Record no. 8492/163/20

IMI Case no. 380803.1

9 December 2022

Final Decision of the Deputy Data Protection Ombudsman

Matter Processing of health information by the employer, accuracy of personal data, informing the data subjects, disclosure of personal data to the police, user log data and the data subject's right of access to data

Complainant [redacted]

Controller [redacted]

Complainant's claims and their justification

1. On 26 October 2020, the complainant instituted a case with the Office of the Data Protection Ombudsman concerning the processing of personal data by a controller. The complainant alleged that [redacted] had maintained an extensive data file containing health information on its employees. It was alleged that this data file included the times of absence due to illness and the employees' diagnoses. The complainant has alleged that her data was stored in this file for 20 years. According to the complainant, she was dismissed in 2017, but the above-mentioned information on her was allegedly still stored until at least 2020. The complainant has also alleged that her data in the file was also partly inaccurate. Furthermore, the complainant has alleged that this data was used against her when she contested her dismissal.

2. According to the complainant, she has asked [redacted] for access to her personal data. In addition, the complainant said that she has requested access to the log data related to the data file in question. The complainant has not been given access to the log data. The complainant was given a number of justifications for why the employer considered that it had the right to store the data. Information on the diagnose listing included in the data file had not been given to the complainant. The complainant eventually obtained the information by other means.

3. The document instituting the case also makes other allegations, including that the health information was stored in a system called MAPS, which is used by all vessels sailing under the Finnish flag. Furthermore, it has been alleged that any nurse working on any vessel would have access to the data of any shipboard employee, regardless of the vessel on which the nurse is working.

Information provided by the controller

<u>The request made by the complainant to the controller</u>

4. The complainant has requested access to the data on at least 10 January 2020 and 3 February 2020. Among other documents, the complainant has delivered the reply given by the controller to her request on 1 April 2020 to the Office of the Data Protection Ombudsman.

5. The reply states that the complainant asked for a copy of her sick leave certificates for 2001–2017. The controller has stated that it is in possession of the complainant's sick leave certificates for 2017 and a single sick leave certificate from 2016. The controller has promised to deliver these copies to the complainant. The controller has also stated that it is in possession of the material related to the trials.

6. Furthermore, the reply states that the disclosure of log data is provided for in the Act on the Electronic Processing of Client Data in Healthcare and Social Welfare. The controller has stated that the Act only applies to the electronic processing of social welfare and health care client data. According to [redacted], it is not a social welfare or health care service provider as referred to in this Act. Therefore, [redacted] considers that it does not have a statutory right or obligation to deliver log data from electronic systems to the complainant.

7. According to the controller, the complainant's request asked the controller to state the basis on which her data was processed in police interviews. In this regard, [redacted] has referred to Article 9(2)(f) of the General Data Protection Regulation (GDPR).

8. According to the controller, the complainant also enquired why a nurse working for [redacted] had disclosed information on forthcoming occupational health discussions to certain employees in the organisation. The controller stated that the question involved email messages related to the occupational health discussions and scheduling a time for the discussion. In this regard, [redacted] has stated that the employer has the right to process an employee's personal data when the processing is necessary for complying with the obligations and special rights of the controller or data subject in the field of employment legislation. Furthermore, the controller stated that an employee's personal data may also be processed for the purpose of assessing their ability to work. The data was only processed by individuals who required the data for performing their duties. Furthermore, the controller stated that access to employees' health information is restricted to individuals tasked with preparing, making or implementing decisions affecting employees.

9. According to the controller, it keeps sick leave certificates for as long as they are required by the rights and obligations related to employment contracts. According to the reply issued by the controller, the data is erased when no longer required. According to the reply, [redacted] is not in possession of the complainant's sick leave certificate copies for a period of 17 years. The controller stated that it has collected the complainant's data from the employer's electronic system in which the information on the employee's sick leave periods has been saved. The reply again refers to points (b), (f) and (h) of Article 9(2) of the GDPR.

Office of the Data Protection Ombudsman's request for information

10. The Office of the Data Protection Ombudsman has asked the controller for information on this matter. The controller replied to the request on 31 January 2022.

[redacted]'s data files containing employee health information

11. The information provided by [redacted] confirms that it has maintained two data files intended for internal use (the MAPS human resources management system and Medakt patient record system), which have contained employees' health information, among other things.

12. [redacted] has said that MAPS is its HR management system used to manage employment contracts and fulfil the employer's obligations, such as salary payment.

13. Medak, on the other hand, is said to be an electronic patient record system used on [redacted]'s vessels, into which the nurses licensed by the National Supervisory Authority for Welfare and Health (Valvira) and working on board record the procedures performed on patients and the medicines administered to them, as required under section 12, subsection 1 of the Act on the Status and Rights of Patients (785/1992). Patients can include both passengers and crew members who have fallen ill during the voyage. Employee health information is recorded in the Medakt patient record system if the employee falls ill while on board the vessel and cannot use onshore occupational health care services.

Data content of the data files used by [redacted]

14. The MAPS system contains the personal data of approximately 6,000 data subjects. Some of these data subjects are current employees of [redacted] and some are former employees. All vessels considered, the Medakt system contained the personal data of approximately 19,350 patients (5,600 employees and 13,750 passengers) at the beginning of 2022.

15. Employment-related information, such as the names and contact details of employees, employment contract status, qualifications, completed training, as well as information concerning salary payment and health care costs, have been stored in the MAPS system. According to chapter 2, section 12 of the Seafarers' Employment Contracts Act (756/2011), the employer has an obligation to pay for the treatment of sick employees and compensate them for the travel costs of getting home from the vessel.

16. The MAPS system has also contained employee absence data, including data on absences due to illness with dates and ICD diagnosis codes, which are used to determine whether the employee is entitled to pay during their absence. [redacted] further stated that not all absences are paid, which is why the employer needs to process data on the reasons for absences due to illness to a certain extent in order to ensure accurate salary payment. In addition to the codes, the diagnoses have been recorded in the system in plain text. However, according to the information provided by the controller, both ICD and plain-text diagnoses were erased from the system in 2018–2019. The system no longer contains such information. At present, only the information that an employee has been absent due to an illness and

whether the absence was paid or unpaid or, for example, family leave, is recorded in the system. [redacted] has assessed that, taking into account the purpose of the system, it is not necessary to record diagnoses in it.

17. The controller has stated the processing described above is based on the provisions of Article 6(1), points (c) and (f) of the GDPR (controller's legal obligation and controller's legitimate interest). The employer's statutory obligations, such as salary payment during illness, are said to be based on either the Seafarers' Employment Contracts Act or the Employment Contracts Act, depending on the employee's position.

18. The employees' dates of birth, names and addresses, as well as employment information such as vessel and rank, have been saved in the Medakt system. According to the information given, personal profiles are not created in the system for passengers as they are for employees. The identifying information of passengers, such as the name and date of birth, are instead saved in a text typed in connection with each appointment. Information on the cause and time of treatment, procedures performed and medicines dispensed from the ship pharmacy are also recorded in the system. According to the information provided, only nurses working on board the vessel make entries in the Medakt system, and only they have access to these entries.

19. The controller has stated that health information is processed by virtue of Article 9(2)(h) and Article 9(3) of the GDPR. Furthermore, the controller's reply also referred to section 6, subsection 1, paragraph 4 of the Data Protection Act (1050/2018), according to which Article 9(1) of the General Data Protection Regulation does not apply when a healthcare service provider in the course of arranging or providing services processes data it has received in the context of these activities on the state of health or disability of the person or on the healthcare and rehabilitation services received by a person, or other data necessary for the treatment of the data subject. The controller has also referred to the legislative materials of the Data Protection Act. According to the controller, the legislative materials state that "service provider" is a general concept that covers both the organiser and provider of a service. According to the controller, these include health care and social welfare units and professionals as well as auxiliary personnel working under them. Therefore, the nurses working on ships are said to process health information by virtue of the derogation referred to above.

20. The reply also refers to the Act on Ships' Medical Stores (584/2015). According to the controller, crew health care and the obligation to record the procedures performed are based on the above-mentioned enactment. The purpose of the Act on Ships' Medical Stores is to ensure that members of a ship's crew have the possibility to receive appropriate first aid and medical care on board the vessel in case of illness or injury. According to section 9 of the Act, vessels of certain categories must have a medical journal regarding the operation of their medical store, in which the relevant personnel shall enter all acquisitions made to the medical store, any drugs dispensed to patients and all performed procedures, as well as drugs and medical supplies removed from the medical store. All personal data must be stored separately from the information regarding drugs and medical supplies. All medical journal entries shall be made in the working language of the

ship. The medical journal must be kept in such a way that the entered data remains intact and unchanged. The medical journal must be preserved for at least five years after the last entry. The medical journal must be kept with the ship's medical store. The provisions on the secrecy of patient record information laid down in the Act on the Status and Rights of Patients (785/1992) are applied to the secrecy of all information entered into the medical journal.

[redacted]'s operations and section 5 of the Act on the Protection of Privacy in Working Life (759/2004)

21. According to its reply to the request for information, the controller has processed employees' health information for the payment of sick pay or comparable benefits linked to the employee's health. When an employee has fallen ill while working on a ship, the ship's nurse has recorded this in the Medakt patient record system. If the illness led to sick leave, this was recorded in the MAPS system after the employee had delivered the sick leave certificate. Furthermore, the controller stated that the nurses serve as part of HR administration when accepting the employees' sick leave certificates. The employees can deliver the sick leave certificate to the ship's nurse or an onshore HR representative.

22. According to the information provided by [redacted], health information has only been processed by its employees tasked with preparing, making or implementing employment-related decisions based on such information. The controller has stated that such personnel is limited to two HR secretaries. The employer has specifically designated the processing of health information as part of these employees' duties. These individuals are under an obligation of secrecy both during and after their employment.

23. According to [redacted], it has stored employee health information saved into the MAPS system so that personnel such as payroll clerks have not had access to diagnoses or ICD codes. Payroll clerks have only had access to information on whether the absence was paid or not. The controller has also stated that it has erased unnecessary health information from the data file as required by section 5 of the Act on the Protection of Privacy in Working Life.

24. With regard to the Medakt system, [redacted] has stated that it has not processed the data saved into the system at all as an employer. According to [redacted], only the nurses working on ships have access to the system. The data stored in the system has not been disclosed to [redacted]'s HR administration, and HR employees do not have access to the system.

Access rights to the data files in question

25. According to the reply to the request for information, HR administration employees whose duties include the processing of data contained in the MAPS system have access to the system. Access rights have been restricted so that employees only have access to data required for the performance of their duties. The part of the system used by the HR administration has access to all data stored in the system but, according to the information provided by the controller, access to this data is

also restricted according to the needs of HR employees. The MAPS Sjölöner system is also used by ship's nurses.

26. MAPS Omborddata, on the other hand, is described as being used on board the company's vessels. Employees who use the system can only access the data of crew members working on the ship in question. Employees have limited access to this data. Supervisors do not have access to all information on their subordinates.

27. In addition to the above, ship's nurses have recorded sick leave and diagnosis information in the MAPS system if the employee fell ill while working on board or delivered their sick leave certificate to HR administration through the ship's nurse.

28. Nurses working on ships and performing duties arising from the Act on Ships' Medical Stores and the Act on the Status and Rights of Patients have had access to the Medakt system. According to the information provided by the controller, no other persons have had access to the system. The Medakt system is not connected to other patient information systems, such as the Kanta service. In other words, information is not conveyed to other health care operators from the Medakt system.

29. As a rule, every employee has their own profile in the Medakt system according to the information provided by the controller. Substitute health care workers on ships use Medakt with a ship-specific user ID. Substitutes have been instructed to sign their entries with their own names. However, the identity of an entry's author can also be determined later from the shift lists.

