GDPR violation case study: Deliveroo italia srl

Chitradeep Dutta Roy

Brown University

Abstract

In the last decade the world has seen a sharp rise in the number of food-delivery startups that mostly operate online via an app. This is rapidly changing the landscape of traditional restaurant businesses by giving birth to *ghost-kitchens* [5]. These apps rely heavily on people who are commonly known as *Gig workers* [6] for the heart of their operations which is delivering food to doorsteps. On the surface often these apps may seem to provide its delivery workers a lot of flexibility and choice but often times workers relying on these apps for their living are forced to sacrifice their privacy, rights. Due to the contractual nature of these jobs and opaqueness of the backend logic that is crucial for their job performance the workers face unfair treatment. On July 22, 2021, Deliveroo was fined a sum 2.5 million Euro for several violations of GDPR by Italian regulator Garante [1]. We present this case to bring to light some issues related to developing such systems.

1 Background

Deliveroo is an online food delivery company owned by UK Roofoods Ltd. They have business in over 10 countries. Other than UK, they operate in Italy, Netherlands, Spain, France, Belgium, Ireland in EU and also in Australia, Singapore, Hong Kong, Kuwait and Arab Emirates. As part of a probe of food delivery businesses the Italian data protection regulator Garante conducted an on-site inspection (known as dawn raid) on Deliveroo's premises in Milan on 19 and 20 June 2019. The inspection found that Deliveroo uses a centralized computer system managed exclusively by its parent company which is hosted on servers in Ireland. At that time around 8,000 so-called *self-employed* contract riders in Italy were using this system. Each rider was onboarded by signing an agreement with the company and then was given access to an app that she needed to install on their personal mobile phone. The app allowed the riders to set their schedule and then respond to delivery requests as received from the server. This app scored the riders' performance in connection with a number of factors including:

- Availability of the riders in critical time slots such as Friday, Saturday and Sunday evening.
- Reliability of the riders which
- Speed of delivery which of course depended on the vehicle used as well as other factors.

This score helped Deliveroo prioritize sending order request to *online* riders.

2 Details of Violations

2.1 Principles of lawfulness, correctness, transparency, data minimization

About data collection Deliveroo stated on their website "when your status is set to" online ..., we collect data relating to your geographic location on a discontinuous basis", whereas during the assessment it became clear that there was systematic geolocation collection from riders' phones every 12 seconds. This was deemed to be a violation of Art. 5 par. 1. lett. a) [2] of GDPR in relation to the principle of transparency with users.

There were similar inconsistencies also in providing information related to how long telephone, chat and email records of various rider, customer care interactions. Their parent company Roofoods had a policy of keeping 28 days of telephone and email data whereas in terms of Deliveroo's policy it was 1 and 6 years respectively. There were never any clear purpose mentioned in terms of why the data would be stored for such a long period of time, and it also affected users who have resigned from Deliveroo. This violated Art. 5 par. 1. lett. c) [2] in relation to being adequate and necessary for processing.

2.2 Data retention limitation

As mentioned above there was no specific approach in order to assess how long a data should persist in the system when it comes to sensitive information like telephone, email, chat records etc. They were kept for an unreasonably long period.

Moreover, there were instances where there was no data retention limit for such as invoices relating to the payment to riders. This was taken as a violation of art. 13 par. 2 let a) [2] which requires an explicit period for storage or criteria on which it is based. Apart from that as Deliveroo used an algorithmic system *Frank* for assignment of orders to riders integrated to their shift booking system, it had an obligation to disclose to some extent how certain data such as GPS location, vehicle information, speed of delivery, reliability and availability in terms of pre-determined (11, 15, 17) time slots would impact the order assignment since it affected a rider's opportunity to conduct the job. The company did absolutely nothing through FAQs or information on their website to inform its riders about the system This definitely violated art. 13 par 2. lett. f) [2].

2.3 Automated treatments including profiling

As the system assigned orders to riders completely solely via *Frank*, and that algorithmic system used a certain set of factors for its decision-making which Deliveroo's riders didn't explicitly know or themselves chose therefore, it was affecting user's right to intervene or contest any decision made by it. And the system profiled its riders to assign them scores for the same purpose. This was considered to be a violation of art. 22 [2] of GDPR.

