10 As 190/2020 - 39 CZECH REPUBLIC JUDGMENT ON BEHALF OF THE REPUBLIC The Supreme Administrative Court decided in a panel composed of President Ondřej Mrákota and judges Petr Šebek and Zdenek Kühn in the legal case of the plaintiff: Nemocnice Tábor, a.s., Kpt. Jaroše 2000, Tábor, represented by attorney Mgr. Jiřím Jarušek, Radniční 7a, České Budějovice, against the defendant: Office for the Protection of Personal Data, Plk. Sochora 27, Prague 7, against the decision of the Chairperson of the Office for the Protection of Personal Data of 13 December 2018, file no. UOOU-08001/18-14, in proceedings on the cassation appeal of the plaintiff against the judgment of the Municipal Court in Prague dated 20 May 2020, no. 14 A 26/2019 - 37, as follows: I. The appeal is dismissed. II. None of the participants is entitled to compensation for the costs of the proceedings. Reasoning: I. Definition of the case [1] Defendant by decision of 12 October 2018, no. UOOU-08001/18-8, found the plaintiff guilty of committing an offense under § 45 paragraph 1 letter h) Act No. 101/2000 Coll., on the protection of personal data and the amendment of certain regulations ("Act on the Protection of Personal Data"), because as a personal data administrator, he did not take measures to ensure the security of personal data processing in connection with the management of electronic health documentation; specifically, the plaintiff was criticized for the fact that from an unspecified period until at least 11/01/2018: a) the audit records (logs) in the hospital information system did not make it possible to determine and verify the reason for which the electronic health documentation was consulted, b) the plaintiff did not carry out regular checks approaches to electronic health documentation. In doing so, according to the defendant, the plaintiff violated the obligation set forth in Section 13, paragraph 1 of the Personal Data Protection Act. He was fined CZK 80,000 for this. [2] Against this, the plaintiff filed a complaint with the president of the defendant, who confirmed the conclusion about the offense committed, but found the imposed fine to be unreasonable and reduced it to CZK 40,000. [3] The plaintiff's claim against the decision of the defendant's chairman was rejected by the Municipal Court in Prague. He came to the conclusion that if the plaintiff made records of who and when personal data was recorded and processed, but did not insist that the reason for access to electronic health documentation and processing of personal data be recorded, he acted in violation of by law. The municipal court did not find any wrongdoing even in the fact that the Act on the Protection of Personal Data was used and not Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data (the "Regulation"). II. Cassation proceedings [4] The plaintiff (complainant) challenged the judgment of the municipal court with a cassation complaint. He believes that the judgment is unreviewable because the municipal court did not deal with his reference

to the commentary on the Personal Data Protection Act. He further objected that the municipal court incorrectly interpreted § 13 paragraph 4 letter c) of the Act on the Protection of Personal Data and illegally assessed the question of which legal regulation should have been applied. According to the complainant, the Personal Data Protection Act should not have been applied, but the regulation, as it does not contain the obligation enshrined in § 13 paragraph 4 letter c) of the Personal Data Protection Act. Such an obligation cannot even be derived from Article 32 of the regulation, as the municipal court incorrectly does. The complainant further objected that the municipal court did not take into account later legislation (Act No. 110/2019 Coll., on the processing of personal data), which is more favorable to the complainant, when assessing the sanction. The Act on the Processing of Personal Data does not allow imposing a sanction for an administrative penalty on a public entity. The complainant considers that he is a public entity, as he maintains medical documentation (according to Act No. 372/2011 Coll., on health services and conditions of their provision), he is a public contracting authority (according to Act No. 134/2016 Coll., on procurement public contracts), a public institution within the meaning of Act No. 106/1999 Coll., on free access to information) and its activity is mainly financed from public health insurance funds. Although the complainant is a person under private law, it was established by the South Bohemian Region for the purpose of fulfilling the public interest. [5] The complainant therefore suggested that the NSS cancel the contested judgment and return the case to the municipal court for further proceedings. [6] The defendant disagrees with the cassation complaint and proposes to dismiss it. He considers the judgment of the municipal court and his decision to be in accordance with the law. He states that at the time of his decision, the Act on the Processing of Personal Data was not yet effective, however, he believes that it is not a norm more favorable to the complainant, as the complainant is not a public entity. III. Assessment of the matter by the Supreme Administrative Court [7] The cassation complaint is unfounded. III. 