MEMORANDUM

To: European Data Protection Board (EDPB)
From: RBS Responsible Business Solutions GmbH

RBS Responsible Business Solutions GmbH
Hegelgasse 13
1010 Vienna, Austria

T +43 (0) 800 30 08 92
E office@rbs-consulting.eu
W www.rbs-consulting.eu

Register No: FN 439861 f
(Commercial Court Vienna)
VAT No: ATU 69938945

11.03.2022

Re: Comments to EDPB's draft guidelines 01/2022 on data subject right - Right of access (Version 1.0)

Dear Members of the EDPB,

Reference is made to the EDPB's draft guidelines regarding the right to access under Art 15 GDPR (the "**Guidelines**").

As the EDPB highlights Art 15 GDPR is a very important data subject right enabling data subjects to obtain information on how his/her data is processed and key to exercise his/her data subject rights, we warmly welcome the opportunity for stakeholders to submit comments.

Before this background, it is of the same importance for controllers to have clear guidelines how to comply with their corresponding obligations under Art 15 GDPR. Without exaggerating, it must nevertheless be emphasized that especially controllers depend very much on clear guidance from the EDPB (even more if no informal guidelines, opinions, FAQ etc from the local DPA may be at hand). Without such guidance, controllers must resolve 'gray areas' in front of the DPAs or local courts, running the risk of high administrative fines and/or civil law compensation obligations for (immaterial) damages. Thus, it is to the benefit of all parties involved that the questions and issues with respect to the scope of the right to access as well as the procedure of providing access are as clearly described and close to daily practice as possible. By no means, these Guidelines should Impose more obligations on controllers or data subjects than GDPR does.

We therefore welcome the Guidelines. In order not to overload this statement, our observations will focus on two main areas which we believe, in our humble opinion, could be still improved to the benefit of both, controllers and data subjects, especially by providing more praxis orientated examples regarding gray areas. We may also draw upon first-hand experience on controversial issues from our practice as external DPO to several data controllers.

1. REQUEST FOR CLARIFICATION

At the outset, we would like to address those points on which, in our opinion, further guidance and clarification are desirable:

1.1 No obligation to provide access to all group companies

1.1.1 In practice, in the case of groups with different independent companies as independent controllers, it happens that data subjects submit a request for information to one company of the group and expect information from all group companies. Independent controllers are not obliged to provide information about other controllers, even if they are group companies, and are also not obliged to forward such information.

1.1.2 Such obligations are not imposed by the GDPR and from a controller's perspective it is desirable to get clarification on this very practical issue also in the Guidelines.

1.2 Retention of proof of identity

1.2.1 For understandable reasons, it is not appropriate in practice to delete the proof of identity after the verification and only store a verification note about the verification of the identity. It may very well happen that ultimately unauthorised persons (identity theft) or a forged proof of identity are presented. The controller may be confronted with subsequent claims for damages or other claims by the persons concerned due to provision of access to an unauthorised person and must therefore be in a position to defend himself and to be able to prove the content of the proof of identity.

1.2.2 Before this background. we kindly ask for further clarification on appropriate retention for proofs of identity.

2. REQUEST FOR MORE PRACTISE-ORIENTED EXAMPLES AND GUIDANCE

2.1 Communication channel - Recital 56, second example

2.1.1 As an example of a request for information via an incorrect communication channel that does not trigger an obligation to provide information, the case is cited where the data subject directs his/her request for information to the cleaning company working for the fitness club instead of to the fitness club.

2.1.2 Unfortunately, this example is not too practice-orientated, since it is clear that in such a case no obligation to provide information is triggered for the fitness club. In our view, controllers would be rather interested to obtain guidance as to whether data subjects could be directed to exclusively use specific contact channels offered e.g. in the privacy notice of controllers, provided that such channels are clear, easily accessible and include both an electronical channel as well as a postal channel so that the right of access of the data subject is not restricted.

2.1.3 We therefore politely ask to include a practice-orientated and helpful example that provides guidance in particular on issues in a grey area, such as the above.

