

DECISION

The President of the Office for Personal Data Protection as a competent appellate authority pursuant to Section 152(2) of the Act No. 500/2004 Coll., the Code of Administrative Procedure, decided pursuant to Section 152(6)(b) of Act. No 500/2004 Coll., the Code of Administrative procedure, as follows:

The Administrative Appeal of the Charged Company

filed against the Decision of the Office for Personal Data Protection ref. UOOU-01025/20-94 of 14 March 2022 **is being rejected** and the Disputed Decision **is being clarified** in the sense that a text consisting of *“(in the scope of pseudonymised data regarding internet browsing history, relating to users in the order of 100 000 000)”* is being inserted after the words “internet browser extensions” in verdict no. I. **The Disputed Decision is upheld in the remainder.**

Reasoning

I. Case delimitation

[1] The procedure concerning a suspected administrative offence pursuant to Section 62(1)(b) and (c) of the Act No. 110/2019 Coll., on personal data processing (hereinafter “Act No. 110/2019 Coll.”) consisting of the transfer of data of users of the [REDACTED] antivirus program and its browser extensions (hereinafter “the [REDACTED] antivirus program”), in particular of the data about the behaviour of these users when using a personal computer and the internet, to a new controller (in the sense of further controller) pursuant to Article 4(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council of the 27 April 2016 on the protection of natural persons with regard to the processing of personal data and of the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) effective from 25 May 2018 (hereinafter “Regulation (EU) 2016/679” or “GDPR”) without legal basis and in breach of the obligation to inform pursuant to Article 13(1) of Regulation (EU) 2016/679, was initiated by the Notice of the Office for Personal Data Protection (hereinafter “the Office”) delivered to the charged company [REDACTED], [REDACTED] (hereinafter “the Accused” or “the Charged Company”) on 27 February 2020. The basis for initiating the proceedings was the Administrative File

collected by the Office upon a filing received by the Office on 22 February 2020, and also the documents gathered within the context of the Inspection filed under ref. UOOU-07166/18 and performed by the Office's inspector, JUDr. Jiřina Rippelová, from 2 July 2018 till 19 March 2019, which was concluded by the Settlement of Objections by the President of the Office under ref. UOOU-07166/18-53 of 4 June 2019, and also the file ref. UOOU-01733/19 in the scope of which the adoption of corrective measures by the Charged Company was handled beyond the administrative procedure.

[2] The decision ref. UOOU-01025/20-94 of 14 March 2022 (hereinafter "the Disputed Decision") found the Charged Company to be guilty of committing administrative offences pursuant to Section 62(1)(a) and (b) of the Act No. 110/2019 Coll., which consisted of the Charged Company, as the controller pursuant to Art 4(7) of Regulation (EU) 2016/679, transferring personal data of the [REDACTED] antivirus program users and its browser extension users to the company [REDACTED] (hereinafter "company"), in order to produce statistical trend analytics, even though that processing was not supported by any of the legal bases within the meaning of Art. 6(1) of Regulation (EU) 2016/679, whereas this activity lasted at least over the period from an undetected day of April 2019 till an undetected day of July 2019, i.e. for at least the whole two calendar months, and that the Charged Company, in relation to the transfer of personal data to the [REDACTED] company, failed to sufficiently inform the data subjects at the time of obtaining the personal data about the purposes of the processing for which the user data were intended and about the legal basis for the processing, also for at least the period of two whole calendar months. For this delictual behaviour, the Accused was fined, in the amount of CZK 351,000,000, and given an obligation to pay the proceedings costs in the amount of CZK 1,000.

[3] The Disputed Decision was delivered to the Charged Company on 24 March 2022 and on 5 April 2022 the Charged Company filed a general Administrative Appeal which was submitted through the Charged Company's legal counsel, and later amended by the Charged Company on 11 May 2022.

[4] The Appellate Authority informed the Accused pursuant to Section 36(3) Act No. 500/2004 Coll., the Code of Administrative Procedure (hereinafter "Act No. 500/2004 Coll.") with a letter ref. UOOU-01025/20-113 of 13 November 2023 of the possibility to comment on the basis for the Decision on Administrative Appeal. At the same time, the Appellate Authority informed the Charged Company about its Preliminary Findings in the Administrative Appeal Proceedings (hereinafter "Preliminary Findings") and gave the Charged Company an opportunity to express its opinion pursuant to Section 36(2) Act No. 500/2004 Coll. The Appellate Authority set the deadline for the Accused's statement on 4 December 2023 in resolution ref. UOOU-01025/20-114 of 13 November 2023. At the same time, the Appellate Authority called on the Accused to raise any potential objections against the members of Administrative Appeal Commission for conflict of interest within the aforementioned deadline.

[5] The Charged Company's statement on the basis for the Decision on Administrative Appeal was delivered to the Office on 4 December 2023. In this statement, the Charged Company reserved its right to supplement its claims and propose evidence at a later date. Subsequently, on 21 December 2023, the Charged Company sent its additional statement to the Office. In both of the aforementioned statements the Charged Company stated that

“it reserves the right to file an objection against a member the Administrative Appeal Commission on the grounds of conflict of interest once the Administrative Appeal Commission is appointed by the President of the Office and the [REDACTED] company is properly informed thereof”.

[6] The Appellate Authority presented the Draft Decision on the Administrative Appeal on 8 March 2024 for consultation to the supervisory authorities concerned within the context of cooperation mechanism pursuant to Art 60(3) of Regulation (EU) 2016/679. However, none of the supervisory authorities concerned raised any relevant and reasoned objections pursuant to Art 60(4) of Regulation (EU) 2016/679 in relation to the presented Draft Decision and it is therefore deemed that they are in agreement with the draft.

II. The contents of the Administrative Appeal and the evaluation by the second-instance authority

[7] For the sake of clarity and consistency of the decision, the Appellate Authority dealt with individual objections as structured by the Accused and the Appellate Authority will maintain this approach while settling them.

[8] With respect to the amendment of the verdict of the decision, the Appellate Authority states that (in accordance with case law; cf. for instance the judgment of the Regional Court in Brno ref. 30 Af 42/2014-71 of 20 July 2016, upheld by the Supreme Administrative Court in judgment ref. 5 As 173/2016-24 of 3 April 2017 and by the resolution of the Constitutional Court ref. III. ÚS 1796/17 of 20 June 2017) it merely specified more precisely the particulars of the act which the Charged Company committed. It represents only a formal change, as it still concerns the same act, the particulars of which were refined, not changed or expanded upon.

Ila. Course of legal proceedings

A. The nature of and grounds for the charges

[9] In the Administrative Appeal, the Charged Company chiefly objects to procedural errors. The Charged Company stated that the Office has not, at any point during the proceedings, familiarized the Charged Company with what it is being charged with in detail and thus violated Article 6(3)(a) of the Convention¹ which states that *“Everyone charged with a criminal offence”* has a right to *“be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him”*. As a consequence of this error, the Charged Company could not duly exercise its right of defence, i.e. could not submit qualified statements, propose evidence to prove its innocence or exercise the right to remain silent and others. The Charged Company refers to a decision of the Municipal Court in Prague ref. 10 Af 38/2017-50 of 14 November 2019, according to which ***“Merely vague and informal knowledge of the existence of a charge is not sufficient (see judgment of 12 October 2000, T. v. Italy, app. no. 14104/88, § 28). The grounds for the charge is meant to be the act that the charged committed and upon which the accusation is based. The nature of the charge is the legal qualification of this act (see judgment of 25 July 2000, Mattocia v. Italy, app. no. 23969/94, § 59)”***. The Accused further stated that in the Notice of Commencement

¹ European Convention on Human Rights.

of Proceedings of 27 February 2020 and in the Notice of Clarification of the Legal Qualification of the Offence of 3 January 2022 only a part of a single sentence is devoted to the grounds for the charges and their nature. The Accused has not received further details about the charges at the Oral Hearing on 28 May 2020. Only from the Disputed Decision did the Accused find out that it processed personal data, that the subject-matter of the proceedings is a specific case of alleged transfer of personal data to the ██████████ company between April and July 2019, why the Office is under the assumption that the secondary purpose for the processing was not compatible with the primary purpose, why the Office is under the assumption that the data was not transferred to the ██████████ company for statistical purposes, why in the Office's opinion the processing performed by the Accused was not supported by legal basis of legitimate interest, and what criteria the Office will take account of when considering the sentence. To this, the Accused has further stated that the Office defined the subject-matter of proceedings so broadly and vaguely that it was not able to prepare its defence and evaluate what documents are in its favour or disfavour, whereby this error of proceedings has had an effect on the legality of the Disputed Decision.

[10] In the Notice of Commencement of Proceedings of 27 February 2020 (hereinafter "Notice of Commencement of Proceedings"), the first-instance administrative authority notified the Accused of the commencement of the proceedings on administrative offence for the *"suspicion of committing an administrative offence pursuant to Section 62(1)(b) of Act No. 110/2019 Coll. in relation to collection and transfer of personal data of the users of ██████████ antivirus program, more precisely its browser extensions (add-ons), particularly data about their behaviour when using personal computer and the internet, to third parties for profit despite not having a transparently given consent by the data subjects therefor, thus infringing upon an obligation pursuant to Article 5(1)(a) of Regulation (EU) 2016/679, and further for suspicion of committing an administrative offence pursuant to Section 62(1)(c) of Act No. 110/2019 Coll. in relation to failing to fulfil obligation to inform towards users, who installed ██████████ antivirus program on their devices, more precisely their browser extensions, thus infringing upon the obligation pursuant to Article 13 of Regulation (EU) 2016/679"*.

[11] In the Notice of Commencement of Proceedings, the first-instance administrative authority further stated that the *"basis for the commencement of these proceedings are expert information and assessment of publicly available sources and statements of the company ██████████, which are a part of the administrative file on the proceedings"*. At the same time, the first-instance authority asked the Accused to *"present the agreements about cooperation and transfer of data between companies ██████████ and ██████████ or rather ██████████; present the texts of consents to processing of personal data valid in the month of April 2019 and the month of December 2019 acquired to allow the sharing of obtained data from devices with installed ██████████ antivirus program both for the free version and the paid version of the program, including the manner of acquisition of the consents; present the text of information on personal data processing pursuant to Art. 13 of Regulation (EU) 2016/679, including where such text was made available for the users in the month of April 2019 and in the month of December 2019; to provide information about numeric identification of the internet browser extensions (add-ons) in the year 2019 and their release dates; to state the contents of information which the internet browser extensions (add-ons) sent beyond the sphere of user devices in the month of April 2019 and in the month of December 2019"*. From the abovementioned it is clear that the first-instance authority dedicated more than "only a part of a single sentence", as stated by the Accused, to the

reasons and nature of charges in the Notice of Commencement of Proceedings. In the Appellate Authority's opinion, the information contained in the Notice of Commencement of Proceedings need to be perceived as a whole with respect to wider context of the entire matter.

[12] To this the Appellate Authority adds that administrative proceedings with the Accused were commenced due to a motion received by the Office on 22 February 2020 and on the basis of information published by the media (Administrative Record ref. UOOU-01025/20-3 of 27 January 2020).

In the days between 10 February 2020 and 20 February 2020 the information about transfer of data by the Accused to [REDACTED] company available from public sources was inserted into the administrative file (Administrative Record of 27 February 2020). As evident from the administrative file, the Accused exercised its right to access the file several times. Specifically on 2 March 2020 (Record of Access to File ref. UOOU-01025/20-6) the data protection officer of the Accused familiarized themselves with the contents of the administrative file, the data protection officer also received copies of documents from the file, specifically the anonymous complaint of 22 February 2020 (ref. UOOU-01025/20-1) containing information about "the case of [REDACTED] company" and two administrative records of 27 February 2020 (ref. UOOU-01025/20-2 and ref. UOOU-01025/20-3).

[13] From the Oral Hearing Official Report ref. UOOU-01025/20-22 of 28 May 2020 it follows that the reason for the Accused's request for an oral hearing at the administrative authority was primarily the clarification of the procedural side of the matter in relation to the Inspection the Office had conducted with the Charged Company in the year 2019, not the clarification of the subject-matter of the proceedings. Furthermore it follows from the Oral Hearing Official Report that the Accused has expressed itself with respect to the contents of news reports ("*Information from news articles are considered to be speculation and they are convinced that personal data processing by the Charged Company was done on the grounds of sufficient legal basis and the data, that are transferred to third parties, have already been anonymised without possibility of identifying data subjects.*") and, for example, even the fact that it was asked to substantiate the reasons for terminating the activities of the [REDACTED] company. From the subsequent statement of the Accused of 29 June 2020, and its other statements (especially the statement ref. UOOU-01025/20-11 of 14 April 2020, the Oral Hearing Report and the Record of Access to Administrative File ref. UOOU-01025/20-22 of 28 May 2020, statement ref. UOOU-01025/20-25 of 29 June 2020, the submission ref. UOOU-01025/20-63 of 29 April 2021, the statement ref. UOOU-01025/20-72 of 31 May 2021, statement ref. UOOU-01025/20-93 of 23 February 2022), it can be hardly concluded, in the Appellate Authority's view, that the Accused had not known what it was being suspected of.

[14] If the Accused states in the Administrative Appeal (item no. 29) that in the course of the proceedings on administrative offence it "*did not know what offence these proceedings were being conducted for*", it could have raised this objection immediately after the commencement of proceedings or whenever during the proceedings before the first-instance

² Available online at: [REDACTED]

administrative authority. The Accused has not done so, on the contrary, in its Statement of 14 April 2020 it expressed that *“[i]f the Office came to a conclusion that [REDACTED] company committed administrative offences it was being charged with, the [REDACTED] company emphasises that it ceased to process data for purposes of statistical analytics of trends even before the commencement of these proceedings, namely with immediate effect as of 30 January 2020”*.

[15] On the basis of the abovementioned, the Appellate Authority has no doubts that the Accused was aware of for what act (reason for charges) forms the substance of the administrative proceedings. The administrative proceedings in question were commenced in relation to a big media scandal (which took place at the turn of the year 2019) in which several newspapers reported (see Administrative Record ref. UOOU-01025/20-3 of 27 February 2020) about transfer of data by the Accused to the [REDACTED] company, whereas this information forms part of administrative file that the Accused has repeatedly familiarized itself with. In the Notice of Commencement of Proceedings, the Accused was requested to present agreements about cooperation and transferring of data concluded with the [REDACTED] company. In its statement of 14 April 2020, the Accused informed that *“the [REDACTED] company has been dissolved, and its activities have ceased”*. The Appellate Authority has therefore concluded that the Accused’s argument about having acquainted itself with the subject matter of the proceedings, that is the specific case of transferring personal data to the [REDACTED] company, from the Disputed Decision only cannot be accepted. On the contrary, the Accused was, in the Appellate Authority’s view, thoroughly introduced to the nature of charges against it even if the act itself was not described in detail in the Notice of Commencement of Proceedings. The subject matter of the proceedings was, according to the Appellate Authority, sufficiently known to the Accused and it could have prepared its defence properly. The argument of the Accused would, if taken ad absurdum, mean that the result of these proceedings should be clear from commencement thereof and that the Accused should have been familiarized with it. However, the right of defence is not designed in this manner and cannot be interpreted so extensively. To this the Appellate Authority further states that the Accused is a big multinational company that was represented by a legal counsel during the entire course of the proceedings and it cannot be therefore concluded that it did not know how to exercise its procedural rights.

[16] With respect to the objection of the Accused that it only found out the time delimitation of the act from the Disputed Decision itself, the Appellate Authority states that the Accused was requested, inter alia, to provide the text of consents to sharing of data gathered from the devices with the installed antivirus program of the Accused, valid in the month of April 2019 and in the month of December 2019, to provide the text of information on personal data processing pursuant to Article 13 of Regulation (EU) 2016/679 for the month of April 2019 and the month of December 2019, and to state the contents of information which browser extensions (add-ons) were sending beyond the sphere of user devices in the month of April 2019 and in the month of December 2019, in the Notice of Commencement of Proceedings. It is clear from the Notice of Commencement of Proceedings, that the suspicion of committing an administrative offence was related to a period from April 2019 till December 2019. This period was narrowed down due to the information found out in the course of administrative proceedings and the Accused was found guilty of committing administrative offences in a period from an undetected day of April 2019 till an undetected day of July 2019. The time delimitation of the act in the verdict of the Disputed Decision could not be, in the Appellate Authority’s opinion, surprising to the Accused (despite the shortening of the period

derived from the Notice of Commencement of Proceedings) and in the Appellate Authority's opinion, this procedure did not interfere with the right of defence of the Accused. The Accused was, in the Appellate Authority's opinion, familiarized with the reason of the charges, that is the act which it allegedly committed. Based on the aforesaid, the argument of the Accused that from the first-instance administrative authority side this was an "investigative fishing expedition" is considered unfounded by the Appellate Authority.

[17] Similarly, the Accused was in the Appellate Authority's opinion familiarized with the nature of the charges; in the Notice of Commencement of Proceedings the Accused was informed that it was suspected of committing administrative offences pursuant to Section 62(1)(b) and (c) of Act No. 110/2019 Coll., which the controller or processor commits by infringing on any of the fundamental principles relating to personal data processing pursuant to Articles 5 to 7 or 9, or alternatively by infringing on the rights of data subject pursuant to Articles 12 to 22 of Regulation (EU) 2016/679, which it should have committed by infringing on obligations pursuant to Article 5(1)(a) and Article 13 of Regulation (EU) 2016/679. In the Notice of Clarification of the Legal Qualification of the Act of 3 January 2022 the Accused was informed that it was suspected of committing administrative offences pursuant to Section 62(1)(b) and (c) of Act No. 110/2019 Coll., as it infringed upon the obligations pursuant to Article 6(1) and pursuant to Article 13(1)(c) of Regulation (EU) 2016/679.

[18] To the next argument of the Accused that "*insufficient statement of charges further damaged [redacted] company insofar that its right against self-incrimination was restricted*", the Appellate Authority states beyond already mentioned above that the legal principle of *nemo tenetur se ipsum accusare* (no one is bound to incriminate himself) needs to be viewed as a prohibition of forcing to self-incriminate. The Accused however does not claim that it was forced to incriminate itself in any way.

[19] Concerning the principle of the prohibition of self-incrimination, the Appellate Authority, in its request addressed to the Accused for the submission of a document (ref. UOOU-01025/20-105 of 9 January 2023), already referred to the judgment of the Supreme Administrative Court of the Czech Republic of 11 August 2015, ref. 6 As 159/2014-52, in which the court stated the following: "The limits of the prohibition of self-incrimination in relation to the submission of information by legal persons in administrative offense proceedings have been set out in the case-law of both the General Court (formerly the Court of First Instance) and the Court of Justice (formerly the European Court of Justice). The referred case-law relates to the protection of competition, but the conclusions on the application of the principle in question can also be applied to the broader legal field of administrative penalties. With a certain degree of generalisation, it is apparent from the relevant case-law, in particular the judgment of the Court of Justice of 18. 10. 1989, *Orkem v Commission* (374/87, Recueil) and the judgment of the General Court of 20. 2. 2001, *Mannesmannröhren-Werke AG v. Commission* (T112/98), that the supervisory authority is entitled to oblige a participant in proceedings to provide all necessary information relating to the case of which the participant is aware and, where appropriate, to hand over relevant documents in the participant's possession, even under threat of penalty, and even where they may serve to prove an unlawful conduct against the participant or against another entity. Granting an absolute right to remain silent would go beyond what is necessary to preserve the rights of defence and would constitute an unjustified obstacle to the exercise of supervisory powers. The General Court made an important conclusion in relation to self-incrimination: "*The mere fact of being obliged to answer purely factual questions put by the Commission and to comply with its requests for*

the production of documents already in existence cannot constitute a breach of the principle of respect for the rights of defence or impair the right to fair legal process. There is nothing to prevent the addressee of such questions or requests from showing, whether later during the administrative procedure or in proceedings before the Community courts, when exercising his rights of defence, that the facts set out in his replies or the documents produced by him have a different meaning from that ascribed to them by the Commission.“ Mere request for cooperation by an administrative authority cannot be viewed as forcing to self-incriminate. Similarly, if a participant in proceedings presents a piece of evidence of their own will, it cannot be considered a violation of said principle if this evidence shall be, in the end, used against them.

[20] On the violation of the prohibition of self-incrimination, the Constitutional Court expressed its opinion in its Resolution ref. II. ÚS 4117/19 of 28 April 2020 stating that *“the mere request for the necessary information relating to the facts under review could not have violated the prohibition of self-incrimination, as it was only a matter of submitting records that the complainant was legally obliged to keep. The prohibition of self-incrimination cannot be interpreted as effectively preventing the exercise of the supervisory powers of the capital market regulatory authority, which, in view of the complexity and volume of transactions taking place on the capital market, is justified by a strong public interest”*. In this context, the Appellate Authority points out that respect for privacy and the right to protection of personal data are guaranteed by the Charter of Fundamental Rights of the European Union (Articles 7 and 8), which explicitly elevates the level of that protection to the level of a fundamental right in the law of the European Union.

