Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 REMINDER AND PRE-WRITING WARNING in personal data protection case no. 2.1.-1/21/535 Issuer of the injunction Data Protection Inspectorate lawyer Signe Kerge Time and place of issuing the injunction 02.07.2021 in Tallinn Addressee of the injunction - personal data processor Defense Force address: Juhkentali tn 58, 15007, Tallinn e-mail address: mil@mil.ee RESOLUTION : On the basis of Section 751(3) of the Government of the Republic Act, Section 56(1), Section 56(2)(8) of the Personal Data Protection Act (ICS), and Articles 5, 9(1) and Article 58(2)(d) of the General Regulation on Personal Data Protection, we issue a mandatory injunction to comply with: - terminate a practice where employees of the Defense Medical Center view the health data of other persons in the health information system without a legal basis, including on the grounds of processing invoices. We set the deadline for the fulfillment of the injunction to be 15.07.2021. Report the fulfillment of the injunction to the Data Protection Inspectorate by this deadline at the latest. REFERENCE FOR DISPUTES: A data subject complainant whose rights are affected by this injunction can challenge this injunction within 30 days by submitting either: - an appeal in accordance with the Administrative Procedure Act to the Data Protection Inspectorate or - an appeal in accordance with the Code of Administrative Court Procedure 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. 2 (8) If a personal data processor from a state institution does not comply with the instructions of the Data Protection Inspectorate, the inspectorate will appeal to the administrative court with a protest on the basis of § 59 subsection 3 of the Personal Data Protection Act. FACTUAL CIRCUMSTANCES: On 10.02.2021, the Data Protection Inspectorate received XXX's complaint, according to which the Defense Force XXX has made inquiries about his health data in the health information system. EXPLANATION OF THE PROCESSOR OF PERSONAL DATA: On 15.03.2021, the Defense Service explained the following in its response: I am forwarding the answers of the Defense Forces to the questions stated in the letter of initiation of the supervision procedure of the Data Protection Inspectorate dated 26.02.2021. 1. Please explain why and on what legal basis XXX has made inquiries into XXX's health data? The inquiry regarding XXX's health data was carried out by XXX in order to fulfill his official duties and was related to the processing of the invoice submitted to XXX for the service provided by

Tartu University Clinic SA and checking whether there is a basis for paying the invoice (whether the person has received the corresponding service). Within the Defense Forces, expenditure areas and procurement managers based on expenditure areas have been regulated and determined (Director of Defense 30.03.2020 kk no. 97). As a result, on 10.09.2020, the commander of the navy approved directive No. 33, which appointed the authorized cost makers and cost managers of the cost areas in the navy at the cost area-specific purchasing managers. With this directive, XXX was approved as a spender, a claimant and a spend manager in the following spend areas: pharmacy goods, medical equipment and devices, and medical services. XXX, acting within the scope of competence arising from his position, has the obligation to make sure in advance of the legality and justification of the invoices submitted by the contractual cooperation partner. 2. Was the making of the inquiries related to the performance of the employee's duties? If so, please specify with which tasks. Yes, the inquiry was related to the performance of duties by the employee. XXX, acting within the scope of competence arising from his position, has the obligation to make sure in advance of the legality and justification of the invoices submitted by the contractual cooperation partner. On 12.10.2020, the e-invoice of Tartu University Clinic SA arrived at the Navy for processing. The processing of the invoice was started on 19.10.2020 due to the absence of XXX. From the invoice sent by Tartu University Hospital SA, it was not clear which service and person it was submitted in connection with, and as a result, a clarifying request regarding the invoice was sent to Tartu University Hospital SA. The received reply was laconic, containing the name of the person, but no content of the service provided. The request regarding personal data was related to the processing of the e-invoice submitted to XXX for the service provided by Tartu University Clinic SA and the legality check, whether there is a basis for the payment of the invoice by the Defense Forces. It turned out from the digital story that it was an occupational health doctor's visit, after which the received invoice was confirmed and directed to be paid. As usual, Esmed Töötervishoid OÜ provides the service of an occupational health doctor to navy personnel, but due to the employment of the company's occupational health doctors, XXX was directed to receive the service of an occupational health doctor at Tartu University Clinic SA. The commander of the medical center of the military branch or structural unit is responsible for the budget and thus approves the invoices submitted for the provision of the service. In order to confirm the validity of the invoices, he must make sure of the content of the invoice and the provision of occupational health services to a specific person. This is the professional competence of XXX. 3. Did the employee have a medical relationship with XXX at the time of the inquiries? According to XXX's explanations, XXX, while serving in the Defense Force, was included in his list in the part that was related to the payment by the Defense Force for

