THE OFFICE FOR PERSONAL DATA PROTECTION
Pplk. Sochora 27, 170 00 Prague 7, Czech Republic
Phone: +420 234 665 111, Fax: +420 234 665 444
posta@uoou.cz, www.uoou.cz

No. UOOU-07166/18-XX
Prague X March 2019

Inspection report

Supervisory authority:

The Office for Personal Data Protection, with its seat at Pplk. Sochora 27, 170 00 Prague 7, ID 70837627, (hereinafter referred to as 'the Office').

The authority's power to exercise inspection results from Article 58(1)(b) of 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 (General Data Protection Regulation), in conjunction with Section 2 (2) and (3) of Act No 101/2000 on the Protection of Personal Data and on Amendment to Some Acts.

Supervisory staff:

[redacted] — the inspector of the Office, inspector's card [redacted],

[redacted]

[redacted]

Inspected party:

[redacted], with its registered office at [redacted], represented by [redacted] on basis of Power of Attorney of 8 November 2018,

(hereinafter referred to as [redacted]).

Subject of inspection:

The subject of the inspection is compliance with the obligations laid down in Regulation (EU) 2016/679 with regard to the processing of personal data of the customers of [redacted] (users of antivirus software, hereinafter 'antivirus SW'), with a focus on the level of protection of the privacy of users of the free version of the antivirus SW with comparison to the paying users.

First inspection act:

Notice on commencement of inspection, No. UOOOU-07166/18-7, delivered on 2 July 2018.

Last inspection act:

Supplemental statement of the inspected party of 30 January 2019, No. UOOU 07166/18-34.

I. <u>Summary of documents:</u>

The inspection report shall be based on the following materials and documents which were collected before and during the inspection and, where appropriate, the documents and information known to the inspection authority from its official activity.

1. Official record of the installation of the free version of the antivirus SW of 25 June 2018, No. UOOU-07166/2018-2, 1 sheet;
2. Official record of the action preceding inspection act of 28 June 2018, No. UOOU-07166/18-6, with annexes:
    a. a notice on the appointment of the Data Protection Officer of 30 May 2018 (information from the Office's information system), 2 sheets,
    b. the website's discussion [redacted] (options for setting the privacy level of the [redacted] products), 2 sheets;
3. Notice on commencement of the inspection, No. UOOU-07166/18-7, delivered to the [redacted] on 2 July 2018, 4 sheets;
4. Reply to the Notice on commencement of inspection and the [redacted] statement on the privacy protection level of users of the antivirus SW of 1 August 2018, No. UOOU-07166/18-12, 11 sheets (both the Czech and the English versions);
5. Request of the Office for an oral hearing of 10 August 2018, No. UOOU-07166/18-13, 1 sheet;
6. Requested documents delivered on 21 August 2018, No. UOOU-07166/18-16, 1 sheet, with annexes:
    a. Assessment of protection, 3 sheets,
    b. Description of the personal data processing operations, evaluation of needs of data protection impact assessment (PIA), 3 sheets;
7. Record of the oral hearing on 29 August 2018, No. UOOU-07166/18-17, 3 sheets;
8. Request of the Office for an oral hearing of 23 October 2018, No. UOOU-07166/18-22, 1 sheet;

9. Record of the oral hearing on 6 November 2018, No. UOOU-07166/18-25, 2 sheets;
10. Record of the access to the inspection file by the [redacted] representative on 14 November 2018, No. UOOU-07166/18-26, including the Power of Attorney, 4 sheets;
11. Statement of the inspected party of 17 December 2018, No. UOOU-07166/18-28, 13 sheets (both the Czech and the English versions);
12. Information concerning the course of the inspection of 16 January 2019, No. UOOU-07166/18-30, 1 sheet;
13. Record of the access to the inspection file by the [redacted] representative on 22 January 2019, No. UOOU-07166/18-31, 1 sheet;
14. Official record of the inspection action (materials from the [redacted] website) of 28 January 2019, no. UOOU-07166/18-32, 1 sheet, with annexes:
    a. [redacted] Privacy Policy, 15 sheets,
    b. Compliance with the GDPR — FAQ, 5 sheets;
15. Supplemental statement of the inspected party of 30 January 2019, No. UOOU-07166/18-34, 5 sheets.