1. Non-reviewability of the municipal court judgment [8] First, the NSS dealt with the contested non-reviewability of the municipal court judgment. [9] The non-reviewability of a decision due to a lack of reasons must be interpreted in its true sense, i.e. as the impossibility of reviewing a certain decision due to the impossibility of ascertaining the very content or the reasons for which it was issued (cf. the resolution of the extended Senate of the NSS dated 19 February 2008, No. 7 Afs 212/2006 - 76). It is not admissible to arbitrarily expand the institute of non-reviewability and apply it also to cases where the court deals properly with the substance of the objection of a party to the proceedings and explains why it does not consider the argumentation of the party to be correct, even if it does not explicitly respond to all conceivable aspects of the objection raised in the justification of the decision and commits 10 As 190/ 2020 - 40 continuation

with partial lack of justification. The annulment of a decision due to unreviewability is reserved for the most serious defects in the decision, when the decision cannot really be reviewed on its merits due to the absence of reasons or lack of understanding. The unreviewability of a decision due to a lack of reasons is therefore particularly the case if the administrative body or court fails to respond completely (and implicitly) to the participant's objection (cf. NSS judgments of 17 January 2013, No. 1 Afs 92/2012 - 45 , or from 29 June 2017, No. 2 As 337/2016 - 64). The fact that administrative authorities and courts are not obliged to deal with every partial objection cannot be overlooked, if they oppose the claim of a party to the proceedings with a legal opinion against which the objections as a whole do not stand up. Such a procedure was found to be constitutionally compliant by the Constitutional Court in its judgment of 12 February 2009, no. stamp III. ÚS 989/08, according to which: "It is not a violation of the right to a fair trial, if the general courts do not build their own conclusions on the detailed opposition (and refutation) of individually raised objections, if they oppose them with their own comprehensive argumentation system, which logically and legally reasonably interprets , that supporting the correctness of their conclusions is sufficient in itself". [10] That was also the case in this case. The municipal court objected to the incorrect interpretation of § 13 paragraph 4 letter c) of the Personal Data Protection Act has been dealt with in detail. He clearly stated why he believes that it is necessary for the record to include information on the reason for the processing of personal data (paragraphs 50 et seq. of the judgment). Thus, the municipal court communicated its opinion on this question in a sufficiently reviewable manner. The mere fact that he did not expressly comment on the applicant's reference to the commentary literature does not make his judgment unreviewable. In the given case, moreover, the municipal court explicitly stated in the judgment that the measures that the complainant considered sufficient to fulfill the obligation (interview with the employee who consulted the database) were not considered sufficient. Non-reviewability is not a manifestation of the complainant's unfulfilled subjective idea of how detailed the judgment should be justified, but an objective obstacle that makes it impossible for the Court of Cassation to review the contested decision (cf. NSS judgments of 28/02/2017, No. 3 Azs 69/2016 - 24, and dated 27 September 2017, No. 4 As 146/2017 - 35). At the same time, the complainant's disagreement with the reasoning and conclusions of the contested judgment does not render it unreviewable (see, for example, the NSS judgments of 12 November 2013, No. 2 As 47/2013-30, or of 29 April 2010, No. 8 As 11 /2010 - 163). III. 2. Incorrect interpretation of § 13 paragraph 4 letter c) of the Act on the Protection of Personal Data [11] The complainant primarily objected that the municipal court had incorrectly interpreted § 13 paragraph 4 letter c) of the Personal Data Protection Act. [12] The complainant was found guilty by the defendant's decision of

violating Section 13, Paragraph 1 of the Personal Data Protection Act. He should have committed this by two acts: a) by the fact that his audit records (logs) in the hospital information system did not allow to determine and verify the reason for which the electronic health documentation was viewed, thereby also violating § 13 paragraph 4 letter c) the Personal Data Protection Act; and b) by the fact that the complainant did not carry out regular checks of access to electronic health records. [13] Pursuant to 13 paragraph 1 of the Act on the Protection of Personal Data, the administrator and the processor are obliged to take such measures to prevent unauthorized or accidental access to personal data, their alteration, destruction or loss, unauthorized transmission, or other unauthorized processing , as well as to other misuse of personal data. This obligation applies even after the end of personal data processing. [14] According to § 13 paragraph 4 letter c) of the Personal Data Protection Act, in the area of automated processing of personal data, the administrator or processor, as part of the measures according to paragraph 1, is also obliged to make electronic records that will allow to determine and verify when, by whom and for what reason personal data were recorded or otherwise processed. 