DATA PROTECTION AND PRIVACY
University of Genoa

Lesson 5: Order against Foodinho S.r.l.

Italian SA's order against Foodinho S.r.l. - June 10, 2021 no. 234

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677611

The order established several infringements of GPDR provisions and the Italian SA issued several corrective measures and imposed an administrative fine amounting € 2,600,000 on the company

Who is Foodinho?

F is an Italian company which delivers, by way of a digital platform, food or other goods supplied by retailers following orders placed by customers; to that end, the company relies on dedicated staff (so-called riders)

The order by the Italian SA concerns the processing of riders' personal data

Infringements regarding the information provided by Foodinho to the riders (1/5)

Article 5(1)(a) GDPR was infringed in respect of the transparency principle on account of the failure to specify the following: the actual arrangements for processing location data as detected in the course of the inspection and as opposed to the generic information provided; the categories of collected data with particular regard to the data on the conversations via chats, emails and/or phone calls with the call centre; the evaluation of riders by retailers and customers

Infringements regarding the information provided by Foodinho to the riders (2/5)

Article 5(1)(a) GDPR was infringed with regard to the fairness principle, since the obligation to inform employees as part of the employer-employee relations also mirrors the general principle of fairness of processing activities

Infringements regarding the information provided by Foodinho to the riders (3/5)

Article 13(2)(a) GDPR was infringed since the information notice only provided high-level as well as inaccurate information on storage periods and it failed to specify the storage periods for certain data categories

Infringements regarding the information provided by Foodinho to the riders (4/5)

Article 13(2)(f) GDPR was infringed since the information notice did not refer to any automated processing activities including profiling, whilst such activities could be found in the course of the inspections and were intended to score riders so as to rank them in terms of priority in booking the time slots as determined by the company for sending delivery orders; additionally 'no meaningful information was provided regarding the logic of the processing and the importance and consequences of such processing for data subjects'

Infringements regarding the information provided by Foodinho to the riders (5/5)

Article 13(1)(b) GDPR was infringed since no contact details for the DPO were provided

Art. 5 (1) (a) GDPR

Personal data shall be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency principles)

Art. 13 GDPR: Information to be provided where personal data are collected from the data subject (1/4)

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
(b) the contact details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

Art. 13 GDPR: Information to be provided where personal data are collected from the data subject (2/4)

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission

Art. 13 GDPR: Information to be provided where personal data are collected from the data subject (3/4)

In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

Art. 13 GDPR: Information to be provided where personal data are collected from the data subject (4/4)

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(d) the right to lodge a complaint with a supervisory authority;
(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
(f) the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Infringements regarding storage period (1/2)

Article 5(1)(e) was infringed since the company stores several categories of riders' data, which were collected for multifarious purposes, throughout the duration of the employment relation as well as until 4 years following termination of employment

Infringements regarding storage period (2/2)

Article 5(1)(e): Personal data shall be:
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

Infringements regarding configuration of the systems relied upon by the company

Article 5(1)(c) GDPR (data minimization principle) and Article 25 GDPR (privacy by design and by default principles) were infringed since the systems relied upon by the company were configured so as to collect and store all the data relating to the handling of orders and to enable authorised operators to jointly and simultaneously use the data collected by both Admin and Customer systems. Furthermore, the chat and email management system was configured to enable each operator to directly access the contents of the chats and emails exchanged with riders without any further steps being required. Of note, there is a considerable number of entities that are authorised by the company to access the said systems on the basis of profiles allowing full access to riders' data, including detailed information

Infringements regarding the security measures in place (1/2)

Article 32 GDPR was infringed since the systems were configured from inception, i.e. from the start of the company's business in Italy in 2016, until at least activation of the so-called city permission so as to enable access by default to a substantial number of personal data by a significant number of system operators in connection with a wide gamut of tasks to be discharged by riders. This did not allow ensuring 'confidentiality, integrity, availability and resilience of systems' on a permanent basis, taking account of the factual risks due to the 'loss, alteration, unauthorised disclosure of, or accidental or unlawful access to the personal data'

