Client Alert: Italian DPA fines Deliveroo & food delivery start-up over AI algorithm use

Date : August 4, 2021

Introduction

On Monday the Italian data protection regulator (Garante per la Protezione dei dati Personali or Garante) fined online food delivery company Deliveroo €2,500,000 for GDPR violations. The case follows another case involving food delivery when Garante fined the operator of an online food delivery platform, Foodinho, €2,600,000 in relation to its use of discriminatory algorithms for managing its delivery riders. Both cases have important lessons for technology businesses in particular and show some of the conflicts between AI and GDPR.

What was the Foodinho case about?

Foodinho is a food delivery business with around 19,000 riders.

This was a joint operation with the Spanish DPA (AEPD) to try to learn more about the operation of the digital platform owned by Foodinho's Spanish holding company, GlovoApp23. The investigation was initiated in response to concerns about how food delivery companies use algorithms to closely monitor workers without adequate transparency about what is happening behind the scenes. (Also relevant is that, under Italian employment law, self-employed workers have certain rights.)

Under GDPR Article 22 (automated individual decision making, including profiling), individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, unless certain exceptions apply and specific protections for those individuals are in place.

The investigation found that the platform's use of algorithms to automatically penalise riders by excluding them from job opportunities if their ratings fell below a certain level was discriminatory, and the fact that there was no opportunity for human review nor the ability to challenge the decision contravened GDPR.

Various infringements were found to have occurred, including:

1. not providing transparent information about how the platform's reputational rating system for riders works
2. not implementing suitable safeguards to ensure that the algorithmic results used to rate riders' performance were accurate and fair – e.g. an unfair weighting was given to negative reviews
3. a lack of safeguards as required under GDPR Article 22, specifically, giving effect to the right of riders to obtain human intervention, to express their point of view, and contest the rider rating generated by the algorithm
4. failure to produce a compliant data protection impact assessment (DPIA)
5. not implementing technical and organizational security measures; and
6. not following data protection by design principles.

In the course of their investigations, the DPAs also uncovered unrelated contraventions related to not appointing a data protection officer where required, and insufficient record keeping.

In addition to the €2,600,000 fine (which took into account failings in Foodinho's cooperation during the investigation, and the high number of riders impacted), the DPA issued an injunction ordering Foodinho take the following corrective measures:

1. implementing measures preventing inappropriate and/or discriminatory use of reputational mechanisms based on customer or partner feedback
2. checking the accuracy and relevance of the data used by the system using a broad range of data points

(i.e. communications between riders and customer care, geolocation every 15-seconds, route mapping, estimated and actual delivery time, handling of current and past orders, customer and partner feedback, device battery level, etc.); and
3. addressing the "*discriminatory risk produced by the rating system, which relies on the application of a mathematical formula that penalizes riders who do not promptly accept orders or reject orders, while prioritizing riders who accept orders on schedule*".

Foodinho's Spanish holding company, GlovoApp23 is apparently considering an appeal.

What was the Deliveroo case about?

The Deliveroo case concerned an on-site inspection (sometimes called a dawn raid) on Deliveroo's premises in June 2019. The inspection found that Deliveroo used a centralised computer system managed by its parent company on servers in Ireland. Around 8,000 delivery riders in Italy were added to the system which scored their performance in connection with a number of factors including:

1. availability of the riders to deliver on Friday, Saturday and Sunday evenings
2. the reliability of the riders
3. the speed of delivery

Again Garante was concerned with Deliveroo's lack of transparency around the way in which it used its algorithm to distribute work. GDPR also has a general fairness requirement (in GDPR Article 5(1)(a)) and as part of that a controller should be able to show that its algorithm is not discriminatory. Deliveroo said that it had changed platforms since the inspection but Garante emphasised that it was incumbent on Deliveroo "to verify, on a periodic basis, the correctness of the results of the algorithms to minimize the risk of distorted or discriminatory effects."

Garante also had other concerns in addition to use of the algorithm including:

1. the collection of geo-location data was excessive
2. some data was kept for too long

In addition to the fine Garante gave Deliveroo 60 days to correct the violations found and a further 90 days to complete the changes to its algorithms.

Does this have broader implications for use of AI?

Yes. We previously published a detailed article, which explains the broader issues related to artificial intelligence and fairness: https://www.corderycompliance.com/ai-and-gdpr-teaching-machines-fairness/.

There is new specific EU AI regulation coming but, if you are using AI, machine learning or algorithms, this can still currently be subject to existing data protection laws.

A concern amongst businesses that sell algorithmic management tools is that they may need to disclose the algorithm, or at least very detailed information in relation to it, either in response to an algorithmic audit from a data protection regulator or a due diligence request from an enterprise customer.

In this scenario, the technology platform is typically a processor and the customer is the controller. It can be challenging for controller organisations to use third party technology for this type of functionality, as often the available product information is not detailed enough to be able to fully understand the workings of the algorithm and the third party will refuse to disclose the algorithm itself as they think it is their "secret sauce". However, from the controller's point of view they need to know enough about the technology and how the algorithm works to be able to comply with their obligations under GDPR, particularly in respect of transparency and fairness.

As a result, if the technology platform's standard product information is not sufficiently detailed, controllers may need to drill down further in their due diligence and possibly even try to secure a right to review (and disclose) the

algorithm or part of it.

What lessons can companies that use algorithmic management of staff learn?

1. **Carry out a DPIA** – there are various privacy risks with this type of technology that need to be properly understood and mitigated.
2. **Ensure that the platform builds in privacy from the start** – the platform design should follow privacy by design principles (e.g. ensure that data minimisation and accuracy checks are built in).
3. **Think about the privacy impact from the individual's point of view** – this should help when assessing the fairness of the platform and also the impact that solely automated decisions may have on them.
4. **Tell individuals how algorithms are using their data** – transparency is key and you should explain to people in easy to understand language about how the technology works and how it can impact their rights and interests, and about their rights when those technologies are used to make decisions that significantly affect them. You will need the platform provider to cooperate with you on this.
5. **Make security a priority** – the platform should deploy robust technical and organisational measures (TOMs) to protect the personal data processed by it, and you will need to carry out information security due diligence to verify that this is the case.
6. **Incorporate proper privacy controls** – this includes checks on accuracy and relevance of the data, algorithmic audits / testing to detect errors and biases, and the safeguards as required under Article 22 that enable for solely automated decisions to be reviewed and challenged. Again, the platform provider will need to work with you on this.
7. **Be prepared for dawn raids** – we're seeing more on-site inspections under GDPR. Make sure that you have a process to follow when a DPA comes knocking.
8. **Ask around** – ethics committees and / or employee focus groups can be useful temperature checks for gauging whether measures are likely to be perceived as overly privacy-intrusive.

For more information

There is more information about this and other data protection topics in Cordery's GDPR Navigator subscription service. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at www.bit.ly/gdprnav.

For more information please contact Katherine Eyres or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

Office: +44 (0)207 075 1784

jonathan.armstrong