No. Fac. 11.17.001.008.226 May 21, 2021 DECISION OF THE PERSONAL DATA PROTECTION COMMISSIONER

SUBJECT: Complaint for insufficient organizational security measures A. FACTS: On 12/15/2020, a complaint was submitted to my Office by the law firm of Hadjianastasiou, Ioannidis D.E.P.E. on behalf of the client XXXXXXXXXXXX, (hereinafter the "Complainant") against Demetra Holdings PLC Company (hereinafter the "Complainant", where he worked. 2. The Complainant claimed that he received a warning letter dated 9/17/ 2020, by XXXXXXXXXXX, CEO of Ms. the complaint, which had been stored in an electronic file located on a common server and to which persons, who are not justified in having access based on their duties, had free access. 2.1. Complaining further, he claimed that the content of this letter contained personal information related to his work performance, that such information is considered confidential and that Organizations/Companies have an obligation to store it in a file to which specific authorized persons have access. 2.2. To confirm his claims, he sent through his lawyers two images of the computer screen. In the first illustration, a word document with the name XXXXXXX is stored in the location Computer, All Users (X), Secretarial, Personel. In the second illustration, it appears that the word document, named XXXXXXX, is no longer stored in Computer, All Users (X), Secretarial, Personel. 2.3. Other matters which were raised both in the complaint form submitted and in the letters exchanged between the Complainant and the Complainant, and which do not concern the responsibilities of my Office, will not be considered. 3. On 21/12/2020 and 20/1/2021, electronic messages were sent to the Data Protection Officer (hereinafter DPO) of the Complainant, with which, in principle, her position was requested in relation to the allegations of the Complainant, and clarifying questions were asked in relation to the complaint submitted. Positions of the Complainant: 4. The Complainant's Office of the Complainant on 1/15/2020 and 4/2/2021 sent responsive emails to my Office, stating, among other things, the following: 4.1 - the Complainant the complaining company, at the material time, employed eight (8) employees, including the Complainant as Director of Business Activities, - all employees are bound by the obligation of confidentiality, regarding the information that comes to their knowledge during the provision of their work , - the document was saved in the information system of Ms. the company's complaint, specifically in the "Personnel" file after the lunch break on September 17, 2020, - in the "Personnel" file, 7 of the 8 employees could have access, (one is the summoner and does not generally have access to the system), - of the 7 who could have access 4 were the CEO who wrote the letter, the Complainant and 2 people from the secretarial staff, - of the remaining 3, 1 person was absent on 3 days' annual leave, - Ms. the complaint, from an investigation she conducted, found that the remaining employees (3 in total), although they could access in the file in question, they did not, - the letter remained in the file

in question stored for 8 calendar days (17/9/2020 – 25/9/2020) and during that time there was a weekend (19/9/2020 - 20 /9/2020), a period during which the Complainant does not exercise any authority, - on 9/24/2020 the Complainant, in a letter to the Chief Executive Officer of the Complainant, among other things raised the issue of technical and organizational measures, regarding the storage of the letter dated 17/9/2020 in the 'Personnel' file, - upon receipt of the Complainant's letter dated 24/9/2020, regarding the storage of the letter dated 17/9/2020, Ms. Complainant, on 25/9/2020 deleted the letter from the file named 'Personnel', - Ms. Complainant claims that, the Complainant's motives are alien and have nothing to do with the storage of the letter dated 17/9/2020 in the file named 'Personnel', - the Complainant, after the incident with the Complainant, carried out technical and organizational measures procedures, - the Complainant was established in 1999 and apart from this complaint has never had any issue with a personal data breach, - this incident was an isolated incident, which was dealt with promptly and without any consequences. 5. On 16/2/2021, an Officer of my Office sent an email to the Complainant's lawyers asking for their positions and opinions on the allegations of the Complainant. 2 Positions of the Complainant: 6. On 9/3/2021, one of the Complainant's lawyers sent a reply email to my Office, stating among other things the following: 6.1. - according to the Complainant, during the material time the Complainant employed nine (9) employees, - during the entire period of the Complainant's employment with the Complainant company he was never asked to be bound by a confidentiality agreement, - neither was there any provision in his employment agreement that provides for a commitment or obligation of confidentiality of the Complainant towards the Complainant company, - the Complainant served as a director of the Complainant company, therefore if he has not committed himself to corresponding agreements and/or from such obligations, it is very remote that other, lower-ranking persons have been bound by such clauses, - organizations are obliged by the legislation on personal data protection to apply appropriate technical and organizational measures to keep secure and confidential information about their employees and not allow t the access to them to persons who are not justified to have access based on their duties. The complaining company, as an organization that employs staff, is also subject to the above obligations from 25/05/2018 when the General Regulation on the Protection of Personal Data (EU) 2016/679 (hereinafter as "GDPR") came into force). - as the Complainant claims, the Complainant admits that on 17/09/2020 she stored a confidential letter in a file of the shared information system, to which all but one of her employees had access, - the fact that those persons had access to the particular file they chose and/or happened not to have access to the letter at the material time, this does not negate the fact that access to personal and confidential information was not strictly and exclusively limited to employees who were justified in