II. Inspection findings:

The inspection was initiated based on a complaint filed with the Dutch supervisory authority on 25 May 2018. The complaint concerned the impossibility to de-activate the default privacy protection settings in the free version of the antivirus SW for Apple Mac. Thus, in view of the contents of the complaint, the subject of the inspection was defined as specified above. In the course of the inspection, the subject of the inspection was specified in more detail as an inspection regarding the level of protection of privacy with respect to the users of the free version of the SW in comparison with paying customers, with a focus on the following areas indicated in the complaint:

a. Processing of personal data of non-paying users of the antivirus SW for marketing activities of the [redacted]
b. Processing of personal data of non-paying users of the antivirus SW for marketing activities of third parties.
c. Processing of personal data of non-paying users of the antivirus SW for analyses by third parties.
d. Processing of personal data of non-paying users of the antivirus SW for SW development purposes.

Thus, the inspection is not concerned with the processing of personal data of paying customers of the antivirus SW for the purpose of making and verifying payments. At the same time, the inspection is not limited to the antivirus SW for Apple Mac.

With respect to the definition of the subject of the inspection, it can be stated in general terms that, as a rule, the Office initiates inspections *ex officio*. Even in cases when an inspection is commenced based on a complaint, it is the Office who determines the subject of the inspection – based on the complaint, but not necessarily exclusively within the scope thereof. The above procedure is in accordance with Act No. 255/2012 Coll., Regulation (EU) 2016/679, as well as Act No. 101/2000 Coll., which continues to be applied to procedural issues of the inspections carried out by the Office [until the government draft law on personal data processing (parliamentary press No. 138/0, senate press No. 25) enters into effect].

Furthermore, it must be noted that it is not the purpose of the inspection to precisely describe the technical aspects and functioning of the antivirus SW, but rather to define the nature of the data processed in connection with its installation and use, and subsequently to assess whether the [redacted] meets its obligations in the area of data protection.

Inspection finding 1.

The Office primarily assessed whether the information processed by the [redacted] in the process of installation of the antivirus SW and its further use constitute personal data in the sense of Art. 4 (1) of Regulation (EU) 2016/679, which defines personal data as "*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".* Further, it was assessed whether the data are processed in the sense of Art. 4 (2) of Regulation (EU) 2016/679, which defines processing as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".*

First, the inspection verified that at the very beginning of the process of installation of the antivirus SW, the [redacted] presents the user with the licence agreement and the language options. Furthermore, basic information is displayed to the user, among others on the privacy level settings in the paid and free version of the antivirus SW. Reference is made to the [redacted] Privacy Policy (document No. 14.a) which the user should look up for more detailed information.

The [redacted] assigns each installation of the antivirus SW with the "Device ID", i.e. the device identifier used for the installation (download) of the antivirus SW. The Device ID is derived from the technical parameters of the device (e.g. the type of processor, graphics card or motherboard). Furthermore, a randomly generated alphanumeric code, the "Installation ID", is assigned to the installation. The Installation ID is assigned to each individual installation of the antivirus SW. For example, if the antivirus SW is uninstalled from a specific device and then installed again on the same device, each of these installations has the same Device ID, but a different Installation ID. This procedure enables the [redacted] to ascertain how many times and in what versions the antivirus SW was installed on the relevant device. In the event of a new installation of the antivirus SW on the same device, the information on the new installation is linked to the information on the original installation through Device ID for the purpose of finding and removing any SW bugs or false positive malware alerts that lead to the uninstallation. The process of generating of the codes does not in any way reflect whether the user selected the paid or free version of the SW (documents Nos. 4 and 7).

Furthermore, the Internet Protocol (IP) address of the relevant device is required for the installation of the antivirus SW. In general terms, IP address can be defined as a series of binary numbers assigned to a specific device for the purpose of its unambiguous identification in

communication within a computer network. The second part of Internet Protocol version 6 (IPv6), the so called "interface identifier", usually contains a globally unique MAC address of the device. Without the IP address, the device cannot communicate via the internet – it cannot send or receive data. Thus, the IP address can be defined as a unique identifier of a device connected to the internet or local network. For the purpose of installation of the antivirus SW, the [redacted] needs to know the IP address of the device. Based on this identifier, the [redacted] determines on what device the antivirus SW will be installed (i.e. where the device is located), and the language version. The [redacted] stores the IP address of the device for a limited period of time, and subsequently pseudonymises it through hashing or replaces it with less specific location information, e.g. city and country (documents Nos. 4 and 14). According to the statement of the [redacted] the pseudonymisation/replacement takes place generally after one moth or 60 days.

