No. 14 A 26/2019 – 37 The agreement with the original is confirmed by: M. V. THE CZECH REPUBLIC JUDGMENT ON BEHALF OF THE REPUBLIC The Municipal Court in Prague decided in a panel composed of President Štěpán Výborný and judges Karla Cháberová and Jan Kratochvíl in the case of the plaintiff: Nemocnice Tábor, a.s., IČO 26095203 registered office kpt. Jaroše 2000, Tábor represented by attorney Mgr. Jiřím Jarušek, registered office at Radniční 7a, České Budějovice against the defendant: Office for the Protection of Personal Data, registered office of Pplk. Sochora 27, Prague 7 regarding the lawsuit against the decision of the President of the Personal Data Protection Office of 13 December 2018, ID UOOU-08001/18-14, as follows: I. The lawsuit is dismissed. II. None of the participants is entitled to compensation for the costs of the proceedings. Reasoning: I. Definition of the matter and the course of the proceedings before the administrative body 1. With the filed lawsuit, the plaintiff seeks the annulment of the decision marked in the header, which amended and otherwise confirmed the decision of the Office for Personal Data Protection dated 12 October. 2018, No. UOOU-08001/18-8 (hereinafter referred to as "first-instance decision"), by which the plaintiff was found guilty of committing an offense pursuant to § 45 paragraph 1 letter h) of Act No. 101/2000 Coll., on the protection of personal data and the amendment of certain regulations, as amended at the time (hereinafter referred to as the "Act on the Protection of Personal Data"), as it did not adopt or implement measures to ensure the security of the processing of personal data, which , as the administrator of personal data according to § 4 letter j) of the Act on the Protection of Personal Data, committed in connection with the management of electronic health documentation from an unspecified period until at least January 11, 2018 by a) audit records (logs) in the hospital information system did not allow to determine and verify the reason for electronic health documentation viewed, b) did not perform regular checks of access to electronic health documentation. By this action, he violated the obligation 14 A 26/2019 Conformity with the original is confirmed by: M. V. 2 set out in § 13 paragraph 1 of the Act on the Protection of Personal Data, i.e. the obligation to take such measures to prevent unauthorized or accidental access to personal data, to their alteration , destruction or loss, unauthorized transmissions, their other unauthorized processing, as well as other misuse of personal data. 2. From the content of the administrative file, the court found the following facts that are essential to the matter. 3. The plaintiff is a provider of complex health services, and in accordance with Act No. 372/2011 Coll., on health services and the conditions for their provision, as amended (hereinafter referred to as the "Health Services Act"), the medical documentation of patients as in both in paper form and in electronic form. 4. On December 7, 2017, the defendant received a complaint from the Regional Office of the South Bohemian Region, according to which the plaintiff's information system had unauthorized

access to sensitive patient data by individual employees of the plaintiff (the complaint was initiated by one of the patients - hereinafter referred to as the "complainant"). 5. On 10 January 2018, the defendant notified the plaintiff of the start of the inspection, the subject of which was compliance with the duties of the personal data controller. 6. According to the control report dated 2 May 2018, No. UOOU-12026/17-14, the defendant concluded that the plaintiff had only taken some of the measures that he is obliged to take as a personal data administrator based on § 13 of the Personal Data Protection Act apply. Deficiencies were found mainly in the case of setting up access to electronic health records, when doctors had actual access to the electronic health records of all patients in the NIS application software, and the plaintiff did not take measures to ensure compliance with the requirements of the Personal Data Protection Act. The plaintiff did not specifically ensure that the specific reason for access to the electronic health documentation could always be ascertained from the audit records (logs) (only the time of access and the accessing person can be traced). In addition, there were no checks of the logos by the plaintiff, which would represent an effective means of checking the employees' compliance with the obligations arising from the adopted internal regulations. These errors were then also confirmed by checking the specific accesses to the electronic health documentation of the complainant, when it was not possible to determine whether it was a simple error by the employees ("over-clicking"). In addition, a nurse also accessed the electronic medical records of the complainant, thus committing a violation of work discipline and violation of § 14 of the Personal Data Protection Act. 7. By order of the defendant dated 5 September 2018, no. UOOU-08001/18-3, a fine of CZK 80,000 was imposed on the plaintiff for failing to comply with the obligations set out in § 13, paragraph 1 of the Personal Data Protection Act. The plaintiff filed an objection against the order. 8. By the decision indicated above, the defendant found the plaintiff guilty of committing the offense defined above. In the justification, he stated that the plaintiff is obliged to act in accordance with both the Act on Health Services and the Act on the Protection of Personal Data, which contains a regulation regarding the security of personal data kept in medical records, when providing health care. As an administrator, the plaintiff is thus obliged to comply with the obligations set out in § 13, paragraph 1 and paragraph 4 of the Personal Data Protection Act. From the logs taken by the plaintiff, however, it is not possible to determine with certainty the reason for which personal data was processed by which specific user. And according to the defendant, a setting in accordance with the law would in no way overburden users or jeopardize the provision of healthcare to patients. And on the part of the plaintiff, there was not even a thorough examination of access controls to electronic health documentation. The defendant did not find a reason for the application of § 21 paragraph 1 of Act No. 250/2016 Coll., on