having access to it under the of their duties, - at the material time, five (5) persons who were not justified on the basis of their duties to have access to the confidential letter concerning the Complainant could, if they wished, have access to its content, - the fact that the letter remained stored for 8 calendar days (17/9/2020 – 25/9/2020) and during this time intervening weekend (19/9/2020 - 20/9/2020), a period during which the Complaining Company does not exercise any authority does not change the nature and/or does not reduce the extent of the breach of the Complainant's personal data and by extension of the national legislation related to the protection of personal data and the GDPR. 3 - it is obvious that the Complainant acknowledges the commission of the violation and the lack of organizational and technical measures during the essential time, which is invoked by the Complainant as the time when his personal data and the GDPR were violated by the The complainant's company, - Ms. the complainant, in her response to the Complainant's letter dated 24/09/2020 denied any responsibility and/or did not acknowledge any violation possibly with the aim of discouraging the Complainant from pursuing his complaint at the Office of the Personal Data Protection Commissioner. However, as he claims, one day later he deleted the confidential letter concerning the Complainant from the shared information system and has already taken technical and organizational measures. It is evident from her actions that she recognized and admitted the breach as well as her non-compliance with the GDPR and attempted to remedy the breach brought to her attention by the Complainant. - the subsequent implementation of technical and organizational measures or the cessation of the violation after the submission of a complaint do not in any case negate the commission of the violation during the essential time. At the same time, it reiterates that the complaining company should have put in place the necessary technical and organizational measures long before the incident with the Complainant, i.e. duringdate of application of the GDPR, and therefore its decision on and/or its actions for their subsequent application does not mitigate the extent of the violation in which incurred, nor does it eliminate its obligations that are triggered because of it.

- finally, regarding the claim of the Complainant "that his motives The complainant is a foreigner and they have nothing to do with her storage letter dated 17/9/2020 in the 'Personnel' folder", he comments that he cannot find it reason for which it was formulated. The purpose of the GDPR is to ensure it protection of the personal data of natural persons during their processing by organizations, while it was established and binds all of them

organizations operating within the European Economic Area and

of the European Union and therefore also the complaining company. Further,

data subjects have the right if they consider that the personal

the data are not managed by the organizations with legal and

transparent way or if they have doubts about how they are processed to

file a complaint with the Data Protection Commissioner

of a Personal Character in order to carry out the necessary verification for the determination

of the possible violation.

B. LEGAL ASPECT:

7. Article 24 par. 1 of the GDPR refers to the responsibility of the person in charge

processing to "apply appropriate technical and organizational measures in order to

ensure and be able to demonstrate that the processing is carried out in accordance with

this regulation. These measures are reviewed and updated when

it is considered necessary." and par. 2 of the same Article states that "2. When

is justified in relation to the processing activities, the measures mentioned

in paragraph 1 include the implementation of appropriate policies for the

data protection by the controller".

8. In accordance with Article 32 par. 1(b), (c) and (d) of the GDPR, the person responsible must

processing and the processor to "apply appropriate technical and

organizational measures to ensure an appropriate level of security

against the risks, including, among others, as the case may be: (…) b) of

ability to ensure confidentiality, integrity, availability and

the reliability of processing systems and services on an ongoing basis, c)

the ability to restore availability and access to data

of a personal nature in due time in case of physical or technical

event, d) procedure for its regular testing, assessment and evaluation

effectiveness of the technical and organizational measures to ensure it

processing security…" taking into account the risks "which

result from the processing, in particular from accidental or unlawful destruction, loss,

alteration, unauthorized disclosure or access of personnel data

character transmitted, stored or otherwise submitted to

processing." (Article 32 par. 2 GDPR) and "The data controller and the executor

the processing take measures to ensure that each natural person

acting under the supervision of the controller or the person executing it

processing that has access to personal data

processed only on the instructions of the controller, unless obliged to do so

to this end by the law of the Union or the Member State". (Article 32 par. 4

GDPR)

C. RATIONALE:

9. Studying the facts before me, I find that Kathy's complaint

it maintained organizational and security measures, which, however, needed revision

and updating.

