areas for a bank's activities – access to credit and compliance with anti-money laundering (AML) obligations**. These categories of data are not currently provided in the feedback usually formulated to interested parties, also considering that, even if provided, **the data may not be comprehensible or actionable to the data subject.** Furthermore, providing this type of data can conflict with specific provisions of sectoral legislation, notably the Consumer Credit Directive (CCD)[1] and the Mortgage Credit Directive (MCD)[2], and could compromise bank's ability to meet anti-money laundering obligations under the relevant legislation, as well as conflict with implementations at national level.

- **Assigning the credit score:** According to Art. 9, point 2 of the CCD, "*If the credit application is rejected on the basis of consultation of a database, the creditor shall inform the consumer immediately and without charge of the result of such consultation and of the particulars of the database consulted...*" The obligation is to inform the consumer about the result but **not about the specific information contained in the database**. This provision applies to all consumer credits when

[1] Directive 2008/48/EC of the European parliament and of the Council of 23 April 2008 on credit agreements for consumers

[2] Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property

the request for credit is denied and the credit provider had consulted a database. The relevant provision in the MCD is Art. 18, point 5, letter c) which states that "*the credit application is rejected the creditor informs the consumer without delay of the rejection and, where applicable, that the decision is based on automated processing of data. Where the rejection is based on the result of the database consultation, the creditor shall inform the consumer of the result of such consultation and of the particulars of the database consulted*". As in the CCD, the obligation is not to disclose the algorithm and the score given to consumers.

Furthermore, Art. 14(f) GDPR, states that the *existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, **meaningful information** about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*". The focus is on meaningful information.

- **Compliance with anti-money laundering rules:** The right to the protection of personal data **requires a balance and a reconciliation with respect to public interests having general relevance and scope**; therefore, under certain conditions, it is foreseen for member states to adopt legislative provisions aimed at limiting certain obligations and rights, if such limitation constitutes a necessary and proportionate measure in a democratic society for the safeguarding of important specific interests, including public security and the prevention, investigation, detection and prosecution of crime or execution criminal sanctions, including the safeguarding against, and the prevention of, threats to public safety. This incudes, for example, the context of combating money laundering (Recital 19 GDPR, Art.23 GDPR).

  It is also important to **consider how AML legislation has been implemented at national level**. For example:

  - Italian law limits the right of access in case of data necessary for AML compliance and, in transposing the European anti-money laundering Directives, has followed up the "communication prohibitions" contained in them referred to, in particular by providing for the prohibition of communicating to the customer or third parties the successful Reporting of Suspicious Transactions (Article 39, Legislative Decree 231/2007[3]).
  - Article 5.2 (2) of the Anti-Money Laundering Legislation in Latvia specifies that the subjects of the Law … shall not provide information to the data subject regarding processing of data performed in the field of the prevention of money laundering and terrorism and proliferation financing, except for the publicly available data[4].

Given the above, it is shown that the generic provision of communication to the interested party of "inferred data relating to compliance of anti-money laundering regulations "could generate interpretative complexity in the task of maintaining the balance between prohibition of "disclosure" imposed on the intermediary and right of access and "transparency" guaranteed to the interested party.

If the "inferred data" is intended to include "only" the risk profile assigned to the customer (and not the logic underlying this assignment), **it is believed that even this information could hypothetically give notice to the interested party of the notification of a suspicious transaction** (in particular where the PDR communicated was 'High').

[3] LEGISLATIVE DECREE 21 November 2007, n. 231 Implementation of Directive 2005/60 / EC concerning the prevention of the use of the financial system for the purpose of money laundering and terrorist financing as well as Directive 2006/70 / EC which provides for its implementation measures.

