



# European Tech Alliance Reaction to the EDPB's Draft Guidelines 01/2022 on data subject rights - Right of Access

March 2022

## “ Foreword

The European Tech Alliance ('EUTA') welcomes the EDPB's efforts to provide clarity on data subjects' right of access under the GDPR in its draft **Guidelines on the right of access** (the '**Guidelines**'). Our members include the most exciting homegrown European tech companies across business models, Member States and sectors. We invest substantial resources in world-class engineers and data scientists to deliver innovative and data-driven services, be this in automated testing, personalising content, delivery of products to respond to individuals' tastes, or service refinement in a wide variety of commercial situations.

As many of us primarily operate within Europe, official EDPB guidelines on the implementation of GDPR can have a substantial impact on our operations. It is therefore crucial that such guidance is proportionate, technically feasible, aligned with market standards, and reflective of the wider data ecosystem in Europe. The Guidelines should also balance the precision they bring for specific, individual cases with the ability of all controllers to address the multitude and often considerable numbers of requests from data subjects (regarding their right of access as well as other rights) and the need to process these within a given time-frame. Absent this balance, the Guidelines risk prioritising individual-case perfection over what is proportionate and workable on an economy-wide level.

With this in mind, we set out some comments and concerns that we believe are important to take into account when finalising the Guidelines on the Right of Access.

*Kristin Skogen Lund*


Kristin Skogen Lund  
President of the EUTA

*Aurelie Caulier*

Aurelie Caulier  
Chair of the EUTA

## **Executive summary.**

- **The requirement to provide tailored and individualised Article 15 information** - EUTA recognises the practical guidance included in the Guidelines, but would urge the EDPB to develop these recommendations to reflect the feasibility of implementation under the technical and operational realities that our members work with daily.
- **Balancing access and accessibility for data subjects** - EUTA would welcome a more detailed discussion of how self service tools can be used to balance access and accessibility; in particular, if it is reasonable for controllers to encourage the data subject to specify their request as to the level of detail they are looking for in text format together with their downloaded data (if any), this should be emphasised.
- **The role of the data subject (1)** - The Guidelines impose additional burdens on the controller that could be mitigated with a more reasonable assessment of the data subject's role in the subject access request process. It should be acceptable for a data subject to interpret Article 15 information based on their knowledge of their own relationship with the data controller.
- **The role of the data subject (2)** - EUTA respectfully encourages 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.
- **Aim of the right to access (Paras. 5, 10)** - EUTA believes the Guidelines should be more nuanced and clarify that the right of access is primarily intended to verify the lawfulness of processing.
- **Right of access in the context of a dispute (Executive Summary & Para. 13)** - EUTA respectfully asks the EDPB to consider providing an exception for honouring requests made in the context of a dispute under the framework of GDPR, to the extent it is evident that such requests are submitted with

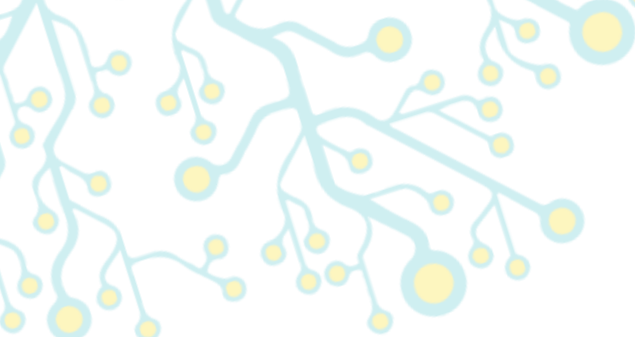


different motives than *‘being aware of, and verifying, the lawfulness of the data processing.’*

- **Time reference point of the assessment (Para. 38)** - EUTA calls for the reference to the retention periods to be removed from the Guidelines, as this overlooks the practical difficulties of adapting the time to respond to a request to the applicable retention period, and seems to go beyond what is required by and provided for under GDPR.
- **Pseudonymized data (Para. 45)** - Regarding the guidance that pseudonymized data that can be linked to a data subject are to be considered within the scope of the request, we would welcome clarification as to whether pseudonymized data need to be provided as well, to the extent the same personal data is provided to the data subject in clear text.
- **Communication channels (Paras. 54-56)** - EUTA suggests the EDPB specifies what is to be considered “random or incorrect” or “clearly not intended to receive requests regarding data subject’s rights”, and

further expand the definition of such terms to factor in the data subject’s own accountability. We would also welcome consideration of providing time flexibility for responding to requests not submitted via the official contact point(s) and/or webforms included in the controller’s privacy statement.