2.4 Register of processing activities

During the inspection it was found that the register of processing activities did not have the date of adoption, the date of the last update and the signature, elements suitable to give the document full reliability, in accordance with the provisions of art. 5, par. 2, of the regulation in terms of responsibility or accountability. Therefore, it also violated art. 30, par. 1, lett. c), f), g) [2] in relation to the procedures for drawing up and keeping the register of processing.

2.5 Security measures

Based on company declaration and as an outcome of the inspection it emerged that at least up to 10 July 2020, Deliveroo's system allowed operators to access the data of all riders operating both in the EU and outside the EU without any segregation of jurisdiction. This was a clear violation of art. 32 of GDPR in relation to confidentiality, security, encryption of personal data of the subjects.

2.6 Notification of the appointment of the data protection officer

Deliveroo designated a Data processing officer at the group level, and it was communicated by its parent company Roofoods to its ICO in May 2018. But it failed to communicate it to their Italian supervisory authority until May 2019. As an independent data controller working with rider information directly they failed to carry out that responsibility and thereby violated art. 37 of GDPR which explicitly asks the controller to publish this contact details.

3 Actions

In light of the number and significance of all the violations the Italian DPA levied an administrative sanction of 2.5 million Euro to Deliveroo. It also issued several injunctions to requiring specific improvements to be made like a notice of 60 days to correct its documents regarding treatment register, impact assessment, retention times of various processed user data. Deliveroo was also ordered to produce the identification of appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, at least the right to obtain human intervention by the data controller, to express their opinion and to contest the decision, in relation to automated processing including profiling carried out through their platform in the same time frame. And they were asked to conduct a verification process for checking correctness and accuracy of the results of their algorithmic systems within 90 days.

4 Discussion

Looking at the revenue numbers at [3], it is clear Deliveroo's business is consistently growing. Since 2015 when the company started its operation in Italy its revenue grew from a measly £18 million to £1.2 billion in 2020 which is nearly a 70x growth. From the revenue numbers and also taking into account other GDPR cases of similar stature the fine of 2.5 million Euro seems to be just about right. More importantly I think compliance overall would improve a lot if regular probes like this incident take place more often since GDPR is so new most companies are reluctant to change their development and operational strategies in order to achieve compliance. We have to keep in mind that achieving compliance is often costly and usually holds no economic incentive for them. This is not a single case, Garante in the beginning of July also fined another food-delivery company Foodinho [4] on accounts of similar violations which points out that there is definitely a steady push to encforce GDPR compliance.

5 Prevention

Following are some preventative measure that we propose,

- It might be a good idea beforehand to perform a Data Protection Impact Assessment as mentioned in Article 35 to analyze the risks and take required steps to mitigate chances of non-compliance with respect to the regulation.

- Privacy of user data should be baked into the design principle from the very beginning.
- It should be taken into account how decisions taken on the basis of various user interactions with an application will impact her various rights in real life.
- Companies should attempt to be as transparent as possible about the details of how their application make use of user data and what purpose they are trying to achieve.
- Security of storage of user data and access control within various parts of an application need to be very carefully thought through.
- All parts of an application that do algorithmic decision-making about its users should regularly audit whether the decisions are fair, justifiable and compliant with the law.

References

[1] Garante. Injunction order against deliveroo italy srl - 22 july 2021, July 2021. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994[Accessed 24 September 2021].

[2] GDPR. General data protection regulation, April 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679[Accessed 24 September 2021].

[3] Business of Apps. Deliveroo revenue and usage statistics (2021), August 2021. https://www.businessofapps.com/data/deliveroo-statistics/[Accessed 24 September 2021].

[4] TechCrunch. Italy's dpa fines glovo-owned foodinho 3m dollars, orders changes to algorithmic management of riders, July 2021. https://techcrunch.com/2021/07/06/italys-dpa-fines-glovo-owned-foodinho-3m-orders-changes-to-algorithmic-management-of-riders/[Accessed 24 September 2021].

[5] Wikipedia. Ghost kitchen. https://en.wikipedia.org/wiki/Ghost_kitchen.

[6] Wikipedia. Gig worker. https://en.wikipedia.org/wiki/Gig_worker.