liability for misdemeanors and their proceedings, as amended (hereinafter referred to as the "Act on liability for misdemeanors"), because the plaintiff did not use the maximum possible efforts to protect processed personal data. 14 A 26/2019 Conformity with the original is confirmed by: M. V. 3 9. To dissolve the plaintiff, the president of the defendant reduced the imposed fine to the amount of CZK 40,000 and otherwise confirmed the first-instance decision. In the justification, primarily with regard to the application of the legislation, she stated that since the offense was committed during the effective date of the Act on the Protection of Personal Data, the proceedings will be conducted according to the previous legislation. The reason is the fact that the previous legislation is more favorable for the plaintiff, as Regulation (EU) 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 and on the repeal of Directive 95 /46/EC (hereinafter referred to as the "general regulation on personal data protection") allows the imposition of a penalty of up to 10,000,000 (or 20,000,000) euros, or 2% (or 4%) of the worldwide annual turnover. 10. Regarding the alleged non-fulfilment of the formal sign of the offence, the chairwoman of the defendant stated that she does not impose any special requirements on the plaintiff beyond the scope of the Personal Data Protection Act, but is based on a requirement defined by the legislator. Therefore, one cannot simply refer to the general and broadly formulated reason for processing the patient's personal data, which is the provision of health care. In the case in question, the inspection found that the plaintiff actually allowed access to the electronic medical records even without giving any reason. And due to the fact that the plaintiff was unable to prove the reason for the processing of personal data on the basis of the logos in all cases, the conditions of § 13 para. 4 lit. c) of the Personal Data Protection Act. Although this obligation was stipulated in the plaintiff's internal regulations, it was not actually enforced. The argument that a healthcare worker is always legally bound by confidentiality was considered irrelevant by the chairman of the defendant. The risk arising from the processing of personal data does not only lie in the further unauthorized uncontrollable dissemination of personal data, but also in other forms of personal data processing, including unauthorized viewing. 11. The chairman of the defendant refused that compliance with legal obligations could result in a significant administrative burden on the medical staff, since in most cases the reason for processing personal data was already stated in the log and in the case of emergency admission rules can be set in advance so that when the user logs in the reason for working with medical documentation can be completely automatically "filled" into the hospital information system. 12. To the objection that the defendant in the challenged decision does not specifically express the fulfillment of the material side of the offense, the chairman of the defendant stated that the

harmfulness of the offense results from the very fulfillment of the factual essence of the offense and is caused by the threat to sensitive personal data processed by the plaintiff. 13. The chairman of the defendant proceeded to reduce the fine to the amount of CZK 40,000, taking into account the fact that the plaintiff already corrected the objectionable situation during the inspection, when he adjusted his information system so that the user was always obliged to select the reason for working with electronic medical documentation. And he also issued an order for an extraordinary control of the use of user rights and the expansion of the audit, the subject of which is the implementation of random checks and the creation of a system for conducting regular log checks. Furthermore, it took into account administrative practice when imposing fines for breach of obligations set out in § 13 paragraph 4 letter c) of the Personal Data Protection Act. II. Content of the action 14. The plaintiff objects that the obligations arising from § 13 paragraph 4 letter c) of the Act on the Protection of Personal Data must be understood to mean that electronic records must be made that allow the scope of information of interest to be determined and verified, but not that the electronic records themselves must contain this information of interest. The law does not preclude the determination and verification of the essential circumstances of personal data processing using electronic records in conjunction with other, associated information and data. According to the plaintiff, the reason for working with personal data may not be apparent from the logo itself. At the same time, the plaintiff was able to find out when and by whom the personal data was processed, and subsequently, through an interview with the healthcare worker in question, he was able to find out why he accessed the personal data in the hospital information system. With this procedure, the defendant's conclusion that the plaintiff leaves "the fulfillment of this obligation entirely to its 14 A 26/2019 Compliance with the original is confirmed by: M. V. 4 employees" does not hold up, because in the event of a question, the employee would have to clarify the reason for the access. The interpretation chosen by the defendant is disproportionately strict and places enormous demands on the personal data manager, which he is unable to meet objectively, as he is not the developer of the information system in question. At the same time, it is not possible to find out from the grounds of the contested decision, nor from the first-instance decision, what, according to the defendant, is the special benefit of the request he made to the data controller in the event of their automated processing. And the defendant also failed to deal with the plaintiff's points to the opposite conclusions of the commentary literature. 15. The plaintiff rejects the claim that he did not carry out regular checks on access to electronic health records. However, these checks should be focused on compliance with organizational measures (compliance with obligations set by internal regulations), not on checking measures of a technical nature, while logging is a technical measure. And no control