[21] Pursuant to Section 68(3) of the Code of Administrative Procedure, the reasoning is to contain reasons for the verdict(s) of the decision, the basis for issuing the decision, the considerations followed by the administrative authority in its evaluation and its interpretation of legal provisions, and information on how the administrative authority dealt with the proposals and objections of the participants and their comments on the basis for the decision. The assessment of whether personal data were processed, the assessment of the purpose of the processing or whether the Charged Company processed personal data on the grounds of a valid legal basis form immanent part of the decision. The Appellate Authority considers that the first-instance administrative authority was not obligated to inform the Accused in advance of its intended decision or of its assessment of the case, since such considerations and legal assessments are included in the decision itself and not in the Notice of Commencement of Administrative Proceedings. The Charged Company thus confuses the obligation to identify the act and its preliminary legal qualification with the reasoning of the decision. The Appellate Authority therefore concludes that, in accordance with the case-law referred to by the Accused itself, the Charged Company was informed of the nature and the grounds of the charges against it and was therefore able to fully exercise its procedural rights.

[22] With regard to the Charged Company’s further claim that it only learned from the Disputed Decision what criteria the Office would take into account when imposing a penalty, the Appellate Authority notes that when imposing administrative penalties, the Office shall proceed in accordance with the law, which in this particular case is primarily Regulation (EU) 2016/679 and Act No. 250/2016 on Liability for and Proceedings on Administrative Offences. However, the Office is not obligated to inform the Accused how it will assess each criterion prior to issuing a decision in the case.

[23] The Charged Company argued in its Administrative Appeal, that the Office's failure to communicate the nature and grounds for the charges was not a mere procedural oversight, since the Office stated in its Resolution ref. UOOU-01025/20-43 of 22 January 2021 that *"it is undesirable for the Company to know the Office's factual and legal considerations prior to the issuing of a decision, as this would have provided it with a stronger position throughout the proceedings itself."*

[24] In the aforementioned Resolution, the Office stated: *"The Administrative Authority further adds that the opinions of the supervisory authorities concerned are not binding in the sense of Section 149(1) of the Code of Administrative Procedure. Nor are they considered to be 'a statement which forms the basis of the decision of the administrative authority', since they are only submitted subsequently, after the decision itself has been drafted (since the decision can only be drafted once all the evidence for it has been collected). This approach also ensures equality of participants in individual cases. Such principle would be contradicted if the participants in procedures falling under Article 60 of Regulation (EU) 2016/679 had privileged access to the factual and legal considerations of the first-instance administrative authority and the supervisory authorities concerned, and therefore to the text of the draft decision (through such considerations or directly). This would provide them with a substantially stronger position than 'ordinary participants' prior to the issuing of a decision. The cross-border aspect of the case does not justify a fundamentally different treatment of participants in relation to the information on the draft decision"*. According to the Appellate Authority, the Charged Company takes this deliberately out of context, as it has been mentioned in the said Resolution solely in relation to the international procedure under Article 60 of Regulation (EU) 2016/679 and certainly not in relation to the entire proceedings, which is evident from the said Resolution. The Accused was not allowed to familiarise itself with the draft decision submitted to supervisory authorities concerned, nevertheless, in non-international cases, the participants are typically also not provided with draft decisions (as there is no such legal obligation). If the Office were to submit draft decisions only to participants in proceedings where Article 60 of Regulation (EU) 2016/679 is followed, i.e. in cases of cross-border processing by the controller where the draft decision is submitted to the other supervisory authorities concerned for their comments, this would lead to a paradoxical situation: in cases that are more serious (affecting data subjects from various Member States of the European Union), the position of the participants would be significantly stronger than in proceedings where only national legislation is followed. As an *obiter dictum*, the Appellate Authority points out that a proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679³ is currently under discussion at European level; this proposal addresses, inter alia, the issue of access to the administrative file, in Chapter IV, which states in particular in Article 19(3): *"The right of access to the administrative file shall not extend to correspondence and exchange of views between the lead supervisory authority and supervisory authorities concerned. The information exchanged between the supervisory authorities for the purpose of the investigation of an individual case are internal documents and shall not be accessible to the parties under investigation or the complainant."*

³ European Commission document COM(2023) 348 final, 11657/23.

B. Participation in administrative proceedings/international procedure

[25] The Charged Company considers that another procedural error is that the case “*was decided in proceedings⁴ in which it was not permitted to participate*”. In that regard, the Accused claims that, in the proceedings before the first-instance administrative authority, there were in fact two parallel proceedings, namely the proceedings before the Office and other, considerably longer proceedings within the framework of international cooperation, in which, according to the Charged Company, the case was in fact decided. The Accused was not permitted to participate in the international cooperation proceedings, nor was it granted access to the documents, and the case was decided in its absence. The Accused further states that the legislation in force does not allow for any separation of proceedings and therefore considers such a practice to be unacceptable. The procedure under Article 60 of Regulation (EU) 2016/679 is, according to the Accused, still part of the national proceedings and is subject to national procedural law, except for the issues specifically regulated by the said Regulation. Further proceedings before the European Data Protection Board (hereinafter “the Board” or “EDPB”) are, according to the Accused, only initiated when the circumstances foreseen in Article 65 of Regulation (EU) 2016/679 arise. However, even in proceedings before the Board, the Charged Company would have the status of a participant and would have full rights of defence.

[26] In the Administrative Appeal, the Accused further claims that the Office had unlawfully denied it access to a key part of the file by not allowing it to familiarise itself with documents related to international cooperation on the grounds that the statements of other supervisory authorities concerned are not considered to be binding opinions, ergo, the Charged Company should not have access to them. The file consists of all the documents relating to the case and the international cooperation documents are relevant to the case. According to the Charged Company, the opinions of the foreign supervisory authorities had a significant influence on the Disputed Decision, since the international cooperation procedure lasted longer than the administrative proceedings themselves and the draft decision was revised during its course. The Accused disagrees with the conclusions of the Office set out in the decision on administrative appeal ref. UOOU-01025/20-82 of 30 August 2021 against the Office’s resolution not to grant the Charged Company’s request for access to the part of the file relating to the international cooperation mechanism under Article 60 of Regulation (EU) 2016/679, since, according to the Accused, it cannot be inferred from the EDPB Guidelines 3/2021⁵ that it should have the right to access the file only after the initiation of proceedings before the Board. Furthermore, the Charged Company does not agree that the international cooperation procedure should be held outside the scope of the Code of Administrative Procedure, since the procedure under Article 60 of Regulation (EU) 2016/679 is part of the national proceedings, and only after the case is submitted to the Board under Article 65 of Regulation (EU) 2016/679 are new proceedings initiated. In this regard, the Charged Company

⁴ The Appellate Authority deems it necessary to stress at this point that the procedure under Article 60 of Regulation (EU) 2016/679 is not administrative proceedings, but a procedure of international cooperation between supervisory authorities.

⁵ Guidelines 03/2021 on the application of Article 65(1)(a) GDPR (version 2.0), adopted on 24 May 2023, Available online at: https://edpb.europa.eu/system/files/2023-06/edpb_guidelines_202103_article65-1-a_v2_en.pdf.

refers to the EDPB Guidelines 2/2022⁶, which state that where “EU law does not provide for specific procedural rules, national procedural law applies. In these cases the principle of national procedural autonomy, which is a general principle of EU law, generally applies”. According to the Accused, the Office itself acknowledges that the documents from the international cooperation are relevant to the case and that the Office took them into account when issuing the Disputed Decision, therefore they should have been disclosed to the Charged Company in order to avoid violations of its rights of defence. In addition, the Accused claims an inconsistency in the Office’s practices, since the international cooperation documents were disclosed to it during the preceding Inspection.

[27] The Charged Company also considers it a violation of its procedural rights that the Office decided on the case in an international cooperation procedure in which it was unable to participate, which is contrary to Article 38(2) of the Charter of Fundamental Rights and Freedoms (Act No. 2/1993 Coll., hereinafter “the Charter”), according to which “everyone has the right to have their case heard in public, without unnecessary delay, and in their presence, as well as to express their opinion on all of the admissible evidence.” According to the Accused, the aforementioned article of the Charter also applies in administrative proceedings, and in particular in those of punitive nature. According to the Accused, the Office must ensure that all rights of defence of the Accused remain preserved even in the case of procedure under Article 60 of Regulation (EU) 2016/679. The Charged Company argues that the Office should have (beyond the above-described access to the file) made its comments and arguments available to the foreign supervisory authorities and allowed it to comment on the opinions of those supervisory authorities. The Accused specifically requested the Office (e.g. in its submission of 31 May 2021) to share its statement with the other supervisory authorities, but the Office did not inform it of such an action and the Accused therefore considers that it did not do so. Similarly, the Office should have given the Charged Company the opportunity to comment on the objections of the other supervisory authorities, which the first-instance administrative authority refused to do in the Disputed Decision on the grounds that there would be an “irresolvable procedural loop”, which, however, according to the Charged Company, cannot occur. Moreover, according to the Accused, the possibility of responding to the supervisory authorities’ objections is explicitly set out in the EDPB Guidelines 2/2022.

[28] Regarding the denial of access to the documents related to the international procedure pursuant to Article 60 of Regulation (EU) 2016/679, the Appellate Authority notes that this has already been ruled on by the Office in decision ref. UOOU-01025/20-61 of 23 April 2021 and subsequently in decision ref. UOOU-01025/20-82 of 30 August 2021, rejecting the administrative appeal against the former decision, the Appellate Authority hereby refers to both those decisions and their reasonings. The Appellate Authority emphasises that, in accordance with Article 60(3) of Regulation (EU) 2016/679, the Office submitted a draft decision to the other supervisory authorities concerned for their opinion, and that this draft decision was only prepared by the first-instance administrative authority after all of the basis for decision has been collected and the Charged Company has been given the opportunity to familiarise itself with such basis and to comment on it. Therefore, according to the Appellate Authority, the procedure under Article 60 of Regulation (EU) 2016/679 itself did not result (nor could result from any objections or comments) in any new grounds for the decision, as

⁶ Guidelines 02/2022 on the application of Article 60 GDPR, adopted on 14 March 2022, available online: https://edpb.europa.eu/system/files/2022-03/guidelines_202202_on_the_application_of_article_60_gdpr_en.pdf.

all the evidence was collected before the draft decision was prepared. The cooperation of the supervisory authorities under Article 60 of Regulation (EU) 2016/679 has no equivalent in terms of the Czech law. It can best be compared to deliberation (in the sense of consideration aiming to reach a consensus), in which the other supervisory authorities concerned have the opportunity to comment on the submitted draft. However, the other supervisory authorities are not seen as the so-called concerned authorities (in the sense of Section 136 of Act No. 500/2004 Coll.) defending their own interest in the case (or a particular public interest), whose opinion would be taken into account by the decision-making authority (in this case the Office) as one of the grounds for the decision. In other words, the other supervisory authorities are not the ones defending their interests which compete with those of the participant. The national supervisory authorities protect the public interest, which is mainly the protection of personal data, therefore there can be no competition with the interests of the participant. Neither the Czech law nor Regulation (EU) 2016/679 provide for a procedural right of a participant to express their views on the draft decision before it is issued within the scope of Article 60(7) of Regulation (EU) 2016/679, or to otherwise participate in such deliberation of the supervisory authorities. However, should the lead supervisory authority and the supervisory authorities concerned fail to reach a unanimous opinion in the framework of the international procedure, Article 65 of Regulation (EU) 2016/679 provides for a mechanism in which the disputed issue is referred to the Board. In such a procedure before the Board, the participant has the right to be heard and to comment on the evidence. Nevertheless, according to the Appellate Authority, the procedure under Article 65 of Regulation (EU) 2016/679 (which did not take place in this case) must be distinguished from the procedure under Article 60 of the said Regulation.

[29] In the event that, in the course of the procedure under Article 60 of Regulation (EU) 2016/679, deficiencies in the administrative proceedings carried out by the lead supervisory authority became apparent (e.g. further evidence would be required or the act were to be qualified differently), the lead supervisory authority would continue the proceedings (in this case under Act No. 500/2004 Coll. or Act No. 250/2016 Coll.), whereby the participant would be given the opportunity to exercise their right to be heard and to comment on the basis of the decision. However, this was not the procedural outcome of the deliberation either. The decision of the first-instance administrative authority was thus adopted on the basis of evidence collected during the administrative procedure, which the Accused had the opportunity to familiarise itself with and comment on. In that respect, the Appellate Authority considers that the Charged Company's procedural rights were not infringed in any way.

[30] For the sake of completeness, the Appellate Authority adds that the procedure under Article 60 of Regulation (EU) 2016/679 was first initiated in the administrative proceedings in question on 31 August 2020, but was not concluded in the manner foreseen by the Regulation, as doubts arose on the side of the first-instance administrative authority itself as to whether the Charged company was given adequate opportunity to comment on the basis for the decision in accordance with Section 36(3) of Act No. 500/2004 Coll. Therefore, the first-instance administrative authority did not continue with this procedure and thus it could not have any legal effect, envisaged in the last sentence of Article 60(6) of Regulation (EU) 2016/679, on the administrative authority or, even less so, on the Charged Company. Only following the proceedings pursuant to Act No. 250/2016 Coll., or as the case may be, Act No. 500/2004 Coll., in which the Accused was given the opportunity to exercise all procedural rights in a standard manner, the procedure under Article 60(3) of Regulation (EU) 2016/679

was initiated on 31 October 2021, by submitting the draft decision to the supervisory authorities concerned. This procedure was concluded by consensus, i.e., no issue arose from it that would be disputed between the lead supervisory authority and the supervisory authorities concerned and would need to be referred to the Board for a decision pursuant to Article 65(1)(a) of Regulation (EU) 2016/679. The first-instance administrative authority therefore continued the proceedings by issuing a decision pursuant to Section 67 of Act No. 500/2004 Coll.

[31] For the sake of clarification, the Appellate Authority adds that a prematurely initiated procedure under Article 60(3) of Regulation (EU) 2016/679, which was dismissed without a legally relevant outcome, cannot constitute a procedural error or unlawfulness of the decision having resulted from the subsequent phase of the administrative proceedings. Particularly since the Charged Company was given the opportunity to exercise its procedural rights afterwards and the draft decision (prepared on the basis which the Charged Company had the opportunity to consult and comment on) was subsequently resubmitted to the supervisory authorities concerned for deliberation in accordance with Article 60(3) of Regulation (EU) 2016/679.


[32] In addition to the abovementioned, the Appellate Authority notes that during the course of the Inspection conducted by the independent Inspector of the Office, some documents from the international cooperation were disclosed to the Accused, however, this occurred in a situation whereby Regulation (EU) 2016/679 had only been in force for a short period of time and the practice of the supervisory authorities regarding the procedure under Article 60 of the Regulation had not yet been clarified even at the level of the Board. Therefore, as a procedural precaution, the Inspector allowed the Accused to familiarise itself with the contents of the documents. For various reasons such approach was redundant, first of all the official report from inspection does not constitute, by definition, a draft decision within the meaning of Article 60(3) of Regulation (EU) 2016/679; at the same time it is clear that these steps preceded (both chronologically and legally) the present administrative proceedings, thus they cannot affect its lawfulness.

[33] As to the argument of the Charged Company that the Office denied it the right to have the case heard in its presence, the Appellate Authority states that the Accused apparently perceives the procedure under Article 60 of Regulation (EU) 2016/679 as a certain form of administrative proceedings. As stated above, the deliberation of the lead supervisory authority and other supervisory authorities concerned is not an application of the provisions of Act No. 500/2004 Coll., it does not take the form of administrative proceedings, and it takes place after the procedural rights of the participant have already been exercised. Neither Act No. 500/2004 Coll., Act No. 250/2016 Coll., nor Regulation (EU) 2016/679 grant participants any additional procedural rights, especially since the fundamental logic of the directly applicable general regulation does not functionally allow for such a form of participation in deliberation. In the course of the procedure under Article 60 of Regulation (EU) 2016/679, the supervisory authorities familiarise themselves with the draft decision and the previous national proceedings and assess these. However, the Appellate Authority emphasises that this is only performed when all procedural steps in the administrative proceedings in question have already been carried out prior to the very issuance of the decision and its delivery to the participants in the proceedings.

[34] Therefore, if the Charged Company is demanding its “procedural participation” in the deliberations, it is essentially claiming that the draft decision prepared by the Office should be delivered to it within the different phases of the procedure under Article 60 of Regulation (EU) 2016/679 for additional statements. However, neither the Czech legislation on administrative proceedings nor the Regulation (EU) 2016/679 guarantee such right.

[35] In Decision ref. UOOU-01025/20-82 of 30 August 2021, the Office stated that allowing the Accused to comment on the objections of the other supervisory authorities could lead to an “*irresolvable procedural loop*”. Should the comments of the Charged Company lead to a change in the draft decision, such a draft would have to be resubmitted to the other supervisory authorities. This procedure could be repeated, *ad absurdum*, forever. Guidelines 2/2022 (paragraph 168) state “*This is without prejudice to the efforts made to reach consensus and to the eventual obligation of the lead supervisory authority to provide the right to be heard again, pursuant to national law, in view of envisaged changes in the revised draft decision that will newly affect the rights of the controller or processor*”. In this paragraph, the Board refers to an “*eventual obligation*” pursuant to national law, and, most importantly, relates this eventuality only to the “*revised draft decision*”, in the context of potential *novelties* that the controller did not have opportunity to comment on or rather which were not based on existing findings. The Czech national law, however, does not provide for an obligation to inform the participant of the draft decision; it does not envisage at all any period of time between the formulation of the draft decision and its completion from the procedural and formal perspective in the legally prescribed form (i.e. through its signature by the authorised official) for the participant to the proceedings to access the administrative file, familiarize themselves with the newly formulated draft decision and to submit additional statement thereon. This may seem as certain externality of the remote written procedure under Article 60 of Regulation (EU) 2016/679, that such period of time, in the order of weeks, in fact occurs, however solely due to communication among supervisory authorities that are not physically present in the same place at the same time. In the case of the approach proposed by the Charged Company, the procedural loop would genuinely occur, as the Charged Company ignores that the “*final say*” is for the supervisory authorities and not for the accused.

C. Legitimate expectations

[36] The Accused raises an objection to another procedural error of the Office, namely an infringement upon its legitimate expectations, since the same act had already been handled by the Office once before. The Accused states that the Office performed the Inspection (commenced on 2 July 2018, ref. UOOU-07166/18) concurrently with these administrative proceedings, which, among other things, also concerned transferring data to the  company. This should be evident from, for example, the Statement of the Accused of 1 August 2018. According to the Accused, the two matters overlapped in time as well, since in relation to the Inspection the Office decided on 18 September 2020 (Administrative Record ref. UOOU-01733/19-31) that it would not commence administrative proceedings, whereby the administrative proceedings currently in progress were already commenced on 27 February 2020. The Accused has further stated that it disagrees with the argument of the first-instance administrative authority that the abovementioned Administrative Record only concerned the development of the antivirus program.

[37] To this the Appellate Authority states that the Inspection (ref. UOOU-07166/18) was commenced on 2 July 2018 due to a referral by the Netherlands Supervisory Authority

(complaint about inability to deactivate preinstalled privacy settings in the free version of the antivirus software for Apple Mac). The subject-matter of the complaint was upholding the duties pursuant to Regulation (EU) 2016/679 in relation to personal data processing of the Accused's (then the Inspected) antivirus software users' data with focus on standard of privacy security afforded to users using the free version of the antivirus software, in comparison to standard afforded to users of the paid version. Inspection Official Report ref. UOOU-0716/18-46 of 19 March 2019 does not mention transfer of data to the ██████████ company or statistical trend analytics at all, which makes it clear that the Inspection was not focused on data transfer to the ██████████ company.

[38] As already stated in the first-instance authority's decision (pg. 5 of the Disputed Decision), the Inspection of the Accused focused on fulfilment of obligations of the controller pursuant to Art. 5(2) of Regulation (EU) 2016/679, i.e. the responsibility for demonstrating compliance with fundamental principles relating to processing of personal data, and also fulfilment of obligation pursuant to Art. 24(1) of Regulation (EU) 2016/679, i.e. the responsibility to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. The Inspection did not directly concern the fulfilment of fundamental principles relating to processing of personal data pursuant to Art. 5(1) of Regulation (EU) 2016/679. This conclusion was stated even by the President of the Office in the Settlement of Objections against the Findings of the Inspection ref. UOOU-07166/18-53 from 4 June 2019.