30. According to the information provided, ship's nurses have had access to the Medakt data of any [redacted] vessel since, like other crew members, nurses can work on different ships. The same nurse is not always on duty, so another nurse may have a justified need to continue a task started by a different nurse and use the data stored in the system to complete the task. However, nurses are only permitted to process data necessary for the patient's care. Only the administrators have rights to make changes in the system. Nurses are not administrators.

Informing the data subjects

31. The controller has stated that the matter at hand has shown that employees have not been sufficiently informed of the processing discussed herein. According to the reply to the request for information, this deficiency will be rectified as soon as possible. [redacted] will inform the data subjects as required by the GDPR.

Storage of data

32. According to the information provided, information on sick leaves and the right to pay is stored in the MAPS system for ten years from the end of the absence. Older sick leave and pay entitlement information has been erased. According to [redacted], all ICD codes and diagnoses have been erased from the MAPS system in 2018 and 2019, and such information is no longer being saved into the system. [redacted] is in the process of deploying a new system. The data storage periods will be revised in connection with the deployment.

33. At the moment, the data in the Medakt system is being stored for an indefinite period. According to the information provided, the health information is saved because it has been considered necessary for monitoring the employees' health. Information on an employee's injuries or health problems can be needed later, for example for the processing of insurance cases or occupational disease surveys. The Medakt system contains information from 2012 onwards. The storage periods will be reassessed in 2022.

Accuracy of the data recorded in the file

34. Data subjects have had the right to review data saved in the MAPS and Medakt systems. The data has also been updated when necessary. The nurses making entries in the Medakt system have been responsible for the accuracy of their entries.

Securing the data files

35. [redacted]'s internal network is protected with safeguards such as a firewall and passwords. Shipboard users log into the MAPS system with task-specific usernames and passwords. Working hours are logged with personal usernames and passwords. HR administration employees have personal usernames and passwords to the MAPS system. As described above, access rights have been restricted to the information needed by employees in the performance of their duties. Only changes saved into the system are stored in the log of the MAPS system. The identity of the author of the original entry is not saved into the log.

36. The Medakt system can only be accessed from the nurse's work computer in the medical cabin. The login process has three stages. In the first stage, the nurse has to log into the Citrix service with their personal username and password. In the second stage, a one-time password is sent to the nurse by email. The Medakt system can then be launched through Citrix. After that, the user still needs to enter their personal username and password to log into the Medakt system. It has also been established that the nurses are aware that they only have the right to access the records of patients who they are actually treating. The system is not connected to any other health care information systems.

The entries involving the complainant

37. During the investigation of this matter, it turned out that it was not possible to save all ICD codes into the MAPS system in 2001. In other words, only a portion of the codes was used. It has thus been possible that absences due to illness may have been saved into the system with different codes than those in the actual diagnosis based on which the sick leave was granted. It is said that the system's users have sought to determine the closest corresponding code that could be entered into the system. In this regard, [redacted] has admitted that the system has been problematic in terms of data protection. The system has since been modified in this regard.

38. The complainant has alleged that the ICD code entered into the MAPS system for an absence due to illness granted in 2016–2017 does not correspond to the code on the sick leave certificate. In this regard, the controller has referred to the request for information addressed to the controller by the complainant on 3 February 2020, which was delivered with four enclosed sick leave certificates for the period in question. The controller has stated that the absence due to illness begun with one code, which was later changed to a different one. According to the information provided by [redacted], it does not, as a rule, change codes retrospectively. In this case it is nevertheless possible that the code was changed, for example at the complainant's request, to correspond to the code of the new period of sick leave. The ICD code saved into the MAPS system corresponds to three of the four codes on the sick leave certificate delivered to [redacted]. [redacted] has stressed that the nurses can also make entries into the system on the request of employees.

39. Furthermore, the reply to the request for information emphasises that [redacted] has had no interest, either as a controller or an employer, to modify the entries in the data file retrospectively unless prompted to do so by the data subject. [redacted] has also stressed that it does not record diagnoses in the system at all any more.

40. In addition, the controller has stated that signed entries saved into the Medakt system can only be edited immediately after saving. Edited entries are marked with a special symbol. All earlier versions of the entry will remain visible regardless of the edit and cannot be erased from the Medakt system. Entries made by another person cannot be edited at all, nor can entries made in the past. The date and time of an entry can be changed, but the actual time stamp will also remain visible regardless of the change.

Use and disclosure of data in the file

41. The data recorded in the MAPS system has been used for HR management, such as salary payment and the verification of its accuracy. As described above, the Medakt system is an electronic patient record system used on [redacted]'s vessels. According to the information provided, data from the files has not been used for purposes other than the original purpose of processing.

42. Regardless of the above, [redacted] has stated that the complainant's health information has been disclosed to the police for the investigation of a criminal matter. According to [redacted]'s response, this was not a correct course of action. The controller continued by stating that, in a pre-trial investigation, a physician or other health professional can be obliged to testify on secret patient information, for example in case of an offence for which the maximum sentence is at least six years of imprisonment. However, the criminal matter referred to herein did not involve such an offence. The controller continues by stating that the information should not have been disclosed for the criminal investigation without the patient's specific written consent.

The complainant's right of access to data

43. According to the information provided by [redacted], the information on the complainant's sick leave certificates was given to the complainant insofar as it was available. The oldest information had already been erased.

44. The response to the request for information referred to the Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (159/2007) repealed on 1 November 2021. According to section 18 of the said Act, a client has, for the purposes of determining or exercising the client's rights related to the processing of their client information, the right to be informed by the social welfare or health care service provider of who has used or received information concerning the client, as well as the basis for such use or disclosure. Such information shall be based on log register data and provided free of charge and without delay upon written request.

45. The controller has proposed that the obligation to disclose log data would apply to health care service providers, meaning health care units referred to in section 2, subsection 1, paragraph 4 of the Act on the Status and Rights of Patients, employers referred to in section 7, subsection 1, paragraph 2 of the Occupational Health Care Act (1383/2001), as well as self-employed health care professionals. The medical care of ship crews, including on the vessels of [redacted], is based on the Act on Ships' Medical Stores. The obligation to record procedures performed on patients is also based on the aforementioned Act. Since the Act on the Status and Rights of Patients does not refer to the Act on Ships' Medical Stores, [redacted] has interpreted the provision on the disclosure of log data to mean that it is not a health care service provider as referred to in the Act and has thus considered that it does not have the right to disclose log data. In addition, [redacted] has stated that the log data concern the users of information systems and cannot thus be disclosed to the subject of processing by virtue of the GDPR alone. Finally, the controller has stated that it has contacted the National Supervisory Authority for Welfare and Health (Valvira) on several occasions to obtain confirmation for its interpretation. According to the information provided by the controller, however, it has not received a reply from Valvira.

Past and future measures

46. According to the information provided by [redacted], it is in the process of deploying a new HR information system, which will be better equipped to meet the requirements of data protection legislation than the old MAPS system. Data protection by design will be emphasised in the new system, for example by limiting storage times, improving the logging of processing data, and by requiring the secure processing of personal data. As the coronavirus pandemic has been especially hard on the tourism industry, including the business operations of [redacted], the development and deployment of this HR system has been delayed.

47. [redacted] has updated the data protection competence of its HR administration personnel through data protection training in 2020 and 2021. The company will continue investing in data protection training in the future as well. It will conduct a meticulous review of its HR data files in 2022. The purpose of this review is to ensure that the data files do not contain any old or unnecessary

information. The company's privacy statements and the data protection section in its intranet will be updated in this connection. Personnel will also be informed of the processing of their personal data before the end of 2022.

Applicant's response

48. [redacted]'s response was delivered to the complainant. After receiving the response, the complainant submitted a brief response to the controller and the Office of the Data Protection Ombudsman. In this email sent on 9 February 2022, the complainant alleged that the response issued by [redacted] contained several inaccuracies. The complainant stressed that she had addressed her request to access her data, sent on 10 January 2020, to a specifically named [redacted] employee since, according to the complainant, this named person had disclosed the complainant's diagnoses saved into the MAPS system to the police from a period of 17 years. The complainant has likewise stressed that this specific person had not been designated as an official processor of health information by the shipping company. According to the complainant, it is unclear how this specific person had gained access to this data. The complainant stated that this person had not given the information to the complainant.

49. The complainant has referred to [redacted]'s response, which stated that the ICD codes and diagnoses saved into the MAPS system had been erased from the system in 2018–2019. This is not true according to the complainant. The complainant has said that she has received written information on her diagnoses in 2020 and is able to prove it.

50. According to the complainant, the claim that the data would only have been stored in the MAPS system for ten years is also incorrect. The complainant has referred to a copy of her diagnoses recorded in the MAPS system, given to her in 2020. She has also delivered this copy to the Office of the Data Protection Ombudsman. The copy shows that the first diagnosis recorded for the complainant dates to 1997. According to the complainant, the data has thus not been erased every ten years.

Supplement to response

51. [redacted] has supplemented its response on 10 February 2022. According to the supplement, the wrong year had been left in the response. The data was erased from the MAPS system in 2020, i.e. not in 2018–2019.

Applicant's response

52. The applicant was provided an opportunity to issue a response in the matter. The applicant issued her response proper on 22 February 2022.

53. The response claims that [redacted] has maintained an excessively comprehensive health information data file and neglected to inform the data subjects of the processing. In the complainant's opinion, the recording of diagnoses was illegal. Furthermore, data has been disclosed to third parties without a legal basis.

Data content of the data files used by [redacted]

54. As her opinion, the complainant has stated that the Medakt system is a patient information system to which the Act on Ships' Medical Stores only applies to a limited extent. The complainant has stated that only the ship's nurses and HR secretaries at the head office have access to the diagnoses. Furthermore, the complainant has expressed the opinion that a HR secretary should only have access to paper copies of medical certificates. If a nurse has both entered the diagnosis and specified whether the sick leave is paid or unpaid in the MAPS system, HR secretaries should have no reason to access the MAPS entries according to the complainant.

55. The complainant has also stated that the entries made into the Medakt system are not limited to cases of illness on board ships, but information such as the details of telephone conversations between the nurse and onshore employees is also entered into the system. Furthermore, according to the complainant, the names of prescription drugs prescribed by any physician on shore and the purchase price of the drugs are also entered into the system. According to the complainant, the shipping company normally compensates its employees for the purchase of such drugs. Compensation for medicines can be obtained for 112 days per illness, after which the employee is liable for their own medicine costs. The drug entries are no longer made after the above-mentioned time.

56. Employees are compensated for the purchase prices of prescription drugs against the receipt. The nurse delivers the receipt given by the employee to the HR secretary. The complainant has suggested that the HR secretaries can misuse the information obtained from the receipts and medical certificates. That is why, according to the complainant, some employees do not exercise their right to compensation for medicines.

57. According to the complainant, the entries made by nurses into the Medakt system normally include the nurse's name and the vessel on which the appointment took place. The complainant has suggested that even these entries are not always accurate. Entries have been known to be made for the wrong ship. At times, the name of the ship is missing from the entry altogether. According to the complainant, it is thus unclear which ship's medical store has been used. If an entry has been made for the wrong ship, that means that the medicine stocks of ships' medical stores cannot be in compliance with the Act on Ships' Medical Stores and/or ship-specific according to the complainant. The complainant states that this prevents keeping stock of medicines dispensed from ships' medical stores. Furthermore, the complainant has alleged that not all entries are related to the provisions of the Act on Ships' Medical Stores, but some of them involve health care on a more general level, such as discussions on work stress or workplace bullying (early intervention model).