measures can ensure that there will never be a violation of the controlled rules under any circumstances. At the same time, the plaintiff carried out checks both as part of regular employee training and also during audits, when a number of organizational measures in the area of personal data protection were randomly checked. And even with this argument, the defendant did not deal sufficiently. It was the defendant's duty to explain from which legal standard the control obligation derives, what is its meaning and significance for the protection of patients' personal data, and why it considers the control measures introduced and used by the plaintiff to be insufficient. According to the plaintiff, the defendant completely ignores the fact that the main purpose for which the plaintiff was established is the provision of health care and meeting the needs of people in the area of public health protection. 16. Taking into account the above, the plaintiff is of the opinion that the conditions according to § 21, paragraph 1 of the Act on liability for misdemeanors have been met, as it was proven in the proceedings that the plaintiff carries out an inspection in the area of dealing with personal data contained in the medical documentation. 17. The plaintiff further states that the reason for the processing of patients' personal data, which is done by viewing the hospital information system, should always be the provision of health services, and in the vast majority of cases this is the case. Otherwise, it will be a deviation from the legally approved reason for processing (see § 65 of the Act on Health Services) and it will be an excess in the actions of the relevant healthcare worker, who will be affected in an individual case. And the protection of the individual rights of the data subject is thus not only possible, but also realistic. The defendant's legal conclusion is incorrect because it has no basis in the Health Services Act and places unreasonable demands on the plaintiff as a provider of health services in connection with the automated processing of patients' personal data. In addition, the plaintiff objected in the resolution that the employer should not be punished for the excess, which has implemented and observes all reasonably required measures to prevent such undesirable behavior on the part of its employees, but the chairwoman of the defendant did not resolve this objection in any way. 18. The plaintiff further objects that the statement of the first-instance decision does not contain all the requirements prescribed by law, as it completely lacks information about the place where the offense was supposed to be committed. 19. The plaintiff further objects to the contested decision that the defendant assessed the plaintiff's actions according to the previous legislation, which is stricter for him. The legal regulation of the processing of personal data and its protection given by the General Regulation on the Protection of Personal Data does not establish an obligation for the administrator of personal data that would correspond to the provisions of § 13 paragraph 4 letter c) of the Personal Data Protection Act. And because the rule on the application priority of European law, which is also a newer regulation, will be

applied, the plaintiff is of the opinion that the earlier legislation is less favorable for him. Therefore, since the defendant is punishing the plaintiff for a violation of a legal obligation, which the current legislation does not recognize, the defendant has violated the legal principle of nullum crimen sine lege certa. 20. The plaintiff finally objects to the non-reviewability of the decision. The defendant did not explain how more detailed logging would be beneficial in relation to the security of personal data and would not be just a formal fulfillment of the demands brought by the defendant beyond the scope of the law. In the same way, he did not adequately deal with the plaintiff's reference to the duty of confidentiality of healthcare workers. 14 A 26/2019 Conformity with the original is confirmed by: M. V. 5 And the plaintiff also questions the defendant's statement regarding the setting of the system in case of emergency income (in addition, according to the plaintiff, this interpretation illustrates how the defendant formally approaches the interpretation of the legal norm in question) The question of social danger also remained unclear of the alleged conduct. III. Statement of the defendant 21. In his statement, the defendant rejected the plaintiff's objections and referred to the justification of the contested decision. According to the defendant, all the arguments presented by the plaintiff, although perhaps in a more concise form and in other words, were already settled during the previous proceedings. 22. The defendant states that the obligation enshrined in § 13 paragraph 4 letter c) of the Act on the Protection of Personal Data must be evaluated in the entire context of § 13 of the cited Act as one of the measures enabling the detection of unauthorized access to information, and subsequently to enable further unauthorized processing of personal data to be prevented without undue delay and also to be able to take steps to the appropriate punishment of a person who has unauthorized access to personal data. At the same time, there is an obvious difference between a situation where the administrator (plaintiff) will verify the already declared reason for access to personal data and a situation where the administrator (plaintiff) will first, after a certain period of time, be asked to state the reason for access to personal data and only then this reason will be investigated. 23. The defendant states that the offense was defined in relation to the keeping of electronic health records by the plaintiff. In this way, the deed was clearly individualized, including the place where the offense was committed, in such a way that it could not be confused with another act. 24. The defendant agrees with the plaintiff that the general regulation on the protection of personal data, the obligation corresponding to § 13 paragraph 4 letter c) of the Act on the Protection of Personal Data does not explicitly enshrine, however, from Article 32, paragraph 1 of this regulation, the obligation to make electronic records can be deduced, which will make it possible to determine and verify when, by whom and for what reason personal data were recorded or otherwise processed. Logging then remains one of the basic requirements for