[39] It is clear from the Administrative Record of 18 September 2020 (ref. UOOU-01733/19-31) that the conclusion about not commencing proceedings on corrective measures has its basis in the documents mentioned in this Administrative Record, which the Accused presented in the interim. For example, neither the General Privacy Policy updated in February 2020 (Attachment no. 6 of the Statement of the Accused of 26 February 2020 ref. UOOU-01733/19-20), nor other updated documents contain information about processing data for trend analytics anymore. In the aforementioned General Privacy Policy, it is stated, "*On the basis of our legitimate interest we will use your Personal Data for: /.../ Third-party analytics to evaluate and improve the performance and quality of our products, services and websites and to understand usage trends, and analyze user acquisitions, conversions and campaigns*". From the Statement of the Accused of 1 August 2018 (ref. UOOU-0166/18-12, under letter C) it follows that the Accused uses third-party analytics tools provided by the companies ██████████

██████████. The documents did not contain information about data analytics at the time of publication of the Administrative Record, and, according to the Accused's statement, the ██████████ company ceased its activities, therefore if there was a mention of third-party analytics, it wasn't meant in the sense of trend analytics but in the sense of third-party analytics from the General Privacy Policy cited above.

[40] It is explicitly stated in the request of the Office's Inspector ref. UOOU-01733/19-5 of 12 June 2019 that voluntary remedial of the deficiencies found by the Inspection [the Inspection found an infringement of Art. 24(1) of Regulation (EU) 2016/679] can prevent the commencement of proceedings for imposition of corrective measures. The Administrative Record ref. UOOU-01733/19-31 contains a conclusion about not commencing proceedings for imposition of corrective measures (that is measures to prevent repetition of found deficiencies in the future). In this respect, the Appellate Authority completely agrees with the

first-instance authority's reflections on the different nature and function of the inspection procedure and of the administrative procedure for corrective measures which may follow it, which exist to ascertain or possibly to ensure that the inspected person acts in accordance with the law (cf. page 4 of the Disputed Decision); in contrast to the procedure on administrative offences, which serves the purpose of finding out whether the act in question actually occurred, whether this act is an administrative offence, who committed this act, and what kind of penalty may the offender be sentenced to. The Office could not, in the Appellate Authority's opinion, induce legitimate expectations that voluntary remedial of the deficiencies would result in preclusion of the proceedings on administrative offence. Similarly, the fact that the Inspector of the Office decided in September of 2020 that based on the updated documents presented by the Accused she would not commence proceedings on imposition of corrective measures to remedy the deficiencies found by the Inspection does not mean that the Office cannot continue the proceedings on administrative offence currently in progress (commenced in February 2020), which are related to the act committed in 2019. Beyond that the Appellate Authority states that the Administrative Record of the Inspector on not commencing the proceedings is not an administrative decision by its nature, i.e. it does not constitute *res iudicata*. The Accused therefore cannot invoke the principle of *ne bis in idem*.

IIb. Evaluation from the perspective of substantive law

[41] The Accused stated in the Administrative Appeal that it did not transfer personal data to the ████████ company, because all of the transferred data were anonymised so that they were usable for trend analytics, but so that the data subjects would not be identifiable either. Direct and indirect identifiers, and even the so-called derivative information that could help to re-identify specific data subjects, were removed from the data for this purpose. The Accused is of the opinion that the first-instance administrative authority erroneously considers the transferred data to be personal data on the basis of the fact that two datasets could (theoretically) be connected together, and thus the data subjects could be identifiable. According to the Accused, it cannot be claimed that every time a data subject could be identified by connecting two datasets will both datasets be considered personal data, as certain information can be personal data in the hands of one person and at the same time not personal data in the hands of another person. If it were to be true that every information in conjunction with another information at the disposal of another person could lead to data subject's identification, it would mean that any information created by processing of what were originally personal data, and which contains certain combination of general traits (even if anonymised in a way which makes it unrelated to a specific person), would virtually always constitute personal data. The Accused is of the opinion that, according to the case law of the Court of Justice, it stands that when assessing identifiability of data subject, it is also necessary to take account of all means utilisable by third parties; nonetheless, it is necessary that these be means reasonably likely to be used by the controller or by third parties. According to the Accused, it cannot be reasonably assumed that third parties will utilise means not approved by law. Therefore, the first-instance administrative authority should, in the Accused's opinion, have examined not only if two such datasets exist but, most importantly, if it were reasonably likely that these two would actually be connected.




[42] Subsequently, the Accused described the utilised process of anonymisation in the Administrative Appeal, stating that before transferring any data to the ████████ company it removed all identifiers, using algorithms and methods described in U.S. registered patent ████████



According to the Accused, this automated process removed not only information directly identifying a specific person (such as the username), but also the information identifying a user indirectly (such as user ID), as well as information that could potentially lead to identification being worked out (such as unique combinations of certain parameters in the URL). The Accused has stressed that it was not a mere removal of direct identifiers, but an overall anonymisation of the data file in question. The complete history of browsed websites was not transferred either, since the result of anonymisation process was only a certain fragment of the complete URL file. The Accused further states that the first-instance administrative authority did not examine the anonymisation process in more detail, and it is therefore unclear how it arrived at the conclusion that personal data were being transferred to the [REDACTED] company.

[43] Identification of data subjects or any other reverse engineering (including connecting two datasets) was, according to the Accused, forbidden by the contractual documents concluded with the [REDACTED] company, and therefore it could not have reasonably assumed. Similarly, such activity would be in breach of law, more specifically in breach of Regulation (EU) 2016/679. To this, the Accused adds that the first-instance administrative authority did not claim nor try to prove that any reverse engineering ever took place via connecting datasets of the Accused and of the [REDACTED] company. The Accused and the [REDACTED] company were companies with independent management that had to abide by their concluded agreements. The [REDACTED] company was not a controlling person within the corporate group, and therefore could not order the Accused to transfer the data necessary for re-identification of data subjects, whereby the [REDACTED] company did not have any means of achieving re-identification of data subjects, and it can therefore be hardly concluded that it was possible to reasonably assume re-identification of the data subjects.

[44] In the Administrative Appeal, the Accused also expressed its opinion regarding the contents of agreements concluded with the [REDACTED] company, which delineate the process taken by the parties in case that transfer of personal data occurs. The Accused has repeated that it was transferring only anonymous data to the [REDACTED] company and only for reasons of adequate assurance did the parties to an agreement set up processes for cases when transferring of data would occur inadvertently and in conflict with the subject matter of the agreement. According to the Accused, the first-instance administrative authority pointed out that the texts of agreements referred to the removal of direct identifiers as anonymisation. Even though the parties to the agreement chose this title (removal of direct identifiers), in reality they understood anonymisation to be a significantly broader process of anonymisation in the sense described above. The first-instance authority should not have, in the Accused's opinion, been satisfied with how the parties called the process in the agreement, but it should have examined what this process looked like in reality.

[45] To the matter of transferred data, the Accused stated that it transferred internet browsing history data, which it anonymised. The information transferred was therefore information with a meaningful value for statistics, it was possible to determine trends in general, consumer preferences etc. According to the Accused, the [REDACTED] company could not, however, identify specific persons, not even with respect to their social identity as the first-instance administrative authority states in the Disputed Decision. The Accused also did not transfer complete browsing history, since the history was anonymised and some URL addresses were not included due to technical reasons (such as websites with Ajax technology), some were not relevant for statistical trend analytics, which is why they were not part of the


datasets. At the same time, the data was collected only from browsers with the  Online Security browser extension installed and enabled, and from mobile applications  Mobile security and  for the Android platform, whereby it is, according to the Accused, a common knowledge that users tend to use more than one browser.

[46] The Accused further stated that in the proceedings on administrative offence it is necessary to ascertain the factual state of the case, so that all doubts in the matter are dispelled, and it is necessary to supply legally relevant evidence to support the conclusions of the administrative authority; unsubstantiated speculation stemming from news articles certainly does not satisfy this. The Office never substantiated what data the  company provided to other persons, and therefore it is not possible to base any conclusions upon these unsubstantiated facts. The purpose of transferring data to the  company was never to find out information about specific persons, but to come to generally valid conclusions relative to specific social segments and types of customers, as only such data are commercially viable.


Rationale of the legal framework and the principle of liability of the controller

[47] By way of introduction, the Appellate Authority emphasises that the rationale of the personal data protection regulation is the prevention, i.e. forestalling or at least minimising the risks of infringement upon data subjects' rights. Practical way in which this preventive approach is displayed, among other things, lies in that all definitions included in the relevant legal provisions need to be interpreted extensively, while at the same time all exemptions are to be interpreted in the most restrictive manner. This is reflected in the long-established practice of the Court of Justice (e.g. judgment in case Lindqvist C-101/01 of 6 November 2003; judgment in case Ryneš C-212/13 of 11 December 2014; judgment in case Jehovan todistajat C-25/17 of 20 July 2018; judgment in case Nowak C-434/16 of 20 December 2017). In contrast to the legislation preceding Regulation (EU) 2016/679 (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), Regulation (EU) 2016/679 explicitly contains a principle of the controller's accountability. According to this principle, pursuant to Art. 24 of Regulation (EU) 2016/679 the controller has to adjust the specific manner of performing the processing operations to the risks arising from such personal data processing. At the same time, the controller is obliged to comply especially with the principles articulated in Art. 5(1) of Regulation (EU) 2016/679 (again in an adequate manner relative to potential risks) and has to be able to demonstrate compliance with these principles pursuant to Art. 5(2) of Regulation (EU) 2016/679; effectively, this transfers the burden of proof onto the controller. The controller is therefore obliged to, most importantly, evaluate the potential risks of the intended (as well as the already in progress) processing. The higher the risk of infringing upon the rights of data subjects, the more thorough must the controller be when evaluating the options of the processing as a whole, whereby it is necessary to primarily focus on fulfilment of personal data protection principles and adherence to them, and only secondarily to focus on finding out whether any of exemptions from these principles pursuant to Regulation (EU) 2016/679 apply. In case of high-risk processing that could lead to considerable interference with the rights of the data subjects, the controller must, to the maximum degree possible, take care to fulfil the obligations pursuant to Regulation (EU) 2016/679, and should not rely on potentially applying any exemptions.




A. Personal data

[48] In its statement in the course of the Inspection (ref. UOOU-07166/18-12 of 1 August 2018), the Accused expressed that with respect to the paid version of the antivirus software, the users were identifiable, because some of the billing details (in the scope of name, email address, city and country in which the user was located, information regarding the licence, information about payment method), which are collected by an authorised third party for the purpose of payment processing, may be provided to the Accused. From the  Privacy Policy (Attachment no. 7 of ref. UOOU-01025/20-11) it follows that the Accused gathers personal data in case of IT support requests in the extent of name, email address, telephone number, address, possibly the IP address, information about hardware, software, URL addresses of visited sites, files saved on the computer, email messages, and similar data. According to the Appellate Authority, it is clear from the aforementioned that part of the antivirus software users, i.e. paying customers and users who requested IT support, were identified for the Accused (not simply identifiable).

[49] In the Product Policy (Attachment no. 7 of ref. UOOU-01733/19-16), it is stated that the Accused processes personal data (aside from account data and billing data, where relevant) in case of utilization of the Antivirus for Desktop (Mac and Windows), specifically that it processes the following service data: identifier of the content (message) being delivered, IP address, malware samples, detections, URLs and referrers, events and product usage; as well as the following device data: internal online identifiers (GUID, Device ID), information concerning computer or device, location, information about applications on the device, other products of the Accused on the device, internet and internet connection, the number of devices on network and browsers (installed, default). It was possible to identify the user, even if indirectly, based on this information. The Accused was therefore processing personal data pursuant to Art. 4 No. 1 of Regulation (EU) 2016/679, which the Accused does not dispute.

[50] It follows from the Statement of the Accused of 1 August 2018 (ref. UOOU-07166/18-12), made in the course of the Inspection, that the Accused assigns a randomly generated alphanumeric code named GUID for each installation of the antivirus software. If there are multiple antivirus software products installed on the device, or if a product is uninstalled and reinstalled again, then each of these installations will, according to the Accused, have a different GUID, and GUID is therefore not a unique static identifier. It is further stated in the  Privacy Policy (Attachment no. 7 to ref. UOOU-01025/20-11) that the GUID is connected to billing data for customers of paid products and services for personal computers.

a) Data transferred to the company

[51] A part of the processed data was being transferred by the Accused to the  company. In the Product Policy (presented by the Accused on 20 December 2019, Attachment no. 7 ref. UOOU-01733/19-16), in the part dedicated to Antivirus for Desktop (Mac and Windows), it is stated: *“If Web Shield function is active and you opt-in for processing of data (internal identifier (GUID), product version, time information, stripped URLs (unless cached), carefully selected aspects of certain pages without identifiers, selected requests) for trend analytics purposes,  consequently provides this data set in a stripped and de-identified form to enable  to build products and services.”* For the Antivirus for Mobile (Android), it is stated: *“If Web Shield is activated and you opt-in for processing of Clickstream*

data (internal identifier (GUID), product version, approximate location, together with stripped URLs and information related to the URL of sites you visit online) for trend analytics purposes, [REDACTED] consequently provides this data set in a stripped and de-identified form to [REDACTED] to build its products and services.” (bolded by the Appellate Authority). Regarding this product, it is further stated that it also shares **time information and application IDs** with the [REDACTED] company. The same scope of the transferred data (except application ID) is declared in the Consent Policy (presented by the Accused on 20 December 2019, Attachment no. 2 of ref. UOOU-01733/19-16).

[52] Exhibit B (“Restated Data License Agreement”) of the Data Order Form entered into between the Accused and the [REDACTED] company on August 30, 2019 (hereinafter “Data Order Form” or “Agreement”) states in Section 1.7 titled “Data Controller”: *[REDACTED] and [REDACTED] acknowledge the Data may include personal data, as defined by applicable legislation („Personal Data“). To the extent Data contains Personal Data, the parties have analysed the nature of the use of Data under the Agreement and have determined that [REDACTED] has discretion to determine its uses of the Data in compliance with this Agreement and thus is a Data Controller.”* According to the Appellate Authority, it is clear from the abovementioned that the Accused was aware that the personal data of the users of its antivirus software could be transferred to the [REDACTED] company not only because of improper anonymisation. The Accused stated in the Administrative Appeal that it had established processes for the eventuality that personal data were inadvertently transferred to the [REDACTED] company, which however, according to the Accused, does not prove that it actually transferred personal data. Paragraph 1.7 of Exhibit B of the Data Order Form shows, though, that the [REDACTED] company was able to make further use of the personal data received. If the [REDACTED] company were only to destroy the accidentally transmitted personal data pursuant to the Agreement, then the [REDACTED] company would not itself be able to decide on its use and would not be in the position of a data controller. If the [REDACTED] company was not supposed to process the personal data at all, then, according to the Appellate Authority, it would make no sense for the [REDACTED] company to be defined as a data controller in the Agreement.



[53] In Exhibit B of the Data Order Form (point 1.1. titled “License”) it is stated that the [REDACTED] company is granted a license *“to download a copy of the Data (as defined and set forth in Exhibit A to each respective Order) /.../ and to use the Data for [REDACTED] business use for incorporation into [REDACTED] products and services in the Exclusive Field, including without limitation, to use the Data in whole or integrated in [REDACTED] services and to grant access to the Data as integrated in [REDACTED] services to authorized third parties, namely [REDACTED] customers”* (underlined by the Appellate Authority). “Exclusive Field” means, pursuant to the Exhibit B of the Data Order Form (Section 1.2), the field of *“the marketing, marketing analytics, advertising technology, marketing automation, marketing optimization, consumer analytics, eCommerce and trend analytics.”* Thus, in accordance with the Data Order Form, the [REDACTED] company could incorporate the received “Data” (representing or containing personal data) into its products and make them available to its customers.

b) Anonymisation and pseudonymisation

[54] According to Recital 26 of Regulation (EU) 2016/679, the data protection principles *“should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural*

person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

[55] Recital 28 of Regulation (EU) 2016/679 further states that “the application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations.”

[56] Article 29 Working Party (WP29) Opinion No. 5/2014 on Anonymisation Techniques⁷ states that the creation a truly anonymous dataset “is not a simple proposition”, since “a dataset considered to be anonymous may be combined with another dataset in such a way that one or more individuals can be identified.” The Opinion further explains the concept of anonymisation, which is understood as “a technique applied to personal data in order to achieve irreversible de-identification”, whereby the data must be in such a form as to make it impossible to identify the data subject by any means reasonably likely to be used by the controller or any other person. To be truly anonymous, the data subjects should not be identifiable even by the controller himself. The Opinion also states that “it is critical to understand that when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data.” Although the Accused transferred data to the  company from which it removed some identifiers (however not e.g. the GUID), according to the Appellate Authority, the transferred dataset cannot be considered to be completely anonymous. Moreover, the recipient of the data (the  company) had the possibility, on the basis of the data transferred, to re-identify the data subjects (see below).

[57] According to the Appellate Authority, anonymisation is therefore to be understood as such a modification of personal data which usually **irreversibly** removes the personal nature of the data itself in absolute terms and not only in relation to one recipient of the data. On the contrary, pseudonymisation is a measure to mitigate the risks arising from the processing of personal data without affecting the nature of the personal data. As a matter of fact, Recitals 75 and 85 of Regulation (EU) 2016/679 speak of “unauthorised reversal of pseudonymisation”, which alone demonstrates the presumed reversibility of pseudonymisation, while preserving the personal nature of the personal data.

⁷ Available online at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[58] The question of the anonymisation limit is related to the issue of the so-called subjective and objective concept of personal data. According to the objective approach, it constitutes personal data if there objectively exists additional information somewhere which, in combination with the anonymised information, can lead to (re)identification of the data subjects. According to the subjective approach, if the controller does not have the necessary information leading to identification of the data subjects, it does not constitute personal data, even though such information may exist outside its reach. Given the strong pervasiveness of the prevention principle as a fundamental purpose of data protection regulation, the concept of personal data should be seen more in the perspective of the objective approach, which is in line with the current case-law of the Court of Justice.

[59] Essential in this regard is the judgment of the Court of Justice in Case C-582/14 Breyer of 19 October 2016, which establishes rather the objective approach. In the judgment (paragraphs 44-46), the Court states: *“The fact that the additional data necessary to identify the user of a website are held not by the online media services provider, but by that user’s internet service provider does not appear to be such as to exclude that dynamic IP addresses registered by the online media services provider constitute personal data within the meaning of Article 2(a) of Directive 95/46. However, it must be determined whether the possibility to combine a dynamic IP address with the additional data held by the internet service provider constitutes a means likely reasonably to be used to identify the data subject. Thus, as the Advocate General stated essentially in point 68 of his Opinion, that would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.”* Consequently, in order for a data subject to be identifiable, all the information necessary for identification does not have to be in the hands of a single controller (objective approach). According to the Court of Justice (following Recital 26 of Regulation (EU) 2016/679), the identification of a data subject is not permissible if it is prohibited by law (not merely contractually, as the Charged Company suggests) or practically impossible.

[60] The Appellate Authority sees a significant difference in whether the identification of data subjects is prohibited by law or by a contract. Compliance with the prohibition on processing arising directly from the law can in general be claimed by anyone and can be enforced by the means of public law. Such prohibition also has an important preventive function, which is essential in the field of personal data processing. The Office does not question the principle of *pacta sunt servanda* (agreements must be kept), however, in private contractual arrangements, the content of which is usually known only to the contracting parties, the possibility of seeking or enforcing compliance with the obligations agreed between the contracting parties (or compensation for damage caused to data subjects) is considerably more limited. It is also not to be overlooked that a contract may be amended by the parties, and that a contract may be void or unenforceable.

[61] In its statement of 4 December 2023, the Accused argues that the recent case-law of the Court of Justice demonstrates a shift from the objective to the subjective approach to the concept of personal data. The judgment of the General Court in case T-557/20 Single Resolution Board of 26 April 2023 does indeed show a shift towards the subjective approach to the concept of personal data, but the conclusions set out in that judgment cannot be applied to the present case, since (as explained below) the ██████████ company had the capacity to identify data subjects, e.g. on the basis of additional publicly available information.

Furthermore, according to the Appellate Authority, the applicability of said judgment is at least limited since it was later appealed to the Court of Justice. It cannot also be disregarded that, regarding the assessment of the concept of personal data, the General Court's decision in question constitutes a clear deviation from previous case-law of the Court of Justice.

[62] While the Court's reasoning in the judgment of the Court of Justice in case C-319/22 *Gesamtverband Autoteile-Handel* of 9 November 2023 suggests the subjective approach, the legally binding conclusion of the judgment confirms the need for broad interpretation of the concept of personal data.

