

Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

12 February 2020

**ICO Draft Right of Access Guidance Consultation**

Dear Sir/Madam

techUK welcomes the opportunity to provide input to the ICO's consultation on the draft right of access guidance. techUK is the industry voice of the UK tech sector, representing more than 850 companies who collectively employ over 700,000 people, about half of all tech jobs in the UK. These companies range from innovative start-ups to leading FTSE 100 companies. The majority of our members are small and medium sized businesses.

We would particularly like to commend the ICO for the level of pragmatism and detail provided in the draft guidance. For example, the recognition that a controller is able to provide information as "transcripts" rather than original documents. In particular its recognition of the challenges, and possible mitigating factors, that organisations can face when receiving large numbers of data access requests and the challenges that can be faced in identifying data subjects. The clarification provided in the guidance that organisations can ask for further information, in order to identify a data subject, is welcomed and supported. Also welcomed is the recognition that the time an organisation has to respond to a request begins when information needed to verify a data subject has been received.

Also appreciated by industry is the recognition in the draft guidance that, in some circumstances, data subject access requests may be technically complex. The acknowledgement that, in such complex situations, deadlines can be extended to enable organisations time to respond is welcomed. However, this is an area where further examples in the final guidance would be seen as useful. The recognition that organisations use of data may continue as a data subject access request is being processed, which could result in data being amended or perhaps deleted, is also supported.

There are, however, a number of areas where similar clarity and certainty in the draft guidance is being sought by industry. These areas include the following:

- **Individuals only entitled to their own personal data** –The guidance clearly states that an individual is not entitled to information "relating to other people" unless their data "also related to other individuals". Further clarification, and examples, are sought on this point to make it clear when this exception would apply.
- **Can a request be made on behalf of someone?** – It is suggested that the guidance should also recognise that in situations where third parties submit requests on behalf of data subjects, but do not provide sufficient information to enable a controller to verify the identity of a data subject or to contact them, controllers may not be able to reach out to data subjects and carry out requests. Also in this area of the guidance it would be useful for further clarification as to whether written authority provided by an email only, from a known professional organisation domain, be adequate and sufficient evidence.
- **Should we provide a standard form for individuals to make a request?** - For organisations dealing with large volumes of access requests the use of standard forms can help the efficiency and effectiveness of responding to requests. It is therefore suggested that the guidance is amended to state that organisations should "invite" individuals to use standard forms, where available, and to encourage organisations to explain the benefits of using such forms (both in terms of speed and security for requestors).

- **Validating an individual's identity** – It is understood that in situations where an organisation receives a subject access request further information may be requested to validate an individual's identity. However, there may be situations where the information received to validate an identity does not match the records held by the organisation and further information is needed to validate identity, Organisations would welcome further guidance, that in such situations further time is allowed to be taken to ensure an individuals identity is fully validated. It is suggested that the guidance could be improved by providing an example in this area.
- **How do we decide what information to supply?** – The draft guidance states that it may be “helpful” to provide a requester with a “mixture” of personal and non-personal data. As this is a rather complex area it is suggested that further guidance, and examples, should be included to help organisations navigate such situations.
- **Who is responsible for responding to a request?** Further guidance is requested to address situations where a processor is initially sent a request that is meant for a data controller. When such a request is not covered under an agreed contract, further guidance is sought on how a processor should proceed under GDPR.
- **When a request is complex** – The recognition in the guidance that requests can be technical complex is welcomed. In the section outlining this issue it is suggested that the guidance could recognise that the media on which personal data may be stored could be a factor in determining the complexity of a request. For example, the media format used may contain information about other data subjects, for example video content. It may also be useful to expand the list of factors in this area to include, for example, where a search may have to be conducted across different operating systems and, possibly, jurisdictions.
- **What does manifestly unfounded mean?** – The clarification in the guidance that a request can be manifestly unfounded when it is malicious is welcomed. However, the term “manifestly unfounded” is used in the draft guidance a number of times in different places. It would be useful if there was a clear definition of this term early on in the guidance when it is first used. Also, further guidance, and examples, would be welcomed in this area of the guidance to help organisations better understand in which situations the use of “aggressive or abusive language” would mean a request would be considered “manifestly unfounded”.
- **Circumstances relating to the individual making the request** – The guidance on what to do if a request involves information about other individuals is helpful. However, it is suggested that an additional example (page 44) would be useful to help organisations better understand how to make judgement calls regarding the confidentiality of a third party when a request is made.
- **Responding to requests made via a third party online portal** – Further guidance is sought in this section as to how organisations should proceed with requests from third party platforms and applications that may not be deemed safe and secure or adhere to organisations own security policies and procedures. As the access request received by a third-party portal, platform or service may not include information that would enable an organisation to contact the data subject directly advice on how organisation should respond in such situations would be welcomed.
- **What about personal data in big datasets** – Further guidance and clarification is sought on the three bullet point recommendations made in the draft guidance (page 27 and 28). The clarifications requested relate specifically to the situation where the controller's purpose does not require an individual to be identified. For example, where the pseudonymous data is being processed for analytics purposes.