the security of personal data processing, even according to the General Regulation on the Protection of Personal Data. 25. The defendant notes that properly practiced logging undoubtedly contributes to ensuring the fulfillment of the obligation of confidentiality. And it is also an important tool to eliminate other forms of unauthorized processing of personal data than their unauthorized dissemination. IV. Assessment of the claim by the Municipal Court in Prague 26. The court decided on the matter without ordering an oral hearing in accordance with § 51 paragraph 1 of Act No. 150/2002 Coll., Administrative Code of Court, as amended (hereinafter referred to as "s. ř. s. "), because the participants accepted such a procedure of the court. 27. Pursuant to Section 75 of the Civil Procedure Code, the court reviewed the decision challenged by the lawsuit, as well as the proceedings that preceded its issuance, to the extent of the points of illegality alleged by the lawsuit, by which it is bound, according to the factual and legal situation on the date of the decision contested by the lawsuit, and concluded that the claim was without merit. 28. Pursuant to 13 paragraph 1 of the Act on the Protection of Personal Data, the controller and the processor are obliged to take measures to prevent unauthorized or accidental access to personal data, their alteration, destruction or loss, unauthorized transmission, or other unauthorized processing. as well as other misuse of personal data. This obligation applies even after the end of personal data processing. 29. Pursuant 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 make it possible to determine and verify when, by whom and for what reason personal data were recorded or otherwise processed. 14 A 26/2019 Conformity with the original is confirmed by: M. V. 6 A) Non-reviewability of contested decisions 30. The court first dealt with the alleged non-reviewability of the contested decision, because in the case of non-reviewability of the decision, it would not be appropriate to assess its legality. 31. Cancellation of an administrative decision due to unreviewability is reserved for the most serious defects of administrative decisions, when due to the absence of reasons or lack of understanding, the administrative decision cannot be reviewed on its merits. Unreviewability due to lack of reasons must, however, be interpreted in its true sense, i.e. as the impossibility of reviewing a certain decision due to the impossibility of ascertaining its content or the reasons for which it was issued (cf. the resolution of the extended senate of the Supreme Administrative Court of 19 February 2008 , No. 7 Afs 212/2006-76). Unreasonably high requirements cannot therefore be placed on the justification of the decisions of administrative bodies. It is not admissible to expand the institute of non-reviewability and apply it also to cases where, for example, the administrative body properly deals with the substance of the objection of a participant in the proceedings and

explains why it does not consider the argumentation of the participant 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 a partial lack of justification (see, for example, the judgment of the Supreme Administrative Court of 17 January 2013, no. 1 Afs 92/2012-45, point 28). Therefore, the decision is not unreviewable due to a partial error in the reasoning, when it must also be taken into account that the administrative proceedings form a single unit and nothing prevents the second-level authority from simply identifying itself and referring to the reasoning of the first-instance decision. 32. The city court did not find the contested decision unreviewable in the above sense. The chairwoman of the defendant in the contested case and the defendant in the first-instance decision accordingly outlined their reasoning and explained why they came to the stated conclusions about the plaintiff's responsibility for the offense committed. At the same time, they carefully addressed the essence of the offense in question, as well as the actions for which the plaintiff was affected. In this way, they primarily evaluated whether the plaintiff ensured that in all cases it was possible to determine the reason for access to the data kept in the electronic health records, and whether he carried out sufficient control of the reasons for access. At the same time, their conclusions are unequivocal and do not raise any doubts about the considerations that guided the administrative bodies in their decision-making. 33. If the plaintiff points to the fact that some of his objections were not explicitly and in detail dealt with, the court must emphasize that this circumstance in itself does not establish the unreviewability of the challenged decisions. As already stated, the court should proceed with the annulment of the decision on the grounds of non-reviewability only in exceptional cases when the legal or factual reasons for the decision cannot be ascertained, but not when all objections raised during the administrative proceedings have not been thoroughly settled. And in the case under consideration, moreover, it is possible to infer from the reasoning of the contested decision the reasons for which the administrative authorities did not accept the plaintiff's individual objections. 34. In general, the court must emphasize that it follows from both contested decisions what the administrative authorities saw as a violation of the obligations set out in the Personal Data Protection Act, including why it is necessary to insist that the logos (individual accesses) can be identified the reason for their implementation. In this way, they repeatedly pointed out the necessity of setting up the database so that it is not possible to view the electronic health documentation without any reason and without proper access control, as this is the only way to adequately protect sensitive patient data. Therefore, the court cannot agree with the plaintiff's claim that the administrative authorities did not explain how more detailed logging would be beneficial in relation to the security of personal data, as the stated reason can be clearly identified from the contested decisions. 35. If the plaintiff points to the