[63] It is beyond any doubt that the Charged Company collected and further processed personal data of the users of its antivirus software. Also, the process of anonymisation of personal data constitutes one of the methods of processing personal data as defined in Article 4(2) of Regulation (EU) 2016/679. Pursuant to Article 5(2) of Regulation (EU) 2016/679, the controller must be able to demonstrate that the processing of personal data carried out by it complies with the principles for the processing of personal data set out in Article 5(1) of the Regulation. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller has an obligation under Article 24 of Regulation (EU) 2016/679 to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that the processing is performed in accordance with the Regulation. The abovementioned clearly shows that it is the controller who bears the burden of proof and therefore has the obligation to demonstrate to the supervisory authority that its processing is in accordance with Regulation (EU) 2016/679.

[64] The Appellate Authority, by letter ref. UOOU-01025/20-103 of 28 November 2022, requested the Charged Company to provide information on the processing of personal data, specifically:

- Attachment 1 of Exhibit A "Scope and Structure of Existing Data" to the Data Order Form concluded between the Accused and the ~~XXXXXXXXXX~~ company (the Data Order Form was provided by the Accused to the Administrative Authority on 14 April 2020 via electronical data mailbox without the said Attachment);
- detailed specification of the data, transferred to the ~~XXXXXXXXXX~~ company during the reviewed period, including its structure;
- representative sample of the data submitted to the ~~XXXXXXXXXX~~ company, including the data in its original form, i.e. before the removal of the identifiers (before "anonymisation" as the Charged Company refers to this process) from which the transferred dataset was created;
- specification of how accurate was the time-related information (e.g., with accuracy to the millisecond) that the Accused transferred to the ~~XXXXXXXXXX~~ Company during the reviewed period, together with URL addresses (as set out, for example, in the Consent Policy, the Product Policy, which the Charged Company sent to the Office on 20 December 2019);
- information on whether an address in the following format, for example, could have been transferred to the ~~XXXXXXXXXX~~ company during the reviewed period: <https://www.amazon.com/gp/buy/addressselect/handlers/edit->

address.html?ie=UTF8&addressID=REMOVED&addressIdToBeDeleted=&enableDeliveryPreferences=1&from=&isBillingAddress=&numberOfDistinctItems=1&showBackBar=0&skipFooter=0&skipHeader=0&hasWorkingJavascript=1;

- information about whether data were being transferred to the ████████ company from which it was possible to determine, for example, the following information: Device ID: (e.g. abc123x), Date: (e.g. 2019/12/01), Hour Minute Second: (e.g. 12:03:05), Domain: (e.g. Amazon.com), Product: (e.g. Apple iPad Pro 10.5 - 2017 Model - 256GB, Rose Gold), Behavior: (e.g. Add to Cart); and if not all of the above, then to what extent;
- more detailed explanation of the term “aggregated data” received and used by the ████████ company from the Accused (set out in the General Privacy Policy dated 19 December 2019 and in the Privacy Notice - document sent to the Office by the Charged Company on 5 August 2019);
- Disclosure of how many users of the Charged Company’s products (or devices) were involved in the data transfer (the ████████ company claimed on its website that the data came from 100 million devices).

[65] However, the Charged Company did not provide the Office with the requested information. Pursuant to Section 36(1) of Act No. 500/2004 Coll., participants are entitled to propose evidence and to make other motions during the whole course of proceedings until a decision is issued, and pursuant to Section 52 of Act No. 500/2004 Coll., participants are obliged to identify evidence to support their claims. In the proceedings before the first-instance administrative authority, and now before the Appellate Authority, the Charged Company merely repeats that it anonymised the personal data, i.e. that it did not transfer any personal data to the ████████ company, without describing the anonymisation process in detail and without providing (despite the Office’s request) a sample (output of the anonymisation process) of the transferred “anonymised” data or in any other way specifying the extent of the transferred data, or commenting in any way on the extent of the transferred data referred to in the Office’s request (dated 28 November 2022). Nor does the Data Order Form, on the basis of which the Accused claims to have been transferring data to the ████████ company, give a more precise (let alone detailed) specification, despite the express designation of Attachment 1 to Exhibit A as “*Scope and Structure of Existing Data*” and the text “*Exact scope and structure of the Existing Data from each source is shown in Attachment 1 to this Exhibit A below*” (Article 1 of Exhibit A). The Charged Company has repeatedly referred to the use of robust anonymisation techniques (patented process) but has not proven that the anonymisation it carried out resulted in truly anonymous data, contrary to the principle of the controller’s responsibility.

c) Possibility of re-identification of data subjects

[66] According to the Appellate Authority, the Accused was not transferring (only) anonymous data since it was possible to re-identify the data subjects.

[67] A natural person is identifiable if it is possible to distinguish them from others in a way that allows the holder of information to treat this person differently than towards other persons. A person is **directly identifiable** if the holders of information can identify the person, to whom the data pertain, only by using information and methods easily available to the

holders themselves; a person is *indirectly identifiable* if this is only possible by obtaining additional information or by using methods that are not easily available. Obtaining such additional information may require certain effort, such as searching the internet. Identification can also be based upon a combination of data that are not unique in isolation, but only when evaluated jointly in a given context, whereby additional information enabling the data subject's identification do not have to be at the disposal of one person. The Appellate Authority is aware that complete anonymisation of some data can be, considering the amount of publicly available data and technological progress (including newly employed artificial intelligence), very complicated and in some cases even impossible. A controller must consider and regularly evaluate the probability and severity of risks of data subject's re-identification, in case they process anonymised data. Anonymisation should be irreversible, i.e. it should prevent any re-identification of data subject, whereby the risk of re-identification by any person using means reasonably likely to be used should be very low (ideally non-existent).

[68] The Accused states in the Administrative Appeal that it removed any identifiers before transferring the data to the ██████████ company. However, as stated above, the Accused was transferring to the ██████████ company, among others, the generic user identification number (GUID), which is the identifier of the installation. From the Data Order Form (Attachment no. 10 of ref. UOOU-01025/20-11, specifically Art. 3 of Exhibit A) it follows that the ██████████ company is obliged to replace the GUID with a different unique identifier (JID) and destroy the GUID, whereby the ██████████ company is contractually forbidden to make any further use of the GUID. To this the Appellate Authority states that the Accused was transferring data including the unique identifier to the ██████████ company and was aware of it.

[69] From the Data Order Form (Art. 5) it further follows that real time data feed were being transferred, delayed by the time necessary for anonymisation, minimum once per every hour. In the Data Order Form (Art. 3 of Exhibit A) it is further declared that the ██████████ company cannot use the GUID for any other purpose than assigning a proper JID to relevant data and checking whether a proper JID was assigned to relevant data. From the abovementioned it follows that the same JID was always assigned to a single GUID, thus the transferred data (internet browsing history) were not limited to a short period of time, such as only for a single hour. The more data (long browsing history, time information, location data etc.) the ██████████ company had, the greater the uniqueness of chains of viewed URL addresses, which heightened the possibility of a successful identification of data subjects.

[70] Deletion of identifiers from internet site browsing history was performed, according to the Accused, by utilising algorithms and methods described in a patent registered in the USA under ██████████ (in the Administrative Appeal stated as ██████████, apparently a typo). It follows from the aforementioned patent that if there are more users with the same parameter value (component of URL), then this value will not constitute personal data. However, if the frequency of occurrence of the value in the URL is low, then the parameter could contain data leading to identification of data subject. In other words, an often-visited website will probably not contain personal data, whereas a site visited only by a single person can contain personal data. In that case, the value parameters in the URL can be deleted or replaced with a different information, such as the word "private".

[71] To illustrate what data were removed from the URL addresses, or rather which parts of the URL were transferred, it is necessary to refer to the structure of URL addresses. URL addresses have their own firmly established structure, they consist of individual components

sorted in a predetermined order and separated by designated symbols. Some components are not mandatory⁸. URL is typically made up of these parts: protocol a.k.a. scheme (for example HTTP), address part [subdomain, domain name, top level domain – e.g. www.dpp.cz or uouu.gov.cz, port (for HTTP the port number is 80)], path (structure of directory in which the site can be found), query (designated by the “?” symbol, after which the queried parameter follows), and fragment as the last component (links to a specific location on the webpage).

[72] From the Patent (item no. 0043) it follows that especially the path, query, and fragment can differ for various users, and usually contain private information (PII). This information can, however, show up in other parts of the URL addresses. Parts of URL that can contain this private information are described as a “parameter” in the Patent.

[73] From the abovementioned it follows that during the “anonymisation process” only certain parts were removed from the URL addresses (leaving aside the URLs that were not transferred based on this process), which could significantly differ in their contents. From some URLs a large part thereof could have been removed, and a significant part thereof could have remained in others, and some (probably a majority or at least a significant part, since as a rule URL addresses do not contain private information during standard searching for information on the internet or reading the news) remained unchanged, i.e. they were transferred complete. Based on the transferred URL addresses it was (even after removing some parts) possible to track (unique) movement of the user on the internet, what sites they visited, what videos they watched, what articles they read, what they looked up, or what they bought. If these data were to be connected or compared with other data (as described below), it would be possible to identify the data subjects and find out information about their interests, behaviour, preferences etc.

[74] Identification of data subjects was the topic of (for example) a scientific study of the Stanford University⁹, from which it follows that a de-identified browsing history can be connected with social media profiles, like Twitter, Facebook, or Reddit, with the help of publicly available information, by practically any attacker with access to browsing history. This study has shown that 72% of 374 users were successfully deanonymized (re-identified). According to the Appellate Authority, the ██████████ company alone or any of its employees, who had access to the browsing history, could connect this data to data from publicly available sources (such as social media), or from other sources (according to the Accused, the ██████████ company had multiple data sources), and therefore identify individual users. It is not decisive whether or not it would be possible to identify all users or only some of them.

[75] The ██████████ company itself could have identified data subjects by using publicly available information. Route planning (for example, on Google Maps) can be used as an example. If the starting point or end point of the route repeats itself often for one user (for example if it is often inputted as a starting point in the morning and as an end point in the evening), then it can be assumed that the user lives in this point. The user can be identified in a number of cases by using the user’s address, especially in a situation when it is possible to find out a lot of other information from an internet site browsing history; if London, 221B Baker Street was to be such an address, then other additional information would not be necessary at all (note that the Appellate Authority deliberately chose a fictional character’s

⁸ See: <https://en.wikipedia.org/wiki/URL>.

⁹ De-anonymising web browsing Data with Social Network. Jessica Su. Sharad Goel. Stanford University. <https://dl.acm.org/doi/pdf/10.1145/3038912.3052714>.

address for illustrative purposes). Possibilities of user identification could be even more extensive, since the ██████████ company had more sources of data. As already mentioned before, combining data from multiple sources (including those that are publicly available) can lead to identifying users. In case of the Antivirus for mobile devices (Android) product, the data about approximate location was also being transferred, which not only simplifies the identification of data subjects but can also lead to significant interference with their privacy.

[76] The risk of re-identification has been the subject of Article 29 Working Party Opinion 05/2014, in which the ways of re-identifying data subjects based on anonymised data are described (pg. 30 – 31). It follows from this Opinion that anonymised data about movie ratings that were inputted by users of the Netflix service during the period of 14 days represents such unique data that in combination with data from a publicly accessible database for movie ratings (IMDB) a re-identification of data subjects occurred (based on the fact that the users in question gave the same ratings to the same movies in the same time intervals). Even if this case does not have much in common with the present case, it is clear that the ██████████ company (and anyone who had or would have had access to data about visited URL addresses) could have identified users based on, for example, the fact that they made a comment, wrote a review, or gave a rating on some internet site they visited.

[77] It follows from the administrative file that the Accused published a post on the Twitter social media site *“As troubling as it sounds, it’s very easy to identify you in an anonymized data set. A new study finds that it doesn’t take much to de-anonymize data and trace it back to you.”*, whereby it linked to an article called *“Sorry, your anonymized data probably isn’t anonymous”* of 23 July 2019¹⁰, from which it follows (with reference to a study published in the Nature Communications magazine¹¹) that based on a de-identified web browsing history it is possible to identify specific users. Said post was later deleted. According to its Statement of 4 December 2023, the Accused considers the scientific study of the Stanford University inappropriate, as it concerned connecting profiles on social media sites with complete browsing history. According to the Appellate Authority, the referenced study further illustrates how it can be relatively easy to re-identify data subjects, whereby the Appellate Authority is of the opinion that data subjects can be identified even through incomplete browsing history, which can be evidenced further by the study published in the Nature Communications magazine, referenced by the Accused itself on its Twitter account and which the Accused does not contest. To this the Appellate Authority adds that complexity of anonymisation, i.e. difficulty of achieving complete anonymisation, is not something that has been addressed only recently in relation to Regulation (EU) 2016/679, but has been a long-term discussion point among experts¹². The Appellate Authority considers necessary at this point to emphasise that the Accused is not a company providing any generic software, but a company providing antivirus software, which should primarily serve as a tool for protecting data and privacy of users. Even users who are not well versed in information technology and cyber security who do not know how to secure their privacy in these environments rely on companies providing antivirus software. Excellent or above par level of professional knowledge (including that of expert knowledge in the area of personal data protection) and

¹⁰ Available online at: <https://mashable.com/article/anonymous-data-sets-easily-de-anonymized>.

¹¹ Available online at: <https://www.nature.com/articles/s41467-019-10933-3.pdf>.

¹² E.g. article *„Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization“*, published in the UCLA Law Review in 2009 (Volume 57, Issue 6, pg. 1701-1777), Available online at: <https://www.uclalawreview.org/pdf/57-6-3.pdf>

level of ethical standards of conduct is expected in this regard. That is, that a company offering privacy protection will not transfer or sell data which could expose anything about users' privacy to other entities. The Accused, as a professional in the field of protecting user privacy, should be aware of risks (challenging achievability of complete anonymisation of data) and should be certain (without any doubt) that the data it is transferring do not contain any personal data and that no possibility of interference with users' privacy due to subsequent processing of the transferred data exists.

[78] In an interview for ČT24 [\[redacted\]](#)¹³, the CEO of the Accused, [\[redacted\]](#) stated, in response to a question about his reaction to findings of foreign specialized magazines, that it was possible to relatively easily de-anonymize data that originated from [\[redacted\]](#) antivirus and which the Accused resold to the [\[redacted\]](#) company, i.e. that *“it is possible to connect specific behaviour of specific users, what they do on the internet”*, , that *“there exist studies, which research this in some kind of manner”*. He further stated that the Accused had concluded an agreement with the [\[redacted\]](#) company (and similarly, the customers of the [\[redacted\]](#) company had concluded agreements with it), in which it was *“explicitly forbidden to do any such sort of things”*, by which the conduct in question was protected against from the legal perspective. The Accused had, according to the Appellate Authority, known about (the existence of studies) that it was possible to relatively easily identify a user based on their behaviour on the internet (internet site browsing history). Later, the CEO of the Accused stated in the aforementioned interview that the Accused had not known this could happen, as the data did not contain any personally identifiable information (a.k.a. PII). The Accused argues in its Statement of 4 December 2023 that the administrative authority has taken individual parts of the interview out of context, because while CEO [\[redacted\]](#) admitted that studies which focused on the possibilities of re-identification in general did exist, he emphasised that the data went through complex anonymisation and, at the same time, contractual mechanisms prohibiting any re-identification attempts were in place. This claim and public statement of the Accused's CEO are, however, in the context of the Accused being aware of that *“it's very easy to identify you in an anonymized data set”* (and sharing this information on the Twitter social media site), considered purposive by the Appellate Authority.


[79] If the Accused knew about the possibility of re-identification of data subjects based on their de-identified internet browsing history, it is not clear to the Appellate Authority how the Accused could have been under the impression that if it deleted the so called PIIs, it would not be possible to identify the data subjects. In case of processing anonymised data, it is the controller's duty to examine whether the data are still anonymous, taking into account the technological progress, or if there isn't a possibility of identifying data subjects retroactively. In that case the data can no longer be considered anonymous and it is necessary to treat them as personal data

[80] The internet site of the [\[redacted\]](#) company¹⁴ [\[redacted\]](#) as of 24 June 2019 contained, among others, the following information: ***“Market smarter with consumer journey analytics. Examine every search, click, and buy. On every site; See it all. From search to purchase. Get a super-detailed view of every buyer path, as it twists and turns; Analyze with***



¹³ ČT24 is a 24 hour news channel of the Czech TV; the interview is available online at: [\[redacted\]](#)

¹⁴ Available online at: [\[redacted\]](#)

the internet. It is then possible (if not with an absolute certainty) to figure out, for example, interests of the data subjects, data about their behaviour or their habits (where they move, where they shop), their residence, but even their education, profession, religious conviction, political opinions, health status, or sexual orientation. Whatever other use of this information, which can be highly sensitive, can significantly interfere with data subject's privacy.

[85] In addition, the possibility of the data being connected by an employee is described in the abovementioned Patent, in the part explaining implicit private information. To this the Appellate Authority adds that connecting of databases cannot necessarily only occur on the basis of an identifier. In case of browsing history, which is essentially unique to every user, it is possible to compare anonymised data with data accessible to, for example, the abovementioned online store and to recognize the customer by their "route on the internet". This identification can be very simple in some cases, since even information about specific merchandise being put in cart and purchased at a certain time would suffice. Comparison of this information with own database about sales of this merchandise in the given time can easily identify the customer. Uniqueness of the data in the present case therefore does not lie in personal data being contained in URL, but in uniqueness of user behaviour on the internet. The  company had the data on movement of users on the internet (URL addresses and time information that were tied to GUID or JID identifier), even if (according to the Data Order Form) this internet browsing history was incomplete.

[86] Even a relatively small part of anonymised history can lead to re-identification of a data subject in the case at hand, therefore, from the perspective of the possibility of re-identification, it is not a decisive factor whether the Accused transferred complete browsing history, or only a part of it. Such question would be relevant in relation to what can be found out about the identified person in entirety. The bigger the part of browsing history at someone's disposal, the easier (and more probable) the successful identification. Concurrently, it is easier to gather more (detailed) information. At the same time, the Appellate Authority emphasises that it is not necessary to be able to identify all users. If even a small part of them can be identified, it is not possible to speak of anonymous data. Considering that the Accused was transferring anonymised browsing history from roughly 100 million devices (compare above), and considering the abovementioned possibilities of re-identification by third parties, even if only a small part of users were to be identified, it would still interfere with privacy of many data subjects. For the sake of completeness, the Appellate Authority states that in the present case it is not decisive whether re-identification of data subjects actually occurred, because it suffices that an infringement upon a legally protected interest, i.e. personal data protection and protection of data subject's privacy, could have occurred (or could occur in the future).

[87] It can be asserted that anonymous data do not fall within the scope of Regulation (EU) 2016/679, and neither does the obligation to properly secure data pursuant to Article 32 of said Regulation apply. The data transferred by the Accused to the  company cannot, however, be considered anonymous; as explained above, in case of a data breach or a data disclosure there is a high probability of re-identification of data subjects, which could lead to a significant interference with their privacy. At the same time, there exists a whole range of entities (including the customers of the  company, i.e. companies with massive databases of their own) that could identify internet users based on anonymous browsing history. To this the Appellate Authority further adds that (as described above) the Accused was aware of the existence of third parties that could re-identify individual users.

d) Aggregated data

[88] In General Privacy Policy of 19 December 2019 and in Privacy Notice (document sent to the Office by the Accused on 5 August 2019) it is stated that the ██████████ company received and used aggregated data from the Accused. The Accused was asked by the Appellate Authority via a request dated 28 November 2022 (ref. UOOU-01025/20-103) for a more thorough explanation of the term "aggregated data" (among other things). However, the Accused has not provided the requested information to the Office.

[89] To explain the term "aggregation" it is possible to use Article 29 Working Party Opinion WP29 05/2014 on Anonymisation Techniques, according to which the aim of the aggregation technique is to prevent a data subject from being singled out by grouping them with, at least, x other individuals. To achieve this, the attribute values are generalized to an extent such that each individual shares the same value. Aggregated records merge information about individual with information about groups of persons, and it is impossible to single out individual data subjects from them. Movement of users on the internet is unique, therefore it is highly unlikely that different users would browse different internet sites at the same time, in the same order, and spent the same amount of time on them etc. The ██████████ company was offering its customers an opportunity to examine "every click of the buyer". According to the agreement, the data were transferred to the ██████████ company in "real-time, delayed by the time necessary for anonymization, minimum once per every hour". The Accused was transferring browsing history together with a unique identifier GUID, i.e. the transferred data consisting of internet site browsing history were divided according to individual installations of antivirus software, or by the internet browser extension, respectively. With respect to everything mentioned above these were not and could not be aggregated data. The Appellate Authority is aware of the GUID being the identifier of installation, whereby one device can be used by multiple persons, it is nonetheless possible to identify multiple individual users based on browsing history (for example, in case that multiple users of a single computer each have their own social media account and/or if they shop online). It can be further stated that in the present time many of these devices are used by a single person, especially mobile phones.

e) The Agreement

[90] The data transfer between the Accused and the ██████████ company had its basis in an agreement called Data Order Form. In the final provisions of this agreement it is stated, "*The Agreement constitutes the sole and entire agreement of the Parties with respect to the subject matter of the Agreement and supersedes, terminates and replaces, with the effect as of the Effective Date, any other prior or contemporaneous written or oral understandings, agreements, arrangements, representations and warranties with respect to such subject matter, including without limitation the agreement between the Parties dated August 30th, 2014 consisting of Order page, Order conditions, Data Description and Data Licence Agreement*". It is further stated in the agreement that "*the term 'Agreement' as used herein consists of this Order, Exhibit A – Data Description (including the Attachment 1), and Exhibit B – the Licence Agreement*". In Exhibit B of Data Order Form (item no. 12.3.) it is declared that no amendment to or modifications of this agreement is effective unless it is in writing.

