**Judgment
COURT OF AMSTERDAM**

**Authority**

Amsterdam District Court

**Date of judgment**

11-03-2021

**Date publication**

11-03-2021

**Case number**

C / 13/692003 / HA RK 20-302

**Jurisdictions**

Civil law

**Special features**

First instance - multiple

**Decision**

Content indication

**Summary** Uber drivers fight termination of their contract due to fraudulent actions. This would have been decided (purely) automatically. After referring the majority of claims to the ordinary civil proceedings in the so-called track switch decision, requests for inspection based on AVG and a request for immaterial compensation for violation of the AVG remain. No decisions based solely on automated processing. Uber still has to partly provide insight into the concrete allegations that led to the decision to deactivate the accounts. Insufficient substantiation of non-material compensation.

Case number / application number: C / 13/692003 / HA RK 20-302

Order of March 11, 2021

in the case of

1. [applicant 1], residing [residence] (United Kingdom ),

2. [applicant 2], residing in [residence] (United Kingdom),

3. [applicant 3], residing in [residence] (United Kingdom),

4. [applicant 4], residing in [residence] (Portugal ),

applicants, attorney at law Mr. AH Ekker in Amsterdam,

against

the private company with limited liability

UBER BV,

established in Amsterdam, defendant, attorney at law Mr. GH Potjewijd in Amsterdam.

The Applicants will hereinafter be referred to separately as [Applicant 1], [Applicant 2], [Applicant 3] and [Applicant 4] and jointly [Applicants] Defendant will be referred to as Uber.

*1. The procedure*

1.1. The course of the proceedings is evidenced by:

* the interim decision of 3 December 2020 and the (procedural) documents referred to therein,
* the official report of the oral hearing of 16 December 2020 and the (procedural) documents referred to therein.

1.2. In an interim order of 3 December 2020, the court referred some of the requests of [applicants] to the summons procedure for further processing. In this petition procedure, the requests referred to in the petition of [applicants] under IV and some of the requests under III and V are dealt with.

1.3. Subsequently, after arrest, a decision was taken today. With the consent of the parties, this case was handled jointly with the case with application number C / 13/687315 / HA RK 20-207 to which partly the same applicants and Uber are parties. In that case, a decision is also given today.

*2. The facts*

2.1. Uber is part of an internationally operating concern that offers online services in the transport sector by means of a digital platform. Uber connects passengers to drivers via applications. Passengers use the Uber Rider app, drivers use the Uber Driver app.

2.2. [Applicants] worked as Uber drivers, using the services of Uber via the Driver app.

2.3. Uber has drawn up a 'Privacy Statement' (hereinafter: the privacy statement) in which it has included general information about the processing of personal data. This privacy statement states about automated decision-making:

“*9. Automated decision-making*

*We use personal data to make automated decisions relating to use of our services. This includes: (…) Deactivating users who are identified as having engaged in fraud or activities that may otherwise harm Uber, its users, and others. In some cases, such as when a user is determined to be abusing Uber's referral program, such behavior may result in automatic deactivation. ”*

2.4. The [applicants] have each received a separate message from Uber informing them that their Uber Driver account has been deactivated because Uber has determined that they have violated the applicable contractual terms and conditions of Uber by being guilty of fraud. [applicant 3], [applicant 2], [applicant 4] and [applicant 1] received this message on July 7, 2018, July 16, 2019, July 2, 2020 and August 4, 2020, respectively. Subsequently, [applicant 1], [applicant 1], [ Applicant 2] and [Applicant 4] each received a message from Uber separately on different dates, containing the following text:

*“Upon review of your account, we noticed a continued pattern of improper use of the Uber application.*

*(…)*

*We are not able to go into great details but the examples of improper use include using your rider and driver account at the same time, creating duplicate accounts, accepting trips without the intention of completing them, claiming false fees or charges, the installation, and use of software which has the intention or effect of manipulating the Driver App and trip details.”*

2.5. The attorney of the [Applicants] ordered Uber in a letter dated 9 September 2020 to undo the deactivation of the accounts and to allow [Applicants] to resume their activities.

2.6. In emails dated September 18, 2020 and September 25, 2020, Uber informed (the attorney of) [applicants] that it saw no valid reasons for revoking the decisions to deactivate the accounts.