[4] https://likumi.lv/ta/id/178987-noziedzigi-iegutu-lidzeklu-legalizacijas-un-terorisma-un-proliferacijas-finansesanas-noversanas-likums

In light of the above, **we would recommend removing the refence of "assign a credit score" and "comply with anti-money laundering rules" under the "Data inferred from other data". At a minimum, the guidance should note that there may be member state laws that limit the disclosure of these kinds of data, as permitted under Article 23 GDPR.**

The same concerns we flagged above also apply to **paragraph 98,** which indicates that "*in case of an access request and unlike a data portability request, the data subject should be provided not only with* ***personal data provided to the controller in order to make a subsequent analysis or assessment about these data but also with the result of any such subsequent analysis or assessment*****."** If the aim of the GDPR is to allow the data subject to verify the lawfulness of the processing and the accuracy of the processed data, how it will be possible to do the assessment of derived or inferred data without also analysing the logic of the analysis carried out by a bank, for example.

This would mean having to reveal to the data subject logic, evaluation algorithms that must remain confidential also in consideration of the fact that, almost certainly, they would not be comprehensible to the data subject. This seems to be in **conflict with paragraph 166** "***That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software."***

Article 15 (4) and article 23 of the GDPR refer to the rights and freedoms of others. We are concerned with the **example in paragraph 95**, especially with the following sentence "*Moreover, the controller needs to provide the data subject with the summary of the interview,* ***including the subjective comments*** *on the behaviour of the data subject the HR officer wrote during the job interview*". Whereas there the data subject - in this example, the applicant - is entitled to obtain information on a decision of the data controller, employees (the HR officer in the example) should be able to put their thoughts on internal notes, memos and internal analysis without these having to be disclosed to the data subject.

On the one hand this is in line with the CJEU, Joined Cases C-141/12 and 372/12, YS and Others, that an analysis does not constitute personal data. On the other hand, and in addition, it should be noted that the disclosure of such personal, subjective thoughts, especially when they are not part of a final decision affecting the data subject (the applicant in the example), would affect the HR officer's right and freedom to order thoughts and impressions before a final conclusion is reached.

In **paragraph 97** we would welcome a clarification on if the following guidance applies to documents such as office forms, family books, insolvency proceedings and vulnerable customers: "*personal data which are contained in paper files as part of a filing system, or which are intended to form part of a filing system, are covered by the right of access in the same way as personal data stored in a computer memory by means of binary code, or on a videotape.*"

Under **paragraph 99** the EDPB writes about selecting what constitutes personal data and not. We find this challenging and the explanation offered in the guidelines is too abstract to be of any guidance, **specifically where to draw the line about "inextricably linked with personal data".** For example, for banks, a product comes with a set of agreement terms, such as credit limit, approval date, interest rate, which T&C that apply, applicable SEKKI, etcetera. Would all of this constitute personal data? We can in fact relate this to a specific customer, but we would not classify this as data to give out, it is more product related than customer related. Therefore, developing further the idea of "inextricably linked" is needed in our view.

b. The personal data the right of access refers to (4.2)

We suggest providing an exemption under **paragraph 104** in the case of access requests made for joint/shared accounts to avoid having to anonymize all the documents which could include references to the other account holder.

In **paragraph 105**, which takes the case of identity theft, the EDPB notes that "*even after the controller learned about the identify theft, personal data associated with or related to the identity of the victim and therefore constitutes personal data for the subject."* However, from a bank perspective, **fraudulent activities need to be managed separately and not to be merged together with the right of access according to GDPR**. For example, if a victim of fraud asks his/her bank for a recording of the fraudulent phone call made to the bank, this would normally be considered personal data of the fraudster and therefore not available to the fraud victim. The Guidelines should recognize these different practices.

In cases it is considered a right of access, we would also appreciate further clarification on the following questions:

- What would be considered an appropriate way of authentication (e.g. police report and ID)?
- What personal data should be provided? Even though there is a link with name and surname there could also be data from third parties (i.e. email, telephone number).