medical bills related to 3 (8) persons and submitted to the Defense Force. In the sense of a specific active disease case (the patient comes with complaints and is referred for examinations or consultation of a specialist, i.e. incurring expenses), there was no medical relationship at the time of the inquiry. 4. Has XXX forwarded XXX's personal data (including special types of personal data) to anyone? If so, please specify to whom and on what basis. 1) On 06.01.2021, at the request of the Navy lawyer, XXX gave explanations to the questions sent by XXX's representative, regarding the request made in October 2020 to XXX's health data. 2) In connection with the request of the Data Protection Inspectorate on 26.02.2021, XXX forwarded to the Chief Data Protection Specialist of the Defense Forces information about the request for XXX's health data in order to prepare a response letter. 5. Please provide your own explanations and justifications that you consider necessary to include in this matter. XXX would like to point out that it certainly did not make a malicious request regarding XXX's personal data from the digital story. The Data Protection Inspectorate then submitted an additional inquiry, and the Defense Force responded to it on 12.05.2021: I am forwarding the responses of the Defense Force to the Data Protection Inspectorate's additional inquiry on 27.04.2021 in the matter of personal data protection. 1. On which legal basis listed in article 9 of IKÜM did XXX view XXX's health data in the health information system? If such processing of personal data is prescribed by national legislation, please refer to the specific provision. According to XXX's explanations, he viewed the health data on the basis of Article 9(2)(h) of the IKÜM, which states that Article 9(1) of the IKÜM does not apply if the processing is necessary for reasons related to preventive medicine or occupational medicine, to assess the employee's ability to work, to make a medical diagnosis, to provide health services or social welfare or to enable treatment or to organize the health care or social care system and services, based on the law of the Union or a Member State or the contract concluded with a health care worker and on the condition that the conditions referred to in paragraph 3 are met and protective measures are established. According to § 13 (1) p. 62 of the Occupational Health and Safety Act, the employer is obliged to organize the provision of occupational health services and bear the related costs. Section 131, subsection 7 of the same law stipulates regarding the health check-up that the employer bears the costs related to the health check-up. The health check-up is carried out during working hours and the employee is paid the average working day's wage during that time. Section 351(1) of the Defense Forces Organization Act (KKS) states that in the Defense Forces, a healthcare worker provides health care services in accordance with the provisions regulating the provision of general medical care and specialized medical care in the Health Services Organization Act. According to KKS § 352, a structural unit of the Defense Forces may include a medical center in which at least one of the following medical services is

provided: general medical care, Defense Forces emergency room, out-of-hospital medical care. § 41 subsection 11 point 1 of the Act on the Organization of Health Care Services states that a health care service provider who has a statutory duty of confidentiality has the right to process personal data, including special types of personal data, for the purpose of planning the provision of health care services, based on the purpose specified in § 2 subsection 1 of the same law. § 768 (1) of the Law of Obligations Act stipulates the duty of confidentiality of the healthcare service provider. Starting from 2020, the budget of the Defense Forces was divided into 4 (8) purchase managers based on the area of expenditure (Head of the Defense Forces 30.03.2020 kk no. 97). As a result, on 10.09.2020, the commander of the navy approved directive No. 33, which appointed the authorized cost makers and cost managers of the cost areas in the navy at the cost area-specific purchasing managers. With this directive, XXX was approved as a spender, a claimant and a spend manager in the following spend areas: pharmacy goods, medical equipment and devices, and medical services. XXX, acting within the scope of competence arising from his position, has the obligation to make sure in advance of the legality and justification of the invoices submitted by the contractual cooperation partner. In the general guidelines for purchasing management