10. As can be seen from what Kathis has mentioned in the complaint, the under reference

letter was filed under the name "Personnel" on 9/17/2020 and

deleted on 9/25/2020, after the Complainant raised the issue.

10.1. At the material time, 7 of the 8 had access to the letter in question

employees who worked for the Complainant, i.e. the Managing Director

who drafted the letter, the Complainant, 2 people from the secretariat

staff, where they had the responsibility of keeping and deleting the letter and others 3

people could have access but they didn't and therefore no

became aware of the content.

10.2. After the incident is committed and the letter is deleted from the file

under the name "Personnel", Kat'is updated and revised the complaint

security and organizational measures.

11. The Complainant was a manager of the Complainant

company. The content of the letter in question was related to employment issues

nature between the Complainant and the Complainant.

12. Kat'is the complaint had and still has an obligation to observe measures

security and organization, both by virtue of the GDPR and by virtue of others

laws governing the employment relationship.

13. It is admissible from Kat'is's complaint that the letter in question does not

it should have been saved in the specific file named “Personnel”,

since it was also accessed by employees, whose responsibilities are not

were related to the specific issue.

14. I have not found bad faith in this act of the Complainant,

that is, keeping the letter in question in the file under the name

"Personnel".

14.1. The letter was deleted, on 25/09/2020, immediately after Kat'is received the

letter of the Complainant dated 09/24/2020.

14.2. No other complaint against her has been submitted to my Office

Take the complaint.

14.3. After the Complainant's letter dated 24/9/2020, Kat'is the

complaint proceeded to update and review security measures

and organization that it maintains, without this meaning that it should not continue to

undertakes additional measures as well as reviewing and updating them

existing measures at regular intervals. Additionally, proceed and

to delete/move the letter in question from the named file

"Personnel".

14.4. No damage from custody has been reported by the Complainant

of the letter in the file named “Personnel”.

15. I note that both the Complainant through his lawyers and the Ministry of Internal Affairs

Ms. the complaint, they cooperated with the Commissioner's Office from the beginning

investigation of this complaint.

D. END:

16. Taking into account all the above, I judge that the custody in question

letter in the file named "Personnel", for the specific period

period that remained there, without the appropriate security, organization and

access (e.g. limiting access to those who were necessary), recommends

violation of Articles 24 and 32 of the GDPR.

17. Article 58.2. of the GDPR, gives power to the Data Protection Commissioner

Of a Personal Nature, inter alia, to impose remedial powers and

in addition to or instead of the measures referred to in this article, to impose administrative

fine under article 83, always depending on the circumstances of each case

individual case.

18. Summarizing the above, I took into account mitigating and aggravating factors

factors and specifically

- the relatively short period of time that the said letter remained in custody

in the file named “Personnel”,

- the small number of people who had unauthorized access, 3 in total

as well as the fact that unauthorized persons did not ultimately become aware of it

content of the letter,

- the fact that the Complainant does not state what damage he suffered or could suffer

from the storage of the disputed letter in the file under reference,

6

- the immediate actions of the administration as soon as it was indicated to them by the Complainant i

incorrect storage of the letter in question, the admission as well as the

cooperation of Kathi the complaint, I judge that, in this particular case, not

the imposition of an administrative fine but the taking of a corrective measure is appropriate.

19. Therefore, pursuant to Article 58(2)(b) of the GDPR, I reprimand the

Read the complaint, for violation of Articles 24 and 32 thereof.

20. I recommend that in order to avoid similar incidents, Kathys proceeds to

regular intervals to review and update the procedures

security and organization, both those concerning the termination of cooperation with

employees as well as more generally in security, confidentiality and

implementing organization.

21. In the event that it is established that the Complainant makes a similar complaint

breach of the GDPR in the next two (2) years, this reprimand will

measured in the eventual imposition of an administrative sanction against it.

Irini Loizidou Nikolaidou

Data Protection Commissioner

Personal Character

7