- **Cookie Identifiers (Para. 67)** - The Guidelines significantly widen the scope of right to access data collected via cookies and similar online identifiers as they do not seem to require authentication of the data subject as a starting point for providing the data. EUTA urges the EDPB to reconsider the example in Para.67, stating that controllers who already provide online authentication means to data subjects would need to provide access to data subjects that are not authenticated during a visit on a service and also afterwards via email or regular mail.
- **Use of ID cards to identify the requesting person (Paras. 73-78)** - EUTA would welcome specific reference to Recital 64 of the GDPR in the Guidelines as well as confirmation that requesting a



copy of an ID card together with a cookie identifier can be proportionate in certain situations to address the risk of fraud and identity theft.

- **Personal data in backup (Para. 108)** - EUTA urges the EDPB to reconsider the statement that when more or different personal data relating to the data subject is stored in the back-up, the controller should provide access “*where technically feasible*” to personal data stored in back-up besides the live production system. This does not take into consideration the technical limitations in verifying the log of deletions and reconciling with data in back-ups since, realistically, that would be nearly impossible to achieve.
- **Layered approach (Paras. 139,141,144, 145)** - EUTA encourages the EDPB to consider permitting controllers to provide a

more simplified first layer of Article 15 information in response to general data access requests, which could leverage information from their privacy statement where appropriate.

- **Handling large number of requests in specific circumstances (Para. 162)** - EUTA welcomes the acknowledgement that extraordinary events could be a legitimate reason for prolonging the time of the response, but suggests a specific reference to situations such as cyber attacks, security incidents and data breaches as examples justifying more flexibility.
- **Freedoms and rights of others (Executive Summary & Paras. 170-171)** - EUTA would welcome recognition of the effort the controller may have to undertake to balance the conflicting rights and freedoms and more detailed guidance on how those interests can be best balanced, taking into account the strict timelines that controllers need to adhere to.
- **Excessive request (Paras. 187 & 188)** - EUTA recommends that the EDPB specifically condemn the use of improper or impolite language in communicating with the data controller and recall that some of these behaviours can be criminally sanctioned under national laws.




## In more detail

- **Practical impact of the requirement to provide tailored and individualised Article 15 information (throughout):** We respect the right of the data subject to access information about the processing of their personal data. However, the practical impact of the requirement to provide tailored and individualised information about the processing of their personal data (i.e. information provided pursuant to Articles 15.1 (a)-(h)) requires further assessment. Like businesses operating across Europe today, our members can receive significant numbers of Article 15 requests every year, sometimes in the millions. Manually responding to all of these requests with the level of individually tailored information required by the Guidelines is simply not feasible. **We recognise the practical guidance included in the Guidelines (e.g. on layered information as discussed further below), but we would urge the EDPB to develop these recommendations to reflect the feasibility of implementation under the technical and operational realities that our members work with daily.**
- **Balancing access and accessibility for data subjects (throughout):** The Guidelines recognise the tension inherent in (a) providing the data subject with complete personal data, and (b) avoiding overwhelming the data subject with information that they are *‘not interested in and cannot effectively handle’* (para. 35(b)). Yet the Guidelines do not offer an effective solution to this conflict. We would welcome a more detailed discussion of how self service tools can be used to balance access and accessibility; **in particular, if it is reasonable for controllers to encourage the data subject to specify their request as to the level of detail they are looking for in text format together with their downloaded data (if any), this should be emphasised.**
- **The role of the data subject (1) (throughout):** The Guidelines impose additional burdens on the controller that could be mitigated with a more reasonable assessment of the data subject’s role in the subject access request process. **It should be acceptable for a data subject to interpret Article 15 information based on their knowledge of their own relationship with the data controller.** For example, Article 15 information could list recipients (or categories of recipients) who receive the individual’s personal data *if* the individual is using



a specific service feature, rather than undertaking for each data subject an analysis of the specific features they use in order to prepare a highly-customised list of recipients for each data subject. In most cases this would provide the data subject with relevant and sufficiently detailed information for them to understand the data processing, and avoid unnecessary additional data processing on the controller's part. A requirement to analyse, compile, and produce information about a data subject's use of a service as required by the Guidelines contradicts the principle of data minimisation in GDPR Article 5.1 (c), especially if the information must be produced by default with every request to receive a copy of personal data even if the data subject has not requested the tailored information in text format. **We therefore suggest the more general response is appropriate, supplemented with the layered approach suggested above, whereby the controller will engage with any data subject who needs additional information or specificity on a case-by-case basis.**