absence of settlement of the objection of non-fulfilment of the parameter of social harmfulness of the offense, then the chairperson of the defendant clearly pointed to the actual fulfillment of the offense itself and, with it, the threat to sensitive personal data. Despite the brevity of this justification, the defendant's conclusion about the fulfillment of the material aspect of the offense follows from it, including the reasons that led him to the stated conclusion. 14 A 26/2019 Conformity with the original is confirmed by: M. V. 7 36. Regarding the alleged absence of argumentation regarding the duty of medical professionals to maintain confidentiality, the court states that the chairman of the defendant sufficiently addressed this objection on p. 4 of the contested justification, where she outlined the reasons for which considered this objection to be irrelevant (see the non-existence of a relationship between the obligation to maintain confidentiality and the risk of unauthorized viewing of personal data, including erroneously leaving the fulfillment of this obligation only to the plaintiff's employees). 37. With regard to the arguments regarding the setting of rules for emergency admission, the court states that this issue was in no way essential for issuing the contested decision and finding the plaintiff guilty of committing a misdemeanor. The defendant and the chairwoman of the defendant only reacted to the claim of the plaintiff in this way and refuted that the operation of emergency income would preclude the plaintiff from being able to fulfill the obligations given by law. Therefore, the court also considers the settlement of this argument to be sufficient. 38. If the plaintiff objects that the defendant did not explain from which legal standard the control obligation derives, what is its meaning and significance for the protection of patients' personal data, then, according to the court, this follows from the overall context of the challenged decisions and the emphasis placed by the defendant on the necessity of records reasons for access to electronic health documentation. In this way, it can be seen from the contested decisions that not only the erroneous provision of access to electronic medical records without stating the reasons for access, but also the absence of appropriate controls caused non-compliance with the obligations set out in Section 13, Paragraph 1 of the Personal Data Protection Act. 39. The court therefore found that the defendant proceeded in accordance with § 68, paragraph 3 of the Administrative Code, and the challenged decision does not suffer from internal contradictions, incomprehensibility or insufficient justification. B) Applicable legislation 40. The plaintiff further objects that the defendant incorrectly assessed which legislation is more favorable to him. In this way, the plaintiff considers the regulation contained in the General Regulation on the Protection of Personal Data to be more favorable, while the defendant, on the other hand, considers the regulation contained in the Personal Data Protection Act to be more favorable. 41. Regarding this objection, the court first of all notes that the principle of applying later, more favorable legislation is enshrined in Article 40,

paragraph 6 of the Charter of Fundamental Rights and Freedoms and is subsequently specified in Section 112, paragraph 3 of the Act on Liability for Offenses, so that on determining the type and amount of the sanction for previous offenses and other administrative offenses, from the date of entry into force of this Act, the provisions on the determination of the type and amount of the administrative penalty shall be applied, if it is more advantageous for the offender. When deciding which assessment is more favorable for the offender, one cannot limit oneself to comparing criminal rates, but a specific case must be preliminarily assessed according to all the provisions of the old and new law, and then taking into account all the provisions on the conditions of criminal (here misdemeanor) liability (also regarding the reasons for its termination) and punishment (also regarding the possibility of a suspended sentence, waiver of punishment, etc.) to consider what is more favorable (see judgment of the Supreme Administrative Court of 5 June 2018, no. 4 As 96/2018 – 45). 42. It follows from the above that it was the duty of the defendant to pay more attention to the relationship between the two legal regulations and not to focus only narrowly on the amount of sanctions that individual legal standards allow to impose on the plaintiff for the alleged conduct. However, the court considers it crucial for the assessment of the plaintiff's objection that it did not find the defendant's conclusions erroneous. 43. The court, in agreement with the defendant, must agree with the plaintiff that the regulation contained in the general regulation on the protection of personal data does not explicitly establish an obligation that would correspond to the provisions of § 13 paragraph 4 letter c) of the Personal Data Protection Act. However, the stated obligation can be derived from Article 32 of the cited regulation. This provision regulates the obligation of administrators and processors to secure personal data using appropriate technical and organizational measures, demonstratively giving several examples of such measures and a list of which aspects are particularly necessary to evaluate when assessing the level of risks. And among these measures it would undoubtedly be possible to also include the obligation 14 A 26/2019 Conformity with the original is confirmed by: M. V. 8 to ensure proper protection of personal data in such a way that it is not possible to access them without giving a reason, or that the reason for access can be ascertained without further and verify. After all, this obligation can already be deduced from the very purpose of the given regulation and the principles on which it is based. Therefore, the plaintiff's reference to the content of the obligations contained in the general regulation on the protection of personal data does not hold up, since it is also possible to infer obligations that the plaintiff did not comply with according to the contested decisions. And the same conclusion was reached by the Supreme Administrative Court (see judgment of 27/06/2019, no. 4 As 140/2019 – 27), when assessing the relationship between § 13, paragraph 1 of the Personal Data Protection Act and Article 32 of the

general regulation on the protection of personal data. 44. Therefore, the defendant was not wrong if he applied the law on the protection of personal data to the matter, because this law was more favorable to the plaintiff, because it penalized the same conduct, but allowed a less severe sanction to be imposed when the offense was committed. 45. C) Shortcomings of the decision statement 46. The plaintiff further objects that the first-instance decision statement does not contain all the essentials, above all, it lacks the definition of the place where the offense was committed. 47. The necessary elements of a decision on an administrative delict (or misdemeanor) were defined by the extended panel of the Supreme Administrative Court in the resolution of 15 January 2008, reference no. 2 As 34/2006 – 73. In this decision, he emphasized that the purpose of the legal requirements for defining the subject of the proceedings in the statement of the decision on the offense is to specify the offense in such a way that the sanctioned conduct is not interchangeable with other conduct. In a decision of a criminal nature, which is also a decision on a misdemeanor, it is necessary to establish for sure what specific conduct the subject is affected for. This can only be guaranteed by concretizing the data containing the description of the deed by indicating the place, time and manner of its commission, or by specifying other facts that are necessary so that it cannot be confused with another. Such a level of detail is necessary to avoid double punishment for the same act, to avoid obstruction of the matter decided, and also to ensure a proper right of defense in the event of an appeal being filed. 48. According to the court, the sentence of the first-instance decision completely fulfills the stated conditions, as it clearly defines the conduct for which the plaintiff was criminally affected. If the plaintiff objects that the place where the offense was committed is not stated in the statement, he can be found guilty, but at the same time the court emphasizes that the place where the offense was committed can be inferred from the statement as the place where the plaintiff kept the electronic health records. At the same time, the requirements placed on the statement of an administrative decision on an offense cannot be considered as self-serving, so a possible formal error consisting in the failure to specify one parameter of the offense does not establish the illegality of the decision, if otherwise the statement of the decision is sufficiently definite and understandable so that it cannot be confused with another. And this happened in the above case, because despite the failure to state the place where the offense was committed, the alleged conduct cannot be confused with another, because the defendant defined it with sufficient certainty by the time and manner of commission, while the place of commission of the offense was not so essential that its failure to state caused a substantial defect in the statement. Especially in a situation where this place of the crime could be deduced from the wording of the statement without much difficulty. 49. Therefore, the court did not find the objection justified. D) The substance of the

