Subject: No. 2.1.-3/21/1931

Dear Cansu Safak

Thank you for the correspondence received to date which relates to the portability request on behalf of Drivers from the Worker Information Exchange in correspondence dated 20 April 2021.

The data portability request received by Bolt concerned 36 Drivers operating on the Bolt transportation marketplace.

Authentication, Verification, and Art.(5)(1)(f)

In your request, WIE states it is "*issuing a data portability request in the sense of art. 20 GDPR*" on behalf of the "*Bolt Cabs drivers*". WIE states that this request relates to those named in an excel file which lists the names, email addresses, phone numbers and home addresses of 36 individuals. A final column in the excel spreadsheet indicates that Bolt is the 'Driver Platform'.

The request asks that a response is sent to each driver using the email address associated with their Bolt Driver account. WIE asks that the data is sent in a commonly used, structured, machine-readable format. WIE asks to be informed once the information is sent.

The request states that each driver has authorised WIE to send Bolt this request on their behalf. This authorisation is through a mandate form which appears to be accessed online through the WIE website. This takes the individual to a service called *'Scrive'* which purports to check electronic signatures and undertake an identity verification. Attached with the WIE request is a folder of documents relating to each of the 36 requesters. Each document provides information about the requester and a check to confirm the following statement:

"*I give Worker Info Exchange (WIE)* a mandate to file a Subject Access Request** and Data Portability Request*** on my behalf with the platforms selected above and a mandate to lodge a complaint with a supervisory authority on my behalf, to exercise the rights referred to in Articles 77, 78 and 79 General Data Protection Regulation (GDPR)**** on my behalf, and to exercise the right to receive compensation referred to in Article 82 GDPR on my behalf, where provided for by Member State law*."

The document provided by WIE purports to provide verification of the signature and the name, which is verified by another service provider called '*Onfido*'.

WIE state that each requester has had their identity verified by Onfido using a passport, driving licences, identity card or residence permit. Bolt has not been provided with a copy of these identification documents.

Although WIE has indicated that the requester has provided identification documentation to it, we're unsure how this was verified. It appears entirely justifiable, and indeed a requirement in

data protection law itself, for Bolt as the Controller to undertake its own diligence. It is the Controller's obligation.

It is, for one, necessary to ensure that the email addresses said to be used by the Drivers in the mandate match those email addresses associated with the Driver Accounts. The email addresses of Drivers provided by WIE do not corroborate with those addresses associated on the Bolt Driver platform - and this is a key failsafe mechanism for authentication. The use of the in-App channel for the exercise of user rights would, ordinarily, ensure a prompt authentication check relying on the login credentials and associated email addresses.

And so follows that the request is refused to ensure that the Controller does not breach its compliance obligations.

Extent of Compliance (in any event)

WIE states clearly that this is a data portability request. The request asks for porting of personal data, listing the following information as outlined in the Bolt Privacy Policy for Drivers:

- Name, e-mail, phone number, place of residence.
- Geolocation of drivers and driving routes.
- Information about vehicles (including registration number).
- Driver's efficiency and ratings.
- Driver's license, photo, profession and identity documents.
- Data about criminal convictions and offences. The financial data of providing transportation services is not considered as personal data, because drivers provide services in the course of economic and professional activities.

The personal data that Bolt is required to provide under the portability request is limited in law to the personal data concerning the requester, specifically:

- which the requester provided to Bolt themselves;
- which is being processed on the basis of consent under Article 6(1)(a) or as necessary for the performance of a contract to which the driver is subject under Article 6(1)(b); and
- where the processing is automated.

Information about the driver's "efficiency" is feedback provided by passengers - not information provided by the requestor - and so falls outside the scope of a data portability request. Bolt is currently undertaking a review of the Driver Privacy Policy with a view to improving the choice of wording here, enhancing transparency around the driver ratings function on the platform.

Access is already provided regarding trip data to the Drivers. Any further geolocation data beyond this - in particular, the driving routes - would any event be refused as such a disclosure would damage the rights and freedoms of others; those freedoms extend themselves to economic activity

and related freedoms, protection of intellectual property, and maintaining meaningful competition between enterprises for Bolt.

First, the maturity and sophistication of Bolt's navigation systems, including the integrations with data such as travel dependencies and related variables, may be discovered from the wholesale release of this data should it be delivered in a structured and machine readable format. This would be commercially devastating to Bolt. Our navigation system and our route mapping is a trade secret. Bolt remains commercially viable and able to compete with other transportation operators and transportation marketplace services on price, speed and efficiency of the route suggested to Drivers.