*3. The dispute*

3.1. After referring part of the application to the summons procedure, [applicants] in this application procedure - in summary - also request that the court, in an order declared provisionally enforceable:

I. orders Uber to, within one month of service of the order [applicants], provide access in a common electronic form, about the existence of automated decision-making, including the profiling referred to in Article 22 (1) and (4) GDPR1, and at least in those cases, useful information about the underlying logic, as well as the importance and the expected consequences of that processing for [applicants],

II. orders Uber to compensate the immaterial damage suffered by [applicants] due to the violation of provisions of the GDPR, plus statutory interest,

III. orders Uber to pay a penalty of € 10,000 per day for each day or part of the day that Uber fails to comply with the order to be given in these proceedings,

IV. pay the costs of the proceedings.

3.2. The [applicants] base their request on the following. According to [applicants], Uber's decision to deactivate their accounts was taken completely automatically without meaningful human intervention. The decision has legal consequences and [the applicants] have been significantly affected by it. The decision led to the immediate termination of the agreement between Uber and [applicants] and to loss of income. In addition, deactivation by Uber may result in a driver's taxi license being revoked. [Applicants] have not given explicit permission to Uber for the use of automated decision-making. Nor was its application necessary for the performance of the agreement between Uber and [applicants]. Uber has not taken appropriate measures to protect the rights and freedoms and legitimate interests of [applicants]. [applicants] were not given the opportunity to express their views or to contest the decision. All of this is in violation of Article 22 GDPR. The requirements of proportionality and subsidiarity have also not been met.

3.3. Furthermore, prior to the application of the automated decision-making and / or profiling, Uber did not inform [applicants] about the underlying logic thereof and the importance and expected consequences of that processing for [applicants]. under f, article 14 paragraph 2 under g and 15 paragraph 1 under h GDPR. Uber also violated the principle of transparency because Uber did not inform [applicants] of the type of fraud they are accused of and did not inform [applicants] that their accounts would be blocked in the event of fraud. In addition, Uber failed to explain the grounds for the decision in intelligible words.

3.4. As a result of the violation of the aforementioned provisions of the GDPR, [applicants] suffered immaterial damage estimated at € 750 per applicant. Uber must compensate for that damage under Article 82 GDPR.

3.5. Uber has put up a defense. According to Uber, the request must be rejected with a joint and several order of [applicants] for the costs of the proceedings, including subsequent costs, plus statutory interest.

3.6. The arguments of the parties are discussed in more detail below, insofar as they are relevant.

*4 The assessment*

*Jurisdiction and applicable law*

4.1. The court must investigate of its own motion whether the Dutch court has jurisdiction and, if so, whether this court has relatively jurisdiction to hear the [applicants] request. This is the case because Uber is located in the Amsterdam district (Article 4 of the Brussels I bis Regulation2 and Article 262, opening lines and under a of the Rv3).

4.2. Insofar as the request of [applicants] is based on the GDPR, it is directly applicable as a European regulation. From the fact that the parties also base themselves (additionally) on Dutch law, the court infers that the parties implicitly made a choice of law for the application of Dutch law as referred to in Article 3 paragraph 1 of the Rome I Regulation4.

4.3. It is not disputed between the parties that Uber is to be regarded as the controller within the meaning of Article 4 under 7 GDPR.

*The legal framework*

4.4. [Applicants] argue that Uber has infringed their right not to be subject to automated decision-making. They further argue that Uber has not complied with its transparency obligations within the meaning of Articles 13, 14 and 15 GDPR. They request access to the existence of automated decision-making and profiling.

4.5. The rights and obligations included in the GDPR concern different categories of automated processing of personal data in the context of automated decision-making. The following categories are mentioned in the Guidelines on automated individual decision-making and profiling5:

- general profiling without decision-making;

- decision-making based on profiling that is not exclusively automated;

- exclusively automated decision-making, including profiling, which has legal consequences or which otherwise significantly affects the data subject.

4.6. In all cases, the controller must provide the data subject with concise, transparent, comprehensible and easily accessible information about the processing of their personal data pursuant to Article 12 (1) of the GDPR.

4.7. Pursuant to Article 15 (1) of the GDPR, the person whose personal data are being processed has the right to obtain from the controller whether or not they process personal data and, if that is the case, to inspect those personal data. The purpose of this article is to enable the data subject to become aware of the personal data that has been collected about him and to verify whether that data is accurate and lawfully processed (see recital 63 GDPR).