10 As 190/2020 [15] The complainant believes that the cited provisions do not require that the reason for recording or other processing of personal data be included in the electronic record (log) itself, but that it is sufficient that this reason is ascertainable afterwards. However, we cannot agree with that. Although an explicit purely grammatical interpretation of § 13 paragraph 4 letter c) of the Act on the Protection of Personal Data to indicate the opinion of the complainant, the municipal court correctly proceeded from the meaning of the cited provision and evaluated the established obligation in the context of the entire § 13 of the Act on the Protection of Personal Data. He also referred to the NSS judgment of January 30, 2013, ref. 7 As 150/2012 - 35, in which NSS explicitly stated that the so-called logos according to § 13 paragraph 4 letter c) of the Act on the Protection of Personal Data are "records of who recorded or otherwise processed personal data, when and for what reason". Only such a record, which contains information not only about who and when processed personal data, but also the reason for this processing, is then eligible to fulfill the purpose of the Personal Data Protection Act, because only then can it be retroactively traceable and verifiable "who, when, how and why" processed personal data in the information system. Such a requirement also has a high preventive effect against the misuse of data from the information system, as everyone who works with it legitimately must be aware that it is possible to verify retrospectively who, when and how they worked with the information system, and whether this happened rightfully so. As stated by the NSS in the above-cited judgment no. 7 As 150/2012 - 35: "any person who unauthorizedly handles data contained in a system that processes it automatically must be aware that his actions can be traced back and revealed using

such a record". [16] The NSS therefore agrees with the municipal court that the reason for the recording or processing of personal data must already be contained in the electronic record (log) itself. The complainant's reference to the possibility of conducting a follow-up interview with the employee who accessed the database, and thereby finding out the reason for his access, cannot stand, as it does not respect the wording of § 13 paragraph 4 letter c) of the Personal Data Protection Act or the meaning of the personal data protection legislation. In such a case, it is not possible to carry out a proper ongoing or subsequent check, whether there was no unauthorized access to the database. [17] Even the complainant's reference to the commentary on the Personal Data Protection Act cannot change anything about what has just been stated. The conclusion of the municipal court does not contradict the comment. If the comment allows the fulfillment of the obligation enshrined in § 13 paragraph 4 letter c) of the Personal Data Protection Act also "in combination with appropriate organizational measures", the complainant does not mention any such appropriate organizational measures that would be eligible to fulfill the obligation. A subsequent interview with the person who viewed the database is not such a measure. It is certainly necessary to agree with the complainant that the legitimacy of the reason for the processing of personal data must be verified by the administrator himself, basically based on the data provided by the person who accessed the personal data. However, this person must state the reason for accessing the database immediately before accessing the personal data or immediately after. It cannot be agreed that he will give such a reason only at the follow-up inspection, which may be carried out many months after such an approach. First of all, he does not have to remember the specific reason at all (especially in situations where he looks into the information system often, as is certainly the case with the complainant's employees), moreover, the above-mentioned preventive effect is not fulfilled here. In the given case, there was no impermissibly expansive interpretation of Section 13, paragraph 4, letter c) of the Personal Data Protection Act. III. 3. Use of incorrect legislation A) [18] The complainant disagrees with how the municipal court assessed which legislation was more favorable to him. He primarily believes that the defendant should have applied the regulation and not the Personal Data Protection Act. 10 As 190/2020 - 41 continued [19] The municipal court found the complainant right, that when assessing which legislation is more favorable for the offender, one cannot limit oneself to just a comparison of penalty rates, but a specific case must be preliminarily assessed according to all provisions old and new legal regulations and then, taking into account all the provisions on the conditions of criminal (here misdemeanor) liability (including the reasons for its termination) and punishment (also the possibility of conditional sentencing, waiver of punishment, etc.), consider what is more favorable (judgment of the NSS of 5 June 2018, No. 4 As 96/2018 - 45).