Following the installation of the antivirus SW, the [redacted] collects service data, i.e. information on applications installed on the relevant device, information on files or attachments saved on the device, and information on links to the websites (URL) accessed from the device. This information is necessary for ensuring the functioning of the antivirus SW, i.e. to search for malware and protect the device from malware attacks. If the SW detects unknown or new malware, it sends this information (or a sample of the relevant file) to the [redacted]; the report is paired with the Device ID and Installation ID. Consequently, through Device ID and Installation ID, the thus-collected information can be paired with the specific device, or rather the specific installation of the antivirus SW, even retrospectively. The malware samples processed by the [redacted] are stored for a de facto unlimited period of time, i.e. during malware detection, prevention and research. Device ID in combination with Installation ID allow the [redacted] to determine the scope of the contamination (location of the source or occurrence and speed of the spread of the virus), since based on this information, the [redacted] is able to assess the number, type, version and location of the affected devices (documents Nos. 4 and 7).

Within the SW settings (Privacy Settings), the users of both paid and free version of the antivirus SW can choose whether their device will send a sample of the detected malware to the [redacted] virus data base, and whether the information obtained from their devices may also be analysed by third parties with whom the [redacted] co-operates ([redacted]). Furthermore, the users of the paid version have the option to switch off the offers of other products of the [redacted] and offers of third-party products [redacted]). At any rate, the offers of third-party products [redacted]) are displayed only in the mobile version of the antivirus SW. Furthermore, the users of the paid version of the antivirus SW may refuse the processing of information for the purpose of development of new products of the [redacted]

In mobile devices, the procedure described above differs in that only Installation ID is generated for the purpose of installation, and not Device ID. The process of protection against malware is essentially identical to that on the desktop versions, except that mobile devices update their malware database from the database of the [redacted] every day. The users of the paid version of the antivirus SW for mobile devices may disable sending of the detected malware samples for further analysis by the [redacted] this option is not available to the users of the free version. Same as in the desktop version, all users of the mobile version may refuse third-party processing of data for the purpose of analysing the use of the application (document No. 7).

It follows from the above that for the installation, as well as for proper functioning of the antivirus SW, it is necessary that the [redacted] has the IP address of the device on which the antivirus SW is installed, at least for a limited period of time. The reports sent through the antivirus SW are thus linked to both the Device ID and Installation ID of the device, as well as to the current IP address (until the IP address is replaced by less specific data).

In order to assess whether the [redacted] processes personal data of users of the antivirus SW, it is necessary to assess whether the collected information can be attributed to an identified or identifiable natural person. An identified person is an individual whose identity can be directly determined based on the collected information (i.e. a unique identifier such as birth identification number, or a unique combination of identifiers, such as name, surname, address). An identifiable person is an individual who cannot be directly identified from the collected information itself, but whose identity can be determined on the basis of that information (using other available information and means). It also holds that unambiguous identification of an individual does not require determination of the full "civil" identity of the individual; on the internet in particular, unambiguous individualisation of a user based on a certain element can suffice in some cases. For example, based on Recital 26 of Regulation (EU) 2016/679, a natural person is identifiable when means such as singling out can be used. Thus, individualisation may be achieved by pairing data with individual identifiers, such as the IP address, MAC address or other device identifier of a device usually used by individuals. It is typical for the internet that a file containing information on user behaviour, in particular when it contains data collected over a long period of time, may facilitate identification.