*Automated decision-making and profiling*

4.8. Pursuant to Article 22 GDPR, [applicants] have the right, subject to a number of exceptions, not to be subject to a decision based solely on automated processing (including profiling), which has legal consequences for them or which otherwise significantly affects them. .

4.9. In Article 4 part 4 GDPR, profiling is defined as any form of automated processing of personal data in which certain personal aspects of a person are evaluated on the basis of personal data, in particular with regard to his professional performance, economic situation, health, personal preferences, interests, analyze or predict reliability, behavior, location or movements.

4.10. A decision based solely on automated processing exists if there is no meaningful human intervention in the decision-making process. The Guidelines state that in order to achieve effective human intervention, the controller must ensure that all oversight of decision-making is meaningful and not merely a symbolic act. This intervention must be carried out by someone who is authorized and competent to change the decision. He must include all relevant data in his analysis.

4.11. The Guidelines further state that the threshold for “significant extent” should be comparable to the extent to which the data subject is affected by a decision to which a legal effect is attached. According to the Guidelines, data processing affects someone significantly when the effects of the processing are large or significant enough to merit attention. The decision must have the potential to significantly affect the circumstances, behavior or choices of the persons concerned; have a long-term or permanent effect on the data subject; or, in extreme cases, lead to the exclusion or discrimination of persons. Recital 71 of the GDPR mentions as examples of automated decision-making: automatic refusal of a credit application submitted online or processing of applications via the Internet without human intervention.

4.12. Automated decision-making is permitted, among other things, if the decision in question is necessary for the conclusion or performance of an agreement between the data subject and a controller or is based on the explicit consent of the data subject (Article 22, paragraph 2, opening words and under a and c GDPR). In that case, the controller must still take appropriate measures, including at least the right to human intervention, the right of the data subject to make his point of view known and the right to challenge the decision (Article 22 (3) GDPR and recital 71 GDPR ).

4.13. Automated decision-making in the context of an agreement or on the basis of consent is about transparency about the extent to which automated decision-making plays a role in the implementation of the agreement. When entering into the agreement, the data subject must be aware of the possible use of automated decision-making and profiling.6

4.14. Article 15, paragraph 1, opening words and under h of the GDPR provides that the data subject has the right to obtain from the controller an information about the existence of automated decision-making, including profiling, and, at least in those cases, useful information about the underlying logic, as well as the importance and the expected consequences of that processing for the data subject. Articles 13, paragraph 2, heading and under f and 14, paragraph 2, heading and under g GDPR oblige the controller to communicate the existence of automated individual decision-making, including profiling, and the underlying logic of automated decision-making in every provision of information to data subjects.

4.15. The controller can refuse access if this is necessary for the protection of the rights and freedoms of others (Article 15 paragraph 4 GDPR and Article 41 paragraph 1 sub i UAVG7). It follows from legal history (on the predecessor of the UAVG) that the controller himself is also understood to be 'others' in this context. This provision contains an exception to conferred rights and must therefore be interpreted restrictively. Whether in a specific case there is such a ground that should lead to the limitation or rejection of the application must be decided by the court after weighing up all the interests involved. When invoking this exception provision, the obligation to provide information rests in principle on the controller (in this case Uber).

4.16. Applying the aforementioned principles, the court assesses the request as follows.

*Automated decision-making?*

4.17. [Applicants] argue that it follows from the Uber privacy statement and information published on its website that they are subject to fully automated decisions within the meaning of Article 22 GDPR. That there was no significant human intervention is evident from the standardized and very general messages that [applicants] received from Uber. In these messages, Uber did not explain which specific fraudulent acts [applicants] were guilty of, according to [applicants]

4.18. Uber argues that it has not deactivated the accounts of [applicants] solely on the basis of automated decision-making, so that Article 22 GDPR does not apply. It will not deactivate driver accounts until it concludes, based on a thorough investigation, that the driver in question has committed repeated or serious fraudulent activity. According to Uber, the text from its privacy statement quoted above under 2.3 does not relate to fraud prevention in the European Union and the United Kingdom, where it does not use solely automated decision-making when it deactivates a driver's account.