Second, the amalgamation of a larger dataset from individual disclosures to Drivers increases with cumulative effect the likelihood of successfully identifying third parties - i.e passengers. In the past, re-identification of individuals has been shown possible through what looks to be innocuous .CSV data disclosures by other Data Controllers in response to similar requests. For someone so inclined, a genuine attempt with a very real prospect of success can be made to identify a passenger; very simple queries and formulae, in actual fact, could be used to achieve this. Trends and patterns can be pulled from recurring pin-point pick-up and drop-off locations and corroborated across other Driver portability disclosures, and disclosures also from industry peers. The disclosures can also be matched against other personal data available in the public domain such as that which is available on, for example, a passenger's social media profile. The rights and freedoms of others, in particular the right to privacy and an obligation to preserve the security and integrity of personal data, would prevail in refusing a disclosure in this instance. In short, passengers have a reasonable expectation that their rides, and day-to-day or other routines, will remain private.

The privacy notice for Drivers states that information about criminal convictions and offences is processed under legal obligation. These checks are required by law in order for Drivers to operate in a licensed environment. It follows, therefore, that this information also falls outside the scope of a valid data portability request.

The privacy notice for Drivers also states that driver personal data is processed on the ground of legitimate interests in investigating and detecting fraudulent payments. Bolt is only obliged to disclose data under a portability request processed on a relevant legal basis. It follows, therefore, that once more this information also falls outside the scope of a valid data portability request.

Therefore, in principle, Bolt would have looked to comply - having satisfying the relevant authentication checks - with any such portability request through the provision of that which remains within the scope of the obligation:

• Name, e-mail, phone number, place of residence.
• Information about vehicles (including registration number)
• Driver's license, photo, profession and identity documents.

This information is already available to Bolt Drivers in the account portal, and can be inspected and retrieved.

Refusal

The security and integrity of Driver data is Bolt's foremost concern in its handling of this request, and in similar requests from data intermediaries and third party requesting organisations. Such requests present novel data protection risks around mandate, authentication and verification where there are elevated security concerns.

Bolt has been unable to corroborate the email addresses of all 36 Drivers represented by WIE with those same email addresses associated with the Bolt driver accounts. On failing this authentication check Bolt cannot move to comply with the disclosure of the limited data that would fall under the disclosure obligations in this instance.

Other matters

Delay

We would like to apologise for the paucity in a more prompt response on this matter.

It was not Bolt's intention to ignore its obligations to a requesting entity, nor was there any hesitation to afford a fuller explanation regarding the grounds for refusal.

Earlier this year, Bolt HQ was impacted by an outbreak of Covid-19 among staff. At the end of August 2021, the DPO was made unavailable - having taken responsibility to respond to the Inspectorate and WIE in this particular case on behalf of the Controller - due to a personal Covid-related illness, and subsequent bereavement in his family.

Bolt ought to have explained the situation to the relevant parties. For this, the DPO sends his sincere apologies, personally, to WIE. This explanation has been shared with AKI in our latest correspondence with the Supervisory Authority.

Assurances

By way of assurance to WIE, the Privacy Team and DPO function space is set to expand by a further two individuals in December 2021. And a further two individuals will be recruited in early 2022. One of these recruits will have responsibilities to deputise for the DPO. This will afford greater resilience in the event Covid-19 were to again impact the HQ function and resources.

The Controller and the DPO sought the advice of external experts, at significant expense, to determine whether Bolt could proactively overcome the challenges in complying with the WIE request. Workarounds and alternative arrangements were explored to assist those Drivers who

purportedly relied on WIE as a proxy for exercising the right to portability. Work was all-the-time being undertaken in the spirit of the right. On this point, more follows in ‘Next Steps’ below.

In light of this particular case, it was recognised that there are potential program enhancements to help Drivers understand Bolt’s (in actual fact very limited) processing activities even further, and perhaps opportunities to enhance access to their personal data, too; and so resources were also steered to this extent. Work was all-the-time being undertaken in light of the receipt of the WIE request and the appetite evidenced from Drivers in your correspondence and from your website. On this point, more follows in ‘Next Steps’ below.

Next steps

In the spirit of user rights afforded under data protection laws, Bolt is inclined to contact each of the 36 Drivers using the email addresses associated with their Bolt Driver accounts. In that correspondence, we would rehearse the Privacy Notice for Drivers and Couriers. We would also invite Drivers, should they so wish, to submit a request directly through the in-App channel which would afford the necessary authentication check to comply with any request thereafter received directly from the Driver. We hope this goes some way to demonstrating the sincerity in which the request has been received from WIE.

The DPO, having inspected the WIE website, and in light of a strategic vision which touches upon many of the ambitions your organisation, would be willing to discuss the enhancement and empowerment of Drivers and Couriers as data subjects with you, including the elevation of transparency and controls to be made available. The DPO, Calum Liddle, will reach out directly to you in this respect.

Close

While we appreciate that this response is likely disappointing, we hope the refusal is understood bearing in mind the compliance obligations in data protection law both in terms of the extent of the right to data portability, and the Data Controller’s security obligations.

We look forward to engaging with you further.

Yours truly,

Privacy Team