[91] In item no. 3 of the Data Order Form called Data Description it is stated that "*Definition of the Data to be provided under this Order ("Data") is attached as Exhibit A*". According to Exhibit A, called Data Description, Existing Data means "*all anonymized usage data provided*

to ██████████ on the Effective Date that is collected by ██████████ through the following computer programs, mobile applications, services or features thereof”, whereby “Exact scope and structure of the Existing Data from each source is shown in Attachment 1 to this Exhibit A below” (underlined and bolded by the Appellate Authority). However, Attachment 1 of Exhibit A (in the form in which it was presented to the first-instance administrative authority on 14 April 2020) contains only the headline “Scope and Structure of Existing Data”, without any other contents.

[92] The Office therefore asked the Accused via a letter of 28 November 2022 (ref. UOOU-01025/20-103) to present the abovementioned Attachment, as well as to state and present other information about the data transferred by the Accused to the ██████████ company. The Accused reacted to this request in a letter of 14 December 2022, in which it stated that it had “decided not to supply the requested information with reference to the prohibition of self-incrimination and other procedural guarantees pursuant to the Charter of Fundamental Rights and Freedoms, the ECHR, and the EU Charter”. The Office has therefore sent another request on 9 January 2023 (ref. UOOU-01025/20-105), in which it asked specifically for Attachment 1 of Exhibit A “Scope and Structure of Existing Data”, for Exhibit 2 “Competing Entities”, and Exhibit 3 “Material Columns of Data” to be submitted. Upon the Accused’s request, the Office extended the deadline for the submission of the requested documents and clarified that it demanded the submission of the original of the Agreement, including all of its addenda. The Accused informed in a letter of 7 February 2023 that the addenda requested by the Office were never finalised, nor signed. Further, the Accused stated that the Agreement was concluded in the summer of 2019 and signed on 30 August 2019, therefore outside the time period when the alleged administrative offence investigated by the Office in the present proceedings was committed. The Agreement should have, according to the Accused, been concluded with a retroactive effect from February 2019¹⁸. Before the Parties were able to finalise the Agreement, their cooperation was terminated, and shortly thereafter in February 2020 the ██████████ company ceased its activities. Even if the addenda were never finalised it does not mean, according to the Accused, that it was not clear between the companies what was being transferred. The goal of the Agreement was merely to formalize the current exchange of data between the companies. Finally, the Accused stated that the ██████████ company was a part of a single corporate group, whereby the scope of exchanged information between the parties was clear.

[93] To this the Appellate Authority states that the subject-matter of the Data Order Form was data transfer by the Accused to the ██████████ company, it is, however, impossible to ascertain therefrom what data the Accused was to transfer to the ██████████ company, and to ascertain the subject-matter of performance. In its Statement of 4 December 2023 (in reaction to the Preliminary Findings of the Office), the Accused stated that the Data Order Form was governed by the law of California, and the Accused therefore found unclear the grounds of the Office’s assumption that the law of California required a written form for this type of agreement. It follows from Exhibit B item no. 12.6. of the Data Order Form called “Governing Law. Submission to Jurisdiction.” that the Agreement is governed by the laws of the state of New York, i.e. not the law of California. The requirement of written form, i.e. the written delimitation of the scope of transferred data, is being inferred by the Appellate Authority from the explicit terms agreed upon by the parties to the Agreement (compare items [90] and [91]

¹⁸ According to the Data Order Form (item no. 1), combined with Art. 9.1, the Agreement were to be effective as of 1 January 2019.

above). In the Data Order Form it is explicitly stated that *“The Agreement constitutes the sole and entire agreement of the Parties with respect to the subject matter of the Agreement /.../”*, and that the precise scope of the data which should be provided based on the Agreement is specified in the Data Order Form. From the abovementioned it is clear that the parties to the Agreement agreed upon a written form of the Agreement, including the specification of transferred data. It is therefore only possible to speculate about why the parties to the Agreement did not fulfil this agreement. Based on the abovementioned, the Appellate Authority therefore considers the claim of the Accused that the scope of the transferred information was known to the parties to the Agreement irrelevant.

[94] As to the argument of the Accused that it did not manage to finalise the Agreement, the Appellate Authority notes that the transferred data were not specified in more detail in the previous agreement (Data Licence Agreement), concluded between the Accused and the ██████████ company on 30 August 2014, either. It stated only that *“Data’ means the anonymized usage data collected and made available by ██████████ for download and use by ██████████”*. The Accused therefore had 5 years to specify the subject-matter of the Agreement (up until the execution of a new agreement in 2019). With respect to the aforementioned, the Appellate Authority considers this argument of the Accused purposive.

[95] In the Administrative Appeal the Accused stated that it was not reasonably likely to assume the possibility of data subjects’ re-identification since it was contractually forbidden, and referred to Art. 4.6 of Exhibit B of Data Order Form: ██████████ *may not use the Data in any manner in an attempt to identify, or reverse engineer any direct identifiers related to the Data or otherwise attempt to derive or gain access to such direct identifiers”*. In this respect, the Appellate Authority states that it is certainly possible to contractually forbid any attempts to identify natural persons. Such legal guarantees usually represent a way of strengthening other measures undertaken by the controller in order to lower the risks related to the processing of personal data by making the measures legally enforceable and are therefore primarily instruments which hold the authorised recipients of anonymous (pseudonymous) information accountable. Even though these guarantees can lower the risks of identification, they do not replace anonymisation itself.

B. Legal basis and purpose of personal data processing

[96] The Accused further claims in the Administrative Appeal that if the President of the Office came to the conclusion that personal data was being transferred, then it was in accordance with Regulation (EU) 2016/679. The Accused, according to its statement, transferred subsets of anonymised product data, which allowed the ██████████ company to create a product mapping out general internet trends, not interests of individual users. In the Disputed Decision, the first-instance administrative authority does not dispute that the Accused had legal basis for collecting personal data, it does, however, state that it did not have a legal basis for their transfer to the ██████████ company. According to the Accused, the purpose for transferring data to the ██████████ company was compatible with the primary purpose for processing pursuant to Recital (50) and Article 5(1)(b) of Regulation (EU) 2016/679, because processing of personal data for statistical purposes is a processing with a compatible purpose. The goal of statistical analytics performed by the ██████████ company was to ascertain general findings about consumer behaviour, their preferences, and other relevant

circumstances. This activity used statistical methods and lead to statistical results, which showed general tendencies and trends, not information about individual persons. The Accused concedes that it was a commercial activity, but even a statistical activity serving commercial interest does, according to the Accused, comply with the definition of statistical activity pursuant to Regulation (EU) 2016/679.

[97] The Accused further stated that even if it had transferred personal data to the ~~XXXXXX~~ company and the purpose of transferring the data had not been compatible with the primary purpose of processing, it would have had legal basis for transferring data to the ~~XXXXXX~~ company in the form of legitimate interest. The Accused disagrees with the conclusion of the first-instance administrative authority that said transfer of data was not expectable, especially as the Accused did not explicitly inform the data subjects about transferring the data to the ~~XXXXXX~~ company. According to the Accused, processing of pseudonymised or anonymised data for the purposes of statistical analysis is not in any way unexpected, since it is a generally well-known fact that digital companies generally track trends among their customers and use acquired data for this purpose. In case of data transfer to the ~~XXXXXX~~ company, the legitimate interest of the Accused overrode the interests of the data subjects because the transfer of the data did not present any risk for the data subjects, and the data subjects could have rejected the data transfer through an opt-out mechanism. Opposite to this minimal interference are the legitimate interests of the Accused, be it the commercial interest or general interest in generally improving its products and figuring out consumer preferences.

[98] On the matter of legal basis for processing of personal data (transferring data to the ~~XXXXXX~~ company) the Appellate Authority states that with respect to the obligation to inform the data subjects about legal basis at the time of obtaining personal data [Article 13(1)(c) of Regulation (EU) 2016/679] the controller has to establish the legal basis before collecting the data themselves. The selected legal basis cannot be changed in the course of processing at will. According to the Appellate Authority, it is not possible to accede to the Accused's arguments that it transferred anonymous data [to which Regulation (EU) 2016/679 does not apply], in case these data were not anonymous it processed personal data for statistical purposes, and if this purpose was not compatible with the primary purpose of processing, then the processing was covered by the legal basis of legitimate interest. Even though the Appellate Authority is convinced that the Accused had not even determined the legal grounds for processing in advance, i.e. that it did not have a legal basis, it will still comment on the individual legal bases that were argued by the Accused.

[99] According to Article 5(1)(b) of Regulation (EU) 2016/679 it follows that personal data have to be *“collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’)”*. Similarly, according to Recital (50) of Regulation (EU) 2016/679 *“Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations”*. Even though it follows from the cited above that further processing for statistical purposes is not considered incompatible with original processing purposes, it is not possible to interpret these provisions as a general exemption from purpose limitation, i.e. that it is possible to process personal data for statistical purposes per se. Article

89(1) of Regulation (EU) 2016/679 explicitly provides that even the processing for statistical purposes is subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject; same as Article 5(1)(e) of this Regulation presumes implementation of appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject.

[100] Compatibility of purposes when processing data for statistical purposes was the topic of Article 29 Working Party WP29 Opinion 03/2013 on purpose limitation, in which (part III.2.3.) the Article 29 Working Party expressed its opinion regarding Article 6(1)(b) of the then applicable 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 [said provision being analogous to Article 5(1)(b) of Regulation (EU) 2016/679], that this provision “*should not be read as providing an overall exception from the requirement of compatibility, and it is not intended as a general authorisation to further process data in all cases for historical, statistical or scientific purposes. Just like in any other case of further use, all relevant circumstances and factors must be taken into account when deciding what safeguards, if any, can be considered appropriate and sufficient*”.

[101] In the appellate Authority’s opinion, disproportionate interference with data subjects’ rights must not occur even in case of processing of personal data for statistical purposes. The controller should, even in case of processing of data for statistical purposes, adequately consider circumstances mentioned in Article 6(4) and in Recital (50) of Regulation (EU) 2016/679, i.e. “*The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations*”. In the case at hand the Accused should have considered risks and potential consequences of further processing for the data subjects. As was already stated above, it was possible to re-identify data subjects based on the data transferred to the ██████████ company, and to potentially find out a possibly large amount of sensitive data (including special categories of data), which could lead to a significant interference with the privacy of data subjects and cause them harm. In case of statistical data analysis, it is also necessary to differentiate between situations when such further processing is to be carried out by the original controller, and situations when personal data will be transferred for this further processing to a third party (it can be compared to processing data through cookies of the owner of the internet site and through third party cookies). The Appellate Authority agrees with the Accused that an average user is aware of controllers using collected data for statistical purposes. These expectations are, however, tied to statistics relating to the subject-matter of the controller’s activity, in relation to the Accused that would be the operation or improvement of the Accused’s antivirus software functions. However, users were not, in the Appellate Authority’s opinion, usually expecting that the Accused, as a company providing products for users’ data

protection and privacy protection, would process their data with no relation to provision of services of the Accused in the name of “trend analytics”, and that it would transfer (sell) these personal data to a third party, who would then use such data for their own commercial interests, i.e. to sell them to customers with their own large sources of data

The fact that the [REDACTED] company is a sister company of the Accused changes nothing, as it was an independent controller from the perspective of Regulation (EU) 2016/679.

[102] According to the Accused, the purpose of the statistical analytics laid in tracking of trends, not in identifying individuals, and by its nature, it was supposed to be transfer of impersonal data (cf. the Statement of 4 December 2023). However, the evaluation of whether the data are personal data is not dependent on the intended purpose, i.e. the result of data processing. What is decisive in the case at hand is that the Accused transferred data which the [REDACTED] company was to process further. The result of this processing, declared by the Accused, were supposed to be completely anonymous summary statistics. It cannot be disregarded, however, that the data transferred to the [REDACTED] company were such that it could have identified data subjects therefrom on its own; at the same time, it is not decisive for evaluating if these were personal data whether the [REDACTED] company did so or did not.

[103] With respect to the commercial activity of the [REDACTED] company, the Appellate Authority further states that in item no. 1.1 of Exhibit B of the Data Order Form it is stipulated that the Accused grants to the [REDACTED] company the “*licence to download a copy of the Data (as defined and set forth in Exhibit A to each respective Order) /.../ and to use the Data for [REDACTED] business use for incorporation into [REDACTED] products and services in the Exclusive Field, including without limitation, to use the Data in whole or integrated in [REDACTED] services and to grant access to the Data as integrated in [REDACTED] services to authorized third parties, namely [REDACTED] customers*”. In the Appellate Authority’s view, it follows from the abovementioned that the [REDACTED] company further processed data it received from the Accused, and that it disclosed these data (incorporated into its products or services) to its customers. The [REDACTED] company therefore used the data for its own commercial interests.

[104] In this context it is crucial to evaluate whether the [REDACTED] company processed personal data for the purposes of creating statistics. Statistical purposes, according to the Recital (162) of Regulation (EU) 2016/679 “*mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. /.../ The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person*”. According to the Academic Dictionary of Foreign Words¹⁹, statistics is understood to be “*1. numerical recording and researching of mass phenomena; 2. a field of study focused on researching, processing, and quantitatively characterizing mass phenomena and large data sets*”. The fact that the results of statistics are general findings, and not information about individuals, is conceded even by the Accused in the Administrative Appeal (compare item no. 98 of the Administrative Appeal, for example). As stated above, the [REDACTED] company offered an opportunity on its internet websites to gain “*super-detailed view of every buyer path*”, which reveals that the

¹⁹ Available online at: <https://prirucka.ujc.cas.cz/?slovo=statistika>.

Company did not use the data for statistical purposes. The Appellate Authority concedes that the Company could have offered its customers products that contained statistical results as well, however it evidently (also) offered data, which cannot be considered results of statistical activity. It cannot therefore be said, according to the Appellate Authority, that the data was transferred to the Company and further processed only for the purpose of creating statistics. The Appellate Authority is in agreement with the Accused about the fact that statistical results can be used for other purposes, even for one's own commercial interests. Nonetheless, in case of the Company it was not about manufacturing statistics or about offering, or selling, purely statistical results. This is supported by the contractual terms cited above that the Company is entitled to "use the Data in whole or integrated in services and to grant access to the Data as integrated in services to authorized third parties", from which stems no requirement that the data should be further modified before such incorporation and disclosure, as could be expected if the data were truly supposed to be used for "statistical trend analytics" only.

[105] In its Statement of 4 December 2023, the Accused notes that proclamations from websites of the Company cannot be used as evidence, because they are marketing declarations, which are by their very nature simplistic and their purpose is not to precisely describe the legal and technical processes employed. Marketing statements should not be misleading or false, however. It is unclear to the Appellate Authority how else to interpret the information that the Company offered data "about every click" but that it offered truly detailed information about users and not only aggregated statistics. The Accused presents itself as a serious company on the market. The Appellate Authority finds it implausible that its sister company would attempt to reach out to new customers through misleading marketing statements. Furthermore, the customers of the Company at the time in question, among which belonged big multinational companies (as mentioned above), would easily see through false statements.

[106] With respect to the assertion of the Accused, that for transferring of the data to the Company the processing would be covered under a legal basis of legitimate interest, the Appellate Authority points out, that it is an obligation of the controller pursuant to Article 6(1)(f) of Regulation (EU)2016/679 to firstly evaluate whether they have a legitimate interest, whether the processing is necessary for the purposes of such legitimate interest, and if those interests are not overridden by the interests or rights of the data subject (to carry out a balancing test). Considering that the Accused was and still is, according to its statements, convinced that it was transferring anonymous data to the Company, it did not carry out a balancing test properly. On one hand, there is the legitimate interest of the Accused. As the Accused stated in the Administrative Appeal, it is a commercial interest and an interest in general improvement of products and finding out consumer preferences. On the other hand, there are the interests and fundamental rights and freedoms of personal data protection and privacy protection of the data subjects. As stated above, it was possible to re-identify the users of internet browsers, and in combination with their internet browsing history a significant interference with their privacy may occur, inter alia, as the data could be abused. Had the Accused carried out a balancing test properly it would conclude, in the Appellate Authority's opinion, that its legitimate interest does not outweigh the interests of data subjects.

[107] In case of processing of personal data pursuant to Article 6(1)(f) of Regulation (EU) 2016/679 it is necessary to take into consideration whether the data subject can reasonably

expect such processing [see Recital (47) of Regulation (EU) 2016/679]. Based on the information provided by the Accused (more on that in the part dedicated to the obligation to inform) the users could expect that the Accused would transfer (share) only anonymous data. Moreover, it was not clearly specified for what purpose, on which legal basis, and with whom the data will be shared. If the data subjects did not have sufficient and relevant information about processing of their data, they could not have a real idea about how the data processing would be performed and could not reasonably expect such processing.

[108] The relationship between the users and the Accused, an antivirus software provider, is vital from the perspective of legitimate interest as well. According to the Appellate Authority, one of the main reasons why users acquire an antivirus software is for protection of their data and the relating protection of their privacy. The Accused itself declared on the trend analytics activation screen of (from April 2019)²⁰ that users can be assured of their privacy being respected.

[109] The CEO of the Accused, [REDACTED], stated in an interview for ČT24 [REDACTED] that he understood the surprise of users, which the transferring of data to the [REDACTED] company could have caused, since they would not necessarily have read the screen on which they had to confirm the transfer of the data (according to his words, the Accused had apologised to users). To this the Appellate Authority clarifies that the confirmation of data processing, that is giving consent to the processing, took place from July 2019 and until then (verifiably from April 2019) the users could only click on a “continue” button below the displayed information. The Appellate Authority considers necessary in this context to mention that neither the users of the antivirus program, nor the users of the [REDACTED] Online Security extension could have expected that their data would be transferred (sold) to another controller. The users trusted the Accused, since it offered products for privacy protection, and therefore they were not sufficiently cautious about transfer of data by the Accused as they did not foresee transfers of data that could interfere with their privacy. The CEO of the Accused further stated in the interview that the news about transferring data to the [REDACTED] company had stirred up some animosity towards the Accused, i.e. certain loss of trust. To that the Appellate Authority states that if the users reasonably anticipated the transfer of data and if they were properly informed about it (i.e. including the selling of the data), they would not have been surprised by the news about monetisation of their data. The surprise of the users is further evidenced by the fact that in relation to their data being collected and sold, a consumer-protection organization from the Netherlands, [REDACTED], filed a class-action against [REDACTED], joined by more than 10,000 users of the antivirus program users from the Netherlands (according to publicly available sources²²). Transfer of data to the [REDACTED] company (and third entities) by the Accused was also addressed by the American Federal Trade Commission²³ which, among other things, banned any sale of internet browsing data for marketing purposes by the Accused.

[110] In its statement of 4 December 2023, the Accused stated on the infringement of Article 6 of Regulation (EU) 2016/679 described in the Preliminary Findings, that it was found guilty

²⁰ Attachment no. 5 of ref. [REDACTED].
²¹ Available online at: [REDACTED].
²² Available online at: [REDACTED].
²³ Available online at: [REDACTED].

of infringement of Regulation (EU) 2016/679 in the decision of the first-instance administrative authority, which it should have committed by relying upon the legal basis of legitimate interest during the processing of personal data for the purposes of statistical trend analytics. The Accused found out from the Preliminary Findings that it had processed personal data without any legal basis, which it considered to be a surprising conclusion. In the verdict of the Disputed Decision, the first-instance administrative authority has concluded that the Accused was found guilty of processing personal data without a legal basis. It is therefore unclear to the Appellate Authority why the Accused considers the same (preliminary) conclusion of the Appellate Authority to be surprising. The Appellate Authority concedes that the reasoning with regard to the legal basis has been significantly supplemented in the Preliminary Findings (and similarly so in the reasoning of this Decision), which is, however, in reaction to the arguments presented by the Accused in the Administrative Appeal.

