No. Fac. 11.17.001.008.122 July 22, 2021 BY ELECTRONIC MAIL DECISION OF THE COMMISSIONER FOR THE PROTECTION OF PERSONAL DATA Complaint for insufficient organizational security measures and unauthorized access to information A. FACT: On 31/7/2020 a complaint was submitted to my Office by XXXXX (XXXXXXXX) Complainant) against the Department of Commercial Shipping (TEN) later the Deputy Ministry of Shipping (hereinafter YFYN) and XXXXXXXXXXXXXXXX, (hereinafter Complainant). 2. The Complainant claimed that the Defendant in the complaint against and/or about 2012, secured unauthorized access to personal data concerning him which was in the possession of the National Health Service. 2.1. Specifically, the Complainant made the allegation that the Complainant had direct access to application data kept in his file or obtained it indirectly from a person who had the right to access his file. In addition, it is his contention that the Complainant did not have the right to access the specific file, because he did not serve in the Marine Training and Certification Division, did not conduct an official investigation that would have given him the right of access, nor did he have any other form of access authorization in an application file of the year 2000-2001. 2.2. In addition, he asserts that the complaint before my Office was filed more than 8 years late, because the Department of Public Health prevented him from submitting the complaint. 3. On 4/8/2020, 19/8/2020, 12/11/2020 and 7/12/2020, an employee of my Office sent electronic messages to the Data Protection Officer (hereinafter DPO) of the Ministry of Health, initially requesting the position of the Complainant's allegations, asking clarifying questions and requesting that anything else related to the submitted complaint be reported. 4. Other issues raised before my Office by the Complainant and the Complainant and which do not concern the competences of my Office, will not be taken into account and will not be examined. Positions of the Ministry of Internal Affairs and Communications as reported by the Ministry of Internal Affairs and Communications: 5. The Ministry of Internal Affairs and Communications of the Ministry of Internal Affairs and Communications on 5/11/2020, 6/11/2020, 20/11/2020 and 23/12/2020 sent reply emails to My office, mentioning among others the following: legal authorization many Officers 5.1 During the investigation of the complaint, the DPO contacted and was informed both by the Complainant and by Officers of the Ministry of Health, who, due to their position, were aware of it matter and proceedings, during the material time. 5.1.1. The DPO noted and stated that the alleged incident occurred more than eight (8) years ago and with regard to the Complainant's claim that the Directorate of the Ministry of Health prevented him from submitting a complaint to investigate the manner in which the information was obtained on behalf of the Complainant, the Ministry of Foreign Affairs stated that no direct or indirect written reference to this was found, either from the management of the TEN, or later from the YFYN. 5.1.2. Additionally, the DPO

stated that, after a written communication he had with the Complainant, he told him that as far as he remembers, a verbal complaint was submitted to one of the Senior Directors of the 2012/2013 period, but not imperatively and as a requirement. 5.2. At the material time, i.e. 2012, the information held in the personal file of the Complainant, as a seafarer, was very easy for the Complainant to have come to the knowledge of, as it was then (in 2012) registered in the MARCOS electronic system and on the SEAFARERS icon, which they had access to with the HYFN, including the Complainant. 5.3. The authorization of the Complainant was granted in the context of his duties, by the Minister of Transport and Works (later Ministry of Transport, Communications and Works, hereinafter YMEE), by virtue of its provisions on Merchant Shipping (Issue and Recognition of Certificates and Maritime Education) Law of 2000 as subsequently amended, for the issuance of seafarers' certificates and the recognition of certificates of a member state or a third country. Consequently, the Complainant also had access to seamen's files and could request that any file be presented to him, based on the Authority of Legitimacy. 5.4. Regardless of the Department that the Complainant was in charge of, the authorization that was legally granted to him, gave him access to the files of the sailors and information that was in them and by extension also to the file of the Complainant. The DPO adds that it did not emerge from the investigation that further instructions were given to the Complainant to investigate the Complainant's certificates. 6. The Ministry of Foreign Affairs, in an electronic correspondence with the Complainant, informed him that the matter of the Complainant's qualifications arose during the examination of an official matter. 6.1. The Complainant stated that he received the information in question orally from the Complainant himself and raised questions/questions related to the matter in question initially to the Director, Deputy Directors and Head of the relevant department during the relevant time, but received no reply. For this reason, he sent a letter to the General Director of the YMEE, with a notification to the Senior Director of the YFYN, without mentioning the details of the Complainant, but describing the situation and raising questions/questions. The defendant in the complaint claimed that he submitted the questions from his professional position and by virtue of the authority assigned to him by the Minister for the inspection of ships, the issuance of certificates and the investigation of maritime accidents. 2 7. In the e-mail dated 20/11/2020 sent to my Office by the DPO of the Ministry of Internal Affairs and Communications, the Complainant questioned the procedure followed by my Office during the examination of this case. 7.1. In a reply email dated 7/12/2020, an Officer of my Office mentioned, among other things, to the Complainant, that the complaint examination process by my Office is carried out through the DPO of the respective data controller. The Office addresses the DPA and the DPA addresses any other person involved, asking him questions and clarifications which he later