plaintiff's unlawful conduct 50. The plaintiff was found guilty of committing an offense pursuant to Section 13, paragraph 1 of the Personal Data Protection Act by the challenged decisions. The aim of this provision was, among other things, to prevent unauthorized or accidental access to personal data or their other unauthorized processing. The Personal Data Protection Act did not define the individual means of ensuring the security of personal data in Section 13, paragraph 1. These were defined in more detail in § 13, paragraphs 3 and 4, respectively § 13, paragraph 3 of the Act listed specific risks and paragraph 4 established the obligations that the administrator of personal data was obliged to accept in order to exclude the realization of the mentioned risks. 14 A 26/2019 Conformity with the original is confirmed by: M. V. 9 51. According to the defendant, the plaintiff violated the obligation stipulated in § 13 paragraph 4 letter c) of the Act on the Protection of Personal Data, according to which it was the duty of every controller and processor of personal data to obtain electronic records during automated processing, which will allow to determine and verify when, by whom and for what reason personal data were recorded or otherwise processed (changed, deleted, but even just displayed). The aim of this measure was to more or less determine with certainty who and when did what operation with personal data, but also for what reason. 52. The reason for the acquisition of these records (including the reasons for their implementation) was the fact that the records serve the administrator or personal data processor himself to check the fulfillment of the obligations of his employees and other persons cooperating in the processing of personal data – logs can be used for random (preventive) control, or for subsequent control in the event that the administrator or processor suspects misuse of personal data by a specific person. As the Supreme Administrative Court also stated in the judgment of 30 January 2013, No. 7 As 150/2012-35, "in general, the processing of personal data in this way, i.e. using computer technology, results in higher risks of leakage of personal data, their unauthorized changes, destruction, loss, processing or other misuse. This is because computer technology enables fast and detailed processing of a large amount of data (especially their structured arrangement and analysis according to specified combinations of criteria), as well as their easy and subsequently difficult-to-detect copying without special measures, including unauthorized copying. In essence, it is precisely information systems operated with the help of computer technology, which by their nature are a typical potential object of misuse of personal data on a mass scale, in a way that is highly socially dangerous in terms of commercial and other possibilities of using the data obtained in this way. This higher risk then justifies the establishment of a specific obligation, the fulfillment of which does not entail any disproportionate costs. If automated processing of personal data is used, it cannot be a problem in the current state of the art to implement another secondary function into the personal data processing system used

- recording certain operations so that their nature and extent can be traced back. Such a measure 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 it was done so legitimately . 53. Therefore, if the plaintiff took records of who and when personal data was recorded and processed, but no longer insisted on recording the reason for access to electronic health documentation and personal data processing, he acted in violation of the law. At the same time, as follows from the above, the stated obligation cannot be trivialized, since on the one hand it contributes to the prevention of unjustified access to personal data (in the case of medical records even to sensitive personal data) and on the other hand it gives the administrator of personal data the opportunity to properly and without further control , whether there is already unauthorized reading or other handling of personal data (see § 13, paragraph 3 of the Personal Data Protection Act). 54. Provisions of § 13 paragraph 4 letter c) of the Personal Data Protection Act unequivocally stipulated that the reason for the recording or processing of personal data must already be included in the electronic record (log) itself. The plaintiff's reference to the possibility of subsequently conducting an interview with the employee who accessed the database and thus finding out the reason for his access does not hold up, as it clearly does not respect the wording of the cited provision of the law. And in the same way, it does not respect the goals of the adopted legislation, which, as explained above, is primarily the possibility of easy ongoing and subsequent control, whether there is no unauthorized access to the database. And in the case in question, it was also proven that the plaintiff did not carry out this interim or follow-up inspection sufficiently, or rather that such inspection did not bring conclusive conclusions, as the case of the complainant showed. The court considers the plaintiff's argumentation to be trivializing the alleged breach of duty, with which, however, it cannot agree. The subject of the proceedings before the administrative authorities was the fault of the plaintiff in taking measures to prevent unauthorized or accidental access to personal data or any other way of their misuse. And this misconduct is extremely serious also with regard to the scope and subject of personal data that the plaintiff processes (primarily data on the health status of patients), without the personal data subjects being able to influence it in any way. 14 A 26/2019 Conformity with the original is confirmed by: M. V. 10 55. At the same time, the court cannot convince the plaintiff that § 13 para. 4, similar to § 13 para. 1 of the cited law, includes only a demonstrative list of measures left to the choice of the controller or processor. Both of these legal norms share a different regime. While in general the law required the achievement of a certain goal regardless of the specific measures chosen (paragraph 1), in special situations (automated processing of personal data) it "also" insisted on the

