OFFICE OF
THE DATA PROTECTION OMBUDSMAN

Letter TSV/35/2019

3 February 2025

Recipient: [redacted]

Letter from the Office of the Data Protection Ombudsman

The Office of the Data Protection Ombudsman initiated an investigation on 20 March 2019, into a matter concerning the transfer of data. The Office became aware of the event in question through a combination of whistleblower reports, general news coverage, and a statement issued by [redacted]. Allegations regarding the event suggest that data originating from [redacted] was transferred outside the European Union and the European Economic Area.

The Office of the Data Protection Ombudsman has reviewed a statement published on [redacted]s website on 22 March 2019. According to the statement, the issue pertained to a specific batch of [redacted] devices that had been mistakenly installed with software intended for phones sold in the Chinese market. Due to this erroneous software, the devices attempted to send 'activation data' to third-party servers of a Chinese telecommunications operator. The statement asserted that no data was processed in a way that could identify any individual, nor could an individual be identified based on the data. Furthermore, the statement claimed that the issue had been identified and corrected as of February 2019, with a patch deployed to all affected devices. However, at the time of the statement's publication, the patch had not yet been installed on all devices.

The infographic included in the statement described data collection from the device. According to the infographic, [redacted] collected data to initiate the phone warranty ('start phone warranty'), enhance user satisfaction, and improve the product experience. The data collected was categorized as activation data and phone diagnostics data.

The Office of the Data Protection Ombudsman requested clarification from [redacted] regarding the matter. The company provided written explanations on 10 May 2019, 28 February 2022, and 27 March 2023.

The Office of the Data Protection Ombudsman concludes its handling of the matter with the following guidance.

Guidance from the Office of the Data Protection Ombudsman

Under Article 4(1) of the General Data Protection Regulation (GDPR), personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an

online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Under Article 4(12) of the GDPR, a personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The GDPR imposes several obligations on data controllers in the event of a personal data breach. According to Article 33, the data controller must notify the supervisory authority of a personal data breach unless it is unlikely to result in a risk to the rights and freedoms of natural persons. Additionally, under Article 34, the data controller must communicate the data subject of the breach if it is likely to result in a high risk to the rights and freedoms of natural persons.

In this case, certain [redacted] devices attempted to send specific activation data to a Chinese telecommunications operator. The activation data included, among other things, the IMEI code, IMSI code, Cell ID, and MAC address. [redacted] has asserted that this activation data did not constitute personal data in its operations or those of the telecommunications operator. According to the company, it was not possible to identify a natural person solely based on the activation data. Furthermore, the company stated that it could not practically combine the activation data with other information to identify a natural person, nor could the telecommunications operator identify individuals or combine the data with other information.

The Office of the Data Protection Ombudsman considers that activation data may, in certain contexts, be information related to an identified or identifiable natural person. Activation data pertains to a specific individual, and it is possible to indirectly identify the individual based on the data.

Data controllers are obligated to identify situations involving personal data breaches to comply with the obligations outlined in Articles 33 and 34 of the GDPR. In this case, [redacted] did not notify the Office of the Data Protection Ombudsman of a personal data breach and did not consider the event to constitute such a breach.

The Office of the Data Protection Ombudsman advises [redacted] to ensure in the future that it identifies situations involving personal data breaches and, if necessary, submits notifications in accordance with Articles 33 and 34 of the GDPR.

Signature

[redacted]
Data Protection Ombudsman

OFFICE OF
THE DATA PROTECTION OMBUDSMAN

[redacted]
Senior Officer

Contact information

Office of the Data Protection Ombudsman
E-mail: tietosuoja@om.fi
Postal address: P. O. Box 800, 00531 Helsinki, Finland
Tel. (switchboard): +358 29 566 6700
Website: tietosuoja.fi