C. Obligation to Inform

[111] In the Administrative Appeal, the Accused further disagrees with the conclusions of the first-instance administrative authority about infringement of the obligation to inform. To this the Accused states that it informed its customers about transferring data for the purpose of statistical analytics. The Accused considers the rebuke by the first-instance authority of the Accused's designation of the data as anonymous to be unfounded and formalistic. The Accused so informed because it was, and still is, under the impression that it anonymised the personal data. Even in case the Office concluded that the data were merely pseudonymised, the Accused is convinced that it informed its customers sufficiently. According to the Accused, it cannot be expected that customers will know the definitions of anonymisation and pseudonymisation. The purpose of Article 13 of Regulation (EU) 2016/679 lies in informing the data subjects in comprehensible language, whereby everyone understands the term anonymisation as removal of identifiers. In the examined case it was, according to the Accused, important that users were informed about the Accused "*removing everything that could personally identify the customer*" (item no. 136 of the Administrative Appeal).

[112] The Accused also disagrees that it did not state which data were processed for statistical purposes in the information about third party analytical data. In ~~§§§§~~ Privacy Policy in April 2019 the Accused, according to its statement, informed its customers about the fact that URL addresses of visited pages would be used for statistical purposes after removing identifiers. According to the Accused, it is impossible to always repeat the same information since the documents would then be disproportionately long and un navigable. In ~~§§§§~~ Privacy Policy from April 2019, in the part on third party analytic data, it is stated that the Accused transfers data that it collects about the users. Which data are being collected is then stated in other relevant parts of the Privacy Policy. The Accused therefore, according to its statement, duly informed its customers about the fact that it collects, among others, information about internet browsing.

[113] The Accused presented in its statement from 14 April 2020 (Attachment no. 5) the "screenshot of trend analytics activation process and privacy settings from April 2019". According to the Accused the users could have raised an objection against processing at any time. The following information was displayed to the users: "*Nearly every software product you use collects information about you. Search engines, games, everything. We do the same. This allows us to provide better products and services for you. **But we promise to respect your privacy.** We also promise that we will never publish or share any of your personal information*"

outside [REDACTED], nor allow anyone else to use it to contact you for marketing purposes without your consent. We do use the information that we collect to help us understand new and interesting trends. We may share this information with third parties outside [REDACTED]. However, before we do that, we will remove anything that identifies you personally. For more information, read our Privacy Policy. If after installing this product, you'd prefer not to participate in data sharing with [REDACTED] and third parties, **you can opt-out at any time** by unchecking the 'participate in data-sharing' box in the settings (bolded by the Accused)".

[114] In the [REDACTED] Privacy Policy (Attachment no. 7 of ref. UOOU-01025/20-11) it is stated:

[115] „When personal data is no longer needed we limit or stop using it in line with the minimization principle. For example, your email, the URLs of websites you have visited, your files, are scanned for malware detection and protection; then we remove your email address and other personal data or we hash any identifiers turning the Service Data into pseudonymized or anonymized data for paid users and anonymized data for free users before we re-use the Service Data for research, analytics, statistics, reporting, cross-product development, in-product messaging, and marketing.“ (chapter H. Service Data).

[116] „We also share statistical data that has been anonymized and aggregated geographically and so, cannot be used to identify individuals, with third parties for trend analytics.“ (Chapter 1. Our Policy's Aims; item 1.7).

[117] „We may use anonymous browsing data for third party trend analytics. All users may turn off data sharing in product Settings – Personal Privacy.“ (chapter Service Data Specific to Your Mobile – Web Shields).

[118] „We pseudonymize and anonymize the Clickstream Data and re-use it for cross-product direct marketing, cross-product development and third party trend analytics.“ (chapter [REDACTED] and [REDACTED] AntiVirus & Internet security products & services).

[119] It follows from the stated information that the Accused informed users of its products about sharing **anonymous** data. Users were therefore not informed about the fact that their personal data are being transferred, to what extent, or to whom. Similarly, the information about the purpose of the data processing itself is insufficient, in the Appellate Authority's opinion. Statements that “We do use the information that we collect to help us understand new and interesting trends.”, and that “This allows us to provide better products and services for you.” are too generic and say nothing about, especially, the manner of the processing, what data are necessary for the processing, or who is involved in the processing. The Accused did not inform data subjects even about the exact meaning of the “trend analytics”. The Appellate Authority does not, even after detailed review of the information provided by the Accused to the data subjects, find the information about the processing of the data to be sufficiently clear and understandable, all the more reason to consider it not to be sufficiently understandable for an average user. Furthermore, as substantiated above, it was not a (purely) statistical activity. Information about the processing was therefore, in the Appellate Authority's opinion, insufficient and misleading.

[120] The Accused did not duly inform about the legal basis, on which it based transferring of personal data to the [REDACTED] company, either. Incidentally, it could not have done so, in the Appellate Authority's opinion, since the Accused was not able to, and judging by the contents of the Administrative Appeal still is not able to, clearly identify the legal basis at all.

[121] First of all, the Accused considers the transferred data to be anonymous, not falling within the scope of Regulation (EU) 2016/679. The Accused then claims in the Administrative Appeal the compatibility of the processing for statistical purposes pursuant to Article 5(1)(b) of Regulation (EU) 2016/679. At the same time, it states that its processing should have been covered under the legal basis of legitimate interest pursuant to Article 6(1)(f) of Regulation (EU) 2016/679 as well. From July 2019 onwards, the Accused then implemented consent with personal data processing, even though it claims that the processed data were completely anonymous²⁴ (period from July 2019 onwards is not the subject-matter of these administrative proceedings, however).

[122] To the argument of the Accused that it sufficiently informed its customers about what data it processed for statistical and analytical purposes, the Appellate Authority states that the information was contradictory and disorganised. As the Accused informed about transfer of anonymous information, the users would not necessarily feel the need to thoroughly familiarize themselves with the Privacy Policies. Furthermore, the information in the actual Privacy Policy is scattered throughout multiple places and un navigable for the average user. The Accused informed the users about what data it collected within the scope of providing its services, it did not, however, sufficiently inform about the precise nature of the data transferred to the ██████████ company and for the purpose thereof. For example, in the Privacy Policy it informed about the removal of e-mail address and other personal data. The users therefore could not have known what data was removed and what was transferred. Similarly, they could not have known how the removal of identifiers from URL was performed and had to rely on the information from the Accused that the data transferred to the ██████████ company were anonymous. Incidentally, the Accused argues in the Administrative Appeal that the Office did not sufficiently deal with the process of anonymisation. The Accused therefore claims on one hand that it was sufficiently clear from its Privacy Policies what data was being transferred, and on the other hand it argues that the Office did not ascertain the exact scope of the transferred data, i.e. that it did not sufficiently concern itself with the process of anonymisation.

[123] The Appellate Authority emphasises that the Accused was found to be guilty of infringement of Article 13(1)(c) of Regulation (EU) 2016/679, i.e. it did not inform its customers about the purposes of the processing for which the personal data are intended nor about the legal basis for the processing at the time when personal data were obtained. The subject-matter of the Appellate Authority's considerations is therefore not the usage of an incorrect term (anonymisation or pseudonymisation) or other wording, but rather the reality of personal data processing by the Accused. What matters is that removal of identifiers did not result in anonymisation of data in the sense it is understood by the public (as stated by the Accused in the Administrative Appeal) because (as explained above) the users can be re-

²⁴ In July 2019, the Accused introduced the possibility to consent to data transfer for the purposes of trend analytics. The following information was displayed to users: „Mind sharing some data with us? **Other companies might collect data without your permission. But we thought we'd ask.** (bolded by the Appellate Authority) *If you allow it, we'll collect non-identifying data about your computer, network, and the websites you visit. This helps us build better products and services for all of our millions of users – you included. **This data is fully de-identified and aggregated and will not be used to personally identify or target you.** We may share this data with our 3rd-party partners for the purposes of analyzing markets and trends and gathering other valuable insights. **If you ever change your mind, you can always change your Personal Privacy settings anytime right from this app.***“ (bolded by the Accused). The following push buttons were displayed below the information „No, thanks“ and „I agree“ (Attachment No. 1 to the statement of the Accused of 14 April 2020 ref. UOOU-01025/20-11).

identified. When the Accused informed about transfer of anonymous data, then it created a false impression in the users that they could not be identified on the basis of transferred data.

[124] The Appellate Authority further adds, as to the obligation to inform, that the Accused informs the data subjects in the course of providing its products electronically. It is possible to simply provide individual information in layers. The users can thus be provided with basic information in the first layer and in case of further interest they can click on a link, which will lead them to more detailed information (in another layer). The Appellate Authority therefore disagrees with the claim of the Accused that if it provided information in multiple places at once, the users would be disoriented.

[125] The Accused stated in its statement of 4 December 2023 that the infringement on the obligation to inform (second administrative offence) should be subsumed into the first administrative offence in accordance with the absorption principle since the conclusion of the Office regarding insufficient anonymisation is the basis for both administrative offences in question and the Accused should not be liable for them individually. However, the absorption principle means that the more severe penalty will absorb the less severe one, not that the Accused should not be held liable for multiple administrative offences. The purpose of joint procedure on multiple administrative offences lies in the possibility to sentence someone to pay only a single fine, whereby its amount shall be determined based on the thresholds set by the law for the most severe offence. It is clear from the Decision of the first-instance administrative authority (pg. 20) that the Accused was sentenced to pay a fine (in accordance with the absorption principle) for committing administrative offence pursuant to Section 62(1)(b) of Act No. 110/2019 Coll., which the Accused had committed by infringing upon Article 6(1) of Regulation (EU) 2016/679. The fact that the Accused committed multiple administrative offences was assessed as an aggravating circumstance.

[126] In regard to the concurrency of infringements of Article 6 and 13 of Regulation (EU) 2016/679, in its statement of 21 December 2023 the Accused referred to the Opinion of the Advocate General Michal Bobek in the case of SIA "SS" (C-175/20), in which he stated: *"If there is no clear and foreseeable legal basis which permits such data transfers ultimately to take place, it can hardly be expected from the controller who collected the data to inform already the data subject accordingly under Article 13 of the GDPR"*. In the Accused's view, it follows from the cited Opinion that *"infringement Article 6 automatically includes and therefore unavoidably means infringement of Article 13 GDPR in the extent relating to the information about the legal basis"*. In the referenced case the Advocate General came to a conclusion that it was not possible to require fulfilment of the obligation to inform pursuant to Article 13 of Regulation (EU) 2016/679, because the controller in question was not aware of another possible processing of personal data (about a possible obligation to transfer requested data to the taxation authority) at all (the obligation to transfer personal data was not regulated by the national law). This is different from the situation in the preset case, because the Accused knew that it processed (transferred) personal data. The Accused also presented the information about transferring data to the ██████████ company to its users, albeit incorrect, and it was therefore aware of the fact that the obligation pursuant to Article 13 of Regulation (EU) 2016/679 applied to it.

IIc. Penalty determination

[127] The Appellate Authority further addressed Part IV of the Administrative Appeal, according to which the Disputed Decision suffers from a number of errors with regard to the sentence imposed. According to the Charged Company, the Office decided significantly inconsistently with its previous practice, misapplied the severity criterion and took into account virtually only facts against the Charged Company, while ignoring facts in its favour.

A. Consistency with the past decision-making practice of the Office

[128] The Accused refers to Section 2(4) of the Code of Administrative Procedure, according to which the administrative authority shall ensure that no unreasonable differences arise when deciding on factually identical or similar cases. In the case at hand, the first-instance administrative authority, according to the Charged Company, took a decision in apparent and fundamental inconsistency with its previous decision-making practice. The fine imposed on the Accused is more than 5,000 times higher than the sum of all fines imposed by the Office in the three years of the applicability of Regulation (EU) 2016/679. According to the Charged Company, it is hard to imagine that a mere two-month-long and entirely formal (without any real impact on data subjects) breach of Regulation (EU) 2016/679 could be more severe than the sum of all other breaches of that Regulation. Furthermore, the Accused pointed out that the fine imposed on it is more than 50,000 times higher than the highest fine imposed by the Office so far. According to the Charged Company, the relevant difference from the Office's previous decision-making practice is not even the amount of its turnover. The Charged Company considers that the reason why the Office imposed a diametrically different fine on it could lie in the international cooperation procedure. However, according to the Accused, the intention to comply with foreign supervisory authorities is not a legitimate reason for a decision that contradicts previous decision-making practice, since the penalty must correspond to the severity of the administrative offence and other relevant factors on the part of the Charged Company, and not to the procedure used by the Office.

[129] The amount of the fine imposed is, according to the Appellate Authority, incomparable to other fines previously imposed, for the reason that the act committed by the Accused cannot be compared with cases previously dealt with by the Office. The Office has not dealt with similar processing of personal data in the past. The case at hand is completely unprecedented in terms of the manner in which the data were processed, their extent, the number of data subjects concerned and the possible impact on their rights. In this regard, the Appellate Authority notes that the Office would have imposed an exceptionally high fine on the Charged Company even without discussing the case with other supervisory authorities in the framework of the international cooperation mechanism under Article 60 of Regulation (EU) 2016/679. According to the Appellate Authority, the entire case and the amount of the fine imposed must be considered in the perspective of the so-called "Big Tech cases", i.e. cases of large technology companies such as Meta, Amazon, Google, Apple, WhatsApp or Microsoft, which, like the Accused, have hundreds of millions of customers. In this context, the Appellate Authority simply adds for illustrative purposes, that WhatsApp was fined EUR 225 million²⁵, which is approximately 16 times the fine imposed on the Charged Company, and Meta

²⁵ Available online at: <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry>.

Platforms was fined EUR 405 million²⁶, which is more than 28 times the fine imposed on the Charged Company. The comparison with fines imposed by foreign supervisory authorities is, according to the Appellate Authority, entirely relevant, since Regulation (EU) 2016/679 is directly applicable throughout the EU and fines should therefore be imposed according to the same criteria. In this regard, it is not relevant whether the fine was imposed on the controllers by the Office or by another supervisory authority. Regarding the argument of the Accused (set out in its statement of 4 December 2023) that the mentioned technology companies have a much higher turnover than the Charged Company (and the fine imposed is therefore disproportionate according to the Accused), the Appellate Authority notes that were the fine to be imposed in accordance with the EDPB Guidelines 4/2022 on the calculation of administrative fines under the GDPR²⁷ (hereinafter “Guidelines 4/2022”; Chapter 6.2.), its amount would be based on the worldwide turnover for the previous financial year. According to Recital 150 of Regulation (EU) 2016/679, where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. In its judgment of 5 December 2023 in Case C-807/21 Deutsche Wohnen (paragraphs 55-57), the Court of Justice stated: *“As the Advocate General observed in point 45 of his Opinion, the reference in recital 150 of the GDPR to the concept of an ‘undertaking’, within the meaning of Articles 101 and 102 TFEU, is to be understood in that specific context of the calculation of administrative fines imposed in respect of the infringements referred to in Article 83(4) to (6) of the GDPR. In that regard, it should be stated that, for the purposes of applying the competition rules, referred to in Articles 101 and 102 TFEU, that concept covers any entity engaged in an economic activity, irrespective of the legal status of that entity and the way in which it is financed. The concept of an undertaking therefore defines an economic unit even if in law that economic unit consists of several persons, natural or legal. That economic unit consists of a unitary organisation of personal, tangible and intangible elements which pursues a specific economic aim on a long-term basis (judgment of 6 October 2021, Sumal, C-882/19, EU:C:2021:800, paragraph 41 and the case-law cited). Accordingly, it is apparent from Article 83(4) to (6) of the GDPR, which concerns the calculation of administrative fines in respect of the infringements listed in those paragraphs, that, where the addressee of the administrative fine is or forms part of an undertaking, within the meaning of Articles 101 and 102 TFEU, the maximum amount of the administrative fine is calculated on the basis of a percentage of the total worldwide annual turnover in the preceding business year of the undertaking concerned.”* If the Appellate Authority were to base the calculation of the fine on the turnover of the undertaking as defined by the Court of Justice, the fine imposed would be significantly higher, which, however, would be contrary to the principle of the prohibition of *reformatio in peius*. Since a change for the worse is prohibited by the Czech national law, the Appellate Authority did not proceed in a way that would have led to an increase in the fine imposed.

[130] The penalty imposed certainly cannot be considered exemplary. As further indicated below, the Office has imposed a penalty in accordance with Article 82 of Regulation (EU) 2016/679 which it considers to be effective, proportionate and dissuasive, taking into account both all the circumstances of the case and the turnover of the Charged Company. The amount

²⁶ Available online at: <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry>.

²⁷ Available online at: https://edpb.europa.eu/system/files/2023-06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf

of the fine imposed is therefore, according to the Appellate Authority, fully in line with Guidelines 4/2022.

[131] In its statement of 4 December 2023, the Accused argues that the Office's claim that the fine was imposed in accordance with Guidelines 4/2022 cannot be accepted, since at the time of issuance of the Disputed Decision, those Guidelines had not yet been issued, although it is clear, according to the Charged Company, that the Office was aware of them at the time of issuance of the Disputed Decision. Therefore, if the Office acted in accordance with the said Guidelines when imposing the fine, it was, according to the Charged Company, in breach of the principles of fair procedure and it was an unacceptable retroactive application. The Appellate Authority considers it necessary to stress at this point that the EDPB guidelines serve to ensure that Regulation (EU) 2016/679 is interpreted uniformly. Where the Office states that it has imposed a fine on the Accused in accordance with Guidelines 4/2022, this does not imply any change in the procedure of imposing fines, but only that the fine has been imposed in accordance with Regulation (EU) 2016/679, while the correct application of the various criteria was confirmed by the subsequently issued Guidelines. The fine was therefore imposed in accordance with Regulation (EU) 2016/679, not the Board's guidelines on its interpretation, and therefore there can be no impermissible retroactive application of the legislation. If the Appellate Authority were to conclude that the subsequently issued Guidelines 4/2022 interpreted Regulation (EU) 2016/679 more favourably for the Accused, which was not the case here, the Appellate Authority would adjust the findings of the first-instance administrative authority (the fine could be reduced).

[132] Just as it was possible to discover from the "anonymised" data that a particular German judge was interested in pornography²⁸, in the case under review, information (even of a very sensitive nature) could have been discovered about specific data subjects which could be used (also in the future), for example, not only for targeted advertising and the offering of relevant products, but also for a targeted influence on individuals. The Appellate Authority is convinced that the transfer of browsing history (albeit incomplete) to third parties may constitute a significant interference with the privacy of data subjects and in a case of targeted influence may cause them irreparable harm. Therefore, the Appellate Authority strongly rejects the view of the Accused that it has committed only a formal breach of Regulation (EU) 2016/679 without any impact on data subjects.

B. Severity of the conduct

[133] Here, the Charged Company points in particular to the difference between the type and the specific (individual) severity of the conduct, where the decision of the first-instance administrative authority wrongly takes into account the type severity as the severity of the specific act. Instead, according to the Accused, the first-instance administrative authority failed to assess the specific severity of the conduct in question. However, according to the Charged Company, the purpose of assessing the severity of the conduct is not to assess in general terms how serious the conduct in question is (this has already been done by the legislator) but, on the contrary, to assess how severe the act (the specific conduct) is in comparison with other infringements of the relevant provision. In its view, on the contrary, the specific severity of its conduct can be assessed as very low, since the alleged infringement was supposed to last only for two months and the rights of the data subjects were not affected

²⁸ See article linked in Footnote no. 10, referred to by the Accused in its post on Twitter.

in any way, since the alleged potential connection of the datasets never occurred and could not have occurred. Hence, according to the Charged Company, the Office is effectively penalising conduct for which no threat or infringement of a protected interest occurred. Finally, the Office also abandoned proving the exact number of allegedly affected subjects.

[134] Although the Accused may be right that, as a general rule, the type severity expressed in the sanction part of a legal norm cannot be taken into account when determining the penalty, this is clearly not the case. Under Article 83(5) of Regulation (EU) 2016/679, a number of breaches of obligations under Regulation (EU) 2016/679 can be penalised, it cannot go unnoticed that breaches of some of them make the conduct itself more serious in a particular case than breaches of some others. Typically, this is the situation in the case of infringement of legal obligations of such an intensity that the fundamental principles of the processing of personal data are compromised. For example, it can be noted that there is a fundamental difference between a short-term delay in responding to a data subject's request and a breach of the lawfulness of processing in the absence of a legal basis for the processing of personal data, even though both conducts correspond in their classification to an administrative fine of up to EUR 20,000,000 or 4% of the worldwide annual turnover.

