

March 11, 2022

Re: Public consultation reference 01/2022 on data subject rights – right of access

To the European Data Protection Board:

Thank you for the opportunity to provide some feedback on the draft guidelines. Worker Info Exchange is a UK based NGO which advocates for and assists gig economy workers exercise their access and other digital rights at work. We have helped thousands of workers attempt to access their data and transparency of its processing. However, our experience shows that, gig economy platform employers have largely either refused or greatly frustrated the proper right of access.

We would like the EDPB to please consider our recently published report: “Managed by bots: data driven exploitation in the gig economy” as an integral part of our submission to this consultation. <https://www.workerinfoexchange.org/wie-report-managed-by-bots> In section II of the report we detail how workers have been systematically frustrated by employers as they attempt to exercise their access rights.

It is fair to say that workers in the so-called gig economy in Europe come from minority communities who face discrimination and a denial of worker rights protections. They are subject to unfair and opaque algorithmic management which can determine who gets work allocated to them, how much they will be paid and even if they will be dismissed. As such, the stakes are high for this community of digital workers. Data access rights are fundamental to being able to realise broader individual worker rights and collective bargaining power.

3.4 Requests made via third parties / proxies

We suggest that paragraph 79 in the guidance be revised to make clear that when a data subject has clearly requested representation by an NGO or trade union and where that mandate has been clearly expressed, and identity is appropriately authenticated then the data controller must provide the requested access.

As the guidelines anticipate in section 5 when suggesting a layered approach to access, data subjects may need expert assistance and the assurance of representation in making access requests. This is especially the case for app-based gig workers where the data held and processed is extensive and complex. There is also huge asymmetry of power in the relationship which means workers do benefit from representation by an NGO or trade union of their choice.

At Worker Info Exchange, we have invested in a secure two step process where the data subject (i) signs a mandate allowing us to act in making a request and (ii) authenticating their identity through a third-party service called Onfido. However, as we have detailed in our report, most gig economy employers refuse to accept our process which we believe is responsible and proportionate. Further, in the case of Uber, they contact the data subjects directly after we have made the request on their

behalf. We believe that such behaviour crosses a line to intimidate the worker and to suppress the proper exercising of their access rights.

We suggest that the EDPB's guidance clarifies that circumventing the representative appointed by the data subject to communicate directly with the DS and/or the refusal of proportionate measures to authenticate the data subject's authorisation of their representative is a breach of art. 80.

In many cases, gig economy employers insist that workers can only make access requests via in app channels. This makes third party representation impossible, and it also means the data subject loses control of the access request record since the employer controls the correspondence record which can and is often cleared from the employer side. In our experience, platforms such as Uber refuse to provide an email address where subject access requests can be directed. The guidelines should expressly address this point that data controllers cannot insist upon only the use of their own portal as a channel to make requests.

Generally speaking, we suggest that the guidance specifies that controllers must facilitate article 80 representation, and that repeated refusals to acknowledge authentication for false pretext could be construed as a breach of art 80

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

We are concerned that the suggestion of a layered approach to access will be wide open to abuse by unscrupulous gig economy employers who seek to withhold access and maintain the opacity of management control.

Our experience is that gig economy employers attempt to steer drivers to a pre-determined data set they wish to allow access to which is far from complete. In other cases, employers such as Uber limit access to vital device data to one month and have so far refused to provide further access than that.

We believe, the encouragement of a layered approach will lead to even further abuse and manipulation of the process in order to frustrate access.

3.4.2 Exercising the right of access through portals / channels provided by a third party

Paragraph 89 reads as if the data controller is never obliged to accept using the portal used by the data subject representative. But in many cases and particularly in a gig economy, employment context, as demonstrated in our report, without representation and portals, the right of access remains largely ineffective.

We suggest that paragraph 89 is amended to clarify that:

- The burden is on the controller to demonstrate that portal is not secure
- If the portal authenticates data subjects and the representative using the same information as for in-app authentication, then the controller cannot refuse to use the portal. For instance: if a driver's identity is verified in in-app authentication, through sending a code via

SMS on their phone, then (i) a portal using the same verification method must be accepted by the controller and (ii) the controller must recognize the validity of the mandate provided by the representative

6.2 Article 15 (4) GDPR

In our opinion the EDPB could provide clearer guidance on when a data controller can legitimately deny access and when such a denial should be openly declared by the controller according to Recital 63: “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.”

In our opinion, this right is widely abused by gig economy platforms who disguise performance management penalties as ‘fraudulent behaviour’. We believe this enables the platform to hide such performance management as a process of employment misclassification by instead labelling it as anti-fraud detection and management. We have covered such concerns widely in our report as cited at the beginning of this document. Indeed, many gig employers use ‘fraud probability scores’ to profile workers for work allocation decision making which clearly shows that such activity is going far beyond the scope of normal security management into human resource management deliberately misclassified. To avoid further such abuse, the EDPB should provide clearer and more definitive guidance and it should also be made much clearer that the data controller must declare what data is withheld and why so that the worker may challenge such decision.

Once again, thank you for the opportunity to submit our comments. The guidance is badly needed in order to protect the proper functioning of access rights.

Worker Info Exchange is available to provide additional information or engagement if helpful.

James Farrar

Director

jamesfarrar@workerinfoexchange.org

+44 7530 319206

Managed by bots: data driven exploitation in the gig economy

<https://www.workerinfoexchange.org/wie-report-managed-by-bots>