- **The role of the data subject (2) (throughout):** Separately, the Guidelines require the controller to provide information on data subject rights that goes far beyond the requirements in the GDPR. It is not the controller's role to educate the individual on Chapter III nor to assess preemptively what rights are available to them, particularly as this would often involve legal analysis which is not feasible in the subject access request time frame, nor appropriate for the controller to provide. **Respectfully, we would 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.**
- **Aim of the right to access (Paragraphs 5, 10):** The Guidelines repeatedly mention that the objective of the right to access is to enable individuals to "have control" over their personal data. We caution against using the term "control", as this overlooks the fact that in several instances the controller processes personal data on the basis of the legitimate interest, contractual necessity or public interest legal bases. In these instances, individuals have the right to access and correct their data but may not "control" the whole lifecycle of their data and cannot request deletion of their data for instance.



We would suggest that the Guidelines are more nuanced and clarify that the right of access is primarily intended to verify the lawfulness of processing (see Recital 63 of the GDPR). This clarification would avoid misleading individuals as to the extent of their rights in different data processing scenarios.

- **Right of access in the context of a dispute (Executive Summary & Paragraph 13):** The Guidelines describe that the controller should not assess the ‘why’ of a data subject’s access request and 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.

We do acknowledge and agree that potential motives to use data in court/claims against the controller should not, in principle, strip the individuals of their rights under GDPR.

However, we believe it is to be recognised that requests purely of that nature would still require the controller to allocate resources and effort within the timeframes provided by GDPR, even if those requests may not be relevant to uphold data protection rights. In addition, reference is made in Variation 1 of paragraph 13 to limitations of the scope of information to be provided under Member State national law in “prospective” legal proceedings. It is unclear how the controller can comply with/benefit from such laws if a (prior) request for access is to be honoured without any consideration of the motives of the data subject.

We would suggest that the EDPB considers providing an exception for honouring such requests under the framework of GDPR, to the extent it is evident that such requests are submitted with different motives than ‘*being aware of, and verifying, the lawfulness of the data processing*’. At the very least, we argue that such requests should be assessed in the context of “*excessiveness*”, especially when the information provided is not of the data subject’s satisfaction. In these cases, the controller should be entitled to refer the individual to self-service tools, where available, to download his/her personal data. This would also avoid monopolising company resources to

respond to requests made for nefarious purposes when these resources would be better allocated in responding to other legitimate access requests.

In line with the reasoning above, **we would suggest that the EDPB also elaborates on the steps and considerations for the controller to be able to determine when a request “is made under other rules than data protection rules”,** as mentioned in the Executive Summary.

- **Time reference point of the assessment (Paragraph 38):** We believe the Guidelines go beyond the requirement of the GDPR by requesting that the controller “*shall deal with such requests as soon as possible and before the data is deleted*” and that “*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*”. This overlooks the fact that the controller may sometimes receive a huge amount of access requests simultaneously and will work primarily towards complying with Article 12(3) of the GDPR. This also, generally, overlooks the practical difficulties of adapting the time to respond to a request to the applicable retention period, since this may require the controller to respond to a request in a much shorter timeframe than what is required by and provided for under GDPR.

**Similarly, we recommend that the EDPB revisits its statement in the Executive Summary that “where data is stored only for a very short period, there must be measures to guarantee that a request for access can be fulfilled without the data being erased while the request is being dealt with”,** to clarify that this is referring to adapting the timeframes of responding to a request (see above comment in this regard) rather than adapting the retention periods in order to be able to fulfil such request. Otherwise, this may suggest that the controller should retain personal data longer than necessary for its defined purposes, and solely for the purpose of responding to an access request. We also recommend that the EDPB further clarifies this in light of longer retention periods, that may also expire in the meantime.

**EUTA therefore recommends that the EDPB clarifies and in fact revisits its position so as to separate the timely implementation of the data subject**






access request from the retention procedures applicable to the data to which access is requested.

