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.-1/21/1888 Injunction maker Data Protection Inspectorate lawyer Signe Kerge Time and place of injunction 14.07.2021 in Tallinn Recipient of injunction - personal data processor SA Hiiumaa Haigla address: Kärdla city, Rahu tn 2b, 92414 e-mail address: info@hiiumaahaigla .ee Copy: XXX XXX RESOLUTION: § 751 (3) of the Government of the Republic Act, 56 (1), § 56 (2) point 8 of the Personal Data Protection Act (IKS) and Articles 5, 9 (1) and Article 58 (2) point d of the General Regulation on Personal Data Protection on the basis of this, I issue a mandatory injunction for compliance: to stop the practice where Hiiumaa Haigla, as an employer, processes the health data of its employees through inquiries in the health information system without a legal basis. We set the deadline for the fulfillment of the injunction to be 29.07.2021. Report the fulfillment of the injunction to the Data Protection Inspectorate by this deadline at the latest. This order can be disputed within 30 days by submitting either: - a complaint according to the Administrative Procedure Act to the Data Protection Inspectorate or - a complaint according to the Code of Administrative Court Procedure to the administrative court (in this case, the complaint 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 injunction is not complied with by the specified deadline, the Data Protection Inspectorate will impose a fine of 2000 euros on the addressee of the injunction based on § 60 of the Personal Data Protection Act. 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 2 (5) enforcement money. FACTUAL CIRCUMSTANCES: The Data Protection Inspectorate received XXX's complaint, according to which SA Hiiumaa Hospital employees XXX and XXX have made inquiries about his health data in the health information system. In addition, the complainant pointed out that his health data (vaccination-related information) is shared by these employees with third parties. In connection with this, the inspection started the supervision procedure for SA Hiiumaa Hospital. DATA PROTECTION INSPECTION INQUIRY: On 15.06.2021, the Data Protection Inspectorate made an inquiry to Hiiumaa Hospital, asking the following: 1. Please explain why and on what legal basis have the employees made inquiries into XXX's health data? Please provide a specific reason for each request. 2. Was the making of the inquiries related to the performance of the employees' duties? If so, please specify with which tasks. 3. Did the employees have a therapeutic relationship with XXX at the time of the inquiries? 4. Have the employees forwarded XXX personal data to anyone (including special types of personal data; information related to vaccination, etc.)? If so, please

specify to whom and on what basis. 5. How did these employees get information about the applicant's vaccination or non-vaccination? Please comment on the situation where XXX "refuses to be in the same room with unvaccinated employees, telling them to wear a mask and also the corresponding protective clothing, while urging all other employees who are vaccinated and are in the same room to remove their masks. XXX does not want an unvaccinated employee to come into contact with patients, childbirths and newborns - on the grounds that I am a danger to everyone". On what legal basis has the health data become known to this doctor? We would like to point out that Directive 2000/54/EC1 of the European Parliament and of the Council provides guidelines for vaccination. Article 14(2) of Annex VII states that in the case of vaccination, a certificate may be drawn up which should be available to the employee concerned. It does not talk about providing health data to the employer or co-workers. 6. Please provide your own explanations and justifications that you consider necessary to include in this matter. PERSONAL DATA PROCESSOR'S EXPLANATION: On 28.06.2021, SA Hiiumaa Hospital explained the following in its response: 1. XXX viewed XXX's health data on April 19, when he was the doctor on duty at Hiiumaa Hospital. XXX stayed with a child under the age of 14 on the care page from 13 to 19. April 2021 In the Hiiumaa hospital, during the second wave of the Covid pandemic, it was a rule that before returning to work from sick leave and care leave, it was necessary to give a negative Covid test. The order and response to the employee analysis were completed through EMO. XXX also formalized an outpatient epicrisis and sent a digital lock. 1 https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32000L0054&from=EN 3 (5) XXX reviewed XXX's health records to ensure the safety of patients and staff in the maternity ward as was on maintenance page. 2. XXX viewed XXX's health data on April 19, when he was the doctor on duty at Hiiumaa Hospital. XXX stayed with a child under the age of 14 on the care page from 13 to 19. April 2021 In the Hiiumaa hospital, during the second wave of the Covid pandemic, it was a rule that before returning to work from sick leave and care leave, it was necessary to give a negative Covid test. The order and response to the employee analysis were completed through EMO. XXX also formalized an outpatient epicrisis and sent a digital lock. XXX reviewed XXX's health records to ensure the safety of patients and staff in the maternity ward as XXX was on care leave. 3. XXX - yes XXX - no 4. The Hiiumaa hospital has no information that the employees have forwarded XXX's personal data to anyone. 5. XXX, being the caretaker of the maternity ward, has repeatedly stated in the department that he has not been vaccinated and has urged employees not to vaccinate against Covid-19. Based on the order No. 3 of Riina Tamme, a member of the board of Hiiumaa Hospital, from May 17, 2021, vaccinated employees could be in the rest rooms