Although the municipal court found the defendant's approach, which assessed only the penalty rate, to be flawed in this respect, it agreed with the conclusion on the application of the Personal Data Protection Act. [20] According to the municipal court, although the regulation contained in the regulation does not explicitly establish an obligation that would correspond to § 13 paragraph 4 letter c) of the Personal Data Protection Act, however, this obligation can be derived from Article 32 of the Regulation. This provision regulates the obligation of administrators and processors to secure personal data using appropriate technical and organizational measures, which, according to the municipal court, could also include the obligation to ensure proper protection of personal data so that access to them is not allowed without giving a reason. The municipal court also referred to the NSS judgment of 6/27/2019, no. 4 As 140/2019 - 27, which assessed the relationship between § 13 paragraph 1 of the Act on the Protection of Personal Data and Article 32 of the Regulation. [21] According to Article 32 of the regulation, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, as well as the variously probable and variously serious risks to the rights and freedoms of natural persons, the administrator and the processor shall implement appropriate technical and organizational measures, in order to ensure a level of security corresponding to the given risk, a demonstrative list of security methods is also provided and the provision that when assessing the appropriate level of security, the risks posed by the processing, in particular accidental or unlawful destruction, loss, alteration, unauthorized access to transmitted, stored or otherwise processed personal data, or unauthorized access to them. [22] In the present case, the applicant was found guilty of committing an offense under § 45 paragraph 1 letter h) of the Personal Data Protection Act, according to which an offense is committed by a person who, as administrator, does not adopt or implement measures to ensure the security of personal data processing (§ 13). According to the statement of the contested decision of the defendant, the complainant violated § 13, paragraph 1 of the Personal Data Protection Act (obligation to take such measures to prevent unauthorized or accidental access to personal data, their alteration, destruction or loss, unauthorized transfers, other unauthorized processing, as well as other misuse of personal data), by the fact that: a) audit records (logs) in the hospital information system did not make it possible to determine and verify the reason for which the electronic health documentation was accessed, and b) the complainant did not carry out regular checks of access to the electronic health documentation. [23] In the given case, the complainant was thus found guilty of violating Section 13, Paragraph 1 of the Personal Data Protection Act, which he committed in two separate actions. Although one of them (missing reasons for inspection in audit records) is also subordinate to § 13 paragraph 4 letter c) of the Act on the Protection of

Personal Data, the defendant, with regard to the second action (failure to carry out regular checks), found that the complainant violated the more general Section 13, Paragraph 1 of the Act on the Protection of Personal Data with both actions. It does not change the fact that in the justification of the decision the defendant also mentioned a violation of § 13 paragraph 4 letter c) of the Act on the Protection of Personal Data (which, after all, directly refers to Section 13, Paragraph 1), because the ruling, which is binding and enforceable, only found a violation of Section 13, Paragraph 1 of this Act. It is in relation to the last cited provision, the violation of which the complainant is accused of, that it is then necessary to determine whether the later legislation is more favorable to the complainant. 10 As 190/2020 [24] As the municipal court correctly stated in the contested judgment, the NSS has already considered this question and in the judgment no. 4 As 140/2019 - 27 came to the conclusion that Article 32 of the Regulation is not made more favorable in relation to Section 13, Paragraph 1 of the Act on the Protection of Personal Data (paragraphs 25 et seq. of the judgment). Therefore, it is not decisive that Article 32 of the Regulation does not contain such specific requirements as § 13 paragraph 4 letter c) of the Act on the Protection of Personal Data, but whether the regulation of obligations under Article 32 of the Regulation corresponds to the regulation set out in Section 13, Paragraph 1 of the Act on the Protection of Personal Data. According to the NSS, this is also the case. Both provisions regulate the obligation of the administrator and processor of personal data to ensure sufficient security of personal data against unauthorized disclosure or access by means of appropriate technical and organizational measures. Although it does so in different words, minor wording differences cannot be interpreted as meaning that the regulation imposes lower requirements on administrators or processors of personal data than the Personal Data Protection Act, and that it is thus a more favorable legal regulation, as the complainant believes. [25] The NSS therefore agrees with the municipal court that the defendant did not err in concluding that the regulation was not a more favorable legal arrangement for the complainant. B) [26] The complainant also objects that the municipal court should have applied the Personal Data Processing Act when assessing the sanction, as it did not allow imposing a sanction for an administrative penalty on a public entity (Section 62(5) of the Personal Data Processing Act in conjunction with Article 83 paragraph 7 of the regulation). [27] As stated by the extended Senate of the NSS in the resolution of 16 November 2016, no. 5 As 104/2013 - 46, if the regional court in the administrative judiciary decides on a lawsuit against the decision of an administrative body that decided on guilt and punishment for an administrative offense in a situation where the law that was used was changed after the administrative decision came into force or repealed, is obliged to take into account the principle expressed in the second sentence of Article 40, paragraph 6 of the Charter of