**Use of ID cards to identify the requesting person (Paragraphs 73 to 78):** While we agree that requesting a copy of an ID card as part of the authentication process may create a risk for the security of personal data, we believe that this risk should be better balanced with the risk for the controller to provide access to data to another person than the data subject to whom the personal data relates. This is the case in particular when the controller only processes pseudonymised data and needs to receive the cookie ID from the data subject before it can retrieve any information. In order to protect individuals against fraud and identity theft, the controller must ensure that the information it receives is indeed that of the individual and not that of a third party. Otherwise, there is a risk that an individual could access the browsing history of someone else through a simple access to someone's terminal allowing them to obtain the cookie identifier. **To avoid this, the controller should be able to ask for a sworn statement that the individual is the owner of the device together with a copy of an ID card in support of the sworn statement.** Such documents are kept for the time strictly necessary to ensure that the individual is the person to whom the personal data relates and will thereafter be immediately deleted from the controller's systems. This is in line with Recital 64 of the GDPR which provides that : *"The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers"*. Merely requesting the cookie identifier as additional information does not seem to be a sufficient reasonable measure to verify the identity of a data subject to address the risk of fraud and identity theft. **EUTA would welcome specific reference to Recital 64 of the GDPR in the Guidelines as well as confirmation that requesting a copy of an ID card together with a cookie identifier can be proportionate in certain situations to address the risk of fraud and identity theft.** Such clarification from the EDPB would be very useful for the industry as well as for individuals exercising their rights.

- **Layered approach (Paragraphs 139, 141, 144, 145):** We welcome the EDPB's suggestion of using a layered approach to respond to Article 15 requests, but would appreciate additional explanation on this point. For example, we question the logic of requiring the controller to always provide complete individualised and tailored information listed in Article 15.1 (a)-(h) even if the data subject may not request it, as we believe this negates the practical benefit of permitting a layered approach in the first place. **We encourage the EDPB to consider permitting controllers to provide a more simplified first layer of Article 15 information in response to general data access requests, which could leverage information from their privacy statement where appropriate.** We suggest that the Guidelines take into account the principle of proportionality for general and broad data access requests (ECLI:EU:C:2009:293, C-553/07) and that the Guidelines specify that an appropriate layered approach to Article 15 information would then involve engaging with data subjects to provide relevant answers to further questions about data processing that might require the preparation of more detailed or individualised information for the particular data subject.
- **Handling large number of requests in specific circumstances (Paragraph 162):** We welcome the acknowledgement by the EDPB that extraordinary events could be regarded as a legitimate reason for prolonging the time of the response. **We suggest the Guidelines also specifically refer to situations such as cyber attacks, security incidents and data breaches as examples justifying more flexibility in addressing access requests.** In these specific cases, controllers may be facing large amounts of requests, especially if they are under the obligation to notify potentially impacted individuals. Controllers may be investigating the causes and impact of the breach while receiving access requests. In this specific case, controllers may also want to require temporary enhanced identification measures to mitigate possible adverse effects of the breach and prevent fraudsters from taking advantage of the situation.
- **Cookie Identifiers (Paragraph 67):** **The Guideline significantly widens the scope of right to access data collected via cookies and similar online identifiers as it does not seem to require authentication of the data subject as a starting**



**point for providing the data.** Many companies have developed their current practices around online accounts through which data subjects can request access to their data. These practices have been implemented based on previous guidance. In the Guidelines on the right to data portability, it is stated that for various services identifying data subjects and verifying their identity through an authentication process can be done via username and password to an account. In fact paragraph 63 of this Guideline refers to this same point. However, according to the example in paragraph 67, controllers who already provide online authentication means to data subjects would need to provide access to data subjects that are not authenticated during a visit on a service and also afterwards via email or regular mail. **We urge EDPB to reconsider the example when applying to controllers that already provide online authentication means to data subjects, especially related to processing the access request via email or regular mail.** It is possible to use many online services without authentication or online account, this typically means that the provider of the service has no directly identified data about the data subject (such as name or email address). If it would be possible to use the right to access data as ‘unidentified user’ of an online service, controllers would not have the means to know whether the request comes from the correct data subject and whether the online identifier they provide as ‘additional information’ only links to data about said data subject or potentially also to other users. Providing access to data in these circumstances would also lead to a situation where the controller will process new and more identifiable personal data about a data subject only to provide them with access to data.

- **Excessive request (Paragraphs 187 and 188):** The Guidelines recognise that a request should not be regarded as excessive on the ground that improper or impolite language is used by the data subject. **We believe however that the EDPB should go further in specifically condemning the use of improper or impolite language in communicating with the data controller and recall that some of these behaviours can be criminally sanctioned under national laws.** Employees of the data controller are the recipients of such messages and should be free from insults and harassments while performing their daily employee obligations.