58. The complainant has called into question [redacted]'s claim that only ship's nurses have access to the Medakt system. According to the complainant, the system also contains entries made by the representatives of private service providers (such as chiropractors / occupational health physicians who have occasionally visited the ship in port). According to the complainant, such individuals

have access to the information of many employees. The complainant has therefore stated as her opinion that the Act on Ships' Medical Stores does not apply to Medakt entries with regard to granting access to log data. According to the complainant, the system involves more than just offshore procedures or medicines dispensed from the ship's medical store.

[redacted]'s operations and section 5 of the Act on the Protection of Privacy in Working Life (759/2004)

59. The complainant has suggested that employees have only been instructed to deliver their sick leave certificates to the nurses and not to HR representatives. The nurse records the diagnosis into the MAPS system and sends the sick leave certificate to the designated person in HR administration. The complainant continued by stating that the employer has the right to make a copy of this original paper sick leave certificate, keep it apart from other personal data and destroy it as unnecessary in five years at the latest.

Access rights to the data files in question

60. The complainant has suggested that no payroll clerk or head of function has the right to access information on medical diagnoses. Such information is not used in payroll accounting. The nurse makes the necessary entries into the MAPS system.

Data entered into the data files

61. The complainant has alleged that the 60-day sick leave rules is being misused in the MAPS system. According to the complainant, if an employee is on sick leave for their ten-day work period, healthy for the following ten-day period and again ill for their next ten-day work period, [redacted] considers that the employee has also been ill during their free time, even if there is no sick leave certificate for this period of free time. The complainant has alleged that such interpretations have also been applied to situations in which an employee has been on sick leave before their annual holiday and again immediately after their holiday. The complainant suspects that, in such situations, the Finnish Social Insurance Institution (KELA) has not been notified that the employee was well between their sick leaves, with the result that the shipping company has probably also received unjustified compensations from KELA according to the complainant.

62. The complainant has stated that, by acting as described above, the shipping company is able to accumulate 60 days of sick leave as soon as possible, therefore also avoiding a new nine-day qualifying period for further compensations.

63. The complainant has alleged that the Medakt system's administrator is one of the ship's nurses. According to the complainant, this means that it has been possible to edit and erase entries. The complainant has also alleged that every nurse has been able to edit the diagnoses recorded in the MAPS system at any time and in any way.

Informing the data subjects

64. According to the complainant, the employees have not been informed of the extensive data files described herein, so the employees have not been able to, for example, check or request the correction of their data either. No information or instructions related to the controller's processing of its employees' personal data has been available on the company intranet.

65. According to the complainant, the nurses have been unsure of what to do when an employee has requested access to their data. According to the HR manager, such requests should be addressed to the HR manager. The complainant has called this into question, since the HR manager does not have access to data files containing health information. The complainant continued by stating that an employee may not want a certain named employee to even know that they have visited a nurse. In this connection, the complainant referred to the Act on the Status and Rights of Patients, claiming that information about such appointments is not intended for this specific individual. According to the complainant, this person has not been designated as a processor of health information.

Storage of data

66. The complainant again stressed that the claimed ten-year storage period is not true. According to the complainant, data has verifiably been stored for over 20 years. The complainant's diagnose list was printed out on 6 February 2020 and contained information on diagnoses from 1997. The complainant has said that an ex-employee had asked a ship's nurse for their data stored in the MAPS system on 10 February 2022. The nurse delivered the information to this employee on the same day. The data contained information on this person's sick leaves for the period 1990–2013. This person had not worked for the shipping company since 2013, but information on their sick leave was still being stored in the data file. At that time, the data had been stored for 32 years. According to the complainant, such storage can hardly have a purpose related to the payment of salary and benefits.

The entries involving the complainant

67. The complainant has stated that she has never requested that her diagnosis information be changed.

Use and disclosure of data in the file

68. The complainant has alleged that data in both the Medakt and MAPS systems have been used for purposes other than the purpose for which it was originally collected. According to the complainant, data has been obtained by subterfuge and disclosed to third parties, among other things. As an example, the complainant has stated the judgment of the Labour Court in matter R 24/18, issued on 19 December 2019. According to the complainant, the matter was about an employee's health information from 2006 being used against the employee in the Labour Court in 2019. The employee's employment contract had ended in 2006, continued in 2013 and ended again in 2016. According to the complainant, this proves that [redacted] stores quite extensive data on its former employees and, when necessary, also uses such data against the employees later.

69. According to the complainant, a certain nurse on the M/S Amorella named by the complainant violated their secrecy obligation in 2017 and disclosed the complainant's health information to a HR manager named by the complainant and to the controller's lawyer and chief operating officer; the same trio that eventually dismissed the complainant.

The complainant's right of access to data

70. Since the diagnoses had not been erased in 2018–2019, they could have been delivered to the complainant in response to her request made on 10 January 2020. The complainant only received information about her sick leave certificates for 2016–2017.

71. In this connection, the complainant has referred to the Act on Ships' Medical Stores and noted that the Act is principally related to medicines. Nurses licensed by the National Supervisory Authority for Welfare and Health hold appointments at the ship's medical store. These nurses are required to comply with the Act on the Status and Rights of Patients. Not all visits to a nurse are related to medicines, and not all entries are related to the sea voyage.

Conclusion

72. According to the complainant, she has also worked on the [redacted], which sails under the Estonian flag.

Hearing

73. On 29 August 2022, [redacted] was provided with an opportunity to express an opinion on the matter and to submit an explanation of claims and of evidence which may influence the decision, as referred to in section 34 of the Administrative Procedure Act (434/2003). At the same time, [redacted] was provided with an opportunity to raise considerations referred to in Article 83(2) of the GDPR that should, in its opinion, be taken into account in the decision. [redacted] issued its response on 13 September 2022.

74. The response issued for the hearing noted that it does not address claims based on other legislation than the GDPR.

The nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them

75. The response issued claimed that, in the matter at hand, the personal data was not used for the supervision or assessment of the data subjects, nor were negative decisions affecting the data subjects made based on the data. Furthermore, the response claimed that health information was collected for salary payment during sick leave, and data has not been used for other purposes or disclosed to third parties without justification. Therefore, [redacted] maintains that the purpose of the data processing was in line with the original purpose for which the

personal data was collected and with the controller's role as employer. According to the response issued, the data has never been used for other purposes.

76. Furthermore, the response maintains that the system has only been used on ships sailing under the Finnish flag, and that the system has only been used to store the data of individuals employed by [redacted]. [redacted] has thus considered that the processing under review has not been geographically extensive, even though the company operates in the territories of several states due to its passenger ship operations.

77. Furthermore, it is maintained that, with regard to the diagnoses, the response to the complainant's request to access her data and the challenges in complying with the deadline only involved this individual complainant and did not reflect the company's general practices.

78. The response stressed that the processing referred to in the matter at hand did not give rise to discrimination against the data subjects, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation or any other significant economic or social disadvantage to the data subjects. It has been specifically stated that a matter indirectly related to the matter now instituted by the complainant has also been heard in court and, according to the response issued, the court found [redacted] not guilty of discrimination.

The intentional or negligent character of the infringement

79. The infringement concerning the processing of personal data assessed herein, especially with regard to the personal data processed in the MAPS system, cannot be considered intentional according to the response, as the response maintains that intentionality requires the knowing and intentional infringement of the GDPR as well as heedlessness of the obligations imposed by legislation. According to the response issued, the matter at hand has involved none of the above, nor has [redacted] sought to achieve financial or other advantages over its competitors in this regard. Furthermore, it has been maintained that [redacted] has not actively and knowingly decided to, for example, store inaccurate personal data in a personnel data file. According to the response, the company also sought to respond to the request for information as promptly as possible.

80. According to the response, the situation was rather equivalent to human error, as a result of which the system containing the personal data had not been updated to correspond to legislative storage requirements with regard to its content and storage times. The controlled was not aware of the retention of old data and its possible inaccuracy until pointed out by the complainant. When [redacted] became aware of this state of affairs, it began looking into the matter and changed its practices.

Action taken by the controller or processor to mitigate the damage suffered by data subjects

81. When [redacted] had become aware that the health information of its employees had been retained for too long and the data file may also have contained inaccurate data, it reassessed the necessity of the data processed by the company and erased data that was not necessary with regard to the employment relationship. The company conducted an overall assessment of the matter and changed its practices with regard to all employees, not just the data subject who filed the complaint.

82. In addition, the response stressed that the implementation of the complainant's request to access her data was delayed because the company sought to deliver the data containing health information, which the complainant had specifically asked for, to the complainant as securely as possible by email. However, for various reasons due to the complainant herself, the complainant had not registered herself in the service that could have been used to verify her identity. The purpose of this authentication procedure was to avoid the unlawful disclosure of health information to a third party. The complainant and [redacted] had engaged in protracted email correspondence before the disclosure of the data (5 March 2020: [redacted] receives the complainant's request to exercise her right of access; 5 March 2020: [redacted] sends a link to the complainant's email address via an authentication service, which the complainant can use to identify herself and confirm her contact details with her online banking codes; 5 March 2020: the complainant notifies [redacted]'s representative that she cannot find the link sent; 9 March 2020: [redacted]'s replies to the complainant, indicating the name of the sender contained in the email; 9 March 2020: the complainant asks for the link to be resent; 25 March 2020: the complainant again asks for the link to be resent; and 26 March 2020: [redacted] resends the link to the authentication service to the complainant's email address). In other words, [redacted] had sought to deliver the information requested by the complainant to her in a secure manner via encrypted email. The information could certainly have been delivered quicker but, according to [redacted], that would have required compromising on data security, which the company did not consider to be an option according to its response.

83. [redacted] considers that it has done its best to comply with the deadline provided for in Article 12(3) of the GDPR and, therefore, also the provisions of Article 15(1) of the GDPR. [redacted] has admitted to an error regarding the data in the file for the year 1997, because it had not delivered this data to the complainant.

84. [redacted] also considers that it has actively sought to resolve the matter at hand in cooperation with various authorities, such as the Data Protection Ombudsman, the police and Valvira.

<u>The degree of responsibility of the processor or controller taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32</u>

85. According to its response, [redacted] has sought to take into account the requirement of data protection by design and by default, provided for in Article 25 of the GDPR, as well as the appropriate technical and organisational measures

required by Article 32, in order to process the personal data as securely as possible. Access to the personal data in question has been restricted to individuals with duties directly related to the data and for the performance of whose duties the data is necessary. The processing of employees' health information has been restricted as referred to in section 5 of the Data Protection Act, i.e. access rights management has been used to ensure that the data is only processed by individuals entitled to do so. Other individuals have not been granted access rights to the systems in question. Also according to the response, the principle of integrity and confidentiality has been implemented by logging events in the information systems, for example The measures safeguarding the systems against external misuse have also been bolstered.

Any relevant previous infringements by the controller or processor

86. According to its response, [redacted] has not been guilty of any relevant previous infringements, nor have the data protection authorities taken any measures referred to in Article 58(2) against it.

The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

87. Also according to its response, [redacted] has both sought to resolve the matter with the authority and promoted the deployment of a new system to house the personal data of its employees. The problems of the old system have been taken into account in the specifications of the replacement system. [redacted] has repeatedly attempted to obtain an opinion on the issue of the log data of the system used on its ships from the authorities, but has not received a reply.

88. In the matter at hand, [redacted] has complied with the deadlines set by the authority and replied to questions as openly and concisely as possible with a view towards resolving this complaint as efficiently as possible from the authority's perspective.

Conclusion

89. [redacted] has stressed that it has not obtained any indirect or direct financial advantage from the events under investigation. According to the company's response, [redacted] is more likely to incur financial losses from the incident due to reputation damage.

90. The total turnover of [redacted] was EUR 258,243,347.47 in 2021. In this context, the company stressed that the tourism industry suffered badly from the consequences of the coronavirus pandemic. The authority was requested to take the above into consideration when deciding on sanctions.

91. Finally, [redacted]'s response maintained that an administrative fine should not be imposed for conduct that may have been in violation of the provisions of the Act on the Protection of Privacy in Working Life or other legislation apart from the General Data Protection Regulation, nor should considerations based on such other legislation be taken into account as grounds for increasing the administrative fine.

Assessment of cross-border processing

92. The GDPR contains specific provisions on the processing of matters with a cross-border dimension as defined in Article 4(23). Such matters must be processed by a competent supervisory authority as provided for in Article 56 and Chapter VII of the GDPR.

93. In its response, [redacted] has announced that it is the controller with regard to the processing discussed herein. [redacted]'s head office is in Finland, and the Group also includes [redacted] and [redacted] based in Sweden, [redacted] based in Estonia, [redacted] based in Germany, as well as [redacted] based in Finland. The operations of all of the aforementioned companies involve the processing of personal data. Their information systems can be accessed from ships. The ships sail on the territorial waters of Finland, Sweden and Estonia as well as on international waters. The group has ships sailing under the Finnish, Swedish and Estonian flags. The complainant has only worked on vessels sailing under the Finnish flag. The German office only employs one person, and the data files discussed herein are not used in Germany, nor is the data of the German employee processed in them.

94. [redacted]'s central administration is located in Finland. According to the company, decisions regarding the processing discussed herein are made at the offices of this central administration. Furthermore, [redacted] has stated that the central administration also has the power to implement decisions related to the processing discussed herein.

95. The Office of the Data Protection Ombudsman will deal with the matter in accordance with the procedure laid down in Article 60 of the GDPR in cooperation with the supervisory authorities of the participating Member States. In the present case, the concerned supervisory authorities (hereinafter also: “CSAs”) within the meaning of Article 4(22)(b) of the GDPR are the supervisory authorities of Sweden, Norway and Estonia, since the processing affects or is likely to significantly affect data subjects in these Member States.

96. The decision includes sections which are subject to the obligations and rules established in the Finnish national legislation following from Article 6(1)(c) of the GDPR. In accordance with Article 55(2) of the GDPR, the Office of the Data Protection Ombudsman is of the view that those sections are not subject to the cooperation mechanism established in Article 60 of the GDPR. Furthermore, the decision includes sections which are subject to the national legislation implementing Article 88 of the GDPR.

Proceedings in the cooperation mechanism

97. In accordance with Article 56 and Article 60(3) of the GDPR, the Office of the Data Protection Ombudsman as the lead supervisory authority, has 21 March 2022 provided relevant information on the matter to the CSAs while its position as lead supervisory authority was established.

98. The draft decisions of the Data Protection Ombudsman and the Collegial Body for Sanction has been submitted to the CSAs on 10 November 2022 in accordance with Article 60(3) of the GDPR.

99. The CSAs have not made any comments or objections to the draft decision. Accordingly, the draft decision has been approved.[1] The Office of the Data Protection Ombudsman adopts and notifies the decision to the main establishment of the controller. In addition to this the Office of the Data Protection Ombudsman will inform the complainant, the other supervisory authorities as well as the European Data Protection Board of the decision.[2]

Applicable law

100. The processing of personal data is provided for in Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, GDPR). The GDPR has been in force from 25 May 2018. As a regulation, the enactment is directly applicable legislation in the Member States. The rights of the data subject are provided for in Chapter III of the GDPR. The GDPR is specified by the Data Protection Act (1050/2018).

101. More detailed provisions on the processing of health information at the workplace are provided in sections 3 and 5 of the Act on the Protection of Privacy in Working Life (759/2004, Working Life Privacy Act). The storage and recording of patient information is provided for in section 12 of the Act on the Status and Rights of Patients (785/1992; Patient Act) and in the Decree of the Ministry of Social Affairs and Health on Patient Documents (298/2009; Patient Document Decree).

102. The Act on Ships' Medical Stores (584/2015) provides for measures intended to ensure the availability of appropriate first aid and medical care to ships' crews in the event of illness or accident on board.

103. The work of health care professionals is provided for in the Act on Health Care Professionals (559/1994). The Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (784/2021, Client Data Act) provides for the secure processing of client data generated by the social welfare and health care services and welfare data generated by the clients themselves for the purpose of the arrangement and provision of health care and social welfare services. The previous version of the aforementioned Act (159/2007, repealed on 1 November 2021) also has significance in this matter.

Legal question

104. As referred to above, the Deputy Data Protection Ombudsman assesses and decides on the applicant's matter based on the General Data Protection Regulation (EU) 2016/679 and the aforementioned special enactments. The matter involves the following legal questions:

[1] Article 60(6) of the GDPR.
[2] Article 60(7) of the GDPR.

i. Has [redacted] complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when saving diagnoses into the MAPS system?

ii. Has [redacted] complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when storing data concerning the health of its employees?

iii. Has [redacted] taken every reasonable step in accordance with Article 5(1)(d) and Article 25(1) of the GDPR to ensure that the employee health data processed by it is accurate and up to date?

iv. Has [redacted] provided the data subjects with the information provided for in Article 13 of the GDPR when it has obtained personal data from the data subjects?

v. Has [redacted] complied with the provisions of Article 5(1)(b) of the GDPR when disclosing the complainant's personal data to the police?

vi. Has [redacted] fulfilled the applicant's right of access as provided for in Article 12(3) and Article 15 of the GDPR?

vii. Should the controller be ordered to comply with the complainant's request to access the data in the user log under Article 58(2)(c) of the GDPR?

Decision of the Deputy Data Protection Ombudsman

Decision

105. The Deputy Data Protection Ombudsman finds that [redacted] has not complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when saving diagnoses into the MAPS system.

106. The Deputy Data Protection Ombudsman finds that [redacted] has not complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when storing its employees' health information in the MAPS system.

107. The Deputy Data Protection Ombudsman finds that there was a basis for processing patient information.

108. The Deputy Data Protection Ombudsman finds that [redacted] has not taken every reasonable step under Article 5(1)(d) and Article 25(1) of the GDPR in order to ensure that the personal data processed in the MAPS system is accurate and up to date.

109. The Deputy Data Protection Ombudsman finds that [redacted] has not complied with the provisions of Article 5(1)(a) and Article 13 of the GDPR.

110. The Deputy Data Protection Ombudsman does not consider themself competent to assess the existence of possible grounds for disclosure of data to the police more extensively than described in the grounds for this decision.

111. The Deputy Data Protection Ombudsman finds that [redacted] has not complied with the provisions of Article 12(3) of the GDPR when replying to the complainant's request made pursuant to Article 15 of the GDPR.

112. The Deputy Data Protection Ombudsman finds that [redacted] has not complied with the provisions of Article 15(1) of the GDPR when replying to the complainant's request made pursuant to Article 15 of the GDPR.

113. The Deputy Data Protection Ombudsman does not issue an order to comply with the complainant’s request for access to the user log data.

Order

114. The Deputy Data Protection Ombudsman orders the controller to bring its practices for informing the data subjects into compliance with the provisions of the GDPR under Article 58(2)(d) of the GDPR.

Notes

115. The Deputy Data Protection Ombudsman reprimands [redacted] under Article 58(2)(b) of the GDPR. The Deputy Data Protection Ombudsman points out that the measures taken by the controller to fulfil the rights of the complainant are not complied with the provisions of Article 12(3) of the GDPR, nor has the controller fulfilled the complainant's request to access her data pursuant to Article 15 of the GDPR. With regard to the accuracy of the data, the controller has not complied with the provisions of Article 5(1)(d) and Article 25(1) of the GDPR. Furthermore, the controller has neglected its duty to inform the data subjects of its processing.

116. The Deputy Data Protection Ombudsman also points out that the controller has not complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when processing its employees' health information. The Deputy Data Protection Ombudsman notes that the controller's conduct has been particularly reprehensible in this respect. Not only has the processing violated the provision of the aforementioned enactment, but it has also been quite extensive, and the processing cannot be said to have been short in duration. Furthermore, taking into account the subordinate position of the employees with regard to the employer, the processing can be considered to have caused an especially high risk.

Grounds

Processing of employees' health information at the workplace

Facts of the matter

117. According to the response issued in this matter, [redacted] has maintained a HR system (MAPS), which has been used to manage employment contracts and perform the employer's obligations. Information related to the employment contract, such as the names and contact details of employees, employment contract status information, qualifications, completed training, as well as information concerning salary payment and health care costs, have been stored in the MAPS system. The MAPS system has also contained information on employee absences, including absences due to illness, complete with dates and ICD diagnosis codes. In addition to the codes, the diagnoses have been recorded in the system in plain text. However, according to the supplement to [redacted]'s response, the ICD codes and plain-text diagnoses have been erased from the system in 2020. Such information is no longer contained in the system. At present, only the information that an employee has been absent due to an illness and whether the absence was paid or unpaid or, for example, family leave, is recorded in the system.

Legal evaluation

118. Section 5 of the Working Life Privacy Act provides for the employer's right to process data concerning the health of employees. The employer has the right to process data concerning the employee's health status if the data has been collected from the employee themselves, or elsewhere with the employee's written consent, and the data needs to be processed in order to pay sick pay or other comparable health-related benefits or to establish whether there is a justified reason for absence or if the employee expressly wishes their working capacity to be assessed on the basis of data concerning their health. In addition, the employer has the right to process such data in the specific circumstances and to the stipulated extent separately provided elsewhere in the law. The legislative materials of the enactment preceding the Working Life Privacy Act (Act on the Protection of Privacy in Working Life (477/2001))3 specifically state that the employer has the right to process health information, e.g. medical certificates or statements and the diagnoses given in them, with the employee's consent for the purpose of assessing absences due to illness.4

119. Regardless of the employee's consent, the employer is bound by the necessity requirement provided for in section 3 of the Working Life Privacy Act. The employer is only allowed to process personal data directly necessary for the employee's employment relationship, which is connected with managing the rights and obligations of the parties to the employment relationship or with the benefits provided by the employer for the employee or which arises from the special nature of the work concerned. No exceptions can be made to the necessity requirement, even with the employee's consent.

120. It should be noted that sick pay practices are frequently based on the provisions of collective agreements. As a rule, such agreements require the employee to deliver a medical certificate with diagnosis information to their employer. In practice, in the case of a recurring illness, the salary payment

[3] HE 75/2000 vp, p. 17
[4] HE 75/2000 vp, p. 24

obligation is often affected by whether the illness is new or a relapse of an existing condition. The provisions on sick pay have accordingly been interpreted to mean that the medical certificate delivered to the employer must include the medical definition of the disease, i.e. the diagnosis. In practice, this means that the employer determines whether the employee's illness entitles them to sick pay.

121. According to section 5, subsection 4 of the Working Life Privacy Act, the employer must store any data in its possession concerning the employee's health separately from any other personal data it has collected. This means that health entries must not be saved into the employer's other personal data files, such as payroll administration registers.

122. The Deputy Data Protection Ombudsman finds that the employer nevertheless has the right to process, for example in its HR systems, data concerning the dates and lengths of an employee's absence from work due to sick leave (acceptable reason, payment of sick pay). However, information on the causes of the absence due to illness, such as the disease or injury or its nature or diagnosis, may not be saved into HR systems. The medical certificates or statements delivered to the employer by the employee must be stored separately from other personal data concerning the employee. Such data may only be processed to the extent and for the purposes provided for in section 5 of the Working Life Privacy Act. Such purposes are usually specific and as well as different for each absence due to illness. In other words, the provisions of the Working Life Privacy Act do not permit or entitle the employer to keep separate health data files on its employees for the purpose of collecting and storing employee health data, such as diagnoses.

123. Based on the above, the Deputy Data Protection Ombudsman finds that the controller has not complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when saving diagnosis information into the MAPS system. Since the diagnoses have since been erased from the MAPS system, the Deputy Data Protection Ombudsman does not issue an order to [redacted] in this regard.

Storage of employee health information

Facts of the matter

124. The complainant has maintained that [redacted] has stored her health information (including diagnoses) in the MAPS system for 20 years.

125. According to [redacted]'s response, it has maintained two data files for internal use (the MAPS HR management system and the Medakt patient record system), which have contained employees' health information, among other things.

126. [redacted] has said that MAPS is its HR management system used to manage employment contracts and fulfil the employer's obligations, such as salary payment. The Medakt system, on the other hand, has been described by [redacted] as an electronic patient record system used on its vessels, into

which the ship's nurses licensed by the National Supervisory Authority for Welfare and Health (Valvira) record the procedures performed on patients and the medicines dispensed to them, as required by section 12, subsection 1 of the Act on the Status and Rights of Patients (785/1992). Patients can include both passengers and crew members who have fallen ill during the voyage.

127. [redacted]'s response maintains that sick leave certificates are stored for as long as required for fulfilling the rights and performing the obligations related to the employment relationship. The response also stated that information on absences due to illness and the right to pay is stored in the MAPS system for ten years from the end of the absence. According to the controller, all ICD codes and diagnoses were erased from the MAPS system in 2020.

128. At the moment, the data in the Medakt system is being stored for an indefinite period. According to the information provided, the health information is saved because it has been considered necessary for monitoring the employees' health. Information on an employee's injuries or health problems can be needed later, for example for the processing of insurance cases or occupational disease surveys. The Medakt system contains information from 2012.

Legal evaluation

129. As provided for in section 5, subsection 4 of the Working Life Privacy Act, data concerning health shall be erased immediately after the grounds for processing referred to in section 5, subsection 1 of the said Act have ceased to exist. As stated in the grounds under the previous legal question, the purposes of medical certificates or statements or other documents containing health information, delivered by an employee to the employer, are usually separate as well as specific to each individual absence due to illness. As a rule, the appropriate storage period for such data is thus comparatively short. As further provided in section 5, subsection 4 of the Working Life Privacy Act, the grounds and necessity of processing employee health information shall be evaluated at least every five years.

130. Section 9 of the Act on Ships' Medical Stores provides for the medical journal to be kept of ships' medical stores. According to the provision, all acquisitions made to the medical store, any drugs dispensed to patients and all performed procedures, as well as drugs and medical supplies removed from the medical store shall be entered in the medical journal. All personal data must be stored separately from the information regarding drugs and medical supplies. The medical journal must be preserved for at least five years after the last entry.

131. The Deputy Data Protection Ombudsman interprets the Act on Ships' Medical Stores to be a health and safety statute intended to improve medical care on board ships, rather than a statute on the processing of patient information as such. Section 1 of the Act on Ships' Medical Stores provides for the purpose of the Act. The purpose of the Act on Ships' Medical Stores is to ensure that members of a ship's crew have the possibility to receive appropriate first aid and medical care on board the vessel in case of illness or injury. Accordingly, the Act obliges the shipowner to ensure that the ship carries the drugs and medical supplies provided

for in the Act. Section 9 of the Act on Ships' Medical Stores also makes it possible to process personal data in medical journals. In addition, when treatment procedures are due to a transfer of duties performed by a health care professional as referred to in section 5, subsection 3 of the Act on Ships' Medical Stores, the obligation of a health care professional referred to in section 12 of the Act on the Status and Rights of Patients to prepare and retain patient documents as well as other provisions on the processing of patient records shall be taken into account.

132. Based on the above, the Deputy Data Protection Ombudsman finds that [redacted] has not presented any grounds by virtue of which the complainant's data could have been stored for 20 years in the MAPS system. Neither has [redacted] presented any justification for retaining the health information of its employees in the MAPS system for ten years from the end of the absence. The controller has not complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when storing health information on its employees in the MAPS system. Since the diagnoses have since been erased from the MAPS system, the Deputy Data Protection Ombudsman does not issue an order to [redacted] in this regard.

133. According to section 2, subsection 1, paragraph 1 of the Patient Act, the term 'patient' is used of a person who uses health care services or is otherwise an object of them. The legislative materials for the Act refer to an established interpretation of the Patient Injury Act, according to which 'health care and medical care' refers to procedures intended to determine an individual's state of health or to restore or maintain their health, performed by health care professionals or in a health care unit. 'Health care professional' refers to an individual operating based on a legal right or legally licensed by the Social Welfare and Health Administration (currently the National Supervisory Authority for Welfare and Health Valvira).5 More detailed provisions on health care professionals are laid down in the Act on Health Care Professionals. The legislative materials for the aforementioned Act also state that, in unclear cases, the nature and purpose of the operations and the training of the individual providing treatment can be used to determine whether the activity constitutes health care or medical care for the individual.6 In other words, treatment does not have to be provided in an actual health care unit to meet the definition of health care or medical care, provided that the treatment is provided by a health care professional.7 For example, health care or medical care provided by a health care professional in a social welfare unit and the services provided by pharmaceutical professionals in pharmacies fall under the scope of the Act.8

134. [redacted]'s response states that the nurses working on its ships are health care professionals licensed by the National Supervisory Authority for Welfare and Health (Valvira). Based on the above, the Deputy Data Protection Ombudsman finds that individuals making an appointment with a ship's nurse are

[5] HE 185/91 vp, p. 13.
[6] HE 185/91 vp, p. 13.
[7] HE 185/91 vp, p. 14.
[8] HE 185/91 vp, p. 14.

patients as referred to in the Patient Act, while the entries made by the nurses concerning such individuals are patient documents as referred to in the Patient Act.

135. With regard to the actual patient record entries made in the Medakt system, it is noted that the storage of patient information is provided for in the Patient Act and Patient Record Decree. According to section 2, subsection 1, paragraph 5 of the Patient Act, the term 'patient documents' means the documents or technical records used, drawn up or received when the treatment of the patient is arranged and carried out and which contain information on their state of health or otherwise personal information about the patient. According to section 12 of the Patient Act, health care professionals shall record in patient documents the information necessary for the arranging, planning, providing and monitoring of care and treatment for a patient. According to the provision, patient documents shall be stored for a period necessary for arranging and providing care and treatment for a patient, for investigating possible claims for compensation, and for scientific research. Patient documents shall be disposed of immediately after there are no grounds as referred to above for keeping them. Further provisions on keeping patient documents and their storage periods are laid down in the Patient Documents Decree. The storage periods are defined in the Annex to the Decree. As a rule, patient documents shall be kept for 12 years from the patient's death or, if no information on it is available, for 120 years from the patient's birth.

136. Keeping a medical journal and processing the personal data contained in it is based on section 9 of the Act on Ships' Medical Stores, which defines the information to be stored in the medical journal. Thus, there is a justification for the processing of personal data to be included in the medical journal. According to section 5 of the Act on Ships' Medical Stores, a ship must have the capability to provide first aid and medical care to those in need, among other things, and according to subsection 3 of the said section, responsibility for the administration of first aid and medical care, among other duties, can be assigned to a health care professional. In such cases, the health care professional is obliged to draw up patient document entries for the care or treatment provided as stipulated in section 12 of the Act on the Status and Rights of Patients. The controller has thus had a valid basis for processing patient information.

Data inaccuracy

Facts of the matter

137. The complainant has maintained that some of her information saved in the MAPS system has been partially inaccurate. The complainant has maintained that, for example the ICD code entered into the MAPS system for her sick leave granted at the turn of 2016–2017 does not correspond to the code on the sick leave certificate.

138. According to the controller's response, investigation of the matter revealed that not all ICD codes could be saved into the MAPS system in 2001. In other words, only a portion of the codes was used. It has thus been possible that absences due to illness may have been saved into the system with different codes than those in the actual diagnosis based on which the sick leave was granted. It is

said that the system's users have sought to determine the closest corresponding code that could be entered into the system.

Legal evaluation

139. Article 5 of the General Data Protection Regulation provides for the principles of processing personal data. According to Article 5(1)(d), personal data shall be accurate and, where necessary, kept up to date. The controller must take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

140. The data subject has the right to be assessed based on accurate data. Inaccurate personal data can cause a risk to the rights and freedoms of the data subject. Article 16 of the GDPR accordingly provides for the data subject's right to rectification. Data subjects have the right to demand from the controller the rectification of inaccurate personal data concerning them without undue delay. The purpose of this is to prevent the making of incorrect conclusions or decisions based on inaccurate or incomplete data. Inaccurate data means false data that does not correspond to the facts.

141. The provisions of Article 25(1) of the GDPR also have significance in this regard. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means of processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

142. The European Data Protection Board has issued practical guidelines9 on the data protection by design and by default referred to in Article 25 of the GDPR. Among other things, these guidelines describe key considerations regarding accuracy in data protection by design and by default. Such considerations mentioned in the guideline include the degree of accuracy, continued accuracy and data design. The controller shall use technical and organisational design features to decrease possible inaccuracy related to personal data, for example by presenting concise predetermined choices instead of free text fields.10

143. According to the controller's response, diagnose information was entered into the MAPS system with ICD codes. However, the MAPS system did not have

[9] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020.
[10] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, pp. 24–25.

all of the possible ICD codes available for selection, which has enabled incorrect diagnosis entries.

144. Based on the above, the Deputy Data Protection Ombudsman finds that the controller has not taken every reasonable step under Article 5(1)(d) and Article 25(1) of the GDPR to ensure the accuracy of the personal data processed in the MAPS system. Since diagnosis information is no longer being entered into the MAPS system, the Deputy Data Protection Ombudsman will not issue any orders to [redacted] concerning the infringement here established.

Informing the data subjects

Facts of the matter

145. According to the complainant, employees have not been informed in any way of the extensive data files discussed herein. No information or instructions related to the controller's processing of its employees' personal data has been available on the company intranet.

146. [redacted]'s response noted that investigation into the matter showed that employees have not been sufficiently informed of the processing discussed herein.

Legal evaluation

147. According to Article 5(1)(a) of the General Data Protection Regulation, personal data shall be processed in a transparent manner in relation to the data subject. Article 12 of the GDPR lays down more detailed provisions on transparency. The principle of transparency is strongly linked to Article 13 of the GDPR, which provides for the information to be provided to the data subject where personal data is collected from the data subject themselves.

148. It should be noted that the Article 29 Working Party has issued practical guidelines11 ('Transparency Guidelines') on the principle of transparency. These guidelines note that the transparency obligation applies to three central areas: 1) the provision of information to data subjects related to fair processing; 2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and 3) how data controllers facilitate the exercise by data subjects of their rights.

149. It should also be noted that the GDPR does not provide for the form in which the data should be provided or other details. However, the Regulation provides that the controller is obliged to implement ”appropriate measures” to provide the information required by transparency to the data subject.12 This means that the controller must take into account all circumstances of the collection and processing of the personal data when choosing an appropriate method and form

[11] Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018).
[12] See GDPR, Article 12(1).

for informing the data subjects. In particular, appropriate measures will need to be assessed in light of the product/ service user experience.13

150. The data subject should be informed of the scope and consequences of the processing in advance, so that the ways in which the personal data are used will not come as a surprise to the data subject later. This is also important in view of the principle of fairness referred to in Article 5(1) of the GDPR and is related to recital (39), according to which natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data.

151. In the case of personal data collected from the data subject themselves as referred to in Article 13 of the GDPR, the information listed in the Article must be provided to the data subject at the time when the data is obtained from the data subject.

152. Regarding the form in which the data is to be provided, it can be stated that, according to Article 13 of the GDPR, the controller shall ”provide the data subject with all of the following information […]”. The wording ”provide” is relevant here. This means that the data controller must take active steps to furnish the information in question to the data subject or to actively direct the data subject to the location of it.14

153. According to the complainant, the data subjects have not been informed in any way of the data files described herein. The controller has not denied this claim. The controller has admitted that the data subjects have not been informed adequately. The Deputy Data Protection Ombudsman thus finds that the controller has not complied with the provisions Article 5(1)(a) and Article 13 of the GDPR.

154. The Deputy Data Protection Ombudsman orders the controller to bring its practices for informing the data subjects into compliance with the provisions of the GDPR under Article 58(2)(d) of the GDPR.

Disclosure of personal data to the police

Facts of the matter

155. The data recorded in the MAPS system has been used for HR management, such as salary payment and the verification of its accuracy. The diagnosis information entered into the system was originally processed to determine the employee's eligibility for pay during their absence. However, [redacted] has since assessed that entering diagnoses into the system is not necessary in view of the purpose of the system. As described above, the Medakt system is an electronic patient record system used on [redacted]'s

13 Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018), p. 14.
14 Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018), p. 18.

vessels. According to the information provided, data from the files has not been used for purposes other than the original purpose of processing.

156. Regardless of the above, [redacted] has stated that the complainant's health information has been disclosed to the police for the investigation of a criminal matter. According to [redacted]'s response, this was not a correct course of action. The controller continued by stating that, in a pre-trial investigation, a physician or other health professional can be obliged to testify on secret patient information, for example in case of an offence for which the maximum sentence is at least six years of imprisonment. However, the criminal matter referred to herein did not involve such an offence. The controller continues by stating that the information should not have been disclosed for the criminal investigation without the patient's specific written consent.

Legal evaluation

157. According to Article 5(1)(b) of the General Data Protection Regulation, personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation'). Recital (50) of the GDPR likewise states that the processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected.

158. As stated in the grounds under the first legal question, the employer is, as such, entitled to also process diagnosis information related to its employees' absences due to illness. However, the purposes for such processing are separate as well as specific to each period of absence. The purpose of processing patient information, on the other hand, is related to the patient's treatment, while the purpose of processing the data in the medical journal is related to the duties provided for in the Act on Ships' Medical Stores.

159. According to section 14 of the Patient Act, punishment for breaching the secrecy obligation referred to in paragraph 2 and in point 5 of paragraph 3 of section 13, shall be imposed according to section 1 or 2 of chapter 38 of the Criminal Code, unless the offence is punishable under section 5 of chapter 40 of the Criminal Code, or unless a more severe punishment is prescribed for it elsewhere in the law. Since information on the complainant's diagnoses was later disclosed to the police, the Deputy Data Protection Ombudsman finds that the basis for the disclosure may be assessed as a criminal matter. The Deputy Data Protection Ombudsman thus does not consider themself competent to assess the existence of a possible basis for disclosure to any greater extent. The complainant may turn to the police in this matter.

Right of access

Facts of the matter

160. According to the complainant, she has requested access to her personal data from [redacted] at least on 10 January 2020 and 3 February 2020.

161. According to the information provided by [redacted], the information on the complainant's sick leave certificates was given to the complainant insofar as it was available. According to [redacted], it had already erased the oldest data. Copies of the remaining sick leave certificates were delivered to the complainant on 1 April 2020. Before this, the complainant's questions had been answered by email at least on 31 January 2020. Diagnosis information was not provided to the complainant in this connection.

162. However, in this respect, the complainant has referred to a copy of her diagnosis information entered into the MAPS system that she acquired in 2020 and delivered to the Office of the Data Protection Ombudsman. Since the diagnosis information had not actually been erased in 2018–2019, the complainant has stressed that this information could have been provided to her in response to her request made on 10 January 2020.

Legal evaluation

163. Article 15 of the General Data Protection Regulation provides for the data subject's right of access to data. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information specifically listed in the Article.

164. Furthermore, Article 12 of the GDPR provides for detailed rules regarding the exercise of the rights of the data subject. According to paragraph 3 of the Article, the controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. Furthermore, according to paragraph 4 of the Article, if the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

165. In the matter at hand, the complainant had not received the requested diagnosis information in response to her request made on 10 January 2020, even though [redacted] was still verifiably in possession of that information on 6 February 2020, when the complainant obtained it by other means.

166. The complainant filed her aforementioned requests in this matter on 10 January 2020 and 3 February 2020. Copies of the remaining sick leave certificates were delivered to the complainant in response to her requests on 1 April 2020. The complainant and the controller's representatives had engaged in email correspondence in the interim. In other words, the controller replied to the complainant's messages and requests within one month of the complainant's

aforementioned requests. However, the controller did not provide the complainant with the information she had requests within that time period. Neither had the controller given the complainant any reason for this delay in providing the information to her. As the controller did not provide the complainant with all of the information requested by her within one month of the complainant's aforementioned first request, the controller did not comply with the provisions of Article 12(3) of the GDPR when replying to a request made pursuant to Article 15 of the GDPR.

167. The complainant had specifically requested the diagnosis information saved into [redacted]'s systems from the company on several occasions. The controller can thus be considered to have been aware of the complainant's wish to access precisely that information. Regardless of the above, the information was not delivered to the complainant in an appropriate manner. Even though the complainant eventually gained access to the information through a nurse, [redacted]'s conduct in the matter cannot be considered appropriate. The diagnosis information was not delivered to the complainant in the same connection and through the same channel as the other information provided to her. On the contrary, the complainant was led to believe that there was no diagnosis information separately entered into the system. As the controller did not grant the complainant access to the diagnosis information entered into the system, the controller did not comply with the provisions of Article 15(1) of the GDPR when responding to the complainant's request made pursuant to Article 15 of the GDPR.

Right of access to log data

Facts of the matter at hand and information provided in the response

168. The complainant has requested access to the log data concerning the complainant's personal data from [redacted]. The complainant has not been given access to the log data.

169. The response to the request for information referred to the Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (159/2007) repealed on 1 November 2021. According to section 18 of the said Act, a client has, for the purposes of determining or exercising the client's rights related to the processing of their client information, the right to be informed by the social welfare or health care service provider of who has used or received information concerning the client, as well as the basis for such use or disclosure. Such information shall be based on log register data and provided free of charge and without delay upon written request.

170. The controller has proposed that the obligation to disclose log data would apply to health care service providers, meaning health care units referred to in section 2, subsection 1, paragraph 4 of the Act on the Status and Rights of Patients, employers referred to in section 7, subsection 1, paragraph 2 of the Occupational Health Care Act (1383/2001), as well as self-employed health care professionals. The medical care of ship crews, including on the vessels of [redacted], is based on the Act on Ships' Medical Stores. The obligation to enter procedures performed into the medical journal is based on the same Act. Since the Act on the Status and Rights of Patients does not refer to the Act on Ships' Medical Stores,

[redacted] has interpreted the provision on the disclosure of log data to mean that it is not a health care service provider as referred to in the Act and has thus considered that it does not have the right to disclose log data. In addition, [redacted] has stated that the log data concern the users of information systems and cannot thus be disclosed to the subject of processing by virtue of the GDPR alone.

Legal evaluation (General Data Protection Regulation)

171. Article 15 of the General Data Protection Regulation provides for the data subject's right of access to data. Data subjects have the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data as well as the information listed in the Article. In other words, a data subject has this 'right of access' to data concerning themselves.

172. According to the Data Protection Ombudsman's established decision-making practice, user log data does not concern customers, but the employees who have processed customer data. Therefore, the data subject's right of access to data has not been considered to apply to user log data. In the absence of special legislation, the right to access user log data has thus been restricted to the individuals who have processed personal data stored in the data file (see, for example, decision EOA 1433/4/05 of the Parliamentary Ombudsman, issued on 8 February 2007 and the Deputy Data Protection Ombudsman's decision in matter 7681/152/2018, issued on 4 August 2020). Notwithstanding the above, customers have had, by virtue of their right of access, the right to access their actual customer data and any entries included in such data.

173. As stated in the decision practice referred to above, log data has been considered to concern the employees who have processed the customer or register data. Therefore, log data has not been considered to constitute data concerning the data subject and has thus been excluded from the right of access provided for in the aforementioned Article 15. It must nevertheless be noted that the aforementioned Deputy Data Protection Ombudsman's decision 7681/152/2018 has been appealed in the Administrative Court of Eastern Finland, which has in turn requested a precedent on the matter from the Court of Justice of the European Union.

Legal evaluation (special legislation)

174. In addition to the right based on Article 15 of the GDPR, it is possible to obtain log data on the basis of the right of access laid down in other legislation. At the time of a request for log data, section 18 of the now-repealed Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (250/2014, repealed by Act 784/2021) laid down provisions on the patient’s right to obtain information from the provider of healthcare and social welfare services on who used or to whom the data concerning them has been disclosed and on the grounds for the use or disclosure. This was a special right of access to information separate from the right laid down in the GDPR. The Data Protection Ombudsman was not responsible for assessing this right of access to information under the repealed Act.

Although section 26, subsection 4 of the new Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (784/2021) stipulates this task, the provision only applies to requests made after its entry into force (November 1, 2021). Therefore, the Deputy Data Protection Ombudsman does not assess the fulfilment of this right of access to information in this case.

175. However, the Deputy Data Protection Ombudsman provides general guidance on the matter at the end of this decision.

Applicable legal provisions

As set out in the grounds.

Appeals

According to section 25 of the Data Protection Act (1050/2018), this decision may be appealed in the Administrative Court pursuant to the provisions of the Administrative Judicial Procedure Act (808/2019). The appellate court is the Administrative Court of Helsinki.

Instructions for appeal are appended.

Service of notice

Notice of this decision will be served by post against an acknowledgment of receipt pursuant to section 60 of the Administrative Procedure Act (434/2003).

Additional information on this decision is available from the referendary

[redacted], tel. [redacted].

Guidance by the Deputy Data Protection Ombudsman

The complainant has requested access to the log data concerning the complainant's personal data from [redacted]. At least the legislation listed below is relevant to this assessment.

The response issued by [redacted] maintained that the obligation to provide log data applies to health care service providers, meaning health care units referred to in section 2, subsection 1, paragraph 4 of the Act on the Status and Rights of Patients, employers referred to in section 7, subsection 1, paragraph 2 of the Occupational Health Care Act (1383/2001), as well as self-employed health care professionals. In the opinion of [redacted], on ships such as the vessels operated by [redacted], the medical care of the ship's crew is based on the Act on Ships' Medical Stores. The obligation to record procedures performed on patients is also based on the aforementioned Act. Since the Act on the Status and Rights of Patients does not refer to the Act on Ships' Medical Stores, [redacted] has interpreted the provision on the disclosure of log data to mean that it is not a health care service provider as referred to in the Act and has thus considered that it does not have the right to disclose log data.

In the general opinion of the Deputy Data Protection Ombudsman, shipboard health care cannot, based on the above, be excluded from the scope of all basic statutes applying to the processing of patient information. Since health care professionals perform procedures on individuals on the ship, the Deputy Data Protection Ombudsman is of the opinion that section 12 of the Patient Act regarding the obligation to prepare patient documents in principle applies.

The scope of the Client Data Act is relevant to this question. According to section 2 of the Client Data Act, the Client Data Act lays down provisions that supplement and specify the General Data Protection Regulation when social welfare and health care client data as well as welfare data generated by the client themselves is processed electronically for the purpose of providing health care and social welfare services. As stated in the legislative materials for the Act, the Act applies to the social welfare and health care services organised or provided by public and private social welfare and health care service enablers.[15]

According to section 3, subsection 1, paragraph 7 of the Client Data Act, 'service enabler' means an organiser or provider of social welfare and health care services. According to section 3, subsection 1, paragraph 8, point b of the Act, 'service organiser' means a service enabler that, as a private service enabler, has an obligation to ensure that the client receives the service they are entitled to under the agreement. According to section 3, subsection 1, paragraph 9 of the Act, 'service provider' in turn means a service enabler, which a) provides the social welfare or health care service itself in the role of service organiser; and which b) provides a social welfare or health care service on behalf of a service enabler.