In order to assess the nature of information being collected and further used by the [redacted] in connection with the provision of the antivirus SW service, it must be noted that Art. 4 (1) of Regulation (EU) 2016/679 expressly states that a natural person can be identified e.g. by reference to an online identifier. Although, being an online identifier, the IP address constitutes primarily a piece of technical information pertaining to the device, it must usually be deemed personal data, in particular when the device is likely owned by a specific individual. Based on Recital 26 of Regulation (EU) 2016/679, account must be taken of all the means reasonably likely to be used by the controller or by another person, if a certain IP address in itself does not enable permanent identification of a device connected to the internet. Thus, the IP address constitutes personal data for anyone who has a feasible and legal possibility to attribute it to specific individuals regardless of who attributes it, or who can reasonably assume that such a possibility can exist. It is thus not decisive whether the individual is directly identifiable, i.e. whether the controller connects the data itself on the basis of the information that is available to it or that it can acquire, or indirectly identifiable, i.e. whether interaction of several entities is necessary for the identification of the individual.

After all, the same conclusions were already reached by the Court of Justice of the European Union (hereinafter the "CJEU") in connection to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Specifically, in judgment of 24 November 2011 in case C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (hereinafter "Scarlet") and in judgment of 19 October 2016 in case C-582/14, Breyer v. Bundesrepublik Deutschland (hereinafter "Breyer").

In the Scarlet case, the CJEU reached the conclusion that for internet service providers, IP addresses are personal data, because they allow the users of devices connected to the internet via IP addresses to be precisely identified. The Breyer case was concerned with the question of whether dynamic IP address constitutes personal data for the online services provider if a third party (an internet service provider, 'ISP') has the additional knowledge required in order to identify the data subject. In this case, the CJEU found that a dynamic IP address as such may be considered personal data even without names linked to it.

Thus, in its case law, the CJEU took an objective approach to the term "personal data" when it stated that dynamic IP address also constitutes personal data if the online services provider has available legal and reasonably usable means enabling identification of a user through a third party (e.g. internet service provider, prosecuting bodies, telecommunications services provider). In the case at hand, reasonably usable means could include the possibility that in certain cases the online services provider may contact the competent governmental authority who, subject to meeting the statutory conditions, may obtain information necessary for the identification of the data subject from a third party. The fact that the online services provider did not have the opportunity to legally obtain supplementary information from the ISP does not change the conclusion that a dynamic IP address constitutes personal data for the online services provider.

The [redacted] is not in the position of an ISP that is in all cases able to attribute to the IP address to other identification details of the users of its services. As a provider of a website from which the antivirus SW can be downloaded, the [redacted] nevertheless collects the IP address of the device in order to provide for the download and installation of a suitable version of the antivirus SW. The IP address of the device is further necessary to ensure full functionality of the antivirus SW installed on the device.

The [redacted] also usually has available means that can be reasonably assumed to be suitable for the identification of a certain individual. In case of public static IP addresses, these means are publicly available information. In case of dynamic IP addresses, the [redacted] may contact the competent governmental authority who, subject to meeting the statutory conditions, may obtain information necessary for the identification of the data subject from a third party [in particular under Act No. 127/2005 Coll., on electronic communications and on amendment to certain related laws (the Electronic Communications Act)].

Furthermore, it must be stated that at variance with its statements (e.g. in document No. 4), the [redacted] in certain cases most probably has also the identification and contact details of the antivirus SW users, even in case of the free version. This applies in particular in cases where the free version of the antivirus SW is registered via [redacted] account or if the user registers in the [redacted] (this information is also provided by the [redacted] in [redacted] Privacy Policy, document No. 14.a). Furthermore, the [redacted] is able to identify users who subscribe to the newsletter or provide the [redacted] with their identification or contact details, e.g. when using the free trial of the premium antivirus SW.

However, even without the additional information provided in the preceding paragraph, the [redacted] has such information (IP address of the device in connection with Installation ID, Device ID and service data) that, in their sum, could facilitate identification of the user.

Based on the above, the Office concluded that in connection with the provision of the antivirus SW service, the [redacted] collects data that constitute personal data of users. At the same time, it is clear that the [redacted] handles such data in a manner which falls within the definition of personal data processing (i.e. collects, stores, further uses and subsequently destroys the data).

Therefore, in assessing the facts of the matter at hand, the Office concluded that the [redacted] **processes personal data** in the sense of Art. 4 (1) and (2) of Regulation (EU) 2016/679.