On the topic of **distinguishing archived personal data from back-up data**, as covered in **paragraph 108**, the guidelines state that "*with the aim of being transparent to the data subject that exercises their right, a log of deletions in the live production system may enable the controller to see that there are data in the back-up which are no more in the live system as they have been deleted shortly, which has not yet been overwritten in the back-up."* This control is considered almost impossible to carry out and is directly dependent on the moment in which the analysis of the request is started which, although obvious, may not coincide with the moment of its fulfilment in consideration of the average time required for processing the request. It is very complicated to restore backup and regular teams dealing with handling data subject requests and DPOs, usually, do not have access to back-ups.

We note, as per **paragraph 109** of the draft Guidelines, that where a further access request is made by a data subject the "*controller **should not inform the data subject only on the mere changes** in the personal data processed or the processing itself since the last request, unless the data subject expressly agrees to doing so*." We would welcome the EDPB's opinion on whether this aligns to Recital 63 of GDPR, as part of Article 15, which calls out that a data request should seek to assist a data subject with understanding what personal data the data controller holds of them, "in order to be aware of, and verify, the lawfulness of the processing." Depending on the nature of the relationship between the data subject and data controller, as well as the volume of personal data that may be obtained since the previous data request was made, **we believe it may not best serve the data subject to provide a full copy of all personal data versus the specific amendments since the previous/ prior data request(s).**

When recommending informing the data subject as to the applicable legal basis for each processing operation, **paragraph 112 goes beyond the scope of Art.15(1) GDPR.** We would recommend referring the data subject to the Privacy/Data Protection notice instead. The EDPB also states that the "*Information on the purposes according to Art. 15(1)(a) needs to be specific as to the precise purpose(s) in the actual case of the requesting data subject. It would not be enough to list the general purposes of the controller without clarifying which purpose(s) the controller pursues in the current case of the requesting data subject."* The wording of **Article 15 (1)(a) does not refer to the processing purposes relevant to the individual using the right of access**, and hence we suggest changing the wording to non-compelling format (following the paragraphs 113 and 115).

This section could also helpfully cover the situation of archived data (in a digital or physical archive) that is no longer actively processed more directly. With regard to proportionality, where legacy data is archived (especially in a separate location) ahead of being deleted, and action to locate relevant personal data, extract it and review it for redactions would be highly complex and costly, **this should be treated as being out of scope of the right of access.**

c. Information on the processing and on data subject rights (4.3)

According to **paragraph 113**, controllers should provide the data subjects with tailor-made information on the recipients of their personal data in response to data access requests. While the EDPB seems to ascertain that controllers have the possibility to refer to the categories of recipient (end of par. 114) instead of the single recipients (single natural or legal persons), it highlights that controllers, when this specific information is available, should provide it to the requestors. **We think that the interpretation of the EDPB does not take into account the difference between the different processing activities and their complexity.**

In practice, for large organizations sharing data with many third parties, it would be difficult to retrieve the information in due time to respond to a request so that specific single recipients of the personal data are listed for all access requests. This would also further contribute to finding the difficult balance between the need to be transparent while ensuring that information is shared in a concise way (as stated by EDPB itself in par. 141). **We believe that the reason why the legislator has provided controllers with the possibility to share information on the categories of recipients is precisely to address this problem**.

In **paragraph 116**, the EDPB states that "*if the personal data of the data subject is subject to different deletion periods (e.g. because not all data is subject to legal storage obligations), the deletion periods shall be stated in relation to the respective processing operations and categories of data."* We would like to flag that this provision is much more complex in practice, **as the storage times provided for by the applicable legislation may also be different** (for example in the case of data collected as part of the graphometric signature processes). The same data element might also be maintained in different systems which have different retention schedules in application of different legal requirements or serving different legitimate interests. Communicating this type of information to the data subjects is very hard in these cases and might **ultimately result in additional confusion.**

We would therefore suggest using the wording present in Art.15 (d) instead, as this reflects the possible complexities:

"*if the personal data of the data subject is subject to different deletion periods (e.g. because not all data is subject to legal storage obligations),* ***~~the deletion periods shall be stated in relation to the respective processing operations and categories of data."~~ where possible, the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period."***

5. Section 5: How can a controller provide access?

a. How can the controller retrieve the requested data?