'Health care unit' (i.e. service provider) has also been defined in section 2, subsection 1, paragraph 4 of the Patient Act.[16] According to section 7, subsection 1, paragraph 2 of the Occupational Health Care Act (1383/2001), 'service enabler' means both employers and self-employed health care professionals.

According to section 2, subsection 1 of the Act on Private Health Care (152/1990), 'health care services' mean 1) laboratory operations; 2) radiological operations and other comparable examination and imaging methods; 3) other examinations or procedures performed to diagnose an illness or determine treatment; 4) physiotherapeutical operations and other performance-improving and -maintaining procedures and therapies; 5) occupational health care; 6) medical and dental services and other health care, medical care and comparable services; 7) massage; and 8) ambulance services.

According to section 2, subsection 2 of the Act on Private Health Care, 'service provider' means an individual person or company, cooperative, association or other corporation or foundation which maintains a unit that provides health care services. Other self-employed persons or employers who organise the occupational health care services referred to in the Occupational Health Care Act themselves are not considered service providers.

[15] HE 212/2020 vp, p. 74
[16] HE 212/2020 vp, p. 76.

'Self-employed person', on the other hand, is defined in section 2, subsection 3 of the Private Health Care Act as a health care professional referred to in section 2, subsection 1 of the Health Care Professionals Act (559/1994) who practises their profession independently.

According to section 4 of the Act on Private Health Care, a service provider must have a licence granted by the licensing authority for providing health care services. According to section 9a of the Act, a self-employed person must file a written notification of their operations to the State Regional Administrative Agency before providing health care and medical care services referred to in the Act.

For the sake of completeness, we also refer to the written question[17] concerning problems in the interpretation of the Act on Ships' Medical Stores with regard to questions regarding the availability of log data and the patient's right to have their health information recorded, inspected and amended, as well as to the reply to this question given by the Minister of Social Affairs and Health on 17 March 2022[18]. The reply states that the Client Data Act is not applied on board ships, because the ship is not a service provider as referred to in the Act. The reply also states that the Ministry of Social Affairs and Health is in the process of preparing an overhaul of social welfare and health care data management regulations, which will, among other things, combine the regulations concerning the processing of client data laid out in the Act on the Electronic Processing of Client Data in Healthcare and Social Welfare and the Act on the Status and Rights of Patients. The reference to secrecy regulations in section 9 of the Act on Ships' Medical Stores will also be updated in this connection. A draft that has already been circulated for comments only proposes to add a reference to the new Act with regard to the secrecy obligation, but the extension of the general obligations concerning the processing of client data, such as secrecy, log data collection and the client's right of access to log data, can still be discussed in the finalisation phase of the draft.[19]

Notwithstanding the above, the Deputy Data Protection Obmudsman does not consider themself competent to decide the question of whether [redacted] must be considered a service provider as referred to in section 26 of the Client Data Act. Since, for reasons explained in the decision proper, the Deputy Data Protection Ombudsman is not competent to decide the question of the complainant's right of access to log data in the matter at hand, the Deputy Data Protection Ombudsman has not requested a statement on the matter from the authorities responsible for the enforcement of the Client Data Act. However, the Deputy Data Protection Ombudsman will forward this decision to the National Supervisory Authority for Welfare and Health, State Regional Administrative Agency for Southern Finland and the Ministry of Social Affairs and Health for information and possible further action.

This guidance issued by the Deputy Data Protection Ombudsman is not subject to appeal.

[17] Written question KK 78/2022 vp.
[18] Reply to written question KKV 78/2022 vp
[19] Reply to written question KKV 78/2022 vp, p. 2.

Deputy Data Protection Ombudsman _____

Referendary senior officer _____

The document is signed electronically. The legitimacy of the signature can be verified at the registry of the Office of the Data Protection Ombudsman if necessary.

Appendices

Appeal instructions

Distribution

Complainant

[redacted]

Contact information of the Office of the Data Protection Ombudsman

Postal address: P. O. Box 800, FI-00531 Helsinki, Finland

Email: tietosuoja@om.fi

Telephone exchange: +358 (0)29 566 6700

Website: www.tietosuoja.fi

Sanctions Board Final Decision on an Administrative Fine

Controller [redacted]

1. As indicated in the decision of the Deputy Data Protection Ombudsman, [redacted] has not complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when saving diagnosis information into the MAPS system or storing its employees' health information in the MAPS system. Neither has [redacted] taken every reasonable step in accordance with Article 5(1)(d) and Article 25(1) of the GDPR to ensure the accuracy of the personal data processed in the MAPS system.

2. [redacted] has not complied with the provisions of Article 5(1)(a) and Article 13 of the GDPR. Neither has [redacted] complied with the provisions of Article 12(3) nor Article 15(1) of the GDPR when responding to the complainant's request made pursuant to Article 15 of the GDPR.

3. Taking into account the gravity of the infringement in particular, the matter does not consist of a minor infringement as referred to in recital (148) of the GDPR. With regard to effectiveness, proportionality and dissuasiveness and in view of the provisions of Article 83(2) of the GDPR, it must be noted that, in the matter at hand, an order issued by the Deputy Data Protection Ombudsman under Article 58(2)(d) of the GDPR in combination with a reprimand will not be a sufficient sanction in this matter. An administrative fine must be imposed in the matter. The fact that this is not a case of individual infringements of the Working Life Privacy Act and Article 5(1)(a) and Article 13 of the GDPR, but established practices on the part of [redacted], also speaks for the imposition of an administrative fine.

4. [redacted] has not complied with the following provisions referred to in Article 83(5) of the GDPR, and an administrative fine is imposed for their infringement: 1) Article 5(1), points (d) and (a); 2) Article 13; 3) Article 12(3); and 4) Article 15(1). Neither has [redacted] complied with Article 25(1) of the GDPR, which calls for the imposition of an administrative fine pursuant to Article 83(4) of the GDPR.

5. [redacted]'s turnover was EUR 258,243,347.47 in 2021. In the matter at hand, the maximum amount of the administrative fine imposed on [redacted] is EUR 20,000,000. The Sanctions Board consisting of the Data Protection Ombudsman and Deputy Data Protection Ombudsmen ('Sanctions Board') orders, in addition to the corrective powers exercised and corrective measures ordered above by the Deputy Data Protection Ombudsman, the controller to pay the State an administrative fine of EUR 230,000 (two hundred thirty thousand) by virtue of Article 58(2)(i) and Article 83 of the General Data Protection Regulation. The Sanctions Board of the Office of the Data Protection Ombudsman finds an administrative fine of EUR 230,000 to be effective, proportionate and dissuasive.

Grounds for imposing the administrative fine

6. Article 83 of the General Data Protection Regulation provides for the general conditions for imposing administrative fines. Firstly, the imposition of administrative fines shall in each individual case be effective, proportionate and dissuasive. Secondly, administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, the corrective powers provided for in Article 58. In the primary matter at hand, the Deputy Data Protection Ombudsman has ordered [redacted] to bring its practices for informing data subjects into compliance with the provisions of the GDPR and issued a reprimand to the company. The administrative fine is thus imposed in addition to points (b) and (d) of Article 58(2).

7. Due regard shall be given to the considerations listed in Article 83(2) of the GDPR when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case.

8. As mentioned above, [redacted] has not complied with the following provisions referred to in Article 83(5) of the GDPR, for the infringement of which an administrative fine is imposed: 1) Article 5(1), points (d) and (a); 2) Article 13; 3) Article 12(3); and 4) Article 15(1). Neither has [redacted] complied with Article 25(1) of the GDPR, which calls for the imposition of an administrative fine pursuant to Article 83(4) of the GDPR.

9. According to Article 83(3) of the GDPR, if a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

10. The gravity of the infringements shall be assessed on the basis of the considerations listed in Article 83(2) of the GDPR. The assessment must identify the conduct or neglect that can be considered the most reprehensible in view of the details of the matter under assessment.

11. In the matter at hand, the infringements of Articles 5, 13, 12 and 15 of the GDPR, as well as the infringement of obligations arising from Member State legislation adopted in accordance with Chapter IX of the GDPR, are the most serious and fall within the higher administrative fine category provided for in Article 83(5) of the GDPR. The applicable maximum amount of the administrative fine is thus determined pursuant to Article 83(5) of the GDPR and may not be exceeded by virtue of Article 83(3) of the GDPR.

12. Infringements of the provisions of points (a) (Articles 5, 6, 7 and 9) and (b) (Articles 12 to 22) of Article 83(5) shall, in accordance with Article 83(2), be subject to administrative fines up to EUR 20,000,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

13. The Guidelines of the Article 29 Working Party[20] on the application and setting of administrative fines were also given due regard in the assessment of the matter.

Assessment of the gravity of the infringements

14. Due regard was given to points (a), (b) and (g) of Article 83(2) in the assessment of the gravity of the infringements.

Nature, gravity and duration; nature, scope or purpose of the processing

15. According to recital (51) of the GDPR, personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Special requirements have accordingly been set for the processing of special categories of personal data, including that such personal data should not, as a rule, be processed. The processing of such personal data is only permitted when both 1) one of the general requirements for processing provided for in Article 6 of the GDPR is met; and 2) one of the special conditions for processing provided for in Article 9 of the GDPR applies.

16. Even though [redacted] has not processed its employees' health information without meeting the requirements provided for such processing in Articles 6 and 9 of the GDPR in this matter, [redacted] has processed data concerning the health of its employees in violation of the provision of section 5, subsection 4 of the Working Life Privacy Act. In addition, [redacted] has failed to comply with the provisions of Article 5(1)(d) and Article 25(1) of the GDPR. It should be noted that data protection by design and by default is one of the core elements of the GDPR on which the implementation of data protection is founded in practice.

17. Several infringements and shortcomings have been identified in the matter. In addition to the aforementioned infringements, [redacted] has failed to comply with the provisions of Article 5(1)(a) and Article 13 of the GDPR. This right constitutes a right to information, which enables, for example, the exercise of the rights of the data subject provided for in the Regulation. The Sanctions Board finds an infringement of this right to be especially reprehensible.

18. Neither has [redacted] complied with the provisions of Article 12(3) nor Article 15(1) of the GDPR when responding to the complainant's request made pursuant to Article 15 of the GDPR. With regard to the latter, however, due regard was given in the assessment to the fact that [redacted] and the complainant had engaged in email correspondence regarding the matter, demonstrating that the company attempted to respond to the complainant's request within the prescribed time limit. Due regard was also given to the fact that the infringement of Article12(3) and Article 15(1) of the GDPR was limited

[20] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017).

to the individual case discussed herein. No information on large-scale infringements of the aforementioned legal provisions has come to light in the matter.

19. It must be specifically noted that the Working Life Privacy Act has been in force since 2004 and application of the GDPR began in 2018. [redacted] has thus had a reasonable amount of time to bring the processing activities discussed herein to compliance with the law, and the infringements cannot be said to have been brief in duration.

20. Furthermore, taking into account that the incompleteness of the ICD codes available in the MAPS system only applied to 2001, the period of time during which data may have been inaccurate can nevertheless be considered relatively short with regard to the matter as a whole. However, this does not have a mitigating effect on the assessment of the matter, as there was no legitimate basis for recording ICD codes. Instead, the fact that even incorrect diagnosis data have been retained for a considerable period of time is taken into account in the assessment as an aggravating factor. The processing of erroneous diagnosis data poses a high risk to the legal protection of data subjects.