in the Defense Forces based on cost areas, the processing of invoices for the provision of medical services, including invoices for healthcare services, is also outlined. Regarding the processing of invoices, it is stated that the structural unit receives prior approval for ordering the service. When the invoice arrives, the purchasing manager checks the correctness of the invoice, specifies if necessary, makes sure of the availability of budgetary funds and coordinates the invoice. XXX did not have information about ordering an occupational health inspection service for XXX. The XXX of the military unit or structural unit is responsible for the medical budget in his unit and approves the invoices submitted for the provision of the service. In order to confirm the validity of the invoices, he must make sure of the content of the invoice and whether the service was provided to a specific person. Confirming invoices with unverified data is prohibited, and such activity can be qualified as a violation of service obligations within the meaning of the Defense Forces Disciplinary Act. 2. Why were no clarifying questions asked regarding the invoice submitted to the Defense Forces to Tartu University Hospital SA or XXX? On 12.10.2020, e-invoice 20K00991 of the University of Tartu Clinic SA was received by the Navy for processing, the deadline for payment was 21.10.2020. It was not clear from the bill which service and person it was submitted to the Defense Forces in connection with. Due to XXX's absence due to vacation (in the period 12.10.-16.10.2020), the processing of the invoice was only started on 19.10.2020. Based on the above, on 20.10.2020 at 10:12, Tartu University Hospital SA was sent a detailed request regarding invoice no. 20K00991 (amount of €49.79) and the

patient, so that the invoice could be checked, approved and forwarded to payment by the Defense Forces. On 10/21/2020 at 10:06 a.m., Tartu University Hospital SA received an encrypted addendum to the consolidated invoice as a response, which was concise, containing XXX, the name and the date of service provision (15/09/2021), but the content of the provided service was missing. Since the answer received from UT Kliinikim SA did not provide the necessary information to identify the service provided to XXX, there was no information about the possible provision of services to XXX, which should have been paid for from the state budget funds allocated to the Defense Forces, so in order to exclude errors in the payment of the bill and non-targeted use of state funds, a request was made to the patient's health data . Not asking XXX for an additional explanation was related to the fact that XXX was on an incapacity for work sheet in the period 16.09.-22.12.2020 (starting from the day after the occupational health inspection in Tartu) and the employer had no right to bother him. This was made clear by XXX already on 08.04.2020 to the commander of the naval base, who wanted to receive information about the file deletion of document No. 12432 in the document management system on 02.04.2020 by XXX. W´XXX replied to the commander of the naval base that answering was extremely burdensome for him and reminded him that he was on the incapacity for work sheet1. Given that XXX did not have information about ordering the occupational health check-up service for XXX, but additional information was needed to coordinate the invoice, and respecting XXX's previous wish, it was not conceivable to contact the person during the period of his/her incapacity for work. 1 Employment Contracts Act § 19 paragraph 2. 5 (8) XXX points out that at that moment the request for health data was made from the health information system as a last resort. The first request from the health information system regarding XXX was made on 21.10.2020 at 10:10 a.m. and the last one at 10:25 a.m., i.e. immediately after receiving a response from UT Kliinikim SA, which did not clarify the content of the service and because of which it was not possible to direct the bill to payment immediately. The request regarding personal data was related to the processing of the e-invoice submitted to XXX for the service provided by Tartu University Clinic SA and the legality check, whether there is a basis for the payment of the invoice by the Defense Forces. When the health information system revealed that it was an occupational health doctor's visit, the bill was confirmed and directed to be paid. XXX, taking into account the circumstances related to the specification of the invoice, the deadline for payment of the invoice and the obligation to confirm the correctness of the invoice related to the provision of the service, took a discretionary decision in this situation to make a request from the health information system. It can be added that there was definitely no malicious processing of XXX personal data by him. The Defense Force, as a result of this case, is reviewing the current work