The following section in **paragraph 123** raises a concern "…*The same applies when records regarding third persons are likely to contain personal data regarding the data subject*". The controller cannot disclose information that can be found in exchanges with someone of the data subject's family who is in the same bank, except in exceptional cases and for a specific purpose. We would therefore suggest to delete this from the paragraph.

b. Different means to provide access (5.2.2)

Paragraph 132 states that– *that the controller has to consider appropriate technical and organisational measures, **including adequate encryption** when providing information via email or online self-service-tools*. We would like to underline that **it is each controller's choice on how to share the information in a safe and secure way,** in line with the accountability principle and state of the art.

c. Providing access in a "concise, transparent, intelligible, and easily accessible form using clear and plain language (5.2.3)

Paragraph 138 raises the following question – should the controller ensure alternative means for providing access? For example, if the controller has decided to provide answer via email, especially given the large amount of data (as described in example under para. 138 – hundreds of pages), can the data subject ask to provide the response via different channel, e.g., post or in the branch? Printing out documents and sending them via post bears additional costs. Can those be put on the data subject (noting that certain data subjects may have specific accessibility needs)?

Under **paragraph 140,** we would welcome guidance on the way to proceed when requests are lodged in another language than those in which the controller provides its services. In our view, the controller can refuse to accept such a request because it, as a start, cannot identify it as a data subject request and ask the data subject to lodge the request in one of the languages used by the controller.

d. A vast amount of information necessitates specific requirements on how the information is provided (5.2.4)

Paragraph 144 states that *"access to the different layers shall not entail any disproportionate effort for the data subject and shall not be made conditional to the formulation of a new data subject request".* We disagree with such an interpretation and **propose to add that the second layer should be provided *if requested by the data subject*.** In practice, data subjects may not be interested in receiving the second layer, and this has been shown in the vast majority of cases.

- A typical example is when a consumer wishes to access his basic profile data in a platform or product offered by the company. Following the approach of the EDPB, the data subject would not only be given with such basic information (e.g. name, surname, contact details, main activities within the product environment), but also technical information on the profile (e.g. logs, interactions with other platforms, profile history when available, etc).
- In another example, telephone recordings may be useless for data subjects in which case creating unnecessary work.

The guidelines also recognize that in the event that a large amount of data or information is processed (such as in the banking sector), the data controller must also verify the request through a dialogue with the data subject. This is equivalent to obtaining an explicit request to proceed with the sending the second layer **only in the event that the data subject confirms that he is interested in receiving the second layer**.

To avoid misinterpretation, **we propose to add that request for the second layer should be treated as a new request triggering new response timelines: 1 +2 months**. Preparation of data under the second level may require more time and administrative resources on the controller's side.

Overall, given that a layering approach is taken, guidance is missing on how to view the 30-day period. For example, what if a request comes in and the bank responds on the 10th day with the first information, stating that the data subject must verify whether additional information is needed. The data subject then reverts on the 20th day and says that it indeed wants full disclosure. Would this leave the company 10 days to fulfil the whole request, even though it is the remaining one that is truly burdensome? Or would these leave room for a new 30-day period? **As mentioned above, we would suggest that this is treated as a new request, with new response times.**

In **paragraph 145**, the following is included "*The fact that it would require great effort and resources from the controller to provide the information under Art. 15 is not in itself an argument for using a layered approach"*. In our opinion, an argument would be to service data subjects and provide them at least some part of information within one month.

e. Format (5.2.5)

In **paragraph 150** we welcome that there may be a suspension in time to respond until the controller has obtained the information needed from the data subject.