Infringements regarding the security measures in place (2/2)

Article 32 (Security of processing): 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

Infringements regarding the need for a DPIA

Article 35 GDPR was infringed since the processing implemented by the company - which concerned a substantial amount of data of various nature relating to a considerable number of data subjects and was performed by way of a digital platform relying on algorithms to match offer and demand - was clearly innovative in nature and fell as such within the scope of the obligation to carry out a data protection impact assessment. The innovative nature of the technology deployed and therefore of the activities performed by the company lies firstly in the fact that labour is also managed through a digital platform whose operation is based on complex algorithms – indeed, the functioning of those algorithms was disclosed only in part. Secondly, the innovative features of the technology relied upon consist in the use of automated processing, including profiling, which significantly affects data subjects on account of the processing of multifarious data, including geolocation data, and the resulting exclusion of some riders from working opportunities

Infringements regarding automated processing, including profiling (1/2)

Article 22(3) GDPR was infringed since the company carried out automated processing activities, including profiling, both within the framework of the so-called 'excellence system' and as part of the order allocation system; whilst one of the exemptions provided for by Article 22 applied to the specific processing, which was necessary for the performance of a contract between the parties, it does not appear that the company implemented suitable measures 'to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention to express his or her point of view and to contest the decision'

Infringements regarding automated processing, including profiling (2/2)

Article 22 (Automated individual decision-making, including profiling):
1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
(c) is based on the data subject's explicit consent

Infringements regarding communication of the DPO's contact details

Article 37(7) GDPR was infringed since the company communicated the contact details the group-level DPO to the Italian SA via the ad-hoc online procedure made available on the SA's website as late as 1 July 2020

Infringements regarding the records of processing activities (1/2)

Article 30(1), letters a), b), c), f), and g) was infringed since it could be established that the records did not include information on several categories of personal data; there was no specific information on storage periods; there was no general description of the technical and organisational security measures; and finally, the records did not allow keeping track of their change history

Infringements regarding the records of processing activities (2/2)

Article 30 (Records of processing activities):
1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
(b) the purposes of the processing;
(c) a description of the categories of data subjects and of the categories of personal data;
(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation;
(f) where possible, the envisaged time limits for erasure of the different categories of data;
(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1)

Infringements regarding lawfulness of the processing (1/2)

Article 5(1)(a) and Article 88 GDPR, and Section 114 of the Italian data protection Code were infringed since the riders' personal data were processed by the company as part of the relevant employer-employee relations in breach of the applicable employment laws regulating remote surveillance of employees (Law No 300 of 20.05.1970) as well as of the provisions protecting labour on digital platforms (legislative decree No 81 of 15 June 2015)

Infringements regarding lawfulness of the processing (2/2)

Art. 88 (Processing in the context of employment)
Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.
2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place

Outcome of the procedure (1/5)

The Italian SA ordered the company to bring their processing operations into compliance with the GDPR in respect of the following:

- The documents containing the information notice, the records of processing operations and the DPIA, by also ensuring consistency among the processing operations;

- Specification of the storage periods of processed data;

Outcome of the procedure (2/5)

- Suitable measures to safeguard the data subject's rights, fundamental freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision, with regard to the automated processing performed via the platform including profiling

Outcome of the procedure (3/5)

- Suitable measures to regularly check fairness and accuracy of the results of algorithmic systems, partly in order to ensure that the risk of errors is minimised;

- Suitable measures to introduce arrangements that can prevent inappropriate and/or discriminatory applications of feedback-based reputational mechanisms; this assessment will have to be performed each time the algorithm is changed as for the use of feedback information to calculate the scoring

Outcome of the procedure (4/5)

- Application of minimization and privacy by design and default principles in respect of the entities authorised to access the various data categories, by having regard to the tasks allocated in the individual cases;

- Compliance with the provisions made in Section 4(1) of Law No 300 of 20.05.1970

Outcome of the procedure (5/5)

- An administrative fine was imposed in addition to the corrective measures by having regard to the circumstances of the individual case, amounting to EUR 2,600,000.00