Fundamental Rights and Freedoms, according to which the criminality of the offense is assessed and the punishment is imposed according to the legislation that came into force only after the offense was committed, is if it is more favorable for the offender. [28] In the given case, the judgment of the municipal court was issued on 20/05/2020. The Act on the Protection of Personal Data was already repealed with effect from 24/04/2019 by the Act on the Processing of Personal Data, which came into force on the same day. Therefore, if the law on the processing of personal data would be more favorable to the complainant, the municipal court was obliged to proceed in accordance with this law when assessing the legality of the punishment. [29] Pursuant to Section 62, Paragraph 5 of the Act on the Processing of Personal Data, the defendant waives the imposition of an administrative penalty also in the case of administrators and processors referred to in Article 83, Paragraph 7 of the Regulation. [30] According to Article 83(7) of the Regulation, each Member State may lay down rules regarding whether and to what extent it is possible to impose administrative fines on public authorities and public entities established in that Member State. [31] In the present case, the complainant committed an offense under § 45 paragraph 1 letter h) of the Personal Data Protection Act, which consisted in the fact that he did not adopt or implement measures to ensure the security of personal data processing (§ 13). In the new legislation, this offense corresponds to an offense according to § 62 paragraph 1 letter a) of the Personal Data Processing Act in conjunction with Article 32 of the Regulation. [32] Pursuant to Section 62(5) of the Act on the Processing of Personal Data, in conjunction with Article 83(7) of the Regulation, the defendant waives the imposition of an administrative penalty if it is a controller and processor that is a public authority and a public entity. The NSS already reached the same conclusion in judgment 10 As 190/2020 - 42 continuation of 11 February 2020, no. 4 As 376/2019 - 31, also a comment on the Act on the Processing of Personal Data: "If a public authority or a public entity commits an offense, the Office will waive the imposition of an administrative penalty. (see Vlachová, B., Maisner, M. Personal Data Processing Act. Commentary. C.H. Beck, Prague, 2019, p. 131). [33] However, neither the Personal Data Processing Act nor the regulation specifies who is understood as a public entity in the sense of this provision. From the nature of the matter, it is clear that such an entity will usually be established by law and intended to perform tasks in the public interest (otherwise it would not be referred to as public) and at the same time will not have its own assets, but will be financed from public budgets (similarly, cf. already above) cited NSS judgment No. 4 As 376/2019 - 31). On the contrary, it will fundamentally be undecided whether it is a public institution within the meaning of the Act on Free Access to Information or a public contracting authority according to the Act on Public Procurement, nor whether it maintains medical documentation. [34] Without the NSS now having to specifically

define the term public entity in the sense of Section 62, paragraph 5 of the Personal Data Processing Act, it can be concluded unequivocally that the complainant is not such a public entity. [35] The applicant is a joint-stock company with its own property and management. It is possible to agree that it is "mainly financed by means of public health insurance". However, such financing cannot be considered as financing from public budgets. The applicant, as a hospital (joint-stock company), does not receive funds for its operation and functioning directly from public budgets, but receives them as consideration for specific actions and patients that it "reports" to health insurance companies. After all, any other entity providing medical care (private hospital or private doctor) is financed in the same way. Although the complainant provides health care, which is certainly in the public interest, it is a joint-stock company that is not financed from public budgets. Thus, it is not a public entity for which the defendant should decide to waive punishment pursuant to Section 62, Paragraph 5 of the Act on the Processing of Personal Data. Therefore, the Municipal Court did not make a mistake if it did not apply the Personal Data Processing Act, as it is not a legal arrangement more favorable to the complainant. IV. Conclusion and costs of proceedings [36] The complainant's objections were not justified, the NSS therefore rejected the cassation complaint. [37] The complainant was not successful in this court case, so he is not entitled to compensation for the costs of the cassation appeal. The defendant did not incur any costs beyond the scope of his normal official activities. Lesson: No appeals are admissible against this judgment. In Brno on February 25, 2022 Ondřej Mrákota Chairman of the Senate