DOT Europe's response to the EDPB consultation

on the Guidelines 01/2022 on data subject rights - right of access

The European Data Protection Board (EDPB) EDPB draft Guidelines 01/2022 on data subject rights -right of access ('the Guidelines') go beyond the requirements of the General Data Protection Regulation (GDPR).[1] In some instance the Guidelines seem to contradict the GDPR and existing Court of Justice of the European Union (CJEU) jurisprudence. This will result in an unhelpful outcome for data subjects and data controllers alike. We fully understand that the aim of the right of access is to provide data subjects with information that allows them to understand and verify the lawfulness of the processing of their personal data. However, as the Guidelines are drafted, they will result in data subjects receiving excessive and unnecessary information which would only serve to confuse, distract, or overwhelm. DOT Europe would like to share its reflections on the Guidelines with the EDPB to highlight those areas that we believe need further clarification

Proportionality

The GDPR specifies that the right to the protection of personal data is not an absolute right and makes reference to proportionality. The EDPB's interpretation that the right of access "*is without any general reservation to proportionality with regard to the efforts the controller has to take to comply with the data subject´s request*" seems to be in direct conflict with Recital 4 GDPR and the general principle of proportionality found in EU law. It is clear from both the language of the GDPR and the case law of the CJEU, that the right of access is not absolute and it should be applied in a proportionate manner.[i]

A reasonable and proportionate approach should therefore be adopted with respect to assessing the data that is produced in response to a data subject access request. The EDPB's interpretation that the right of access "*is without any general reservation to proportionality with regard to the efforts the controller has to take to comply with the data subject´s request*" would impose a significant burden on data controllers of all sizes and in all industries, without any appreciable benefit for data subjects. To provide concrete examples of how the Guidelines are both cumbersome and technically difficult to comply with please consider the following contexts:

<u>Emails and other 'free' formats:</u>
Organisations of most sizes are likely to have millions, if not billions, of emails and other electronic documents, especially with respect to employees. Emails often consist of a mixture of different types of information that may (intendedly or unintendedly) relate to various individuals. Emails might contain information on a number of different topics or about a number of different individuals. Thus, for information in emails, data controllers are sometimes unable to accurately identify information about a particular individual without processing more data to this effect. Furthermore, broad searches of an organisation's employees' email inboxes in order to satisfy a SAR disproportionately invades employee privacy and is contrary to Article 7 Charter Fundamental Rights and Freedoms - that "Everyone has the right to respect for his or her private and family life, home and communications". A broad interpretation of this requirement could even see colleagues gain access to content of other colleagues' email inboxes,

[1] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Rue du Trône, 60
1050 Brussels, Belgium

Tel: +32 (0) 472 26 83 02

WWW.DOTEUROPE.EU

Transparency Register: 53905947933-43
DOT Europe was formerly known as EDiMA

corporate devices by submitting SARs, and while an individual's name may be edited in the content returned to the requester, various other parties within the business would need to review the employee's potentially private correspondence to determine what is in scope and what should be disclosed, thus a material loss of privacy.

Also, it would be challenging to assess whether an Article 15(4) exception should apply to safeguard the rights and freedoms of others in these cases without a manual review of each individual email and produced electronic document.

Databases/data warehouses:
Additionally, many companies are likely to have to maintain databases/data warehouses to store the data generated by their services "offline." Such databases/data warehouses may be unstructured and searching across these information sources would be disproportionate, costly and technically challenging. More importantly the data subject would more than likely get minimal, if any, benefit from receiving this data as it would be "raw data" that does not help the data subject to understand how their data was processed. in response to a data subject access request and be unlikely to provide the data subject with information required to understand and verify the lawfulness of the processing of their personal data (i.e. such disclosure would not further the purpose of Article 15 GDPR).

Back-ups or archives:
Data can be stored in a number of different formats for different use cases. The Guidelines suggest that where "*technically feasible*" data controllers would need to look at their back-ups for any data held on the back-up systems and in effect process these data for new purposes. Restoring such back-ups would be in direct conflict with the principles of data minimisation and purpose limitation. Please note that this would also mean a duplication of data in the Data Subject Access Report to no added value.