implementation of specific measures (paragraph 4). The two rules were therefore relatively independent. From the point of view of paragraph 4 itself, it was not decisive whether and to what extent the goal according to paragraph 1 is being fulfilled at the same time. However, since the measures according to paragraph 4 had to be adopted "also", their adoption did not affect the obligation according to paragraph 1. The same applies to the opposite link between the two paragraphs. The fulfillment of the obligation according to paragraph 1 did not in any way affect the obligations according to paragraph 4, as they had to be fulfilled "also". Therefore, however paragraph 4 contained measures which by their nature were also measures in the regime of paragraph 1 (but not necessarily sufficient), their adoption was clearly not left to the will of the administrator or processor, in contrast to the general rule in paragraph 1. 56. After all, this conclusion also follows from the explanatory report to the law by which the obligations in question were included in the law. The explanatory memorandum emphasized that paragraphs 3 and 4 represent "an expression of the specific obligations of administrators and processors" and "determine the exact content of the measures in the framework of fulfilling the obligations of administrators (and processors) for the security of personal data." The reasoned report therefore confirmed the fact that the obligation according to § 13 paragraph 4 letter c) of the cited Act had to be fulfilled regardless of what other measures according to paragraph 1 were taken by the controller or processor. By establishing a specific obligation with a precise content, it was clearly not intended to leave it to the will of the administrator or processor whether or not to fulfill the given obligation. 57. According to the court, the above interpretation cannot be considered unreasonably strict, as it follows the purpose of personal data protection contained in the Personal Data Protection Act. It is impossible to disregard the fact that, with regard to the content of § 13, paragraph 1 of the Act on the Protection of Personal Data, a breach of duty will occur as soon as a situation arises where the processed personal data is in a certain way endangered due to the absence of appropriate measures or the inconsistent implementation of these measures in practice. Therefore, the occurrence of a certain risk is sufficient to fulfill the relevant factual basis of the administrative offense. This risk could be identified in the case of electronic health records maintained by the plaintiff, as it was demonstrated that users of the software did not always need to enter a reason for accessing sensitive patient health data. And after all, the ongoing proceedings were initiated on the basis of a complaint from one of the patients, which is why we cannot talk only about possible interference with protected data. 58. The fact that he is not the developer of the information system in question cannot change the plaintiff's responsibility, as it was his duty to ensure that the system used by him met the legal requirements. As it emerged from the performed inspection, the system operating until now allowed entering the reason for access, but the user of

the system was not always and under all circumstances required to state this reason before accessing sensitive data. According to the court, modifying the system to make this option mandatory cannot be considered an unfulfillable technical requirement. And the fact that, after the inspection, the plaintiff subsequently took measures to ensure that the system always records not only who and when recorded or otherwise processed personal data, but also the reason for access, is evidence of the aforementioned. 59. The plaintiff cannot absolve himself from the obligations defined above even by claiming that any excess in the actions of the relevant healthcare worker can be found in an individual case. It was the task of the plaintiff to ensure that the operation of the database in basic parameters met the legal requirements (including proper protection of the collected personal data) and if he did not do so, he cannot waive his responsibility by pointing to the possibility of individual punishment of persons who would violate the legal obligations. In addition, the individual penalty stated by the plaintiff would not appear to be sufficient from the point of view of the general requirement for the maximum level of personal data protection, since not individual users, but the system administrator must first and foremost ensure that the system operates in accordance with the legal principles of personal data protection. In addition, only the plaintiff acted 14 A 26/2019 The agreement with the original is confirmed by: M. V. 11 in the position of personal data manager, which is why he was subject to the obligations given in § 13 of the Personal Data Protection Act. 60. The plaintiff further rejects the defendant's conclusion that he did not perform regular checks of access to electronic health records. However, the court must agree with the defendant that the checks carried out by him were not sufficient. As it emerged from the inspection, the plaintiff only adopted internal regulations governing the principles and authorizations of employees when working with electronic health documentation and carried out internal controls focused on the physical storage and security of medical documentation and the logging in and logging out of employees from the PC. However, the plaintiff neglected to check the login to the system in terms of the authorization of accesses, although not only the security of the software itself, but also the control of the authorization of access can lead to the security of personal data protection. The court agrees with the plaintiff that no control measures can ensure that there will never be a violation of the controlled rules under any circumstances. However, the control of user access could ensure that the risk of unauthorized or accidental access to personal data by software users is minimized, as they would understand that, in the event of a control, the legitimacy and reasonableness of their access to the health records of individual patients would be checked. In addition, it cannot be overlooked that such a control could hardly be carried out in the case under consideration, since the plaintiff did not comprehensively record the reasons for accessing the software, so he could only assess with great