[135] On the contrary, the infringement of the lawfulness principle in the form of the absence of any legal basis for the processing of personal data clearly constitutes the most serious type of conduct, since without it there can be no lawful processing of personal data. In the absence of a legal basis, it is fundamentally irrelevant from the point of view of lawfulness whether and how the controller fulfils any subsequent obligations, since such processing is unlawful from the very beginning. Similarly, expert literature also states: *“Legal basis is a condition without which processing is in any case impossible or illegal from the very beginning. Therefore, the existence of a legal basis must always be the first thing the controller must resolve before the intended processing, in addition to establishing the purpose of the processing. If the controller does not have a valid legal basis for the processing, the entire processing is unlawful from the beginning. If such processing is dealt with by the supervisory authority, it is thus very likely that the supervisory authority will order the processing to stop and the unlawfully processed data to be destroyed. At the same time, it should be kept in mind that even if the controller does not have to obtain consent for the processing and can rely on some other legal basis, it must properly comply with all other obligations under the Regulation, such as the obligation to provide information under Article 13 or 14 of the Regulation.”*²⁹

[136] The abovementioned is also confirmed by Guidelines 4/2022 (paragraph 62, Example 5a), which state that the supervisory authority *“attributed significant weight to nature of the infringement, as the infringed provision (Article 6 GDPR) underpins the legality of the data processing as a whole. Non-compliance with this provision removes the lawfulness of the processing as a whole.”*

[137] The fact that the infringement of individual articles of Regulation (EU) 2016/679 is divided into two categories (Article 83(4) and (5) of the Regulation) according to severity does not mean that the severity of all conducts in one category is the same. On the contrary, the more severe the illegal conduct within one category, the higher the fine that may be imposed

²⁹ NULÍČEK, M., et al. Art.6 Lawfulness of processing. In: NULÍČEK, M., a kol. Obecné nařízení o ochraně osobních údajů (GDPR): Praktický komentář [Systém ASPI] (NULÍČEK, M., et al., *General Data Protection Regulation: Practical Commentary*), Wolters Kluwer [cit. 20237-12]. ASPI_ID 1<032016R0679CZ. Available in ASPI. ISSN: 2336-517X.

by the supervisory authorities. According to the Appellate Authority, the existence of a legal basis is a *conditio sine qua non*, i.e. a condition without which the processing of personal data cannot (lawfully) take place. According to the Appellate Authority, the first-instance administrative authority was therefore entirely correct in its assessment that the absence of a legal basis for processing constitutes a fundamental failure to comply with the conditions for processing personal data.

[138] The Charged Company's objection cannot be accepted also in relation to the reasoning of the decision on the infringement of Article 13 of Regulation (EU) 2016/679. There is no other way than to agree with the first-instance administrative authority that, generally speaking, the obligation to inform significantly affects the general possibility of exercising the rights of data subjects to the full extent. Especially when it was the absence of any relevant information about the processing of personal data, its purpose as well as the absence of other information on the basis of which data subjects would be able to make a truly free and informed decision regarding their personal data, as required by Regulation (EU) 2016/679.

[139] The question of the duration and the related severity of the conduct is a relative question, as this period must be assessed in the light of other circumstances of the case. It may be stated that, although two months does not constitute an extremely long period, it cannot be regarded as a short period in the present case. As the first-instance administrative authority correctly stated, in view of the severity of the infringement and the number of data subjects affected, that period cannot be regarded as a mitigating circumstance, since even a single day would be significant. It is therefore irrelevant whether there was an actual connecting of datasets or other specific identification of data subjects. In this context, it is first necessary to recall that the data protection legislation does not duplicate the ex-post protection of personality under the Civil Code. Rather, the existence of data protection legislation is primarily aimed at preventing possible misuse of personal data and, to this end, it lays down a number of principles for the processing of personal data, including the requirement to have a valid legal basis, data minimisation, technical and organisational measures, etc., precisely in order to minimise the risk of possible, even potential, misuse. Simply put, it is sufficient for the administrative offence under Regulation (EU) 2016/679 that the rights of the data subjects have been compromised (endangering offence), i.e. there does not have to be a real infringement of their rights by the unauthorised processing of their data (which could however be assessed as an aggravating circumstance). In the case under review, the Office therefore dealt primarily with the consequence of the administrative offence, which is the endangerment of a legally protected interest, and not with its impact. The Appellate Authority does not accuse the Charged Company of having infringed the rights of individual data subjects, but that it cannot be ruled out (it is not certain) that this did not occur because the datasets in question containing personal data were transferred (sold) to a third party.

[140] In its decision, the first-instance administrative authority stated that the duration of the administrative offence has been proven to the extent specified in the verdict of the decision, and further stated that for the purpose of determining the gravity of the facts, account was taken only of the absence of the initial time-limitation of the reproached processing, but not of the actual period preceding the established (decisive) period. It is clear from the Disputed Decision that the first-instance administrative authority considered that the processing "*did not start at the beginning of the proven period precisely but entered as already 'running' into the established period.*" According to the Appellate Authority, the Disputed Decision clearly shows that the Accused was found guilty and a fine was imposed for

the infringement of the data controller's obligations during the period *"from an undetected date in April 2019 to an undetected date in July 2019"*. The first-instance administrative authority explicitly stated that the previous processing was not taken into account in determining the severity of the conduct, but only the indefinite nature of the beginning of the processing. The Appellate Authority agrees with the first-instance administrative authority that it is not possible to determine the exact date of the beginning or the end of the processing in question, therefore the time of the administrative offence is defined by the month and the year, not by the exact date. The Accused's activities prior to April 2019 or after July 2019 are not at issue in these proceedings and were therefore not taken into account by the Appellate Authority.

[141] Concerning the numbers of data subjects actually (and potentially) affected, the Appellate Authority first of all recalls that the legislation considers conduct affecting even a single data subject to be penalizable. The eventual quantification is then particularly relevant in the context of the penalty determination for the conduct in terms of its severity - and as such, the number of data subjects affected or potentially affected by the conduct of the Accused was reliably found to be enormous, i.e. rendering the infringement serious from a quantitative point of view. In support of this conclusion, the judgment of the Supreme Administrative Court of 31 January 2019, Case ref. 9 As 380/2017, may be cited: *"It is evident that it would be a disproportionate burden on the defendant to have to quantify the exact number of data subjects affected for the purposes of the offence specification. This would, of course, be appropriate in situations where the delict concerns a single or a few individual data subjects or when a more precise number can be determined without disproportionate effort (e.g. where the personal data are processed by automated means and are therefore precisely quantified). Generally, however, it is to be expected that, especially in the area of supervision of the processing of personal data, which is generally processed in bulk, there will often be situations in which the personal data, data subjects and other circumstances involved are identified only in a general way, with a reasonable estimation of their number (and, of course, their type). The Supreme Administrative Court agrees with the reasoning of the appealed judgment, which states, among other things, that 'in relation to the assessment of the severity of the appellant's offence, the Court does not consider it necessary that the number of personal data subjects affected by the appellant's conduct be quantified with an absolute precision (down to one); the order of magnitude of the thousands of subjects - given the number of units administered or owned by the appellant and quantified in the verdict of the decision - is, in the Court's view, quite sufficient for the assessment of the severity and extent of the illegal conduct"*. As stated above, the transfer of data to the ~~XXXXXX~~ company involved data collected from approximately 100,000,000 devices. A single device may be used by multiple users and likewise a single user can use multiple devices, therefore, according to the Appellate Authority, it is impossible to know exactly how many customers of the charged company were affected by the data transfer. However, the Appellate Authority agrees with the conclusion of the first-instance administrative authority that the number of data subjects affected was enormous.

[142] As correctly stated by the first-instance administrative authority, the processing of personal data was part of the professional activity of the Accused, i.e. connected to its business activity, and it was a systematic, not random, activity. The personal data of the Charged Company's customers were processed by means of information technology. The Charged Company informed its customers of this sophisticated processing only in a very

superficial and, moreover, misleading manner. It was virtually impossible for the data subjects to find out (verify) what data were being transferred and for what purpose, and they had to rely on the information of the Charged Company, as a professional in the field whose products are used to protect data and privacy. The users could not have known that the Charged Company was transferring (selling) data that were not anonymous, nor that they could be identified and consequently their privacy could be fundamentally infringed. The customers of the Charged Company could not have expected the data processing in question and could not have defended their rights. The purpose of the unlawful processing in question was to support the business activities of the Charged Company, i.e. to make a profit. In terms of the extent, the Appellate Authority emphasises the international, virtually global nature of the processing in question (the Charged Company offers its products in more than 150 countries).

[143] According to the Appellate Authority, the harm caused to data subjects cannot be individually examined due to the large number of data subjects affected. As already stated, the privacy of data subjects has been compromised by the conduct of the Accused, and the effects on the rights of individual subjects may become apparent in the future. Furthermore, it cannot be safely stated that users have not been identified, nor that they are not already being targeted in any way based on knowledge of their preferences or behaviour.

C. Additional criteria for the calculation of fine set out in Regulation (EU) 2016/679


[144] According to the Accused, the Office took into account (often incorrectly) all the circumstances that were against it, but ignored (with one exception) or disregarded without justification the circumstances that were in its favour.



[145]



In January 2020, a number of Czech and foreign media reported that the Charged Company had sold the data of its customers to the [redacted] company (some of these articles are included in the administrative record ref. UOOU-01025/20-3 of 27 February 2020). The Office merely reacted to this media case with the press release in question, with the aim of informing the public that it had taken notion of the case and would deal with it. The Appellate Authority is convinced that it was the publication of the information in the media, and not the Office's press release, that had a negative impact on the Charged Company. This is supported by the fact that the Charged Company's shares on the Prague Stock Exchange had significantly fallen even before the press release was issued (for example, on the website of Czech Television, in an article titled [redacted]).



[146] The individual circumstances which the Accused claims were incorrectly taken into account when deciding on the amount of the administrative fine were assessed by the Appellate Authority as follows.

a) Culpability (Fault)

[147] As the first relevant criterion, the Charged Company identified the culpability, i.e. whether the infringement was committed intentionally or negligently (Article 83(2)(b) of Regulation (EU) 2016/679). In this regard, the Accused pointed out that culpability has two components, namely knowledge and volition. The decision of the first-instance administrative authority states, on culpability, that the Charged Company knew what it was doing and therefore acted intentionally. However, according to the Accused, the mere knowledge constitutes negligent culpability. The knowledge component alone is not sufficient for intentional culpability and a volitional component is also required. The argument of the first-instance administrative authority that the Charged Company acted in the course of its business activity cannot, according to the Charged Company, be sufficient to meet the high evidential standard for intentional culpability. According to the Accused, the first-instance administrative authority does not indicate, let alone prove, any intention on the part of the Charged Company to infringe the provisions in question. Furthermore, the Charged Company claims that it acted in an excusable mistake of law (*error iuris*), which excludes culpability, since the Charged Company anonymised the transferred data and did not know that it was transferring personal data. In its further statement of 21 December 2023, the Accused referred to the recent judgments of the CJEU in cases *Nacionalinis visuomenės sveikatos centras* (C-683/21) and *Deutsche Wohnen* (C-807/21), both of 5 December 2023, regarding the subjective aspect of culpability.

[148] According to the said recent case-law of the Court of Justice (C-683/21 and C-807/21), a fine may be imposed on an controller for an infringement of Regulation (EU) 2016/679 only if the controller committed that infringement culpably, i.e. intentionally or negligently, whereas in the case of legal persons, it is not necessary that the infringement was committed by its management body or that this body had knowledge of the infringement. The judgment of the Court of Justice (C-683/21, paragraph 81) further states on fault that *„the question whether an infringement has been committed intentionally or negligently and is therefore liable to be penalised by way of an administrative fine under Article 83 of the GDPR, that a controller may be penalised for conduct falling within the scope of the GDPR where that controller could not have been unaware of the infringing nature of its conduct, whether or not it was aware that it was infringing the provisions of the GDPR.“*

[149] No specific definition of intent and negligence can be found in European law or in the CJEU’s case law, and the interpretation of these terms in the Court’s judgments is not always entirely consistent and unambiguous. According to the EDPB (WP 253) Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (pg. 11), “intent” includes both knowledge and wilfulness in relation to the characteristics of

³⁰ Available online at: [\[Redacted URL\]](#)

an offence, whereas “unintentional” means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law. The Guidelines specifically state that *“intentional breaches, demonstrating contempt for the provisions of the law, are more severe than unintentional ones and therefore may be more likely to warrant the application of an administrative fine. /.../ Circumstances indicative of intentional breaches might be unlawful processing authorised explicitly by the top management hierarchy of the controller, or in spite of advice from the data protection officer or in disregard for existing policies, for example obtaining and processing data about employees at a competitor with an intention to discredit that competitor in the market. Other examples here might be amending personal data to give a misleading (positive) impression about whether targets have been met /.../, the trade of personal data for marketing purpose i.e. selling data as “opted in” without checking/disregarding data subjects’ views about how their data should be used.”* Indications of **negligence** might be, according to WP 253 Guidelines, *“failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them). Enterprises should be responsible for adopting structures and resources adequate to the nature and complexity of their business. As such, controllers and processors cannot legitimise breaches of data protection law by claiming a shortage of resources.”* Routines and documentation of processing activities follow a risk-based approach according to the Regulation. This concept of intent and negligence is also adopted in the following EDPB Guidelines 4/2022 (Chapter 4.2.2).

[150] Pursuant to Section 15(2)(b) of Act No. 250/2016 Coll., an administrative offence is committed intentionally if the offender knew that by their actions they may violate or endanger an interest protected by law and in the event that they violate or endanger it, they were aware of this (indirect intention). As stated above, the Accused knew that the data it sold to a third party could be re-attributed to specific data subjects, i.e. that it was personal data. However, the Charged Company did not take sufficient steps to ensure that the data subjects could not be identified and that their privacy was not invaded. The contractual prohibition cannot be considered a sufficient measure in the context of the threat of infringement of the rights of data subjects. Due to the way in which the personal data were processed, the Charged Company could not verify the way in which the data transferred were further processed or detect whether the data subjects were actually re-identified, nor could it effectively prevent this. Moreover, it cannot be overlooked that the ██████████ company on its website essentially encouraged its clients to connect the data obtained from the ██████████ company with their own customer databases, which could (even if unintentionally by these clients) identify users of the Charged Company’s antivirus software. As the Accused pointed out in its statement of 4 December 2023 (paragraph 33), the ██████████ company had multiple data sources. Thus, by combining data from different sources, the ██████████ company was able to identify the data subjects.

[151] According to the Appellate Authority, the intrusion into privacy of data subjects (violation or endangerment of interest protected by law) was apparently not the primary objective of the Accused in selling data to the ██████████ Company. The aforementioned negative impact on the rights of data subjects, although it did not necessarily occur, must, according to the Appellate Authority, be seen as a collateral consequence of the Charged Company’s conduct and the Charged Company was aware of this consequence. If the intrusion into privacy was the purpose of the processing, then there would be direct intent, which would

constitute an even more serious breach of Regulation (EU) 2016/679. The Appellate Authority considers that the Accused was aware that the data transferred to the ██████████ company could re-identify data subjects and was aware that an intrusion into the privacy of users could occur. The Appellate Authority stresses at this point that any contractual prohibition on re-identification of data subjects does not render personal data anonymous.

[152] The abovementioned conclusion of the Appellate Authority is also confirmed by a former employee of the Charged Company, ██████████, in an interview with ██████████, in which he stated that the non-personalised data transferred by the Charged Company can be personalised quite quickly, and that some of the Charged Company's employees knew this, brought it to the attention of the Accused, and some even left because of it. With regard to the Accused's objection, set out in the statement of 4 December 2023, that ██████████ did not describe in that interview the tools needed to re-personalise the data or whether the ██████████ company had such tools at its disposal, the Appellate Authority notes that ██████████ statement is set out only in the context that it confirms the conclusions reached by the Appellate Authority. Based on that interview, the Appellate Authority does not infer how the ██████████ company could have identified the data subjects.

[153] In Guidelines 4/2022 (point 55, example 4), the circumstance indicating an intentional breach is provided by the example of *“the trade of personal data for marketing purpose i.e. selling data as “opted in” without checking/disregarding data subjects’ views about how their data should be used”*. In the present case, while it was not primarily the sale of personal data for direct marketing purposes, it was nevertheless the trading of personal data that could be used for marketing purposes (the interests and behaviour of data subjects could be obtained from their browsing history and products and services could be offered to them in line with their interests). In the case at hand, according to the Appellate Authority, it is not the marketing purposes that are crucial, but the fact that the sale of personal data was involved, with the views of the data subjects being completely ignored by the Accused. The Charged Company gave the data subjects the choice not to have their data transferred (opt-out). However, due to the lack of compliance with the obligation to inform (the Charged Company did not inform the data subjects at all that their personal data was being traded, nor how their data would be specifically used further), this cannot be considered as a genuine choice, as users made decisions based on incomplete or misleading information. The Appellate Authority is therefore convinced that its conclusion that the Accused acted intentionally is consistent with the EDPB guidelines.

[154] With regard to the excusable mistake of law claimed by the Accused, the Appellate Authority states that the Accused acted intentionally and knew that its act was unlawful. Even if that was not the case, the Charged Company is a company dealing with protection of privacy, whose relationship with the users of its antivirus products is, by its nature, based on trust, and expertise along with a high ethical standard of conduct is expected. The Accused should have assessed very carefully before the transfer of data to the ██████████ company (i.e. before starting the processing of the personal data in question) whether the data in question were indeed anonymous, as it must have been aware that the transfer of data which could be attributed to specific users, and on such a large scale, could lead to a significant invasion of the

³¹ Available online at: ██████████

privacy of data subjects. The Charged Company could have therefore avoided the possible alleged mistake of law by putting in sufficient effort. The Appellate Authority therefore finds that the Charged Company could not have acted, and did not act, in excusable mistake of law. Additionally, pursuant to Section 17(1) of Act No. 250/2016 Coll., a person who, when committing an administrative offence, does not know that his act is unlawful is not guilty if he could not have avoided the mistake. The cited Section 17 is included in Title II of Act No. 250/2016 Coll., regulating the liability of a natural person for an administrative offence. Title III on the liability of a legal person for an administrative offence does not mention the institute of mistakes of law. Therefore, the concept of mistake of law is explicitly addressed in Act No. 250/2016 Coll. only in relation to natural persons, not legal persons.

[155] At this point, the Appellate Authority considers it necessary to recall that the Charged Company provides software designed to protect the privacy of its users. As a professional in the information and cyber field, the Charged Company is thereby also expected to be extremely knowledgeable in the field of data protection. The Accused was aware of the risks of data processing and of the difficulty of achieving complete anonymisation of data (especially in a rapidly evolving technological environment) but decided to monetise the data of its users in the abovementioned manner anyway.

b) Degree of responsibility of the controller taking into account technical and organisational measures implemented by it

[156] According to the Charged Company, the first-instance administrative authority should have taken into account the technical and organisational measures implemented by the Charged Company pursuant to Article 83(2)(d) of Regulation (EU) 2016/679. At the very least, the Charged Company pseudonymised (in its view, anonymised) the data transferred. Pseudonymisation is mentioned in Article 32 of Regulation (EU) 2016/679 as one of the methods of securing personal data, therefore the first-instance administrative authority should have considered pseudonymisation as a mitigating circumstance.

[157] The Appellate Authority agrees with the Accused that the first-instance administrative authority should have assessed the technical and organisational measures implemented by the Charged Company, even though the scope of the present proceedings does not include infringement of the obligations under Articles 25 and 32 of Regulation (EU) 2016/679. As already mentioned above, although the Charged Company has implemented certain measures by removing certain identifiers from the URL addresses (first name, surname, email address, etc.) or by contractually prohibiting the re-identification of data subjects, these measures were not sufficient to allow the data transferred to be considered anonymous, however. Even at the request of the Appellate Authority, the Accused did not provide information from which the Appellate Authority could conclude that the measures taken by it were sufficient. As can be seen from the Guidelines 4/2022 (point 81.), the adoption of technical and organisational measures should be considered mitigating factor only in exceptional circumstances, where the controller or processor have gone above and beyond the obligations imposed upon them. In general, however, the level of accountability of the controller will be considered an aggravating or a neutral factor. In the case at hand, according to the Appellate Authority, the Accused has implemented certain measures which may have made it more difficult (but not impossible) to re-identify the data subjects, therefore the level of responsibility of the controller is considered by the Appellate Authority as a neutral factor. Like the first instance-

administrative authority, the Appellate Authority has therefore not assessed the level of responsibility of the Charged Company as an aggravating or mitigating circumstance.

c) Previous infringements

[158] In the view of the Accused, it should have been taken into account that the Charged Company has not yet been punished for illegal conduct in connection with the personal data processing. According to the Charged Company, it is a common practice to abstain from punishment or to impose a penalty at the lower end of the statutory sentencing range for a first illegal conduct, since a warning (or a minimum penalty) alone can be expected to deter future illegal conducts.