Raw data

The EDPB's position is that "*data in a raw format*", which may not be "*directly meaningful*" to the reader, is covered by the right of access and that when providing data in a raw format it is important that the data controller "*takes the necessary measures to ensure that the data subject understands the data, for example by providing an explanatory document that translates the raw format into a user friendly form*". However, the GDPR and findings in CJEU case law support a view that the EDPB's position that raw data must be provided in response to a data subject access request is incorrect[ii]. The Guidelines themselves also seem to be contradictory on this particular point stating "*It should be stressed that the information provided to the data subject always must be in a human readable format*" while "data in a raw format" is often not in a human readable format. It is therefore necessary that this contradiction is clarified especially bearing in mind the minimal added value to the data subject.

Layered approach to Article 15 requests

We would appreciate additional elaboration on how a layered approach to respond to Article 15 requests could be done in practice. The Guidelines do not specify how to bridge the requirements to provide a '*summary of the data'* (par. 23) and to give the '*broadest effect to the right of access*' (par. 35(b)).

In addition, the Guidelines seem to presume that a general Article 15 request should be treated as a request for the complete record of an individual's personal data (para. 51). Should the data controller

Rue du Trône, 60
1050 Brussels, Belgium

Tel: +32 (0) 472 26 83 02

WWW.DOTEUROPE.EU

Transparency Register: 53905947933-43
DOT Europe was formerly known as EDiMA

always provide the complete personal data set in response to a data subject request or when they have not narrowed down their request at the outset, this would undermine the benefit of enabling a layered approach.

We encourage the EDPB to consider allowing data controllers to provide a more simplified first layer of Article 15 information in response to requests, except when the request warrants a more detailed response from the outset.

Article 15(4) GDPR

The Guidelines state that "*in principle any right or freedom based on Union or Member State law may be considered to invoke the limitation of Art. 15(4) GDPR*". However, the Guidelines contradict this by stating that not every interest should be taken into account when assessing Article 15(4): "*For example, economical interests of a company not to disclose personal data are not to be taken into account*". This is not a correct interpretation of Article 15(4) / Recital 63 and it directly contradicts Article 12(5).

- As currently drafted, the broad exclusion of economic interests from the balancing assessment to be carried out under Article 15(4) is an incorrect interpretation of the GDPR and should be corrected. Article 15(4) and Recital 63 anticipate taking all rights and freedoms of others, including economic interests, into account. For example, data controller's trade secrets, IP and the ability of providers of online services to offer safe and secure service should be taken into account[iii]. Limiting 'rights and freedoms' to 'protected rights' only would create confusion around what constitutes such a 'protected right' and result in a narrow interpretation of Article 15(4).
- It is also important that the Guidelines properly acknowledge that in certain circumstances controllers cannot provide specific information to data subjects about the reasons why data has not been disclosed in response to an access request. This is particularly relevant where disclosure of such information would reveal the operation of tools and procedures used to detect bad actors or breaches of terms and policies. Requiring that data controllers disclose this information undermines the security of online services and prejudices the rights and freedoms of the users of online services, who have a right to be protected from bad actors.
- Furthermore, DOT Europe finds this section problematic as it is common practice to use personal data to detect fraud, e.g. to refuse payment, credit, or to detect cheating in video games, to detect cyber exploits or unlawful access to IP content. Giving all data related to a ban in a data subject access request would likely help developers of fraudulent technology improve it. A lot of data is used in very complex detection; any single piece of information might be useful to understand fraud detection processes. We would recommend reviewing this section, delete example 3 and give the opportunity to data controllers to retain "trade secrets" on the technology and data used to detect fraud.

Tailoring information required under Article 15(1)(a) – (h) and Article 15(2)

The EDPB states that the information required under Articles 15(1) and 15(2) could be based on text taken from the data controller's privacy notice but may have to be "*updated and tailored to the data subject making the request*". The GDPR and CJEU case law clearly stipulate that the right of access should be

Rue du Trône, 60
1050 Brussels, Belgium

Tel: +32 (0) 472 26 83 02

WWW.DOTEUROPE.EU

Transparency Register: 53905947933-43
DOT Europe was formerly known as EDiMA

applied in a proportionate manner. The requirement to tailor the information to be provided in Articles 15(1) (a)-(h) and 15(2) contradicts this.

It is practically impossible to tailor the information about the data for each user. Data controllers receive thousands (or more) of requests a month and it is materially impossible to tailor each of them manually, as suggested in this section. In addition, privacy policies disclose this information and apply generally to all users of the same service.

As currently drafted the Guidelines go beyond what is required by EU law and should therefore be adapted to reflect the legal framework:

- Article 12 contains no indication that the information or communication needs to be "*tailored*" to the particular data subjects.
- Article 15 and Recital 63 do not require that the information to be provided in Articles 15(1) (a)-(h) and 15(2) should be "*tailored*" to the data subject.