4.19. Uber has explained the decision-making process as follows. A specialized team of Uber employees (the 'EMEA Operational Risk team', hereinafter: Risk team) investigates potential fraudulent activities. In doing so, use is made of software with which potential fraudulent activities can be detected. Depending on the severity or duration of the activities, such a signal is followed by a warning to the driver or an investigation by an employee of the Risk team. Employees must adhere to internal protocols with indicators that may indicate various fraudulent activities when conducting the investigation. The protocols require employees to analyze the potential fraud signals and the facts and circumstances to confirm or rule out the existence of fraud. They also use facts and circumstances that they consider relevant on the basis of their knowledge and experience. If, based on the investigation, an employee determines that there is a consistent pattern of fraud, a decision may be made to deactivate the driver's account. This requires a unanimous decision from two employees of the Risk team. In the event of conflicting conclusions, an investigation is carried out by a third employee from the Risk team.

4.20. According to Uber, [applicants] repeatedly committed fraudulent activity and their accounts were deactivated after the Risk team identified a consistent pattern of fraud. [Applicants] were informed about this in the messages referred to under 2.4. After receipt of the summons letter of 9 September 2020 referred to under 2.5, employees of the Risk team conducted another investigation into [applicants]. They have come to the same conclusions. Uber informed [applicants] about this in the messages referred to under 2.6.

4.21. Uber has explained the following about the fraudulent acts alleged by [applicants]. [Applicant 1] committed fraudulent acts on or before 3 August 2020 by wrongly collecting cancellation costs from Uber. In doing so, [applicant 1] simultaneously used the Uber Rider app and the Uber Driver app and acted as both passenger and driver. The account of [applicant 1] was deactivated after an investigation and assessment by employees of the Risk team on August 4, 2020, according to Uber.

4.22. According to Uber, the fraudulent actions of [Applicant 2] and [Applicant 4] involve many different activities on or before July 12, 2019 and July 1, 2020, respectively. Their accounts have been deactivated after investigation and assessment by employees of the Risk team, Uber said. .

4.23. According to Uber, on or before June 4, 2018, [applicant 3] used software that manipulated the Uber Driver app to identify more expensive journeys by allowing the passenger's destination to be viewed before the driver accepted the ride (which is not permitted to avoid cherry picking). Using software, Uber has signaled the use of the manipulated app. An Uber employee contacted [applicant 3] by text message and email and examined his account. In a personal conversation on 5 June 2018, an Uber employee explained to [applicant 3] that his account would be deactivated if he used the manipulated app again. A written confirmation of this was sent to [applicant 3] by e-mail dated 6 June 2018. Because [applicant 3] subsequently made use of the manipulated app again on 12 June 2018, his account was deactivated after an investigation by the Risk team, according to Uber.

4.24. The [applicants] have not disputed the above explanation by Uber about its decision-making process. In the absence of evidence to the contrary, the court will assume that the explanation provided by Uber is correct. On the basis of that explanation, it cannot be concluded that the decision to deactivate the accounts of [applicant 1], [applicant 2] and [applicant 4] is based solely on automated processing. Uber has argued without contradiction that this decision was taken by (at least) two employees of the Risk team on the basis of an investigation conducted by an employee in response to fraud signals. According to the undisputed explanation of Uber, the decision to deactivate the account of [applicant 3] was taken after an employee of Uber had investigated the signals about the use of the manipulated app and had spoken to [applicant 3]. In all cases, this involved significant human intervention as referred to in the Guidelines (see 4.10 above).

4.25. It follows from Uber's explanation of its anti-fraud process that it gave to the hearing that after a fraud signal, the driver's access to the Driver app is temporarily blocked until the driver has contacted an Uber employee. Access to the Driver app is reactivated as soon as the driver has made contact. In view of this explanation from Uber, the court assumes that the decision to temporarily block access to the Driver app after a fraud signal will be taken automatically, without human intervention. However, this temporary blocking has no long-term or permanent effect, so that the automated decision has no legal consequences or significantly affects the driver as referred to in the Guidelines (see above under 4.11).

4.26. The conclusion is that it has not been found that Uber has taken automated decisions within the meaning of Article 22 (1) of the GDPR with regard to [Applicants]. Since Article 13, paragraph 2, heading and under f, Article 14, paragraph 2, heading and under g of the GDPR and Article 15, paragraph 1, heading and under h of the GDPR only relate to such decisions, the request for access to the existence of automated decision-making, including profiling, and useful information about the underlying logic, as well as the importance and expected consequences of that processing for [applicants].

*Violation of transparency obligations?*

4.27. The argument of [applicants] that they were not informed in advance by Uber about the possible consequences of fraudulent acts is not supported by the facts. After all, it is not disputed between the parties that different conditions apply to the contractual relationship between Uber and the drivers, including 'Community Guidelines', 'Driver Terms' and 'Services Agreements'. These terms include provisions that prohibit fraudulent activity and may result in loss of access to Uber apps.

