Path: Home page > Main menu > Supervisory and decision-making activity Control of the processing of personal data of antivirus software users (Avast Software s.r.o. company)

On the basis of a complaint filed with the Dutch supervisory authority, the Authority carried out an inspection, the subject of which was the processing of personal data of users of anti-virus software. Given that the matter in question involves cross-border processing of personal data, with the main establishment located in the territory of the Czech Republic, the Office is in the position of the leading supervisory authority within the meaning of Article 56(1) of Regulation (EU) 2016/679, concerned supervisory authorities are the supervisory authorities of all member states of the European Union and the European Economic Area. The subject of the complaint was the inability to disable the preset privacy options in the free version of the antivirus software. During the inspection, it was found that each individual installation of antivirus software is assigned a unique designation (Device ID and Installation ID) and, further, that in order to ensure the proper functionality of the antivirus software, it is necessary for the inspected person (at least for a certain period) to have the IP address of the device, on which the antivirus software is installed. Device data and operational data (for example, information about searched URL pages, installed applications, saved files) sent by antivirus software are thus associated with both the Device ID and Installation ID of the given device, and for a certain period of time also with the current IP address (until the IP address is replaced with less specific data). With regard to the audited person's claim, the auditors particularly addressed the question of whether the data processed by the audited person constitute personal data. In this regard, the auditors relied, among other things, on Recital 26 of Regulation (EU) 2016/679, according to which, for example, single-out selection is sufficient for the identification of a certain person. The individualization of a person can thus be done by combining data with individual identifiers, for example with an IP address, a MAC address, or another identifier of an installation or device that is usually used by natural persons. Article 4 point 1) of Regulation (EU) 2016/679 also explicitly states that a natural person can be identified, for example, by reference to a network identifier. Another basic starting point was that for the assessment of the nature of information as personal data, it is not decisive whether this information enables the direct identification of the data subject (i.e. that the administrator will connect the data with a specific natural person himself on the basis of the information he has or can obtain), or indirect identification (i.e. that it is necessary to use the cooperation of several entities to identify a person). This conclusion also corresponds to the jurisprudence of the Court of Justice of the European Union, for example the judgment of the second chamber of the Court of Justice of the European Union of October 19, 2016 in case C-582/14 (Breyer v.

Bundesrepublik Deutschland), in which this court leaned towards an objective concept of the concept of personal detail. The Office therefore came to the conclusion that the controlled person has information that, in its entirety, can lead to the identification of the user, and on the basis of which the natural person can be identified. Therefore, in connection with the provision of the anti-virus software service, the controlled person collects and further processes such user data that is personal data. At the same time, this conclusion applies to all versions of antivirus software (intended for Windows, Apple Mac and Android operating systems), both for their paying and non-paying users, since the installation process and further functioning of the antivirus software do not differ in essential parameters. The inspectors therefore came to the conclusion that the inspected person is in the position of administrator of personal data of users of anti-virus software. However, during the inspection, the inspected person repeatedly stated that he does not process personal data (beyond the data necessary to make a payment for paying users of antivirus software) and that the data of non-paying users is anonymized. The conclusion made by the inspectors in relation to the nature of the processed personal data was rejected by the inspected person. Although the inspected person during the inspection provided detailed information about his activities, or on the installation and basic functionality of the anti-virus software as well as on the processing of data for secondary purposes (in particular statistics, analyses, further product development and marketing), the inspectors came to the conclusion that the inspected person did not demonstrate compliance of his procedures with the basic principles in the sense of Article 5, paragraph 2 of the Regulation (EU) 2016/679, i.e. that it violated the principle of responsibility and at the same time Article 24, paragraph 1 of Regulation (EU) 2016/679, i.e. it did not prove that the processing is carried out in accordance with Regulation (EU) 2016/679. Therefore, at this stage, the controllers could not assess the fulfillment of the principles set out in Article 5, paragraph 1 of Regulation (EU) 2016/679, in particular, what legal basis the controlled person determined in relation to all sub-purposes of personal data processing and whether, under the given circumstances, such a legal basis is applicable. The President of the Office partially complied with the objections that the inspected person filed against the inspection findings, and canceled the conclusion of a violation of Article 5, paragraph 2 of Regulation (EU) 2016/679. If the inspected person does not rectify the illegal situation himself, the Office in the matter initiates proceedings to impose measures to eliminate identified deficiencies. The inspection was conducted by the inspector JUDr. Jiřina Rippelová. Recommendation: Also, data on the use of a certain device, if this device is uniquely identified and if these data are linked to a unique identifier, can in their summary lead to the identification of a specific natural person. Such data are then personal data, even if the identification of data subjects is not

carried out and is not the intention of the controller.

ContextLocation: Document folders > Site map > Main menu > Supervisory and decision-making activities > Completed inspections > Inspections for 2019 > Inspection activity in the field of personal data protection - 1st semester > IT technology > Inspection of personal data processing of antivirus software users (Avast Software company s.r.o.)View current documents | document archive | documents including the archive