[159] Neither on this point did the Appellate Authority find the Charged Company's argument relevant. Based on the diction of Article 83(2)(e) of Regulation (EU) 2016/679, the Appellate Authority is obliged to take into account *any relevant previous infringements by the controller or processor*. Here, the European lawmaker is merely reflecting that recidivism in general is itself a harmful aspect of the personality of the offender and indicates a lack of corrective effect of the previous measure, which has to be taken into account in the penalty determination. The absence of a previous infringement is not envisaged as a mitigating circumstance by that provision. Neither did the Appellate Authority consider that, in a case of such a serious and socially harmful conduct, the fact that it is the first administrative penalty imposed on a particular controller or processor within the competence of the administrative authority should be substantially taken into account. Regulation (EU) 2016/679 (like any other generally binding legislation) is based on the assumption that its recipients, i.e. in this case controllers and processors, will comply with their obligations under it. Therefore, the fact that they have not yet been punished for infringements should not be considered as a mitigating circumstance.

[160] The same conclusion results from Guidelines 4/2022 (point 94.), which state that the existence of previous infringements can be considered an aggravating factor in the calculation of the fine. The absence of any previous infringements, however, cannot be considered a mitigating factor, as compliance with the GDPR is the norm.

d) Categories of personal data

[161] According to the Accused, the first-instance administrative authority should also have considered the fact that the unlawful processing did not involve special category of personal data. According to the Charged Company, it cannot be argued that the conduct in question is as serious as if the processing of a special categories of data was involved.

[162] The Appellate Authority disagrees with the Charged Company's conclusion. The prohibition on processing without a relevant legal basis, or proper information about that processing, applies generally to any personal data. The additional (stricter) conditions set out in Regulation (EU) 2016/679 for the processing of special categories of data represent a specific addition to the processing of "standard" personal data. The processing of special categories of data would undoubtedly be a factor substantially increasing the harmfulness of the assessed conduct, given their sensitive nature. However, this does not mean that the unlawful processing of merely "standard" data without such nature constitutes a mitigating

circumstance. It would only be found to be a non-aggravating circumstance, as the first-instance administrative authority correctly assessed.

[163] The same conclusion results from Guidelines 4/2022 (point 57.), which, regarding the requirement to take account of the categories of personal data affected (Article 83(2)(g) of Regulation (EU) 2016/679), state that the Regulation clearly highlights the types of data (data falling under Articles 9 and 10 of the Regulation) that deserve special protection and therefore a stricter response in terms of fines. According to the Appellate Authority, it cannot be inferred from those Guidelines that the unauthorised processing of solely “standard” personal data should be a mitigating circumstance. On the contrary, unlawful processing of a special category of personal data shall be treated more strictly.

e) The manner in which the conduct became known to the supervisory authority

[164] In the Disputed Decision, the first-instance administrative authority claims that the Office learned about the conduct in question from the media. According to the Accused, this is not true, since it had already notified the Office of all its data operations, including the transfer of anonymised data to the ██████████ company for statistical analytics purposes, on 1 August 2018. According to the Charged Company, it could not have notified the Office that it was committing an administrative offence because it did not know (and still disagrees with such conclusion). The Accused believes that it notified the Office of all relevant factual information prior to the initiation of the current administrative proceedings. According to the Accused, the media reports on the ██████████ case simply drew attention to the matter and forced the Office to take action. The fact that the Office learned the relevant information about the ██████████ company’s data transfer from the Charged Company should, according to it, be taken into account as a mitigating circumstance.

[165] When assessing the circumstance under Article 83(2)(h) of Regulation (EU) 2016/679, the manner in which the infringement became known to the supervisory authority may be taken into account, in particular whether, and if so to what extent, the controller or processor notified of the infringement. As the Accused states in the Administrative Appeal, it did not notify the Office of the infringement of Regulation (EU) 2016/679. It is true that the Accused, during the Inspection carried out under ref. UOOU-07166/18, by letter dated 1 August 2018, informed the Office that it was transferring data to the ██████████ Company, but it indicated (as it has claimed so far) that the data were anonymised. At that time, the Office had no evidence to dispute the Charged Company’s claims and therefore did not further examine the transfer of anonymised data. It was only on the basis of information from the media and the complaint of 22 February 2020 that the Office suspected that the Accused had transferred personal data, not anonymised data, to the ██████████ company. The Appellate Authority thus came to the same conclusion as the first-instance administrative authority, i.e. that the manner in which it became aware of the infringement could not be regarded as a mitigating circumstance. In accordance with Guidelines 4/2022 (point 99.), the Appellate Authority views this circumstance as neutral.

f) Previously ordered measures

[166] In the Administrative Appeal, the Accused further argues that the first-instance administrative authority in the Disputed Decision did not take into account the criterion set out in Article 83(2)(i) of Regulation (EU) 2016/679, i.e. the compliance with the measures

previously ordered against the Charged Company with regard to the same subject matter. Although the Charged Company agrees that the Office did not issue a corrective measure in the sense of Article 58(2) of Regulation (EU) 2016/679 against the Charged Company, it considers that the first-instance administrative authority omitted the fact that the Accused fully complied with the requests sent by the Office in the “preliminary proceedings” prior to the commencement of the administrative proceedings, which led to the Office not commencing the proceedings on corrective measures. According to the Charged Company, the imposition of the corrective measure did not take place, but only because the Charged Company cooperated with the Office. If the compliance with the previously ordered measures is a mitigating circumstance, it is even more so, according to the Accused, that the remedy was achieved without the imposition of such measures.

[167] Pursuant to Article 83(2)(i) of Regulation (EU) 2016/679, when imposing a fine, the supervisory authority shall take into account the compliance with measures previously ordered against the controller or processor with regard to the same subject-matter. As the Charged Company itself states, no measures have been imposed on it by the Office. According to the Appellate Authority, compliance with a measure that has not been ordered cannot be assessed. At the same time, as already mentioned above, the Inspection under ref. UOOU-07166/18, on which the Charged Company voluntarily adopted corrective measures, did not focus on the transfer of personal data to the ██████████ company, since the Office was not aware that personal data were being transferred. Therefore, according to the Appellate Authority, the condition of the same subject-matter is not fulfilled either. The first-instance administrative authority correctly assessed the circumstance under Article 83(2)(i) of Regulation (EU) 2016/679 as neutral. According to the Appellate Authority, this conclusion is fully in line with Guidelines 4/2022 (point 102.), which state that since compliance with measures previously ordered (which were not even ordered in this case) is mandatory for the data controller or processor, it should not be taken into account as a mitigating factor per se.

g) Nature of the ██████████ Company

[168] According to the Accused, the authors of Regulation (EU) 2016/679 clearly did not intend the nature of the controller to be relevant for the amount of the fine, otherwise they would have stated so in the Regulation. The Charged Company, according to its statement, provides antivirus software and does not hide the fact that its services are associated with trust from its clients, however, this applies to a range of other services. The Charged Company strongly rejects the claim of the first-instance authority that it should have disappoint the trust of its customers by transferring anonymised data for the purpose of trend analytics without their knowledge. The Charged Company informed its customers properly and, moreover, the trend analytics cannot be considered illegitimate, since they constitute a socially beneficial activity (they enable the improvement of the service and the overall customer experience) which most internet companies do.

[169] In this respect, the Appellate Authority notes first of all that, according to Article 83(2)(k) of Regulation (EU) 2016/679, the supervisory authority is to take into account any other aggravating or mitigating factor applicable to the circumstances of the case when deciding on the amount of the fine. In this regard, Guidelines 4/2022 (point 109.) state that the said provision deliberately leaves room for the discretion of the administrative authority with regard to the socio-economic context in which the controller or processor operates, legal context and the market context. According to the Appellate Authority, the assessment of the

nature (business activities) of the [redacted] Company and the products it offers (i.e. the socio-economic and market context) must be included in the assessment of the circumstances which may affect the amount of the fine. The Charged Company makes and offers products that are designed to protect the information and privacy of their users, in this case in an online environment [redacted] Online Security product). Users therefore expect from the Charged Company, as a data protection professional, among other things, an above-average level of protection of their personal data. The customers of the Charged Company gave the Charged Company access to their data because they expected it to remain confidential. By using the Charged Company's tools, users wanted to prevent or at least minimise the risk of misuse or unauthorised access to their data. However, the Charged Company's conduct endangered their privacy in a highly hazardous manner. Although the Charged Company allowed users of its antivirus software and browser extensions to decline the transfer of data to the [redacted] company, it did not sufficiently inform users of what data was being transferred. The Appellate Authority is convinced that far less users (if any) would have allowed the transfer of data had they known that their personal (rather than anonymous) data was being transferred. The relevant aspect, according to the Appellate Authority, is that the Accused transferred users' personal data which it had obtained specifically in connection with the antivirus software. The fact that, according to the Data Order Form, the Accused was selling these data to the [redacted] company and thus transferring it for profit cannot be overlooked.

[170] Also in its decision-making practice, the European Data Protection Board considers Article 83(2)(k) of Regulation (EU) 2016/679 *"of fundamental importance for adjusting the amount of the fine to the specific case"* and that *"it should be interpreted as an instance of the principle of fairness and justice applied to the individual case"*³². The EDPB also recalls that Article 83(2) of Regulation (EU) 2016/679 contains a nonexhaustive list of assessment criteria to be considered by the supervisory authority in determining the amount of the fine corresponding to what is necessary in each individual case to be effective, proportionate, and dissuasive in accordance with Article 83(1) of the Regulation. The Appellate Authority therefore, in agreement with the first-instance administrative authority, considers the nature of the Charged Company's conduct to be an aggravating circumstance.

h) Duration of the proceedings

[171] According to the Accused, the first-instance administrative authority should have taken into account the unreasonable duration of the proceedings. As a consequence of the long duration of the administrative proceedings (more than two years), the penalty lacks a corrective and motivational effect, since the Charged Company cannot reflect the outcome of the proceedings in its practice. The Charged Company has voluntarily rectified the alleged deficiencies and the fine imposed is therefore inconsistent with the individually preventive function of an administrative penalty. According to the Accused, the unreasonable length of the proceedings is one of the criteria to be taken into account when assessing the penalty in criminal proceedings, and the principles of criminal law are also applicable accordingly in the framework of administrative penalties. According to the Charged Company, the duration of the proceedings is also relevant for decision-making under Regulation (EU) 2016/679. The Accused refers to a decision of the Norwegian Privacy Board (Personvernemnda), which

³² Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), point 368.

annulled a fine imposed by the Norwegian supervisory authority on the grounds of the excessive length of the proceedings, which lasted almost three years. Personvernemnda also stated that, if it had not annulled the fine, it would have recommended that the supervisory authority reduce it.

[172] The Office admits that the administrative proceedings took a relatively long time. The complexity of the case had a significant impact on the duration of the proceedings, both at first instance and before the Appellate Authority. As the Appellate Authority has already stated above, the examined case is completely unprecedented in the Office's decision-making practice in terms of the manner and the scope of the processing of personal data. In the administrative appeal proceedings, the Accused did not support its claims regarding the anonymisation of data (contrary to the principle of accountability) and refused to provide the Office with the requested information. The Appellate Authority therefore had to thoroughly examine all the circumstances of a complicated case without the participation of the Charged Company, which led to delays.

[173] The administrative file demonstrates that the Office was not inactive in the case. The Accused exercised its procedural rights plentifully (numerous accesses to the file), submitted numerous statements and repeated requests for extensions of time for its motions. The length of the proceedings was also contributed to by the fact that during the proceedings the Office decided on the Charged Company's motion for an oral hearing (decision rejecting the motion, ref. UOOU-01025/20-43; decision rejecting the Charged Company's administrative appeal, ref. UOOU-01025/20-81) and on the Charged Company's request for access to all the records of the cooperation mechanism under Article 60 of Regulation (EU) 2016/679 (decision rejecting the request, ref. UOOU-01025/20-61; decision rejecting the Charged Company's administrative appeal, ref. UOOU-01025/20-82). The length of both the first-instance procedure and the administrative appeal proceedings was also influenced by the cooperation mechanism with other supervisory authorities under Article 60 of Regulation (EU) 2016/679, since the draft decisions of both the first-instance administrative authority and the one on the Administrative Appeal were submitted to the other supervisory authorities concerned.

[174] The Appellate Authority disagrees with the Charged Company's view that the imposed fine lacks the individually preventive function of an administrative penalty. The individual preventive function of the penalty is to deter the offender from committing further offences in the future. Moreover, the individual preventive function is not the only function which an administrative penalty is intended to fulfil. In the present case, neither the preventive function, whether individual or general, nor the punitive function, can be ignored.

[175] Concerning the Charged Company's argument regarding the decision of the Norwegian Privacy Board, the Appellate Authority states that it fully agrees with the first-instance administrative authority that the said decision is inadequate to the significance and scope of the Charged Company's conduct which is subject to the present proceedings. At the same time, the Appellate Authority points out that the Office is not bound by any decision of another supervisory authority which has reduced or cancelled a fine on the grounds of excessive length of proceedings in its proceedings in accordance with Regulation (EU) 2016/679 and its national law.

i) Newness of the relevant regulation

[176] According to the Accused, the fact that the incriminated conduct occurred only one year after the entry into force of Regulation (EU) 2016/679 should have been taken into account. The newness of the legislation in question and the technical complexity of the relevant processes (the need to create complicated technical solutions) should have played a significant role. According to the Charged Company, such approach is confirmed by earlier statements of the Office, which itself emphasised that the aim of its activities in the initial phase of the applicability of Regulation (EU) 2016/679 would be primarily to achieve compliance and not repressive measures.

[177] At this point, the Appellate Authority is left with no choice but to express a certain degree of wonder, or even concern, about the possible activities of the Charged Company prior to the applicability of Regulation (EU) 2016/679. The necessity of having a valid legal basis for handling or processing of personal data is a fundamental principle of data protection legislation and of any intrusion into a person's privacy in general, and this was unconditionally valid in an essentially unchanged form already under Act No. 101/2000 Coll., on the protection of personal data and on the amendment of certain acts, which transposed Directive 95/46/EC³³ into the Czech national law. Similarly to Regulation (EU) 2016/679, Act No. 101/2000 Coll. linked the processing of personal data to the existence of legal basis on the part of the controller and the related compliance with other obligations, including the obligation to inform. Discussions about minor nuances in the diction of the individual legal bases pursuant to Article 5(2) of Act No. 101/2000 Coll. and Article 6(1) of Regulation (EU) 2016/679 may be admitted, but in the context of the case these differences are completely irrelevant. Similar is the case with the definition of personal data. Indeed, the Accused itself must obviously have been aware of those obligations, since in paragraph 200 of its Administrative Appeal it explicitly refers to the rules on the protection of personal data in force before Regulation (EU) 2016/679, and confirms its knowledge of them by pleading that the absence of any penalty for their infringement should be taken into account. In any event, it cannot be concluded that any new regulation worthy of special consideration is relevant to the conduct in question.

[178] Beyond the scope of the Administrative Appeal, the Appellate Authority states that, in agreement with the first-instance administrative authority, it assessed as an aggravating circumstance the fact that the Accused had also committed an infringement of another provision of Regulation (EU) 2016/679, namely Article 13(1)(c), in relation to the same scope of personal data processing. As a mitigating circumstance in the sense of Article 83(2)(f) of Regulation (EU) 2016/679, the first-instance administrative authority and the Appellate Authority took into account the fact that the Charged Company voluntarily took steps in July 2019 to rectify the illicit state by introducing direct consent [even though, according to the Appellate Authority, this consent does not fully comply with the requirements of Article 4(11) of Regulation (EU) 2016/679] to the processing of users' personal data for the purpose of statistical trend analytics and by revising its privacy policy. The criterion set out in Article 83(2)(j) of Regulation (EU) 2016/679 is not relevant in the present case, as the Charged Company has not espoused to an approved code of conduct under Article 40 or a certification

³³ 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.

under Article 42 of Regulation (EU) 2016/679 and has therefore not been assessed by the Appellate Authority.

[179] The Appellate Authority also assessed the circumstances under Article 83(2)(c) of Regulation (EU) 2016/679, i.e. the steps taken by the Charged Company to mitigate the damage caused to data subjects. The Guidelines 4/2022 (point 76.) indicate that the measures taken by the controller must be assessed in particular with regard to the element of timeliness and their effectiveness. Measures that are spontaneously implemented before the controller becomes aware of the investigation conducted by the supervisory authority are more likely to be considered as a mitigating circumstance than actions taken after that point in time. The [REDACTED] company ceased its activities in January 2020, which, while seen positively by the Appellate Authority, could not have led to mitigation of the harm caused (or avert the threat of harm) to data subjects whose data had already been transferred to the [REDACTED] company, which further processed and disclosed them to third parties. The Appellate Authority is not aware of any further steps taken by the Charged Company to mitigate the potential impact of its conducts on data subjects. Based on the above, the Appellate Authority did not assess the circumstances resulting from Article 83(2)(c) of Regulation (EU) 2016/679 as mitigating or aggravating.

[180] The Appellate Authority thus fully agrees with the approach of the first-instance administrative authority in calculating the administrative fine and its amount.

[181] Furthermore, the Appellate Authority points out that when calculating the fine, the Administrative Authority based its calculation on the Charged Company's turnover for the year 2020, which, according to the financial statements of the Accused published on the website justice.cz, was [REDACTED]. When determining the amount of the fine, the supervisory authorities are to base it on the turnover of the accused at the time of the issuing of the decision, not at the time of the administrative offence. According to the Charged Company's financial statements for the year 2022³⁴ (the financial statements for the whole year 2023 had not been published by the date of this Decision), the Charged Company's turnover amounted to [REDACTED], which is almost CZK 1 billion higher. Pursuant to Section 152(6)(a) of Act No. 500/2004 Coll., the decision on the administrative appeal may be amended if the administrative appeal is fully upheld and if no harm can be caused to any of the participants. For that reason, in accordance with the principle of the prohibition of *reformatio in peius*, the Appellate Authority did not base its decision on the Charged Company's turnover for the year 2022 and the fine imposed by the first-instance administrative authority cannot be increased.

[182] For the sake of completeness, the Appellate Authority also addresses the possibility to raise an objection against a member of the Administrative Appeal Commission on the grounds of conflict of interest. The Administrative Appeal Commission is only an advisory body which does not decide on the merits of the case and thus cannot be said to be in a conflict of interest in the strict sense. The Accused was repeatedly informed, following its requests for information on the composition of the Administrative Appeal Commission, that a list of all duly appointed members of the Administrative Appeal Commission is published on the website of the Office (<https://uouu.gov.cz/urad/povinne-zverejnovane-informace/rozkladova-komise>) and in the annex to document ref. UOUU-01025/20-118 of 4 January 2024, the list of the

³⁴ Available online at: [REDACTED]

members of the Administrative Appeal Commission was sent to it. In order to preventively protect the Administrative Appeal Commission members from any attempt by the accused to influence their opinion, the Office does not disclose to the accused whether the case will be assigned to a plenary panel or to a specific panel, or to a panel augmented by additional members of the Administrative Appeal Commission from other panels, for consideration by the President of the Office. The Charged Company has repeatedly been informed of the composition of the Administrative Appeal Commission. If it considered that any of the members of the Administrative Appeal Commission was in a conflict of interest, it could have raised an objection without being informed of which specific members of the Administrative Appeal Commission would take part in the hearing. However, the Accused did not object to any member of the Administrative Appeal Commission.

III. Conclusion

[183] In view of the above, the Accused requested that the President of the Office annul the Disputed Decision and terminate the proceedings. However, if the President of the Office finds that the Charged Company committed the administrative offence, he should, according to the Charged Company, impose a penalty in the form of a warning or significantly reduce the fine imposed, since the current level of the fine is, according to the Charged Company, unlawful.

[184] In this regard, the Appellate Authority concludes that the reasons for not upholding the Charged Company's request are set out in detail in the foregoing parts of the reasoning. The guilty verdict is based primarily on circumstantial evidence, which, according to the Appellate Authority (in accordance with case-law, e.g. the Constitutional Court's Resolution of 19 December 2016, Case I. ÚS 1875/16), forms a logical, unbroken chain of complementary evidence which, taken as a whole, reliably proves all the circumstances of the offence. Failure to respect privacy and the right to protection of personal data constitutes a violation of the fundamental rights of the European Union guaranteed by the Charter of Fundamental Rights of the European Union which the Office is called upon to defend. For all the reasons set out above, the Appellate Authority has decided as stated in the verdict of this Decision.

Instruction: In accordance with Section 152(5) of Act No. 500/2004 Coll., the Code of Administrative Procedure, no administrative appeal may be filed against this decision.

Prague, 10 April 2024.

Mgr. Jiří Kaucký
President
(electronically signed)