- **Communication channels (Paragraphs 54–56):** We welcome EDPB’s statement in the Guidelines that *“the controller is not obliged to act on a request sent to a random or incorrect email (or postal) address, not directly provided by the controller, or to any communication channel that is clearly not intended to receive requests regarding data subject’s rights, if the controller has provided an appropriate communication channel, that can be used by the data subject”*.


However, we suggest that the EDPB further specifies what is to be considered *“random or incorrect”* or *“clearly not intended to receive requests regarding data subject’s rights”* (such as an employee’s private address or public profile) and further expands the definition of such terms to factor in the data subject’s own accountability. We argue that consideration should be given to leveraging what the controller already provides as the appropriate communication channel in their privacy statement.

Although we agree that the controller should make all reasonable efforts to deal with such requests, there is a heightened risk of human error and non-compliance if the request is sent to contact points of the controller, not listed as the channel for data subject requests. We would, therefore, suggest that the EDPB considers providing time flexibility for responding to requests not submitted via the official contact point(s) and/or webforms included in the controller’s privacy statement.

- **Freedoms and rights of others (Executive Summary and paragraphs 170–171):** The Guidelines indicate that a request may include data that could concern other persons too, such as communication history (see ‘Scope of the right of access’ in the Executive Summary) and further explain that information concerning others has to be rendered illegible as far as possible (paragraph 171). An example is also given in paragraph 170 of names redaction as part of rejecting specific information in line with Art. 15(4) GDPR.

Although this may be the appropriate solution in certain circumstances, we would recommend that the EDPB further examines providing access in cases



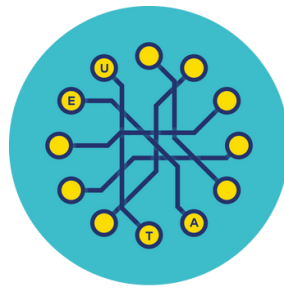


where the identity of other data subjects can be inferred from the actual content, rather than direct identifiers only. That would be particularly relevant, for example, for communications history between (ex) employees, whereby an individual can more easily infer the identity of the other person(s). This also applies to the processing of **personal data in the context of a job interview (Paragraph 95 of the Guidelines)**: The Guidelines consider that a controller is under the obligation to provide a job applicant with the subjective comments made by the HR officer during a job interview. We believe that this example should be aligned with paragraph 171 of the Guidelines. This would enable to better balance the right of access of the job applicant to his/her personal data and the right of the HR officer to the protection of his/her personal data as the subjective comments made by the HR officer are themselves an assessment or opinion of the HR officer. The personal data of the HR manager cannot be subject to a lesser standard of protection than the personal data of the job applicant.

We would, therefore, suggest that the EDPB: (a) adopts a consistent approach throughout the Guidelines on how the right of access and the protection of the freedoms and rights of others are balanced, and (b) offers more detailed guidance on how those interests can be best balanced, taking into account the strict timelines that controllers need to adhere to.

- **Personal data in backup (paragraph 108)**: We note that the Guidelines indicate that when more or different personal data relating to the data subject is stored in the back-up, the controller should provide access “*where technically feasible*” to personal data stored in back-up besides the live production system. **We urge the EDPB to reconsider this statement, taking into consideration the technical limitations in verifying the log of deletions and reconciling with data in back-ups since, realistically, that would be nearly impossible to achieve.**
- **Pseudonymized data (paragraph 45)**: The Guidelines indicate that pseudonymized data that can be linked to a data subject are to be considered within the scope of the request. **We would suggest that the EDPB further clarifies if pseudonymized data need to be provided as well, to the extent the same personal data is provided to the data subject in clear text.**





European Tech Alliance

Adevinta

allegro

BackMarket

bol.com<sup>®</sup>

Bolt

Booking.com

BRAND24

Cdiscount

CODE FOR ALL

CRITEO

Delivery Hero

dreamstime.

eDreams

EMAG

FREE NOW

Glovo

Klarna.

learnWorlds

mestic

ProtonMail

Prowly

Schibsted

sentiance

SEZNAM.CZ

SOUNDCLOUD

Spotify

SUPERCHELL

Testbirds

TOMTOM

trivago

Trustpilot

Vinted

Wolt

xarevision

zalando