GDPR & Non-Compliance: Sanctions Imposed by the Finnish DPA

The role of national data protection authorities in overseeing the implementation of the European Union's Data Protection Regulation (GDPR) by imposing fines for non-compliance has proven to be one of the most attention-catching features of national GDPR implementation. The most recent example is the fine imposed on Amazon EU by the Luxembourg National Commission for Data Protection. In this article, we look at the cases where administrative fines for non-compliance have been imposed in Finland.

The fine of EUR 746 million against Amazon EU, headquartered in Luxembourg, was imposed on 16 July 2021. It is considered to be by far the biggest fine imposed on a company under the GDPR and is a prime example of the power of national data protection authorities in overseeing the implementation of the GDPR.

We are often asked about the enforcement landscape in the Nordics. We outline below the enforcement trends of the Finnish Data Protection Ombudsman by describing some of the Finnish national enforcement decisions and giving an overview of the sanctions imposed.

A variety of breaches led to sanctions

Two years after the GDPR became applicable, the Sanctions Board of the Finnish Data Protection Ombudsman's Office (Data Protection Authority, DPA) imposed its first administrative fines for breaches of the GDPR and the Finnish Data Protection Act (1050/2018). The fines imposed by the DPA prior to July 2021 were between EUR 7,000 and EUR 100,000, ranging from 0.08% to 3.3% of the annual turnover of the relevant companies. The fines related to a variety of data protection breaches, such as:

- lack of data protection impact assessments;
- lack of adequate information to data subjects on the processing;
- inadequate information on data subjects' rights;
- lack of proper consent in electronic direct marketing / robocalls;
- lack of data processing agreements;
- improper processing of location data; and
- lack of legal basis for processing.

The Sanctions Board has considered the following as mitigating factors affecting the amount of the fines: the controllers' active participation in the proceedings, consequent activities to achieve compliance, and a low number of data subjects.

It should be noted that, even in cases where the organizations' actions were deemed negligent, the maximum fines under the GDPR have not been imposed. The highest fine imposed by the DPA (3.3% of the company's annual turnover) was for carrying out direct marketing without the prior consent of the data subjects. It is also worth noting that an Administrative Court has issued the first national judgment in which the validity of the sanction imposed by the DPA has been considered. The sanctions are presented below by category, highlighting the main non-compliance issues that led to the fine. Link to a table highlighting the sanctions

Inadequate preparation for processing

Fine of EUR 16,000 for failing to carry out a Data Protection Impact Assessment

The controller, a regional water supply and treatment company, had processed employee location data for work time monitoring via a vehicle data system, affecting approximately 47 employees from 2017 to 2020. The company had not carried out a Data Protection Impact Assessment (DPIA) to assess the possible risks of the processing on data subjects prior to commencing processing, as required by the GDPR. The company stated that the failure to take the necessary action was due to legal uncertainty regarding data protection during the relevant period. The DPA, however, found the company's omission negligent, since guidelines on DPIAs were available during the period of the processing and the company also had a reasonable time to rectify its practices. The DPA also considered that the company had failed to take sufficient technical and organizational measures in order to protect the rights of data subjects.

The DPA found that there were two factors present that required the company to conduct a DPIA, namely the processing of location data and the use of data to systematically monitor employees who were considered to be in a vulnerable position. As a result, a fine of EUR 16,000 was imposed on the company, which represented less than 0.1 percent of the company's annual turnover of EUR 20.3 million during the preceding financial year. The decision was appealed to the Administrative Court of Eastern Finland, which rendered its decision on 20 May 2021. The Administrative Court found that it was appropriate to impose the fine and the amount was effective, proportionate and sufficiently cautionary.

Fine of EUR 72,000 for failing to carry out a Data Protection Impact Assessment and other failings

The controller, a taxi company, had failed to carry out a DPIA prior to processing camera surveillance data and location data, or prior to commencing automated decision-making and profiling as part of the company’s loyalty program. According to the DPA, processing of voice data in camera surveillance was conducted in some cars, contrary to the principle of data minimization. The DPA further considered that the company had failed to adequately inform the data subjects of the processing of their personal data, as information on voice recordings or profiling and automated decision-making was not made available to them. The DPA also identified additional deficiencies in documentation, as well as in the analysis of processing roles, which the company was ordered to rectify.