organization in the processing of invoices for healthcare services. In order to improve the processing of invoices submitted for health care services and to avoid similar cases in the future, including improving the internal work organization, we can provide structural units with more precise guidelines related to checking and approving invoices within the Defense Forces, in cooperation with the purchase manager of the field. 3. Please clarify your answer to the question of whether the employee had a therapeutic relationship with XXX at the time of making the inquiries. You state that while in service, the person belonged to the XXX list in the part related to the payment by the Defense Force for medical bills related to the person and submitted to the Defense Force. We want to know if XXX was on XXX's list as a patient, i.e. did XXX provide health care to the person? According to XXX, while serving in the Defense Forces, XXX was included in his list as a patient in the part that deals with the right to receive health care in the Defense Forces, for example the provision of emergency care (if it should be needed while serving in the Defense Forces) and payment for the provision of personal health services to the Defense Forces by the Defense Forces (occupational health service, procedures prescribed by an occupational health doctor e.g. massage, visual acuity correction aids). As a result, XXX was listed as a patient of XXX. GROUNDS FOR THE DATA PROTECTION INSPECTION: The object of the complaint is the viewing of a person's health data in the health information system by the Defense Forces as an employer. We first point out that there must be a legal basis for any processing of personal data - either the consent of the person or another basis arising from the General Regulation (Articles 5 and 6 of the General Regulation on Personal Data Protection (GPR). In a situation where special types of personal data (including health data) are processed, the legal basis for data processing can be derived from article 9 of IKÜM. We emphasize that points b and g-j of article 9 paragraph 2 of IKÜM are not independent grounds for processing special types of personal data, the specific basis for processing must be derived from the Union or a member state of the law and meet the requirements of the corresponding point of Article 9, Paragraph 2 of the IKÜM. 6 (8) We add that according to Article 4 of IKÜM, health data are personal data related to the physical and mental health of a natural person, including data regarding the provision of health care services to him, which provide information about his state of health. Therefore, the decision of the health examination and its contents also belong to the health data. Only a doctor who has a medical relationship with a person, a health care provider, has the right to process health data, if the provision of health care services is planned, a contract for the provision of health care services is concluded and executed, or the data is processed for other purposes provided for in § 56 (1) point 7 of the Act on the Organization of Health Care Services. It cannot be extended to other healthcare workers for other purposes, including medical

bill control. It must be distinguished whether an employee of the Medical Department of the Defense Forces provides health care to the employee as a health service provider, as a result of § 351 subsection 1 of the Defense Forces Organization Act (KKS), and for this reason looks at the person's health data from the health information system, or whether the employee of the medical department comes into contact with the person as an employer. In this case, it is a situation where the Defense Force processed a person's health data as an employer. XXX has made an inquiry as a healthcare provider about a person with whom he did not have a medical relationship. For this reason, the request was not legal. TTKS § 593 stipulates who has the right to access digital history data and for what purposes. Pursuant to subsection 2 of the aforementioned section, the health care service provider has access to personal data in the health information system for the purposes and procedure provided for in subsections 1-12 of § 41 of the same Act. A more detailed procedure is provided in the basic regulation of the health information system, according to § 11 (1) the health care provider has access to personal data in the information system for the purpose of planning the provision of health care, concluding and executing the contract for the provision of services, and to the extent and for the purpose provided for in § 56 (1) point 7 of the Act on the Organization of Health Services. In other words, as a result of the above, a medical professional who has a medical relationship with the person has the right to view data from the digital story. According to the complaint, XXX was not the individual's treating physician. Thus, the right to view the data cannot be extended in the same way as if this right were simply for a health care provider who does not have a medical relationship with a specific person. Especially since the data was not viewed for the purpose of providing treatment. Thus, the employee viewed personal data from the health information system without a legal basis. The occupational health doctor, who is assigned this duty, has the right to process the health data of the employees. The obligation to provide the service was given by the Defense Forces to the SA Tartu University Clinic. The employer can decide on the direction of the health check-up of the employees, and the basis for this is outlined in the procedure for the health check-up of the employees2. Whereas the occupational health doctor does not provide health data (including diagnosis) to the employer, but assesses the employee's state of health and makes a decision whether the work environment or work organization is suitable for the employee or not. Health data will only be given to the person who has passed the inspection. 