This conclusion applies to all the versions of the antivirus SW (for the Windows, Apple Mac and Android operating systems), both to paying and non-paying users, since, as described above, the process of installation and subsequent functioning of the antivirus SW is essentially the same. This was also stated by the [redacted] in the course of the inspection (documents Nos. 4 and 7). At the same time, it is not decisive whether the [redacted] made any partial changes in the settings of the antivirus SW prior to or during the inspection, since the privacy settings of the antivirus SW do not influence the nature of the data collected for its installation and further operation.

The statement of the [redacted] that it does not intend to identify users is irrelevant in respect of the legal nature of the data processed by the [redacted] What is important is the factual state, i.e. that the [redacted] has data that could lead to identification of users.

However, the above conclusion in itself does not mean that the [redacted] is in breach of the rules stipulated by Regulation (EU) 2016/679, since the Regulation presumes that certain activities are impossible without processing the necessary scope of personal data and considers such activities legitimate (subject to meeting certain requirements).

Inspection finding 2.

The Office further assessed whether, when the [redacted] processes personal data in connection with the installation and subsequent use of the antivirus SW, it is in the position of a personal data controller in the sense of Art. 4 (7) of Regulation (EU) 2016/679, based on which *"controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"*.

As stated above, in connection with the provision of the antivirus SW, the [redacted] collects and further processes data on paying and non-paying users of the product that must be deemed personal data.

By defining the installation procedures and further use and functioning of the antivirus SW, the [redacted] also defined the purpose and means of personal data processing. In general, the purpose of the relevant personal data processing may be the business activities of the [redacted] and, at the same time, enhanced cyber security of the users. These basic purposes may be further divided into more specific individual purposes, e.g. marketing purposes of the [redacted] or third parties, further development of the antivirus SW or analysis by third parties. The

means are the antivirus SW itself, as well as the website [redacted] intended for its download. At the same time, the [redacted] processes the collected data itself.

Thus, the [redacted] is in the position of personal data **controller** in the sense of Art. 4 (7) of Regulation (EU) 2016/679, since it has defined the purpose and means of the relevant processing, carries out the processing itself or through third parties and is responsible for it.

Inspection finding 3.

The Office further assessed whether and to what extent the [redacted] fulfils the obligations following from Art. 5 of Regulation (EU) 2016/679, which provides for the basic principles of personal data processing. In view of the course of the inspection, in particular the fact that the [redacted] denies that personal data are processed in connection with the installation and operation of the antivirus SW (with the exception of paid users and processing for the purpose of making and verifying payment), the inspectors focused primarily on Art. 5 (2) of the Regulation, which states that the controller *"shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (accountability)"*. At the same time, the performance of the obligation imposed on the [redacted] by Art. 24 (1) of Regulation (EU) 2016/679 was assessed, i.e. the obligation to implement *"appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation"*.

As stated above, the inspection established that the [redacted] collects and further processes personal data on paying and non-paying users of the antivirus SW it provides. Thus, it is the primary obligation of the [redacted] to proceed in compliance with the principles stipulated in Art. 5 (1) of Regulation (EU) 2016/679, and the [redacted] is also obliged to document compliance in accordance with Art. 5 (2) and Art. 24 (1) of the Regulation.

Regulation (EU) 2016/679 does not expressly specify the form of documenting compliance, and it is up to each controller to select appropriate measures ensuring compliance with the obligation under the relevant circumstances. In view of the other obligations imposed on controllers by Regulation (EU) 2016/679, it is nevertheless clear that compliance with the basic principles can be documented e.g. by records of processing activities in the sense of Art. 30 of Regulation (EU) 2016/679 or an analysis to evaluate applicability of the individual legal bases, in particular the balance test under Art. 6 (1) (f) of the Regulation, or compliance with approved codes of conduct in the sense of Art. 40 of Regulation (EU) 2016/679 or approved certification mechanisms under Art. 42 of the Regulation.

According to the Office, the obligation stipulated in Art. 24 (1) of Regulation (EU) 2016/679 must be interpreted as the controller's obligation to take into account any and all relevant circumstances surrounding the processing (including the legal basis) and to adopt a set of measures whose goal is to ensure that any and all personal data processing is carried out exclusively under pre-defined conditions that the controller is able to regularly check and enforce if necessary. At the same time, the nature of the measures must be such that they enable the controller to document compliance with the requirements of Regulation (EU) 2016/679. Thus, this obligation supplements the fundamental principle provided for in Art. 5 (2) of the Regulation.