2.2 Scope of data to be provided - missing example for Recital 100

2.2.1 Of course, we agree that the scope of personal data should be interpreted broadly and should not be unduly limited. Nevertheless, there are cases in practice where certain personal data do not have to be disclosed and which at the same time do not constitute an inadmissible restriction of the right to access. Unfortunately, no such examples were given in the Guidelines.

2.2.2 This includes cases of internal communication (e.g. between two employees) which do not concern the data subject, but e.g. mention his/her name in passing, or an e-mail chain in which the monthly salary report for the internal reporting is requested and which contain the data of the employee requesting access. Providing such data would be beyond the scope of the access obligation, flood the employee with irrelevant information and create a disproportionate burden for companies that employ a large number of employees over a period of years.

2.2.3 Against this background, we therefore consider it appropriate and helpful to add practical examples in which the controller is justifiably not required to disclose documents (including, in particular, internal communications) that contain personal data of the data subject but do not concern him or her.

3. PENDING CJEU CASES REGARDING ART 15 GDPR

3.1 Beforehand we want to highlight the fact that currently a couple of requests for preliminary rulings are pending with the CJEU regarding questions on the scope of Art 15 GDPR (e.g. C-154/21 *Österreichische Post AG;* C-487/21 *Österreichische Datenschutzbehörde and CRIF*; C-579/21 *Pankki S*).

We trust the EDPB is of course aware of them.

3.2 Given the binding effect of CJEU's decision on the interpretation of EU law, including the GDPR, we deem it appropriate in the interest of efficiency to stay the consultancy process and finalization of the respective guidelines after these relevant cases have been decided by the CJEU. Once these cases will have been decided they will a) give strict guidance on certain questions (which otherwise could have been addressed differently in these Guidelines from the final CJEU rulings) and b) may open up different questions not yet addressed in these Guidelines. Therefore, it would not be in the interest of neither the EDPB nor the users of the Guidelines to issue recommendation which might become obsolete after these CJEU decisions.

3.3 However, if the EDPB insists on issuing the whole of the Guidelines as drafted beforehand, we consider it good scientific practice and in the sense of transparency to mark all those recommendations whose core statements are still awaiting clarification by the CJEU. An explicit reference in the specific guidance to the specific procedure of the CJEU would therefore be helpful, particularly for all those controllers who do not continuously keep an eye on the current status of supreme court rulings.

4. RECIPIENTS

4.1 The question of whether *specific* or only *categories* of recipients are to be disclosed according to Art 15(1)(c) GDPR, is currently pending for interpretation by the CJEU (C-154/21). We therefore refer to point 1 above.

4.2 The Guidelines take the general position that specific recipients must be disclosed. In recital 115 the Guidelines only state that actual recipients should be named "unless it would only be possible to indicate the categories of recipients". Further, it continues: "Nevertheless, sometimes naming the actual recipients is not yet possible at the time of the information under Art. 13 and 14 GDPR but only in a later stage, for example when an access request is made. The EDPB recalls in this regard, that storing information relating to the actual recipients is necessary inter alia to be able to comply with the controller's obligations under Art.s 5(2) and 19 GDPR.". This conclusion under recital 115 of the Guidelines is very cryptic, does not explain on what interpretation of the law it is based and how Art 19, 15 and other principles (e.g. data minimization) correlate and thus, above all requires further guidance for practitioners.

4.3 For example the WP29 Guidelines on transparency – endorsed by the EDPB, p. 37 (Annex), to which the draft Guidelines refer explicitly state that the controller has an option: "If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients." (emphasis added by author). However, this is not addressed in these Guidelines which therefore are at risk to be misleading.

4.4 Whereas on the one hand it is true that sometimes the actual recipients can be only identified in a later stage, on the other hand there are in practice many situations where the actual recipients may never be known in relation to the data of the specific data subject. This refers for example to the entire sector of companies who provide marketing services and simply transfer (legitimately obtained and processed) personal data which are grouped in data packages to a recipient. This means that for providing the specific marketing services it is not required that the controller has specific lists/protocols on the level of individual data sets. Consequently, an obligation to have such protocols in place would not serve the purpose of the actual data processing but would have to be kept solely in order to be able to reply to a potential access request, whensoever in the future. Yet, the last sentence referenced in the paragraph 4.4 above states that apparently the

controller is obliged to have protocols in place to comply with Art 19 GDPR. Unfortunately, there is no further explanation in this respect. However, if this sentence would be applied in practice, a contravention against the fundamental principles of data minimization and purpose limitation as specified in Art 5 GDPR as well as Recital 64 GDPR would be the result.