Third party requests

When the data controller offers an easy and secure way to make the request and access the data (at no cost), the data controller should by no means be obliged to use a third-party service (par.88,89). Only the secure system developed by the data controller (when available) to make requests should be used as it ensures authentication, security of the request and access to the document, without any cost or additional intermediary (this should also be echoed in par. 55,56). The mere reception of a third-party request should not be seen as the starting point of the 30-day period. It is often difficult to verify that the proxy has the power to make the request and receive the data on behalf of the data subject. In addition, the information those proxies share is often not relevant for the data controller to authenticate and confirm the ownership of the account as they operate in "bulk", sharing generic account information in one go with multiple data controllers. There is a risk of disclosing data to an unauthorised party, which would be a personal data breach, as mentioned in the last sentence of (par79).

ID card verification

If the data controller doesn't offer two-factor authentication, there is a risk that the account may be taken over when the hacker requests data and the deletion of the account. Data controllers should be in a position to ask for extra identification, should they have enough reasons to do so (e.g. suspicious recent activity on the account; suspicion of fraud, etc.) The last sentence about prohibiting ID card verification (par72,73) when a user is authenticated needs to reflect this possibility.

Cookie identifiers

The Guideline (par67) suggests that the provision of a cookie identifier would be sufficient to enable a data controller to authenticate a request for data associated with that cookie identifier. As there would be no way of confirming that such data identifies or relates to a specific data subject, this approach would present a significant data security risk and could lead to many unintended, adverse consequences for users of online services. This could occur in the case of an abusive situation where an abuser temporarily

Rue du Trône, 60
1050 Brussels, Belgium

Tel: +32 (0) 472 26 83 02

WWW.DOTEUROPE.EU

Transparency Register: 53905947933-43
DOT Europe was formerly known as EDiMA

has access to a victim's device. They could screenshot or copy the relevant identifier and then submit an access request for all data associated with that identifier. This appears directly contrary to the requirements under Art. 32 (1) GDPR for data controllers to ensure that an appropriate level of data security is in place to protect against unauthorised access to personal data.

We would therefore request that the EDPB clarifies this particular point and confirms that the provision of a cookie ID or other similar information alone is inappropriate and would present an unacceptable security risk if relied upon for the purpose of verifying the identity of a data subject.

Overall assessment of the role of the data subject

In order to avoid the application of unrealistic burdens on data controllers, the Guidelines could benefit from a more reasonable assessment of the data subject's role in the access request process. To this end, we offer the following suggestions:

Firstly, data subjects should be able to request certain information and disregard others based on their relationship with a data controller. For example, if Article 15 information could list recipients of the individual's personal data *should* the individual have used a specific feature of the service, instead of the data controller being obliged to provide dense information about the data subject's use of all service features and the subsequent data sharing, this would provide the data subject with relevant and detailed information while avoiding unnecessary data processing on the controller's part.

Secondly, the Guidelines should better align with the principle of data minimization enshrined in the Art. 5(1)(c) GDPR. When the text requires data controllers to analyse, compile and share information about a data subject's use of the service by default and at every request by the data subject, the Guidelines seem to contradict this principle.

Finally, the Guidelines require the data controller to provide information on data subject rights going far beyond the requirements in the GDPR (par. 117). For instance, it is not the data controller's role to pre-emptively assess what rights are available to data subjects. This would often involve potentially extensive legal analysis which is not feasible in the subject access request time frame, nor appropriate for the data controller to provide.

We would therefore encourage the EDPB to reconsider the position of the data subject and afford them greater responsibility for assessing and drawing conclusions about the information that is provided to them and making further enquiries when they seek something beyond that.

---

[i] Recital 4 GDPR recognises that the right to data protection is not absolute and has to be balanced with other rights: "*The right to the 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….*"

Furthermore, the CJEU has previously held that, in cases where the right to data protection runs up against other fundamental rights, it is necessary to strike a *"fair balance"* (C-70/10 Scarlet Extended v. SABAM [2011] ECR I-11959) between the various competing interests.