In this context, the Office deems it of fundamental importance that the personal data processing at hand is implemented on a global scale and concerns a considerable number of data subjects. In such a situation, it is absolutely necessary to pay increased attention to all aspects of personal data processing, in particular on lawfulness of the individual purposes of processing and documenting of compliance and other obligations imposed by Regulation (EU) 2016/679, including procedures facilitating exercise of the rights of data subjects.

Nevertheless, the [redacted] repeatedly stated during the inspection that it does not process personal data (beyond the scope of the data necessary to make a payment in case of paying users of the antivirus SW). The conclusion made by the inspectors in connection with the nature of the personal data processed by the [redacted] on the basis of the arguments provided above was rejected by the [redacted] (most recently in its statement of 30 January 2019, document No. 15).

Although, in the course of the inspection, the [redacted] provided detailed information on its activities and the installation and basic functioning of the antivirus SW and on the processing of data for secondary purposes (statistics, analyses, further product development, marketing), it failed to document compliance of its processes with the fundamental principles in the sense of Art. 5 (2) of Regulation (EU) 2016/679.

Thus, the inspection was not able to assess compliance with the principles of Art. 5 (1) of Regulation (EU) 2016/679, i.e. in particular what legal basis was defined by the [redacted] with respect to all the individual purposes of processing of personal data of the users of the antivirus SW, and whether such legal basis is permissible under the relevant circumstances.

In view of the above, the Office states that the [redacted] **breached** the obligations stipulated by Art. 5 (2) and Art. 24 (1) of Regulation (EU) 2016/679.

[redacted]

In connection with this conclusion, the Office states that it is currently pointless to further assess performance of the other individual obligations to which the [redacted] is subject as the controller of personal data of the users of the antivirus SW.

III. Cross-border processing of personal data and adoption of decisions

The processing of personal data of users of antivirus SW is a cross-border processing of personal data within the meaning of Article 4(23)(b) of Regulation (EU) 2016/679, as this processing is likely to affect data subjects in more than one Member State. [redacted] is therefore processing personal data of users from all these countries.

The central administration of [redacted] and therefore its main establishment within the meaning of Article 4(16)(a) of Regulation (EU) 2016/679, is located in the Czech Republic. The Office is therefore according to the meaning of Article 56(1) of Regulation (EU) 2016/679 the lead supervisory authority for the processing of personal data within the subject of this inspection. The supervisory authorities of all Member States of the European Union and the European

Economic Area shall be in the position of the concerned supervisory authority pursuant to Article 4(22) of Regulation (EU) 2016/679 in conjunction with the Decision of the EEA joint committee, No 154/2018, of 6 July 2018, amending Annex XI (Electronic communication, audio visual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022].

The Office has provided all relevant information to the concerned supervisory authorities within the meaning of the first sentence of Article 60 (3) of Regulation (EU) 2016/679. The preliminary conclusions were consulted in the informal procedure No A60IC 52303 in the Internal Market Information System ("IMI") from 29 November 2018. On February 8, 2019, a draft decision according to the second sentence of Article 60 (3) of Regulation (EU) 2016/679, was submitted to the supervisory authorities concerned in IMI (procedure A60DD 59825). The draft decision in question was adopted in accordance with Article 60 (4) of Regulation (EU) 2016/679 and as such is binding to the supervisory authorities involved.

Consequently, in accordance with Article 60 (7) of Regulation (EU) 2016/679, members of the inspection team, as persons authorized to act on behalf of the supervisory authority in this case have adopted this decision – inspection report.

IV. <u>Information on right of appeal:</u>

The inspected party may file objections to the inspection findings set out in the inspection report to the inspection authority within a deadline of 15 days from the date of delivering the inspection report. Objections are filed in writing, and it must be obvious which inspection finding they refer to, and must contain a justification of the objection to this inspection finding.

If the inspector does not accommodate the objections within a deadline of 7 days from their delivery, the President of the Office will handle them within a deadline of 30 days from their delivery.

Signature clause:

[redacted] Inspector of the Office
……. …… ……..

[redacted] authorized staff member
……. …… ……..

[redacted] authorized staff member
……. …… ……..