4.5 The example provided in Recital 115 shows where such broad understanding would lead: It deals with business trips and a potential duty of an employer to name specific travel agencies and hotels as recipients, once an employee has taken the trip. In practice, employers would retain the invoices for financial and tax purposes but certainly not specifically document each travel agency, carrier, or accommodation on the level of the individual employee. This would lead to an increase of (mere) protocol data / metadata in contravention to the principle of data minimization (Art 5 GDPR) and Recital 64 GDPR (see item 5, below).

4.6 Thus, it would be extremely helpful to obtain the confirmation that there is an option[1] or at least there are possible exceptions to providing specific recipients under Art 15 GDPR. In particular, it would be helpful to state (at least as an example for such exception) that no specific recipients have to be stored solely in order to be able to disclose them under a potential future access request pursuant to Art 15 GDPR as acknowledged in Recital 64 GDPR.

4.7 Whereas with respect to mere processors as well as sub-processors (eg. IT service providers) it should be highlighted in the Guidelines that the information on specific processors and sub-processors as recipients is not required. For big companies which have contractual relationships with a very high number of processors and sub-processors, in particular IT service providers, the disclosure of all specific processors would be an overwhelmingly huge burden in practice (see more below 5.8).

5. NO CONSIDERATION OF PRINCIPLE OF PROPORTIONALITY AND GUARANTEES UNDER THE CHARTA

5.1 The draft Guidelines unfortunately do not consider any legal principles protected by primary EU law, such as the principle of proportionality (Art 5 (4) TFEU) or the other guarantees enshrined in the Charter of Fundamental Rights.

5.2 As Recital 4 GDPR makes clear, data protection law 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.

5.3 Accordingly, the GDPR is "consistent with all fundamental rights and respects all freedoms and principles recognized by the Charter and enshrined in the European Treaties, in

[1] Depending on the answer by the CJEU in the pending case C-154/21.

particular respect for private and family life, home and communications, protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity". (Recital 4 GDPR; emphasis added by the author).

5.4 Art 15(1)(c) GDPR must also be interpreted in the light of these requirements; this provision must not be interpreted in a way that disregards the principle of proportionality (Art 5(4) TFEU) and the guarantees of the Charter of Fundamental Rights. However, those requirements are not met by the interpretation of Art 15(1)(c) GDPR proposed by these draft Guidelines in the sense of a primary obligation to provide information about specific recipients or a right of choice of the data subject in this regard.

5.5 Controllers would therefore be forced to disclose confidential customer lists, suppliers, prospective buyers, legal advisors, private investigators, etc. by name to affected persons (e.g. consumers or - also former - employees) without a proportionality correction. Such information, for example in the context of company transactions, corporate investigations, legal disputes or secret company projects, may constitute business secrets, are protected under Union law by the fundamental right to respect for private life (Article 7 CFR), the protection of personal data (Article 8 CFR), the freedom to conduct a business (Article 16 CFR) and the right to property (Article 17 CFR).

5.6 In the context of the interpretation suggested in these draft Guidelines and the proposed right of choice of the data subject, Article 15 (1) (c) GDPR would, however, lack any proportionality and balancing with the above-mentioned fundamental rights positions. In this respect, the provision would not be "in line with all fundamental rights [...] recognized by the Charter and enshrined in the European Treaties.

5.7 At the minimum there should be reasonable and practical exceptions from the obligation to provide specific recipients, e.g. as in the case that the recording of such recipients is from the outset not necessary for the purpose of transferring data to them; and therefore a recording obligation in this respect would lead to an increase in data in contravention to the principle of data minimization (Art 5 GDPR) and Recital 64 GDPR.