transfers to my Office. The same procedure was followed in the present case. It was stated that when and if deemed necessary by the data before it, my Office may communicate directly with the persons involved. 7.1.2. In addition, the Complainant was informed that as far as my Office is concerned, it does not matter if a question or complaint or complaint or clarification was submitted on his behalf. My Office is considering whether the manner in which it obtained the information relating to the Complainant was appropriate and whether it had a legitimate interest/obligation to use that information in the manner it did. 8. In conclusion, the Ministry of Foreign Affairs stated that, now, all the seafarers' files that are kept in the archives of the Ministry of Defense have been digitized and are not kept in original form. 8.1. In addition, access to both the MARCOS electronic system and the SEAFARERS icon has been significantly restricted by the competent IT sector of the Health and Safety Authority and security barriers have been put in place regarding access to any file. 8.1.2. In particular, access to all data fields of the MARCOS electronic system is controlled and is done after the authorization of each Head of Department, after a written request of the employee requesting access, always according to his duties. Afterwards, codes are granted to each applicant with a duration of three (3) months by the Computerization Department of the National Health Service. Positions of the Complainant: 9. On 4/8/2020, an Officer of my Office sent an electronic message to the Complainant and informed him that a letter had been sent to the DPO of the Ministry of Defense and at the same time expressed the concern of the Office, whether an adequate investigation can be done after after such a long period of time. 9.1. On 5/8/2020 the Complainant sent an electronic message to the Office, in which he stated that he had a telephone conversation with an Officer of the Office, before submitting the complaint and received an assurance that time does not necessarily work as a deterrent, which is why he proceeded to submit of this complaint. 10. On 7/1/2021, an Officer of my Office sent an electronic message to the Complainant, informing him of the positions of the YPD of the YFYN regarding 3 of his allegations against the YFYN and the Defendant of the complaint and requested that it be placed on of these until 4/2/2021. 11. On 15/1/2021 the Complainant sent his positions, but from the vocabulary he used it is clear that he misinterpreted the content of the electronic message dated 7/1/2021, perceiving it as conclusions, instead of a statement of the claims of the Ministry of Health and Where the complaint, on which it was called to place. 11.1. Therefore, on 19/1/2021, an Office Officer sent a new clarifying email to the Complainant (even though the content of the previous email was clear), stating that the positions recorded in the electronic message dated 7/1/2021 are those of YFYN and the Professor in the complaint and not conclusions of my Office. They were brought to his attention, in order for him to comment on them and to have before me all the facts of the case for the issuance of