without a mask, but if there is one unvaccinated employee in the company, everyone had to wear a mask. 6. All documents that Hiiumaa Hospital has approved due to the Covid pandemic have been previously consulted with the infection control department of the Northern Estonian Regional Hospital. · Use of PPE by non-vaccinated employees when communicating with patients (until 31.05.2021). · Executive member's order no. 3 (as of 18.05) Hiiumaa Hospital strongly disapproves when employees receive patients' health data from the digital record without needing it to perform their duties. Hiiumaa Hospital has repeatedly reminded the employees that it is not acceptable to inherit the patient's health data from the digital history without a reason and has shared information about the handling of sensitive personal data. on April 27, 2018 the employees of Hiiumaa Hospital have completed the training "Actual data protection law and changes in hospital work resulting from the reform". GROUNDS OF THE DATA PROTECTION INSPECTION: There must be a legal basis for any processing of personal data - either the consent of the person or another legal basis (Articles 5 and 6 of the General Regulation on Personal Data Protection 2(IC). However, in a situation where special types of personal data (including health data) are processed, the legal basis for data processing can be derived from IKÜ Article 9. Answers to health tests, as well as information about vaccinations, are without a doubt health data. Health data is a special type of personal data according to Article 9 paragraph 1 of the IKÜM. According to the cited articles, it is permitted to process personal data (including special types of personal data) in accordance with the General Regulation on Personal Data Protection. One of the central requirements and principles of the General Regulation is that the processing of personal data must be lawful. 2 https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016R0679&from=EN 4 (5) 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. SA Hiiumaa Hospital responded to our inquiry that during the second wave of the Covid pandemic at Hiiumaa Hospital, it was necessary to give a negative Covid test before returning to work from sick leave and care. The

order and response to the employee analysis were completed through EMO. XXX also formalized an outpatient epicrisis and sent a digital lock. According to the hospital, XXX looked at the applicant's data to ensure the safety of the patients and staff of the maternity ward, as the applicant was on the care sheet. However, he did not have a valid medical relationship with the applicant, the request was made for organizational purposes. The hospital did not point out any other legal basis (including legal grounds) for viewing the applicant's data. Thus, the employee viewed personal data from the health information system without a legal basis. Health data will only be given to the person receiving the health care service. 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. Co-workers have not had the right to receive this information for a long time. Consequently, the employer may not demand the result of the corona test from the healthcare service provider or the employee. A similar situation is with vaccinations - the Estonian law does not provide that the employer has the right to demand information about vaccinations from the employee. The inspectorate is of the opinion that this issue should definitely be regulated at the level of the law, but until the Riigikogu has adopted such a law, the inspectorate cannot creatively apply the existing laws and not apply the requirements of the IKÜM. Therefore, in the current situation, if the work organization or the environment poses risks for the employee, including the risk of being infected with the coronavirus, the employer must take measures (personal protective equipment, the possibility of vaccination) to mitigate the risks, including arranging a visit to the occupational health doctor. However, after the occupational health doctor's visit, the employer is only given an assessment - may/may not be allowed to work or may be allowed to work. 5 (5) We would also point out that Directive 2000/54/EC3 of the European Parliament and of the Council also provides guidelines for vaccination. Article 14(2) of Annex VII states that in the case of vaccination, a certificate may be drawn up which should be available to the employee concerned. It also does not talk about providing health data to the employer. In conclusion, the employer or co-worker who made the request must always have a legal basis for processing health data, which must be clearly stipulated in the law. The inspection is of the opinion that in this situation only consent can be the legal basis, and without the consent of the employee, the employer or co-worker cannot access the health information system of the person, demand the publication of other information by the employee or process his (health) data. Based on the above, Data Protection Inspectorate instructs Hiiumaa Haigla SA to stop such practice and not to process

employee data in this way in the future without a legal basis. On the basis of Section 31(2) of the Misdemeanor Procedure Code4, the inspectorate issues a verbal warning to a specific hospital employee who made inquiries in the health information system. The Data Protection Inspectorate further adds that matters concerning workplace bullying are beyond our competence. We can only assess the circumstances related to the processing of personal data, including the legality of inquiries made in the health information system. To resolve problems related to the employment relationship, the applicant can contact the Labor Inspectorate. More information about the resolution of labor disputes is available on their website, at https://www.ti.ee/et/tookuskæds-toosuhted/toosuhted-toovaidlus/toovaidluste-lahendamine-toovaidluse-lahendamise-siaduse. /signed digitally/ Signe Kerge, lawyer authorized by the Director General 3 https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32000L0054&from=ET 4 https://www.riigiteataja.ee /akt/128052021013?findValid