#### 1. Adequate metadata

Further guidance and clarification is sought on the recommendation that organisations should (particularly when collecting data for Big Data analytics purposes) collect or generate additional metadata to enable identification of data relating to individuals in order to enable responses to data subjects access requests. Particularly the expectation that a controller may be obliged to use that metadata to re-identify pseudonymous data in order to comply with a Subject Access Request.

In many cases Big Data databases and analytics rely on pseudonymisation and anonymised versions of data that do not closely relate back to specific individuals. These pseudonymisation, aggregation and anonymisation processes are in fact specifically designed to help protect individual's privacy. This recommendation to collect metadata to ensure data continues to closely relate to specific individuals would undermine those protections and as currently drafted is not clearly aligned with Article 11 of GDPR. Article 11 makes it clear that the controller is not required to collect or process data to identify data subjects for the sole purpose of complying with the GDPR (including for the purpose of complying with data subject rights set out in the GDPR)

**2. The ability to query your data to find all the information you have on an individual.**

Does this require the controller to re-identify pseudonymous data in order to comply with a subject access request? Depending on the type of pseudonymisation used it may be relatively straightforward for the controller to re-identify an individual in the dataset. For example, if the controller tokenises direct identifiers and stores the token map. However, if the controller does not store the token map it could be extremely difficult to re-identify the data. How much effort is the controller required to expend? As above, Article 11 makes clear that the controller is not obliged to retain the means to re-identify the data (e.g. the token map).

**3. Knowledge of whether the data you process has been truly anonymised, or whether it can still be linked to an individual.**

The draft guidance states that a controller should have “knowledge of whether the data (they) process...can still be linked to an individual”. Further clarity would be welcomed on how a controller would demonstrate this, particularly where the controller believes that the data is anonymous. Also, the draft guidance in this area uses the phrase “truly anonymised”. It is suggested that the use of the word “truly” could cause confusion and that the guidance is clarified to ensure a clear and consistent definition and approach to anonymisation throughout the document.

- **Guidance related to Article 11 of GDPR** – In addition to the point above, it would be useful if the guidance could include examples that would help organisations to comply with the requirements in Article 11 of GDPR
- **What is a commonly used electronic format?** – The example in this section of the guidance suggests that an organisation has not “fulfilled its obligations” if they have provided data in a “commonly used” format but an individual still cannot access their data because they first have to pay for software in order to access data stored in a commonly used format. There is a concern of the possible impact on organisations, particularly SMEs, of the guidance in this area which seems to be suggesting that organisations could be required to provide individual data subjects their data in a variety of non-commonly – used formats in order to enable individuals to access data using exclusively free software. Given the reality that computer devices and systems being used by individuals are likely to be using paid for software and that free to use software alternatives will be available, although they may not be “commonly used” by individuals, it is considered disproportionate to suggest to organisations that they should therefore be required to provide individual data subjects information in non-commonly used formats which may be technically complex, expensive (particularly for SMEs) and possibly insecure for an organisation to use.

Also, the draft guidance in this area suggests that organisations should “establish” the electronic format that information will be provided to an individual “prior to fulfilling” a request. Given the large volume of requests an organisation may receive, it may not be practical for an organisation to take such an approach when responding to each and every request. It is suggested that the guidance should be amended to clarify to individuals that this may not happen. This is an area where further clarification and amendments would be welcomed.

It is in these areas of the draft guidance where techUK would welcome additional information and explanation. We would also like to support the important role the ICO plays in raising awareness of individuals rights under the GDPR and would welcome further work in this area to guide, help and support data subjects on how to make subject access requests

We hope this input is useful to the consultation process and would be happy to discuss in more detail any aspect of the issues raised in this letter.

Kind Regards



techUK