Paragraph 151 provides that the controller should make "*some kind of compilation and extraction of the data.*" In case of a correspondence between the data subject and the controller, **the data subject already has information and, in principle, the data subject is already aware of the processing and can verify the information in such correspondence**. **Reading the correspondence and making some compilations and extracts could amount to excessive data processing**. Even under Article 13 and 14, the data that the data subject already has is exempt from the information obligation. An alternative could be to state how many years of conversation the controller holds.

Paragraph 153 mentions cases involving audio recordings and the need for an agreement between the subject and the controller. **We recommend reconsidering this provision, as audio recordings also contain personal data (voice) of an employee (a data subject category of its own) which the data controller also holds a responsibility towards protecting its personal data.** We would therefore suggest removing the condition "*if agreed upon between the data subject and the controller"*.

The choice and the means to communicate the information to the data subject should remain in the hands of the controllers, depending on their organisation. For example, another way to give access to audio recordings is to provide a transcript of the recorded conversation. The guidelines should also factor in decisions taken at national level on this topic. For example:

- The Finnish Data Protection Authority (DPA) has issued decisions that the data controller may decide whether to give recordings in transcripts.
- In the opinion of the Latvian DPA, the controller is compliant by issuing only the transcript of the reading.
- In Italy, listening to recorded phone calls can only take place through compliance with specific guarantees included in the union agreements regarding the application of Law no. 300/1970.

e. Timing (5.3)

Paragraph 157 provides that the controller can suspend provision of response when the controller asks the data subject to specify the request or provide additional information. We suggest to include **an example in the guidelines on how the time period shall be calculated.** For example, if the request is received on March 5. On March 7, the controller communicated to the data subject the need to provide additional data.

Requested information was provided by the data subject on March 11. By which date shall the controller fulfil the request?

We have some reservations with the following formulation in **paragraph 162** *"the mere fact that complying with the request would require a great effort does not make a request complex".* **Such an assumption does not reflect the reality on the ground**. A great effort is needed due to the large amount of data held in various applications, logs, verifications, making an assessment of what to exclude due to information about other data subjects, trade secrets, legal obligations (AML, fraud) etc. If such a great effort does not make a request complex, **what *does* qualify as a complex request**?

Paragraphs 160-161 include the possibility to extend the time to respond due to the need to redact information when an exemption applies, when further work is required to make the information intelligible – we support this provision.

6. Section 6: Limits and restrictions of the right of access

a. Article 15(4) GDPR (6.2)

In **paragraphs 166** and the ones that follow, it is not clear why other fundamental rights than those applying to the data subject, for example the freedom to run a business under EU Charter Article 16, should not be applied more broadly to require a fair balance between the data subject access right and the costs or burdens imposed on a controller. Article 4 of the GDPR states that "*The right to protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information,* ***freedom to conduct a business****…."*

For instance, paragraph 167 mentions "*… there is no difference justified whether trade secrets are affected by providing a copy or by granting on sight site access to the data subject. Art. 15(4) GDPR is not applicable to the additional information on the processing as stated in Article 15(1) lit. a.-h. GDPR*". **However, companies need to anonymize/pseudonymize data/information if it constitutes trade secrets, which makes the granting on sight site access impossible.**

We would also like to stress that there are situations where the rights and freedoms of others, other than protecting trade secrets for example, need to be taken into account too. See our remarks on the example of paragraph 95.

Furthermore, in paragraph 168, "*economical interests of a company not to disclose personal data are* ***not to be taken into account*** *when applying Art. 15(4) as long as they are no trade secrets, intellectual property or other protected rights*". **Economic interests could constitute highly confidential information.** The guidelines need to recognize these elements; **if not, data controllers are, among other things, at risk of repercussions or non-compliance with other applicable legislation.**

The current prescriptive approach in the guidelines need to take more into account the risk-based approach at the origin of the GDPR and the fair balance with the freedom to conduct a business.

b. Article 15(4) GDPR (6.2)