4.28. It must have been sufficiently clear to [applicant 1] and [applicant 3] from the messages they received from Uber and the explanations given to them by Uber which fraudulent actions led to the deactivation of their accounts. There is therefore no violation of transparency obligations.

4.29. This is different in the case of [applicant 2] and [applicant 4]. Uber has not clarified which specific fraudulent actions resulted in their accounts being deactivated. Based on the information provided by Uber, they cannot check which personal data Uber used in the decision-making process that led to this decision. As a result, the decision to deactivate their accounts is insufficiently transparent and verifiable. As a result, Uber must provide [applicant 2] and [applicant 4] access to their personal data pursuant to Article 15 of the GDPR insofar as they were the basis for the decision to deactivate their accounts, in such a way that they can are able to verify the correctness and lawfulness of the processing of their personal data.

4.30. Uber's appeal to the exception of paragraph 4 of Article 15 GDPR is unsuccessful. Uber has insufficiently substantiated to what extent providing access to the processed personal data will provide [applicant 2] and [applicant 4] insight into the parameters for fraud detection with which its anti-fraud system can be circumvented.

In this state of affairs, Uber's interest in refusing access to the processed personal data of [applicant 2] and [applicant 4] cannot outweigh the right of [applicant 2] and [applicant 4] to access their personal data.

4.31. The claim for compensation within the meaning of Article 82 GDPR will be rejected. Only with regard to [applicant 2] and [applicant 4] is there a violation of one or more provisions of the GDPR. They have insufficiently substantiated with concrete data that they have suffered immaterial damage within the meaning of Article 6: 106 of the Dutch Civil Code as a result of this infringement. In particular, they did not provide reasons for damage to their humanity or good name or damage to their person in any other way.

*Conclusion*

4.32. The foregoing means that Uber must provide access to the personal data referred to above under 4.29. In order to give Uber sufficient time for this, the period within which Uber must provide this information will be set at two months after notification of this decision. For the rest, the requests will be rejected.

*Penalty sum*

4.33. The requested penalty will be rejected. For the time being, the trust is justified that Uber will voluntarily comply with the order for inspection and will endeavor to provide the relevant personal data.

Enforceability

4.34. Uber has requested that the decision not be declared provisionally enforceable, because if it were to comply with the request, its interests would be seriously harmed and this will have irreversible consequences for the security of its service and other users. There is a risk that it will have to divulge its trade secrets, namely information about the anti-fraud process. Here too, as above under 4.30, Uber has insufficiently substantiated how providing access to the processed personal data would conflict with its trade secrets. The court therefore sees no reason in what Uber has put forward to declare the decision provisionally unenforceable.

*Litigation costs*

4.35. Each of the parties has been (un) right on some point. Therefore, the litigation costs will be compensated.

*5 The decision*

The court

5.1. orders Uber to provide [applicant 2] and [applicant 4] with a copy or inspection of the personal data referred to under 4.29 above, within two months of notification of this decision,

5.2. declares this decision provisionally enforceable,

5.3. compensates the legal costs between the parties, meaning that each party bears its own costs,

5.4. rejects the other requests.

This decision was issued by mr. OJ van Leeuwen, mr. MCH Broesterhuizen and mr. MLS Kalff, judges, assisted by mr. ZS Lintvelt, registrar, and pronounced in public on 11 March 2021.

*1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (hereinafter: GDPR).*

*2 Regulation (EU) no. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), OJEU 2012, L 351/1 (hereinafter: Brussels I bis Regulation).*

*3 Code of Civil Procedure (hereinafter: Rv).*

*4 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (hereinafter: Rome I (https://www.navigator.nl/document/ openCitation / id5aba9745150ee0c2ddda46a806a77ad5)), PbEG 2008, L 177/6.*

*5 Guidelines on automated individual decision-making and profiling for the purposes of Regulation (EU) 2016/679 of the Data Protection Working Party Article 29 of 3 October 2017, last amended on 6 February 2018, WP251rev.01 (hereinafter: Guidelines). This group, now called the European Data Protection Board, consists of representatives of the national data protection regulators.*

*6 Explanatory Memorandum to the General Data Protection Regulation Implementation Act, TK 2017-2018, 34 851, no. 3, p. 46. ​​7*

*Implementing Act of the General Data Protection Regulation.*