The violations as a whole had reflected serious failings in respect of the basic conditions for the processing of personal data, and indicated the negligent nature of the company's actions. Since processing of personal data was part of the company's core business and data was processed on a large scale, a significant number of data subjects and various types of personal data were affected. As a result, a fine of EUR 72,000 was imposed. The fine represented around 0.7 percent of the

company's annual turnover of EUR 10.1 million during the preceding financial year. Interestingly, the COVID-19 pandemic was considered as a mitigating factor when calculating the appropriate fine, due to the taxi industry being among the industries the pandemic hit hardest.

Failure to ensure data subjects' rights

Fine of EUR 100,000 for failings in informing data subjects of their rights

Customers of the controller, a major postal service company in Finland, received unwanted marketing after submitting a notification of change of address. Hundreds of thousands of data subjects were affected over a period of several years. The investigation revealed failings in terms of the lawfulness of processing as well as in informing data subjects of their right to restrict processing, especially the possibility to prohibit disclosures of personal data. The DPA considered that providing this information with a link to a privacy notice and terms and conditions on the company's website outside the actual electronic change of address form were not sufficiently active methods of informing customers, as the links were outside the actual electronic change of address form. Further, data subjects were not treated equally, as the information on the electronic form was only provided to paying customers who purchased additional postal services.

The company was fined EUR 100,000, which represents under 0.1 percent of its annual turnover of EUR 1.5 billion during the preceding financial year. Although no material damage was caused, the DPA found that the substantial number of data subjects affected and the long duration of the violation were indications of systematic and intentional non-compliance. The DPA also considered the financial gain made by the data controller through its non-compliance to be a factor affecting the appropriate size of the fine.

Fine of EUR 75,000 for failing to ensure data subjects' rights

The DPA had received several complaints relating to various activities of the controller, a company which operated a parking operating service. For example, the company had failed to provide information about the source of personal data or the basis for processing. Requests had also been made relating to the access to and erasure of personal data, which the company refused to act on before it had verified the requester’s identity. The company had requested that data subjects submit personal data, such as personal identity codes and addresses, to the company. The DPA held that the information requested was not necessary to identify the data subjects and, therefore, the action was contrary to the principle of data minimization. Finally, the DPA also considered that the company's operations regularly violated the GDPR and ordered the company to amend its practices to be compliant with the law. Considering the nature of the violations, their duration and the number of data subjects affected by them, it was held that the company's actions had been intentional and the violations were severe and continuous.

A fine of EUR 75,000 was imposed on the company, which represents approximately 0.6 percent of its annual turnover of in excess of EUR 12 million during the preceding financial year. The decision is not yet final as the company has appealed the decision to the Helsinki Court of Appeal.

Fine of EUR 7,000 imposed for conducting direct marketing without prior consent and for disregarding the rights of data subjects

The controller, a consulting company, had conducted direct marketing without the prior consent of data subjects and, in addition, had failed to uphold their rights under the GDPR. In the direct marketing, advertisements were sent via text messages to data subjects' work numbers. The data subjects continued to receive such marketing despite opting out by responding to the text message.

The company argued that, since the phone numbers were used by the data subjects' employer, no prior consent for direct marketing was needed as it was targeted at companies rather than individuals. However, the DPA emphasized that the company should have evaluated whether the marketing was essentially linked to the data subject's duties. Under the case law of the Market Court, requesting consent for direct marketing via text messages is considered to be electronic direct marketing, which requires an opt-in (unless the requirements for soft opt-in have been satisfied, such as in B2B relationships). Moreover, the company neglected to respond to and fulfil the requests of data subjects regarding their rights to receive transparent information about the processing of their personal data, the right to access their own personal data, the right to erasure, and the right to object to the processing. The company also failed to illustrate the lawful nature of its actions. The DPA considered that the number of similar breaches in a short time and the fact that the breaches occurred within the company's core business activities indicated that the company acted knowingly and intentionally. In addition, the breach occurred within the company's core business activities, in other words providing and marketing a variety of courses.