2 https://www.riigiteataja.ee/akt/117072018003?leiaKehtiv 7 (8) The employer may not require the healthcare service provider or the employee to: - enter a diagnosis in the medical certificate or submit a medical history; - submission of a pregnancy card; - submission of data or documents not mentioned in the law about the employee's health check-up from the occupational health

doctor; - submission of data not specified in the law in case of occupational disease and work accident. Consequently, the employer may not demand from either the healthcare service provider or the employee a description of the content of the service provided to him. Thus, the Health Care and Occupational Safety Act does not regulate the employer's right to receive information about the employees' health data, but regulates the rights and obligations of the employer and the employee to conduct health checks and create a safe working environment. It remains unclear why clarifications about the content of the provided service were not asked from the SA Tartu University Clinic and instead the information was checked from the health information system. The Defense Force has said in its explanation that the clinic's response was not sufficient to confirm the payment of the medical bill, but this would not have prevented the Defense Force from asking for additional explanations to identify the situation. In conclusion, the employer must always find a legal basis for the processing of employees' health data, which must be clearly stipulated in the law. The inspection is of the opinion that in the situation described by the Defense Forces, this can only be consent, and without the employee's consent, the employer cannot go to the health information system to look at the health data of the person or demand the employee to publish other information or process his (health) data. Based on the above, the Data Protection Inspectorate instructs the Defense Force to stop such practice and not to process employee data in this way in the future without a legal basis. REMINDER AND LEAVING THE VALUE PROCEDURE UNINITIATED The Data Protection Inspectorate explains that it is a violation within the meaning of § 71 of the Personal Data Protection Act3. Nothing gives permission to view health data from the health information system without a legal basis. In other words, the right to view data from the information system belongs to a medical professional who has a medical relationship with a person. This was not the case in this case, and therefore such an action is completely unacceptable. The defense force must be able to correctly apply the rules arising from the legislation in the processing of health data and ensure that the employees of the institution are also aware of these rules and follow them. It remains unknown to what extent the said employee personally understands the rules for using health data and the health information system. According to the Data Protection Inspectorate, the Defense Force needs training in the processing of health data. Section 31(1) of the Misdemeanor Procedure Code4 stipulates that misdemeanor proceedings are mandatory, if the act is not minor according to the conviction of the extrajudicial proceeding or there are no circumstances that preclude misdemeanor proceedings provided for in § 29 of the VTMS. According to subsection 2 of the same section, 3 https://www.riigiteataja.ee/akt/104012019011 4 https://www.riigiteataja.ee/akt/128052021013?leiaKehtiv 8 (8) misdemeanor proceedings do not have to be initiated in the case

of a minor misdemeanor and may be limited to a misdemeanor with a verbal warning of the person who committed the act with the characteristics. Considering that XXX did not make inquiries based on his curiosity, the Data Protection Inspectorate considers it justified in this situation to initiate misdemeanor proceedings and to punish an employee of the Defense Force for making inquiries made without a legal basis in a misdemeanor case. Therefore, based on the factual circumstances and the fact that XXX viewed the applicant's health data without a legal basis, we reprimand him on the basis of Article 58(2)(b) of the General Regulation on Personal Data Protection and §31(2) of the VTMS and draw attention to the following: There must be a legal basis for any processing of personal data, which is a special type in the case of personal data, it follows from Article 9 of the General Regulation on the Protection of Personal Data. The processing of personal data is prohibited without a legal basis. Based on the above, we close the supervisory procedure in the matter. Sincerely /signed digitally/ Signe Kerge jurist under the authority of the Director General