Recitals 129 and 61 also illustrate the role of the proportionality principle within the GDPR. Recital 129 GDPR states that: "*In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case*". Recital 62 states that: *"However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort".*

Rue du Trône, 60
1050 Brussels, Belgium

Tel: +32 (0) 472 26 83 02

WWW.DOTEUROPE.EU

Transparency Register: 53905947933-43
DOT Europe was formerly known as EDiMA

Case law confirms the relevance of proportionality in relation to data subject rights:

In *Latvijas Republikas Saeima*, the CJEU recognises that the principle of data minimisation in Article 5(1)(c) gives expression to the principle of proportionality, despite Article 5(1)(c) not expressly referring to the principle of proportionality.

The CJEU *CLIFIT* judgment further makes the point that every EU law must be interpreted in proportion to other provisions of EU law: "*every provision of Community law must be placed in its context and interpreted in the light of the provisions of Community law as a whole, regard being had to the objectives thereof and to its state of evolution at the date on which the provision in question is to be applied.*" (emphasis added).

The principle of proportionality has also been considered by the CJEU in the context of Article 15 TFEU and the right of access to the documents of the European Parliament, the Council and the European Commission (*Hautala v Council*).

The principle of proportionality is also an established general principle in case law that established that an entity is required to do only what is "proportionate in all the circumstances" and does not need to leave "no stone *unturned*" in responding to access request (*See the Court of Appeal decision in Ittihadieh v 5-11 Cheyne Gardens & Deer v University of Oxford [2017] EWCA Civ 121 at para 99)*

[ii] Under Article 12(1), controllers have an obligation to provide data subjects with access to their data in an *"intelligible"* form. Recital 63 is clear that access should be provided in a form that allows data subjects to exercise their rights: "*A data subject should have the right of access to personal data (…) in order to be aware of, and verify, the lawfulness of the processing*". Therefore, it cannot be assumed that Article 12(1) or Recital 63 requires controllers to provide data subjects with access to data that do not enable this purpose to be achieved, such as data stored in its raw or unintelligible form.

The Court of Justice of the European Union ("**CJEU**") and the Irish Court of Appeal have also confirmed that the right of access is not a right for data subjects to access their personal data in its "*original material form*", i.e. raw data. The CJEU has found that the right of access is satisfied once data is provided in an intelligible form, meaning a form which "*allows the data subject to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that that person may, where relevant, exercise the rights conferred on him*".

The CJEU has also found that, if the data is provided in a form which allows an individual to exercise their rights, a data subject has no right to access the underlying raw files which may contain his/her personal data: *"in so far as the objective pursued by the right of access may be fully satisfied by another form of communication, the data subject cannot derive from either Article 12(a) of Directive 95/46 or Article 8(2) of the Charter the right to obtain a copy of the document or the original file in which those data appear."*

This principle was applied by the Irish High Court in *Nowak v. DPC*, where the Irish High Court concluded that "*the obligation on a data controller to provide a data subject with personal data… does not extend to an obligation to provide the data in its original material form or, in the case of a document, to provide the original of that document*". The Irish Court of Appeal in *Nowak v. DPC* endorsed this position and stated that "*the trial judge quite properly relied on the decision in Y.S. which clearly supports the argument ….. that under the Directive the data subject's entitlement is to access to the relevant information/personal data in an "intelligible form", and does not support a right under the Directive to personal data in its original form.*"

While these cases were decided under the Data Protection Directive (95/46/EC) and the Data Protection Acts 1988 and 2003, the principles they contain equally apply under the GDPR. Indeed, the GDPR clearly indicates in various places that interpretations of the GDPR must be conducted in observance of principles espoused in the Directive (95/46/EC) and CJEU case law. Recital 41 provides that "Where this Regulation refers to a legal basis or a legislative measure, [. . .] such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights".

In observance of these CJEU and Irish High Court and Court of Appeal rulings, it is clear that the GDPR requires controllers to provide users with intelligible access to allow them to understand and verify the lawfulness of the processing only. If personal data is processed in an unintelligible format, it is the controller's obligation to determine how they can provide people with information that 'enables them to become aware of this information processed lawfully. The Draft Guidelines should be amended to comport with the controlling case law in this respect.

[iii] this directly contradicts recital 4 which notes that the right to data protection must be balanced against other fundamental rights. Article 16 of the Charter of Fundamental Rights is the freedom to conduct a business - excessively broad and disproportionate interpretation of the GDPR can impact on that right to conduct a business where responding to SARs is prohibitively expensive.

Rue du Trône, 60
1050 Brussels, Belgium

Tel: +32 (0) 472 26 83 02

WWW.DOTEUROPE.EU

Transparency Register: 53905947933-43
DOT Europe was formerly known as EDiMA