The company was ordered to change its conduct. In addition, a fine of EUR 7,000 was imposed on the company, which represents approximately 3.3 percent of its annual turnover of EUR 210,000 during the preceding financial year.

Fine of EUR 8,500 imposed for carrying out direct marketing with robocalls without consent

The controller, a magazine publisher, had used the services of a processor to make automated calls, referred to as "robocalls", for marketing directly to recipients without their consent. Data subjects could not exercise their data protection rights as the automated message did not respond to their questions. The company obtained the consent to direct marketing on its website, in connection with a magazine subscription, which did not sufficiently fulfil the standard for consent required by the GDPR. Consent could not be considered to have been given voluntarily, since it was not separately requested for direct marketing. Additionally, the agreement in which consent was requested did not transparently state how personal data would be processed for direct marketing. In addition, since the calls were carried out by a subcontractor, it acted as a processor of personal data without a proper agreement for such processing.

A fine of EUR 8,500 was imposed on the company, which represents almost 2 percent of its annual turnover of over EUR 400,000 during the preceding financial year. The subcontractor was not fined, as this was considered disproportionate, but a reprimand was issued to the subcontractor for failing to satisfy its obligation to draft such an agreement with the controller.

No legitimate basis for processing

Fine of EUR 25,000 imposed for processing employees' location data without a legitimate basis

The most recent sanction was imposed on 5 July 2021 on a controller, an Institution of Higher Education. The employer monitored working hours of employees, which included processing employee location data. The processing of this location data did not have a legitimate basis as required by the GPDR, and breached the principle of lawfulness, fairness and transparency as well as the principle of data minimization.

These breaches constituted serious offenses under the GDPR and, therefore, a fine of EUR 25,000 was imposed on the controller. This represents approximately 0.4 percent of the controller's annual turnover of EUR 62 million during the preceding financial year.

Fine of EUR 12,500 imposed for processing unnecessary data in a recruitment process

In its recruitment process in 2018 and 2019, a controller company asked job candidates to fill out a form inquiring about data considered unnecessary for the employment process. The personal data encompassed special categories of data, for example military rank, family ties, spouse's profession and workplace, the year of birth of their children, parish, health conditions and possible pregnancy of job applicants who are considered to be a in vulnerable position in respect to the prospective employer. The controller claimed that disclosing the information was voluntary. However, under Finnish employment privacy legislation, consent cannot override the principle of necessity applicable to all processing of employee personal data.

It was concluded that the data may have led to discrimination in recruiting. The number of data subjects potentially affected, compared to the overall number of employees of 150, was not deemed to be especially high. However, the company lacked the required data processing documentation, in other words the records of processing activities required under Article 30 of the GDPR. Even though organizations employing fewer than 250 people are exempt from certain obligations pertaining to records of processing activities, the company was considered to be under the obligation to maintain such records, as it processed personal data of employees systematically and special categories of data were involved.

The company was ordered to delete all data for which no legal basis for processing existed. In addition, a fine of EUR 12,500 was imposed, which represents around 0.08 percent of the company's annual turnover of almost EUR 15 million in the preceding year.

Conclusions

As can be seen from the decisions above, the Finnish Data Protection Authority has not yet imposed many sanctions. The sanctions imposed have been relatively small in comparison to the annual global turnover of the relevant companies, and are definitely not on the same scale as some of the hefty European sanctions, such as the fine imposed on Amazon EU. One possible explanation for the small number of DPA sanctions imposed in Finland is the fact that the proceedings relating to Finnish sanctions did not fully kick into gear until about a year ago. Prior to this, in the first few years post-GDPR, the DPA focused primarily on providing guidance to organizations on the data protection requirements. Having issued guidance on how to be GDPR-compliant, it seems like the DPA is moving on to the next stage of GDPR enforcement via sanctions.

In its list of focus areas for 2021, the DPA has listed the following as areas it will pay special attention to:

- third-country data transfers,
- informing data subjects,
- impact assessments of data protection measures,
- improving the handling of security breaches and accountability for data protection breaches (especially in the application of the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018)).

It remains to be seen whether larger sanctions will be imposed in the future as a result of this.

Article written by Associate Trainees Suvituuli Heikkinen, Johanna Parkkinen and Jennika Sucksdorff.