difficulty in retrospect whether the medical professional entered the medical records of a certain patient for a reason or not (see also the case complainants). And checking the authorization of user access to the database cannot be considered a check of measures of a technical nature, as it concerns the essence of the protection of collected personal data. Therefore, according to the court, the defendant's conclusion that the plaintiff did not properly conduct the inspection is valid. 61. The court does not consider the plaintiff's reference to Section 65 of the Act on the Provision of Health Services to be justified either. The cited provision governs viewing the medical documentation and obtaining its extracts or copies. The provisions of § 13 paragraph 4 letter c) of the Act on the Protection of Personal Data, however, aimed at the protection of personal data in electronic form, when it was required to be able to determine and verify who processed the data that is the subject of protection in any way, including the reason for their processing. The subject of protection here was the securing of only authorized and justified access to personal data, and therefore it was the duty of the data controller to ensure that it was always possible to determine who, when and for what reason viewed the medical documentation. This obligation is not degraded by the regulation of access to medical documentation contained in the Act on the provision of health services, as § 13 para. 4 lit. c) special legislation of the Personal Data Protection Act. 62. And the court does not consider the demands placed on the plaintiff by the defendant to be unreasonable. On the contrary, already in the contested decision, the defendant clearly explained that recording the reason for accessing the database is a simple step that takes a minimum of time for the user accessing the records. The court completely agrees with this assessment, because even according to the court, the time-consuming nature of such a step is absolutely minimal, especially compared to the relevance of the value that is protected by the evidence of the reasons for access to the electronic health documentation. For the sake of completeness, in this regard, the court refers to the conclusions expressed in the contested decisions, including the opinion on ensuring this obligation at the emergency department. 63. Requirements arising from § 13 paragraph 4 letter c) of the Personal Data Protection Act could not be ensured even by the duty of medical professionals to maintain confidentiality. The cited provision was not only aimed at preventing the dissemination of data recorded in the electronic database, but also at preventing unjustified access to them themselves. Therefore, the obligation of confidentiality does not pursue the same goal and object of protection and does not exempt the network administrator from the obligation to ensure protection against accidental or unauthorized access to electronic health records. 64. For all the above-mentioned reasons, the court did not accept the plaintiff's reference to § 21, paragraph 1 of the Act on Liability for Misdemeanors. According to the cited provision, the legal entity confirms compliance with

the original for offense 14 A 26/2019: M. V. 12 is not liable if it proves that it has made all the efforts that could be required to prevent the offence. Exercising all the efforts that could be required, however, does not mean any effort that the legal entity makes, but must be the maximum possible effort that the legal entity is objectively capable of making. As it was stated, already taking into account the fact that the plaintiff did not sufficiently adopt sufficient mechanisms designed to control access to the electronic health documentation, one cannot but come to the conclusion that he did not make the maximum effort to prevent the offense. The mere adoption of internal regulations, the observance of which, however, was not strictly controlled in its essence, cannot constitute grounds for release according to § 21, paragraph 1 of the Act on Liability for Misdemeanors. V. Conclusion 65. The plaintiff therefore failed with his objections; since no defects came to light in the proceedings on the claim, which must be taken into account as a matter of official duty, the municipal court dismissed the claim as unfounded. 66. The court decided on the reimbursement of the costs of the proceedings in accordance with § 60, paragraph 1 of the Civil Procedure Code. The plaintiff was unsuccessful in the case, and therefore has no right to the reimbursement of the costs of the proceedings; the defendant did not incur any costs in the proceedings on the claim beyond the scope of normal official activity. Instruction: A cassation complaint can be filed against this decision within two weeks from the date of its delivery. The cassation complaint is submitted in two (more) copies to the Supreme Administrative Court, with its seat at Moravské náměstí 6, Brno. The Supreme Administrative Court decides on cassation appeals. The time limit for filing a cassation complaint ends with the expiration of the day which, with its designation, coincides with the day that determined the beginning of the time limit (the day of delivery of the decision). If the last day of the deadline falls on a Saturday, Sunday or holiday, the last day of the deadline is the closest following business day. Missing the deadline for filing a cassation complaint cannot be excused. A cassation complaint can only be filed for the reasons listed in § 103, paragraph 1, s. s. s., and in addition to the general requirements of the filing, it must contain an indication of the decision against which it is directed, to what extent and for what reasons the complainant is challenging it, and an indication of when the decision was delivered to him. In cassation appeal proceedings, the complainant must be represented by a lawyer; this does not apply if the complainant, his employee or a member acting for him or representing him has a university degree in law which is required by special laws for the practice of law. The court fee for a cassation appeal is collected by the Supreme Administrative Court. The variable symbol for paying the court fee to the account of the Supreme Administrative Court can be obtained on its website: www.nssoud.cz. Prague, May 20, 2020 JUDr. PhDr. Štěpán Výborný, Ph.D., former chairman of the senate