21. It should be noted that the nature of the infringements must be considered to speak in favour of imposing an administrative fine.

Number of data subjects affected by the infringement and the level of damage

22. The MAPS system is said to contain the personal data of approximately 6,000 data subjects. Some of these data subjects are current employees of [redacted] and some are former employees. None of the parties have claimed that the infringements related to the MAPS system would only apply to a limited group of the data subjects. On the contrary, the infringements discovered reflect a systematic approach and lack of appropriate practices. The processing has affected a significant part of [redacted]'s personnel.

23. In the assessment of the impact of the infringements on the number of data subjects, due regard was also given to the fact that the processing discussed herein was not limited to a national scale, but has also affected data subjects in the area of the EU/EEA who have worked on [redacted]'s vessels sailing under the Finnish flag. The processing has affected data subjects in a vulnerable position in relation to [redacted].

24. The infringements were not single or isolated incidents. The number of data subjects affected by the infringements cannot be considered minor. On the one hand, this number reflects the gravity of the infringements but, on the other hand, no financial damage to the data subjects can be established based on the information provided to the Office of the Data Protection Ombudsman.

25. It should be noted that the number of data subjects affected by the infringements must be considered to speak in favour of imposing an administrative fine in the matter. On the other hand, the fact that the data

subjects have not been proven to have suffered concrete financial or other material damage as a consequence of the infringements can be taken into account as a factor reducing the amount of the administrative fine in the matter.

The intentional or negligent character of the infringement

26. According to the aforementioned Guidelines of the Article 29 Working Party on the application and setting of administrative fines, 'intent' generally requires knowledge and wilfulness n relation to the infringement, while 'unintentional' means that there was no intention to cause the infringement although the controller breached the duty of care which is required in the law. It is generally admitted that intentional breaches, demonstrating contempt for the provisions of the law, are more severe than unintentional ones.[21]

27. The response to the hearing maintained that the matter at hand did not involve intentional infringements. Also according to the response, the controller had not actively made a knowing decision to, for example, keep inaccurate data in the employee register. The response compares the situation to human error, due to which the system containing the personal data had not been updated to comply with the legislation in force. We again refer to the aforementioned Guidelines of the Article 29 Working Party on the application and setting of administrative fines. The guidelines state that human error or, for example, failure to apply technical updates in a timely manner may be indicative of negligence. It should also be noted that it is well established in Finland that ignorance of the content of the law does not in general mean the kind of mistake that would eliminate possible intentionality or negligence. The controller is responsible for ensuring that its operations comply with the provisions of the law. Notwithstanding the above, with regard to the infringements of section 5, subsection 4 of the Working Life Privacy Act, the Sanctions Board finds no cause to assess the matter differently than [redacted] did in its response to the hearing. [redacted] has announced that it had taken corrective measures even before the Office of the Data Protection Ombudsman began its investigation into the matter. It was also taken into account in the assessment that [redacted] had already taken corrective measures based on communication with a single data subject. When assessing the matter as a whole, the Sanctions Board finds that [redacted]'s infringements assessed in this paragraph cannot be considered intentional or negligent.

28. The response to the hearing referred to the email correspondence between [redacted] and the complainant, regarding the complainant's right of access to her data. Even though [redacted] did not fulfil the right within the prescribed one-month time limit, the aforementioned correspondence demonstrates that [redacted] nevertheless sought to fulfil the complainant's right in a timely manner. On the other hand, the Sanctions Board considers it especially reprehensible that, regardless of the complainant's specific request to access her diagnosis information, this information was not delivered to the complainant. Such conduct is indicative of at least negligence.

[21] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017), p. 12.

However, when assessing the aggravating and mitigating factors affecting the amount of the administrative fine, the Sanctions Board does not give weight to the above-mentioned fact. However, for the sake of clarity, it should be noted that the imposition of an administrative fine is not subject to the condition that the infringement found is intentional or negligent. The intentional or negligent nature of the infringement is only one of the factors which, as provided for in Article 83(2) of the GDPR, must be duly taken into account when deciding on the imposition of an administrative fine and the amount of the administrative fine.

29. With regard to the infringement of Article 5(1)(a) and Article 13 of the GDPR established in the primary matter, it should be noted that this was not a case of providing insufficient or incomplete information to data subjects. Rather, the information provided for in the GDPR was not delivered to the data subjects at all. In this regard, [redacted]'s conduct indicates that the company has not sufficiently familiarised itself with the legislation in force and the requirements arising therefrom, which consequently indicates contempt for the provisions of the law.

The categories of personal data affected by the infringement

30. As noted above, the infringements established in this matter affected data concerning the health of the data subjects. The Sanctions Board has already assessed the significance of infringements involving such data to the assessment of sanctions under ”Nature, gravity and duration; nature, scope or purpose of the processing” above.

Assessment of aggravating and mitigating factors

Measures taken by the controller to mitigate the damage caused to the data subject

31. According to the aforementioned Guidelines of the Article 29 Working Party on the application and setting of administrative fines, the controller should do everything in its power to mitigate the consequences of the infringement to the affected parties. According to the guideline, the supervisory authority may take such responsible behaviour or the lack of it into account in the calculation of the administrative fine.[22]

32. [redacted] has announced that it took corrective measures after the complainant had contacted the company. According to the company, it had started looking into the matter even before the Office of the Data Protection Ombudsman began its investigation. As mentioned above, it is also significant that, according to [redacted], it took corrective measures immediately after being contacted by a single data subject. The Sanctions Board commends such a proactive approach.

[22] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017), p. 12.

The degree of responsibility taking into account technical and organisational measures implemented by the controller pursuant to Article 25

33. As provided for in Article 25 of the GDPR, the controller shall take into account in its operations ”the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing”.

34. The response to the hearing stressed that [redacted] has ensured that the personal data in question can only be accessed by individuals whose duties have been directly related to the data and who have required the data in their work. In other words, access rights have been managed to ensure that the data is only processed by authorised persons. [redacted] has stated that it has implemented the principles of integrity and confidentiality by logging events in the information systems, for example.

35. Regardless of the measures taken, it was not possible to save all ICD codes into the MAPS system in 2001. In other words, only a portion of the codes was used. It has thus been possible that absences due to illness may have been saved into the system with different codes than those in the actual diagnosis based on which the sick leave was granted. This error was only discovered later, when the matter was looked into after the complainant had contacted the company. As mentioned above, [redacted]'s announcement that it has taken corrective measures after being contacted by the complainant and before the Office of the Data Protection Ombudsman launched its own investigation into the matter must be taken into account to the company's benefit. In other words, [redacted] can be considered to have taken timely measures to stop the discovered infringement soon after the company became actively aware of it. The Sanctions Board gives due regard to this as a mitigating factor in its assessment.

Any relevant previous infringements and measures ordered with regard to the same subject-matter

36. The aforementioned Guidelines of the Article 29 Working Party on the application and setting of administrative fines also state that the supervisory authority should assess the track record of the unit guilty of the infringement. The supervisory authority should consider that the scope of the assessment here can be quite wide because any type of breach of the Regulation, though different in nature to the one being investigated now by the supervisory authority might be “relevant” for the assessment, as it could be indicative of a general level of insufficient knowledge or disregard for the data protection rules.[23]

37. The Data Protection Ombudsman is not aware of any prior infringements of data protection regulations by [redacted]. Neither have measures

[23] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017), p. 15.

referred to in Article 58(2) of the GDPR been ordered against [redacted] in the past for the infringements discussed herein. The Sanctions Board does not find the above to be either a mitigating or aggravating factor in the assessment of sanctions.

Degree of cooperation with the supervisory authority and the manner in which the infringement became known to the supervisory authority

38. According to the Guidelines of the Article 29 Working Party on the application and setting of administrative fines, the degree of cooperation may be given ”due regard” when deciding whether to impose an administrative fine and in deciding on the amount of the fine. It can be relevant to the assessment of cooperation with the supervisory authority whether the controller has responded to the supervisory authority’s requests during the investigation in a manner that has significantly limited the risk to the rights of natural persons. That said, the guidelines state that it would not be appropriate to give additional regard to cooperation that is already required by law.[24]

39. As provided for in Article 31 of the GDPR, the controller shall cooperate, on request, with the supervisory authority in the performance of its tasks. The controller also has an obligation under Article 58(1) of the GDPR and section 18 of the Data Protection Act to deliver the requested information to the supervisory authority.

40. The supervisory authority has learned of [redacted]'s infringements through a complaint. In its consideration of a reasonable sanction, the Sanctions Board has given due regard to the fact that [redacted] has responded to the authority's requests for information within the time limit. [redacted] has been cooperative with the Office of the Data Protection Ombudsman. However, the Sanctions Board does not consider the aforementioned to be either a mitigating or aggravating factor in the assessment of sanctions.

Any other aggravating or mitigating factor applicable to the circumstances of the case

41. In assessing the amount of the administrative fine, the Sanctions Board gives due regard to the damage suffered by the tourism industry from the effects of the coronavirus pandemic.

42. As mentioned above, the controller has also taken action to remedy the shortcomings identified in this matter largely on its own initiative. The shortcomings in the fulfilling the rights of the data subject can be considered to concern the individual case discussed herein. Nothing that would indicate systematic infringements of the GDPR by the controller in this regard has been brought forward in the matter.

[24] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017), p. 15.

Conclusion

43. According to [redacted]'s response to the hearing, an administrative fine should not be imposed for conduct that may have violated the provisions of the Working Life Privacy Act or other legislation than the General Data Protection Regulation, nor should such matters based on other legislation be taken into account as aggravating factors in the assessment of the administrative fine. In this regard, the Sanctions Board refers to the provisions of Article 83(5)(d) of the GDPR. According to the said provision, an administrative fine can be imposed for infringements of any obligations pursuant to Member State law adopted under Chapter IX of the GDPR. We also refer to the provisions of Article 88. Member States may provide for more specific rules by law to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context.

44. It should also be emphasized that Article 88 of the GDPR does not leave it to the discretion of the national legislator whether to limit the national regulations adopted based on the mentioned article outside the scope of administrative fines.

45. Article 83(7) of the GDPR stipulates how the scope of administrative fines may be limited by national legislation. There is no other national margin of discretion in relation to the scope of application of administrative fines.

The decision to impose an administrative fine has been made by the members of the Sanctions Board of the Office of the Data Protection Ombudsman.

Data Protection Ombudsman _____
[redacted]

Deputy Data Protection Ombudsman _____
[redacted]

Deputy Data Protection Ombudsman _____
[redacted]

Referendary Senior Officer _____
[redacted]

The document is signed electronically. The legitimacy of the signature can be verified at the registry of the Office of the Data Protection Ombudsman if necessary.

Additional information on this decision is available from the referendary

Senior Officer [redacted], telephone [redacted]

Applicable legal provisions

As set out in the grounds.

Appeals

According to section 25 of the Data Protection Act (1050/2018), this decision may be appealed in the Administrative Court pursuant to the provisions of the Administrative Judicial Procedure Act (808/2019). The appellate court is the Administrative Court of Helsinki.

Instructions for appeal are appended.

Service of notice

Notice of this decision will be served by post against an acknowledgment of receipt pursuant to section 60 of the Administrative Procedure Act (434/2003).

Appendices

Appeal instructions

Payment instructions for the administrative fine

Distribution

Complainant

[redacted]

Contact information of the Office of the Data Protection Ombudsman

Postal address: P. O. Box 800, FI-00531 Helsinki, Finland

Email: tietosuoja@om.fi

Telephone exchange: +358 (0)29 566 6700

Website: www.tietosuoja.fi