a decision. 11.2. Therefore, my Office had not reached any conclusions, since it was also waiting for the Complainant's positions before issuing a Decision, and the reference to "conclusions" in his response was not appropriate, since the content of his response would be subject to study and evaluation in within the scope of my Office's responsibilities. 12. The rest of the content of the electronic message dated 1/15/2021 of the Complainant to my Office, mentioned the following: 12.1. The Complainant disagreed with the reports of the National Health Service regarding the electronic system MARCOS of the National Health Service. He claimed that the only information that the Complainant could trace from the MARCOS system was his personal file number (SFN) and what diplomas he had been issued and when, but not what supporting documents were submitted with his application. 12.2. The MARCOS electronic system in the seafarer information option did not include qualification data held in the personnel file and is not a representation of a seafarer's file. It is only a record of the certificates that have been issued by the Seafarer Training and Certification Section of the Merchant Shipping Department, as it was called until 2018, to the applicant for the certificate, a seafarer. The system showed which certificates of seaworthiness were issued, but not the application and supporting documents, which were submitted, in paper form, when the application was submitted. The documents attached to an application are not photographed (scanned) to be saved in the system, and this was never done. 12.3. As the Complainant mentioned, the supporting documents he submitted and which are in his file, also include personal data. With the personal file number that the Complainant may have obtained from the system, he could locate his file, in the warehouse kept in the basement of the Department's building, which had been archived and locked since 2002, which the 1st class Master's diploma was issued. The fact, as he mentioned, that there was a lock in the warehouse where the files were kept, in an area that only the staff of the Training and Certification of Sailors had access to because it was their own warehouse, is proof of the management's intention to control access to the files. As he reported, it was explained to him that the lock was mechanical, with a combination, and the combination of the warehouse mechanical lock was the same as the combination of the 4 mechanical locks that gave access to the staff offices, so it would also be known to Cath complaint, who worked in the Marine Casualty and Incident Investigation Section then housed on the 2nd floor of the building. Therefore he would have access not because he was entitled to it by virtue of position, but because of the fact that the combination of the lock was the same. 12.4. He disagreed that the authorization granted to the Appellant gave him a free right to view the qualifications contained in the seafarers' files. He stated that the Minister's specific authorization to ship inspectors, along with a number of other authorizations, was issued to all of them immediately after they were hired, for procedural reasons. 12.5.

The access of a ship inspector to files that also include personal data was done with the limitation stated by the law in force at the time, as to who has the right of access. 12.6. The Complainant, at the time in question, was serving as the Head of the Marine Accident and Incident Investigation Department and as the Complainant stated, he had no right to ask for a file to be presented to him. 12.7. The Complainant sent excerpts from an email correspondence he had with Kat'ou the complainant, in which he underlined the phrases "... I saw the strange thing that you have 7 years at sea and he has obtained a certificate that required 8. I looked without any disturbance..." and "…where my own unofficial examination showed that you were not eligible for Master…". It is his contention that these reports prove that the Complainant violated the law and obtained the information concerning him by unlawful means. 12.8. The Complainant claimed that he submitted complaints in person on a regular basis to the Senior Director of the YFYN Administration, in special meetings in his office and on at least two (2) occasions he also gave him written complaints, on 17/5/2012 and 24/7 /2012, for the actions of the Defendant the complaint against him. The response he received from the Administration of the National Health Service was not to pursue the matter further and he chose to obey the administration's admonitions. 12.8.1. YFYN was aware of the actions of the Complainant, but in no case did it investigate the manner in which the Complainant secured the information concerning his person. 12.9. The Complainant claimed that the Defendant was not legitimizing the complaint from his professional position and by virtue of the authority assigned to him by the Ministry to inspect ships, issue certificates and investigate maritime accidents, to have knowledge of the data concerning him and that the report The Defendant's complaint that he received the information after a conversation he had with him does not change the fact that he gained access to his personal file to cross-examine it. 12.10. In addition, the Complainant claimed that two internal investigations were carried out, the result of which did not satisfy the Complainant and that is why he sent the letter to the Director General of YMEE as well as to other Services on the subject in question. 5 B. LEGAL ASPECT: 13. Among other things, in Article 4 (1) of the Processing of Personal Data (Protection of the Individual) Law 138(I)/2001 (hereinafter Law 138(I)/2001), it is stated that "The data controller shall ensure that personal data (a) Are processed lawfully and lawfully; (b) are collected for specified, clear and lawful purposes and are not further processed incompatible with these purposes...". 13.1. According to Article 10 par. (3) of Law 138(I)/2001 "... The controller must take the appropriate organizational and technical measures for the security of the data and their protection against accidental or unlawful destruction, accidental loss , alteration, prohibited dissemination or access and any other form of unfair processing. These measures must ensure a level of security commensurate with the risks involved in the processing and the nature of the

data being processed. The Commissioner provides instructions on the degree of data security, as well as on the protection measures that are necessary to be taken for each category of data, in view of technological developments...". 13.2. In Article 5 of the General Regulation of Personal Data (hereafter GDPR) the Principles governing the processing of personal data are mentioned, such as that the data must "a) be processed lawfully and legitimately in a transparent manner in relation to the subject of the data ("lawfulness, objectivity and transparency"), b) are collected for specified, express and lawful purposes and are not further processed in a manner incompatible with those purposes; ... ("purpose limitation"), ...". According to paragraph 2 of the same Article "The data controller bears the responsibility and is able to demonstrate compliance with paragraph 1 ("accountability")." 13.3. Article 24 para. 1 of the GDPR refers to the responsibility of the controller to "implement appropriate technical and organizational measures in order to ensure and be able to prove that the processing is carried out in accordance with this regulation. These measures are reviewed and updated when deemed necessary." and par. 2 of the same Article states that "2. Where justified in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.' 13.4. According to Article 32, paragraph 1, subsections (b), (c) and (d) of the GDPR, the data controller and the data processor should "Take into account the latest developments, the cost of implementation and the nature, the scope, context and purposes of the processing, as well as the risks of varying probability of occurrence and severity for the rights and freedoms of natural persons, and to implement appropriate technical and organizational measures in order to ensure the appropriate level of security against the risks, including, among others, as the case may be: (…) b) the ability to ensure the confidentiality, integrity, availability and reliability of processing systems and services on an ongoing basis, c) the ability restoring the availability and access to personal data in a timely manner in the event of a natural or technical incident, d) a procedure for assessment and evaluation regular testing, the 6 effectiveness of the technical and organizational measures to ensure the security of the processing..." taking taking into account the risks "resulting from the processing, in particular from the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed." (Article 32 par. 2). 13.5. Article 57 par. 1 subsection f) regarding the duties of the Supervisory Authority, states among other things, "Without prejudice to the other duties defined in this regulation, each supervisory authority in its territory: ... f) handles the complaints submitted by the data subject or by a body or organization or association in accordance with Article 80 and investigates, as far as appropriate, the subject of the complaint and informs the complainant of the progress and outcome of the investigation within a

reasonable time, in particular if further investigation or coordination with another supervisory authority, ..." C. REFLECTIVE: 14. To clarify once again, that other issues and procedures that were brought before me and that do not concern the responsibilities of my Office, I did not examine them, nor did I take them into account in issuing this decision. 14.1. Secondly, let me remind you that at the disputed time of the alleged violation, Law 138(I)/2001 was in force, which was repealed and replaced by Law 125(I)/2018, which entered into force on 31 July 2018. 15. I therefore conclude that the essence of the complaint in question can be summarized as follows: 15.1. whether the HYYN applied appropriate technical and organizational security measures regarding the access of its Officers to personal data, before and during the year 2012 and 15.2. (a) whether the Complainant lawfully had access to the information concerning the Complainant and (b) whether the notification of said information to the Director General of the Ministry of Transport and Works later Ministry of Transport, Communications and Works (par. 6.1) constituted: (i) a violation of the Principle of Legality according to Article 4(1)(a) of Law 138(I)/2001, which is also reflected in Article 5(1)(a) of the GDPR and (ii)) if said notification constituted on behalf of the Defendant complaint 2, processing incompatible with the original collection purposes in violation of the Purpose Limitation Principle provided for in Article 4(1)(b) of Law 138(I))/2001 and is reflected in Article 5(1)(b) of the GDPR 16. The National Security Agency must prove that it took security and personal data protection measures to ensure no leakage of the Complainant's personal data, as alleged. 16.1. Furthermore, as the Complainant himself stated, this data was filed in his personal file in 2001/2002, so it could have come to the attention of the Complainant at any time from 2001/2002 to 2012 and not necessarily in 2012. 16.2. The position of the Ministry of Defense, regarding the technical and organizational data access security measures, is that before and during the year 2012 several legally authorized Officers had access to the MARCOS electronic system and the SEAFARERS icon of the Ministry of Defense. In addition, files were kept in original form. 16.3. No other information was given about the disputed period of time, but it was mentioned that after the implementation of the GDPR a) all seafarers' files that are kept in the files of the Ministry of Health, have been digitized and are no longer kept in original form and b) access to the icon SEAFARERS and in all the data fields of the MARCOS electronic system is controlled and is done after the authorization of each Head of Department, after a written request of the employee who requests access, always according to his duties. Afterwards, codes are granted to each applicant by the Computerization Department of the Ministry of Health, which have a duration of three (3) months. 16.4. As the DPO of the YFYN mentioned, the long time that has passed since the alleged incident made it difficult to try to find further information. 16.5. The issue of the time that has passed since the time of the