5.8 No obligation to specify processors (and sub-processors)

5.8.1 Even if specific recipients are to be identified, this obligation should not apply to mere processors (and any sub-processors). A concrete link or allocation as to whether data of the specific data subject was also transferred to a specific processor cannot be traced in most cases due to the lack of such recording. This is also because such a record is not necessary for the purpose of processing the order. Such a record would also produce a large amount of additional data that would only be kept for the purpose of potentially providing information (in conflict with Recital 64 GDPR).

5.8.2 In this respect it must be highlighted that Recital 115 of the Guidelines may be misleading when stating that "The EDPB recalls in this regard, that storing information relating to the actual recipients is necessary inter alia to be able to comply with the controller's obligations under Art.s 5(2) and 19 GDPR." (*emphasis added*) as such statement is too short. It should be added that in fact such a possible storage obligation can only exist if such transfers were *initially recorded in the first place* because this is necessary for the fulfilment of the underlying processing purpose. If, on the other hand, such recordings are not actually made in the first place, there is also no corresponding storage obligation (and also no "original" recording obligation, which without clarification could be derived from the cited sentence in Recital 115).

5.8.3 In contrast to the (possible) misinterpretation in this Recital 115 such an original record obligation does not exist. The opposite interpretation would, however, create a significant burden for controllers to comply with Art 15 GDPR and contradict the principles of the GDPR (see 5.7 above) as well as the principle of proportionality.

6. FORM OF REQUESTS AND SELF-SERVICE TOOLS

6.1 We understand, the EDPB "*encourages the controllers to provide the most appropriate and user-friendly communication channels, in line with Art. 12(2) and Art. 25, to enable the data subject to make an effective request"* (recital 53) and encourages the provision of information by means of self-service tools (recital 136)". This is very welcome, however, it also emphasizes that "*the controller must also handle access requests that are not sent through the established channel of communication*" (referencing in footnote 67 to point 3.1.2 "Form of requests" of the draft Guidelines). Further clarification is needed in this respect.

6.2 Since the draft Guidelines only speak of "self-service tools" it should be clarified that this includes also online forms which guide the data subject through all the information necessary to submit a correct data subject request. Such online forms are – in case a request has been already submitted electronically – helpful especially for the data subject as they indicate which information must be provided in order for the controller to process the request. In the absence of such online forms depicting the necessary fields of information, the typical process in practice (as we have experienced this in many cases) is that there is an email conversation back and forth between the controller and the data subject in order to finalize the minimum required information to handle the request.

6.3 In practice, this can obviously be a nuisance for the data subjects, who may not feel fully serviced, and it may delay the fulfillment of the request. This could be prevented with appropriately pre-formulated query fields in online forms, where the data subject is guided in a user-friendly way to enter the necessary information in the various fields in the online mask. Especially for controllers who are confronted with an extremely large amount of data subject requests, online forms are an efficient solution. Due to the high practical

relevance, we would therefore welcome it if the Guidelines would also expressly address this aspect of online forms.

6.4 However, also the relationship between "self-service tools" or online forms on the one hand and other electronic communication channels on the other hand does not seem to be adequately addressed either. The Guidelines state that "*the controller must also handle access requests that are not sent through the established channel of communication*", which in our view is far excessive in its practical effect: Thus, although controllers maintain an online form and thus a dedicated electronic access to the right of access, controllers would also have to accept and process incoming requests for access via *all other* electronic channels (not only e-mail, but especially also via all sorts of social media a controller may have in operation). This intention cannot be imputed to the legislator, especially against the background of the principle of proportionality (see above).

6.5 A corresponding clarification in the guidelines, including the fact that such approach does not violate the duty to facilitate data subject rights (Article 12(3)), would therefore be an important and highly welcomed practical relief for controllers (whilst it would certainly not be overly burdensome for data subjects and their exercise of access rights).

***

We thank you for your kind consideration of these comments and hope for further, practice-oriented guidelines as regards data subject rights.

Kind regards,

Mag. Gernot Rauter

Responsible Business Solutions GmbH

Mag. Helmut Waitzer

Responsible Business Solutions GmbH