As set out above in relation to paragraph 96, a key concern for banks is that disclosure of certain data could impact on their ability to meet core regulatory and legal requirements,

in particular in relation to preventing and detecting financial crime, and responsible lending through the use of credit scoring. **Section 6.2 of the guidance should clarify that, where disclosing certain data to the data subject would prejudice a controller's compliance with legal and regulatory obligations, the controller can rely on the exemption in Article 15(4).**

We also have reservations with Example 1, particularly the following provisions in **paragraph 171** that precede it: "*if it is impossible to find a solution of reconciliation, the controller has to decide in a next step which of the conflicting rights and freedoms prevails (step 3).*" The example should mention that this **should be part of the controller's suitability assessment if there are a less intrusive way to provide access to the data subject without giving access to another data subjects personal data.** See comments above regarding possibility to provide transcript or listen to the recording on site instead.

c. What does manifestly unfounded mean? (6.3.1)

With regards to an unfounded request or manifestly unfounded request, we would instead suggest to focus on the possibility of misuse of the request or an excessive request – where it is clear, for example, that the client is not using the right to access for what is outlined in the GDPR. Using this mechanism for other purposes can be seen as a misuse of this right. Please see further comments below.

d. What does excessive mean? (6.3.2)

Under **paragraph 182**, the EDPB states that "*the more often changes occur in the controller's data base, the more often data subject is entitled to make a request without being excessive";* but the text does not specify **what qualifies as "a change**". Is it an update of the data, is it a new processing operation? We would welcome further specification on this point.

On the **topic of excessive requests**, the current interpretation of the notion **seems to be too narrow and not clearly explained**. Indeed, in **paragraph 184**, it is stated that *"When it is possible to provide the information easily by electronic means or by remote access to a secure system, which means that complying with such requests actually doesn't strain the controller, it is unlikely that subsequent requests can be regarded as excessive."* The analysis of an 'excessive' request **should focus on the recurrence of the data subject's requests or on the intention of the data subject to cause harm, burden or disruption to the data controller**. **The ease with which the data controller can comply with the request should not be the only relevant criterion** (see also comments below in relation to paragraph 188).

- For example, some customers have already invoked their right of access to recover lost account statements. Although it is not in itself difficult for the bank to comply with this request, it is a request that could be considered excessive for some members and is certainly disproportionate. **As outlined above, firms should be able to confer with data subjects to confirm the data of interest not only on an exceptional basis but also in relation to more routine data access requests in order to address data subject needs efficiently.**
- The amount of data, the different type of data (email, information in non-IT tools, etc.), the obligation to anonymize/pseudonymize such data are not considered as criteria to be integrated in the notion of "excessive" request. For instance, a request may be excessive from the data subject when the documents have already been communicated in the context of exchanges between law firms or when the request for access is made after a dispute. More examples will be helpful.

In addition, in **paragraph 188,** the EDPB is of the opinion that "*a request may be found excessive, if the individual has explicitly stated, in the request itself or in other communications, that it intends to cause disruption and nothing else"*. In practice, no data subject has admitted that the request is lodged just to cause disruption. Usually, this could be understood from the data subject's behaviour after receiving the response. **The guidance should be amended to say that *where the conduct of the individual makes clear* that the intention is to cause harm or disruption, the exemption can apply**, rather than requiring that the individual state so explicitly.

In some cases, for example, individuals may threaten to lodge a subject access request, if certain demands are not met. **Paragraph 188, bullet one of the guidance should be expanded to cover this scenario,** in addition to the situation where the request is first lodged by the individual, who then offers to withdraw it in exchange for some benefit.

Relating to **paragraph 191**, where the guidelines state that :" ….*if controllers refuse to act on a request for the right of access in whole or partly, they must inform the data subject without delay and at the latest within one month of receipt of the request of*…..", we propose to remove the obligation to inform individuals of the right to seek judicial remedy as this is not provided for by the GDPR (only redress before the Data Protection Authority).

ENDS

For more information:

Liga Semane

Policy Adviser – Data & Innovation

l.semane@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu