Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 PRELIMINARY WARNING in personal data protection case no. 2.2.-2/21/3116 Issuer of the injunction Data Protection Inspectorate lawyer Ive Eevel Time and place of the injunction Tallinn Addressee of the injunction - personal data processor Estonian Health Insurance Fund address: Lastekodu 48 10144, Tallinn e-mail address: info@haigekassa.ee Personal data processor responsible official of the board chairman RESOLUTION: On the basis of § 751 (3) of the Government of the Republic Act, art. 58 (1a) of the General Regulation on the Protection of Personal Data, 56 (1) of the Personal Data Protection Act (IKS), § 56 (2) point 8, I issue a mandatory injunction for compliance: 1. Find out whether and by whom , where the documents were found, previously had access to, 2. Find out the retention period of the found documents. I set the deadline for the execution of the order as 4.12.2021. Report compliance with the order to the Data Protection Inspectorate by this deadline at the latest. REFERENCE FOR DISPUTES: This order can be challenged within 30 days by submitting either: - an appeal under the Administrative Procedure Act to the Data Protection Inspectorate or - an appeal under the Administrative Court Procedure Code to the administrative court (in this case, the appeal in the same matter cannot be reviewed). Challenging a precept does not stop the obligation to fulfill it or the implementation of measures necessary for fulfillment. WARNING If the processor of personal data fails to comply with the instructions of the Data Protection Inspectorate, the Data Protection Inspectorate may contact the higher-ranking institution, person or whole party of the personal data processor to organize official supervision or initiate disciplinary proceedings against the official on the basis of § 59 (1) of the Personal Data Protection Act. EXERCISE MONEY WARNING: If the injunction has not been complied with by the specified deadline, the Data Protection Inspectorate will impose an extortion fee of 1,000 euros for each point of the injunction to the addressee of the injunction based on § 60 of the Personal Data Protection Act. 2 (7) A fine may be imposed repeatedly - until the injunction is fulfilled. If the recipient does not pay the penalty, it will be forwarded to the bailiff to start enforcement proceedings. In this case, the bailiff's fee and other enforcement costs are added to the enforcement money. FACTUAL CIRCUMSTANCES: On 18.09.2021, the Estonian Health Insurance Fund submitted a violation notice to the Data Protection Inspectorate regarding the 1993-1994 documents that came out during the demolition of 50 Staadion Street in the city of Tartu, and which were submitted to the Health Insurance Fund of the City of Tartu. PERSONAL DATA PROCESSOR'S EXPLANATION: According to the breach notification, on 16.09.2021, the Estonian Health Insurance Fund's helpline was informed that during the demolition of the Staadion 50 building in Tartu, invoices from the Health Insurance Fund's membership card containing personal data were found. The informant himself

brought some folders to the Tartu office of the Estonian Health Insurance Fund and informed that there are more of them there. A representative of the Estonian Health Insurance Fund visited the site and took with him all known folders/boxes handed over by the construction company that may contain personal data. Analyzing the material, the conclusion is that these are documents of the Health Insurance Fund of the city of Tartu, and during the initial inspection there are three types of documents (invoices of the health insurance fund membership card (currently called treatment invoice), medical records, care records). The documents contain special types of personal data (health data) and date from 1993-1994. These are documents that have been submitted to the Tartu City Health Insurance Fund and were the basis for fulfilling the insurance obligation at the time, i.e. invoices for payment of treatment or illness/care certificates for payment of disability benefits. At the address Staadioni 50, Tartu, Eesti Haigekassa has not been known to have leased archive space, and as of the notification, Eesti Haigekassa does not know for what reason, by whom and when the paper documents containing personal data were left at Staadion tn 50 and were not properly stored/destroyed. This information may not be obtained by the Estonian Health Insurance Fund even by further investigation of the circumstances, since these are documents created about 30 years ago. Also, according to the current structure, the Estonian Health Insurance Fund has existed since 2002, the documents may belong to the city of Tartu. The number of persons affected by the breach is 1000-4999. The Health Insurance Fund does not consider it necessary to notify individuals of a violation, because it is known to be a one-time incident where paper documents have been stored incorrectly for a longer period of time. At the same time, there is no reason to believe that the documents have been seen/processed by a larger group of persons. According to the circumstances, the documents have been hidden from the public for a long time and came out during the demolition of the existing building. The documents have been delivered to the Estonian Health Insurance Fund immediately after discovery. The Estonian Health Insurance Fund has adopted organizational measures that make personal data inaccessible to persons without access rights. All known documents containing personal data related to the violation are in the possession of the Estonian Health Insurance Fund and in a locked room to which outsiders and third parties have no access. According to the preliminary assessment, documents containing personal data are not necessary to organize the work of the Estonian Health Insurance Fund or to ensure the rights of individuals. Medical bills and disability certificates have been paid and/or the corresponding claims have expired by today. Today, medical bills and disability certificates are submitted electronically to the database of the Estonian Health Insurance Fund. Thus, it is a so-called problem from the distant past, which has no relation to modern work organization. Today, the

personal data necessary to organize the work of the Estonian Health Insurance Fund and to ensure the rights of individuals are only stored electronically in the database of the Estonian Health Insurance Fund. The Estonian Health Insurance Fund has no reason to believe that there are other similar cases. The discovered document will be destroyed as soon as possible. Notifying all those involved would require a disproportionate effort. The personal data comes from a period almost 30 years ago. There is no way to clarify 3 (7) their actual contact details for a large number of persons, and some of the patients have also left by today. The Estonian Health Insurance Fund has no reason to believe that more third parties than the company performing the demolition work have seen the personal data. In order to solve the violation, mitigate and prevent harmful effects in the future, we will try to find out why the data found at the address of Staadion 50, Tartu. Considering the result of the previously mentioned measure, additional locations where there may be personal data stored in a similar way will be identified if possible. In the event that there are still similar cases, the proper preservation or destruction of the found documents is ensured. Documents with personal data found are stored in a manner inaccessible to third parties and destroyed if it is clear that there is no need to store the documents and there is approval from the Data Protection Inspectorate. Nowadays, disability certificates and medical bills are not stored on paper, but electronically. Thus, a similar violation cannot occur in the present or in the future. The Estonian Health Insurance Fund has reached an agreement with the employees carrying out the demolition of the building, that if additional documents are found in the building, representatives of the Estonian Health Insurance Fund will be contacted immediately and the documents will be handed over to the Estonian Health Insurance Fund. On 12.10.2021, AKI submitted a follow-up inquiry to the Health Insurance Fund, requesting answers to the following questions: 1. In the meantime, have you investigated and found out by whom and when the said documents were left at the given address or to whom do the documents belong? 2. Has the retention period for all found documents expired? 3. What health data did the documents contain? 4. According to the statute of the Health Insurance Fund database, among other things, the person's place of residence according to population (address) is entered in the Health Insurance Fund database. If the found document concerns a person whose data is available in the Health Insurance Fund's database, please explain why the Health Insurance Fund's notification cannot be sent to the person by post? 5. Given that the Health Insurance Fund was recently able to send vaccination invitations to people via SMS, the Health Insurance Fund therefore had people's phone numbers for this purpose. Please explain why it is not possible to inform people about the violation in the same way, by phone? 6. There is no violation notification, did you consider submitting a notification, e.g. through the media, and why did you not consider such a notification

necessary? 7. On what basis do you find that there is no reason to believe that the documents have been seen/processed by a larger group of persons than the company performing the demolition work? 8. Have you investigated whether or who previously had access to the building where the documents were found? Were the documents stored in such a way that they could not be seen/processed by persons who had access to the building? According to the response of the Health Insurance Fund on 19.10.2021: The Estonian Health Insurance Fund has not received an answer by whom and when the said documents were left at the given address or to whom the documents belong, nor has it identified the exact retention period of the documents. Sickness and care sheets do not directly contain health data. The person's name, the length of the page's issuance and the reason for issuance in general form are indicated. The medical bill shows the diagnosis (in Latin) along with the types of service provided. Regarding notification, the Health Insurance Fund found that notifying individuals can help individuals protect themselves from the harmful consequences of a breach. At the same time, people must be protected from unnecessary information fatigue. In this case, notifying individuals would not help to protect them from possible harmful consequences. 4 (7) We have shown in the violation notification that at least ONE of the circumstances specified in Article 34, paragraph 3, points "a" and "b" are present: the Estonian Health Insurance Fund has adopted organizational measures that make personal data inaccessible to persons without access rights. All known documents containing personal data related to the violation are in the possession of the Estonian Health Insurance Fund and in a locked room to which outsiders and third parties have no access. According to the preliminary assessment, documents containing personal data are not necessary to organize the work of the Estonian Health Insurance Fund or to ensure the rights of individuals. Medical bills and disability certificates have been paid and/or the corresponding claims have expired by today. Today, medical bills and disability certificates are submitted electronically to the database of the Estonian Health Insurance Fund. Therefore, it is a so-called problem from the distant past, which has no relation to modern work organization (point a) The personal data necessary to organize the work of the Estonian Health Insurance Fund and to ensure the rights of individuals are today only stored electronically in the database of the Estonian Health Insurance Fund. The Estonian Health Insurance Fund has no reason to believe that there are other similar cases. The discovered document is destroyed as soon as possible (point b). Notification leads to greater confusion for the data subject than non-notification. As mentioned above, the Estonian Health Insurance Fund is not able to answer questions that people may have - who left the documents there, when and why they were left there, etc. Considering the change in the organizational structure of the Health Insurance Fund over time (the current Health Insurance

Fund has been operating on the basis of the law since 2001), it is not possible to say with certainty who is the responsible processor of the documents. Since the Estonian Health Insurance Fund does not have the information, the assumption that the documents have definitely been seen by a larger group of people cannot be valid, and the Estonian Health Insurance Fund does not have data on how access was organized and how the documents were stored. Eesti Haigekassa has no known connection with the building at 50 Staadion Street. We can only rely on the information provided by the construction company carrying out the demolition that found the documents. AKI wanted to review the found documents in order to decide on further proceedings. At the suggestion of the Health Insurance Fund, AKI agreed to the encrypted transmission of sample documents. The Health Insurance Fund provided AKI with one sample for each type of document found (care card, sick card, medical bill). REASONS FOR THE DATA PROTECTION INSPECTION: 1. First of all, it must be determined whether the Estonian Health Insurance Fund is the responsible processor in the documents that were found and related to the documents of the Health Insurance Fund of the city of Tartu. Although the Health Insurance Fund claimed that the Estonian Health Insurance Fund has existed according to its current structure since 2002, and since the Estonian Health Insurance Fund has not rented an archive space in the building located at Staadion 50 in Tartu, the documents may belong to the city of Tartu, AKI believes that this is not the case. § 3 of the Health Insurance Act of the Republic of Estonia1 adopted by the Supreme Council on 12.06.1991 stipulated that mandatory health insurance is organized by county and republican city (paragraph 1). Paragraph 2 of the referred section stated that health insurance for residents is organized by health funds established by the government of a country or a republican city. There is at least one health insurance fund in every county or republican city. 1 https://www.riigiteataja.ee/akt/30518 5 (7) Regulation No. 39 of the Government of the Republic of 01.02.1994 "Organization of the health insurance system"2 was given to organize the health insurance system according to the new principles of health care organization and to bring it into line with the local government's order and the introduction of a unified social tax in order to perform the related tasks, the Ministry of Social Affairs was tasked with organizing the health insurance system, preparing the corresponding budget, and organizing accounting and reporting by March 1, 1994. The Central Health Insurance Fund is under the administration of the Ministry of Social Affairs. By Regulation No. 63 of the Government of the Republic of 17.02.1994 "On the new statute of the Health Insurance Fund"3, the Ministry of Social Affairs was given the task of developing and approving the new statute of the Health Insurance Fund. In the same regulation, the Government of the Republic established that the health funds established on the basis of the new statute of the health fund are the legal successors of the health funds that

operated as self-sustaining insurance institutions of county governments or former republican city governments in all property and non-property relations. Regulation No. 17 of the Minister of Social Affairs of 25.02.1994 approved the basic regulation of the Health Insurance Fund4. Clause 5 of the said bylaws provides that the health funds operating in accordance with this bylaw are the legal successors of the health funds of the county government or the republican city government that operated as a self-sustaining insurance institution of the county government or the republican city government in all property and non-property relationships. Section 48 of the Estonian Health Insurance Fund Act5 adopted by the Riigikogu on 14.06.2000 provided for the termination of the central health insurance fund and health insurance funds and the transfer of their assets to the Estonian Health Insurance Fund. Considering the above, it is appropriate to state that the Estonian Health Insurance Fund is responsible for the activities of the Tartu City Health Insurance Fund. Since the Estonian Health Insurance Fund is responsible for the relevant documents, issuing an injunction to the Estonian Health Insurance Fund to clarify the circumstances is justified. 2. The Health Insurance Fund does not consider it necessary to notify individuals of the violation, as it is known to be a one-time incident where paper documents have been improperly stored for a longer period of time. First of all, AKI does not agree with the claim of the Health Insurance Fund that it was a one-time incident. As early as 1998, the press wrote about how the archive documents of the Tartu Health Insurance Fund were lying behind an unlocked door in the basement of the building on Pepler Street, being accessible to anyone who was curious6. Therefore, it is reasonable to suspect that such situations may arise even more. All the more so if the Health Insurance Fund does not even know that it has legal responsibility for the documents that were transferred to the Central Health Insurance Fund and the health insurance funds. 3. The Health Insurance Fund considers that informing all covered persons would require disproportionate efforts. The personal data comes from a period almost 30 years ago. There is no way to find out their actual contact details for a large number of individuals, and some of the patients have also left by today. The Estonian Health Insurance Fund has no reason to believe that more third parties than the company performing the demolition work have seen the personal data. Therefore, it can be concluded that the Health Insurance Fund does not consider the violation to be significant. AKI already explained in the inquiry that according to Article 34(3c) of the IKÜM, notifying the data subject is not required if it would require disproportionate efforts, but according to the second sentence of the mentioned paragraph, in such a case, a public announcement is made or another similar measure is taken, which informs all data subjects in an equally effective way. 2 https://www.riigiteataja.ee/akt/13024157 3 https://estlex.ee/?id=76&aktid=10686&fd=1&leht=1 4

https://www.riigiteataja.ee/akt/28243 5 https: //www.riigiteataja.ee/akt/26422?leiaKehtiv 6 https://www.postimees.ee/2541979/tartu-haigekassa-vanad-dokumendid-keldris-laokil 6 (7) According to the guidelines of the data protection working group established under Article 297, the if the violation involves personal data revealing racial and ethnic origin, political views, religious or philosophical beliefs and trade union membership, as well as genetic data, data on health, sex life and criminal convictions and offenses and related security measures, consider the occurrence of great harm likely. The Health Insurance Fund's reference to the fact that such notification could cause unnecessary notification fatigue, as it would not help protect them from possible harmful consequences, is irrelevant. Even if an individual cannot do anything to protect their rights, they have the right to know if the state has stored their data insecurely. Article 34(3) sets out three conditions, if met, there is no need to notify individuals of the breach. These are: The controller has applied appropriate technical and organizational measures to protect personal data before a breach, in particular those measures that make personal data unreadable by anyone without authorization to access the data. Immediately after the breach, the controller has taken steps to ensure that the major threat to the rights and freedoms of individuals is unlikely to materialize again. For example, depending on the situation, the controller may have been able to immediately identify the person who accessed the personal data and take action against him before he could do anything with the data. Contacting individuals requires a disproportionate effort, for example, when their contact information has been lost due to a breach or was not initially known. Controllers should, in accordance with the principle of accountability, demonstrate to the supervisory authority that they fulfill one or more conditions. Since in the present case, neither the first nor the last condition is met (if measures regarding the proper storage of documents had been introduced before the violation, the violation could not have occurred and, as mentioned above, the persons could be informed also through a public announcement), it is necessary to assess whether the second condition is met. However, it is not possible to do this until it has been found out whether and who could previously have had access to the premises where the documents were found. Since this has not been done at the moment, it cannot be unequivocally certain that the mentioned condition has been met. In order to assess the further realization of the threat, the relevant circumstances should therefore be found out at the Health Insurance Fund. 4. The Health Insurance Fund wants AKI to allow the destruction of the found documents, but has not yet been able to identify the exact retention period of the documents. However, the retention period of the documents is important to decide whether the documents should be sent to the archive or can be destroyed. However, determining the retention period is the responsibility of the Health Insurance Fund,

not AKI. 5. The Health Insurance Fund also announced that the sickness and care sheets do not directly contain health data. The person's name, the length of the page's issuance and the reason for issuance in general form are indicated. The medical bill shows the diagnosis (in Latin) along with the types of service provided. The 3 documents submitted to AKI (sickness sheet, care sheet and medical invoice) contained the person's name, date of birth, place of residence and diagnosis (the care sheet contains that of the person being cared for), and the care sheet also contains the name and date of birth of the person being cared for. 7 Guidelines regarding the reporting of a breach of personal data on the basis of Regulation 2016/679, available at https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised/isikuandemtega_seotud_rikkumistest_teavitamise_juhend.pdf 7 (7) Therefore, the procedure of the Estonian Health Insurance Fund submitted false information to AKI during The Data Protection Inspectorate draws the attention of the Health Insurance Fund to the fact that according to § 279 and § 280 of the KarS, both obstructing the supervision procedure and providing false information are punishable. Therefore, it is particularly important that the Health Insurance Fund clarify all relevant issues before the AKI can give its assessment of the violation. /digitally signed/ Ive Eevel lawyer under the authority of the director general