alleged incident, is a matter that has also concerned my Office, since it makes it difficult and in some cases prevents the clear and thorough documentation of the facts. The information presented to me by the YPD of the Ministry of Health regarding technical and organizational measures that were in force during the disputed period, in the light of Law 138(I)/2001, do not allow the conclusion to be safely drawn that there were insufficient measures that might constitute a violation of Law 138(I)/2001 and the GDPR. 16.5.1. Therefore, a reasonable period of time to bring a complaint before me is an important part of the proper and most informed investigation, both by the parties involved and by my Office. 16.6. I add that, based on the GDPR, the adoption of technical and organizational security measures must be a continuous process, proportional to the type and nature of the processing, technological developments and the risks for the data subjects, which means that the measures that were in force at the material time may have been appropriate. 16.7. Therefore, I cannot safely conclude that the measures in force at the material time constituted a violation of Law 138(I)/2001 and subsequently of the GDPR on the part of the then TEN. 17. The issue arose in 2012, and this was not disputed by any involved party, during a study and/or job announcement related to the HYYN. 17.1. The Complainant, on the other hand, claimed that the Complainant received knowledge of the data concerning him either directly or indirectly from his personal file, and the Complainant claimed that the data concerning the Complainant, on the one hand, he learned from the Complainant himself in a discussion that 8 had with each other and on the other hand from his professional position he had a legal right to know them. 17.2. The claims and positions of the Complainant and the Defendant are diametrically opposed and there is no evidence to support one position more than the other. 17.3. The YFYN claimed that the Complainant had legal authorization to access seamen's files 17.4. The e-mail sent to me by both parties, which was considered by them to be helpful, refers to matters that are not related to the responsibilities of my Office but to administrative matters and procedures. Individual statements do not constitute facts or evidence. 18. The Complainant initially used the information relating to the Complainant within the National Health Service, after sending an email and/or letter to the Deputy Director of the Health Service. 18.1. At a later stage, since he did not receive an answer to the questions he raised before the Deputy Director of the YFYN, he sent a letter to the General Director of the YMEE with notification to the Senior Director of TEN, now YFYN. 18.2. In the letter he sent to the General Director of YMEE dated 29/11/2012, the Defendant did not use the Complainant's name, but described the professional qualifications possessed by the Complainant and compared them with the professional qualifications provided by the claim of the Merchant Shipping (Issue and Recognition of Certificates and Maritime Training) Law of 2000 (L. 109(I)/2000). 18.3. In the reply letter of the General Director of the YMEE

dated 31/5/2013, reference is made for the first time to the last name of the Complainant (page 2, paragraphs 4 and 7). The rest of the content of the letter does not concern the responsibilities of my Office. D. CONCLUSION/CONCLUSION: 19. First of all, it is reiterated that the long delay in submitting the complaint before my Office made the entire investigation of the case difficult. 20. Therefore, the claim of the Complainant that the National Health Service did not implement appropriate technical and organizational security measures regarding the access of its Officers to personal data, before and during the year 2012, is deemed unfounded, since according to the data before me I can safely conclude that the measures that were in force at the relevant time constituted a violation of Law 138(I)/2001 and subsequently of the GDPR on the part of the then TEN. 21. Regarding the question of whether the Complainant legally had access to the Complainant's information, in the light of what I mention in paragraph 16.7 and 20 above and taking into account everything that has been put before me, it appears that the the Complainant lawfully accessed the Complainant's data. 9 22. In relation to the question I ask in paragraph 15(2)(b)(ii), meaning that the correspondence that the Complainant had with the then Deputy Director of the National Health Serviceand the then Director General of YMEE regarding the Complainant, was

internal and not unrelated to the Ministry's responsibilities was not recommended

on behalf of the Defendant, the complaint is a violation of the Limitation Principle

Purpose.

23. Having regard to the facts, the analysis as explained above,

as well as the provisions of Article 57 paragraph 1 paragraph f), I have not established

violation pursuant to the provisions of Law 138(I)/2001 and GDPR by

YFYN and Kat'ou's complaint. Therefore, I do not think it is justified

any further action to impose administrative sanctions.

Irini Loizidou Nikolaidou

Data Protection Commissioner

Personal Character