No. Fax: 11.17.001.007.068 September 25, 2019 Mr. XXXXXXXXXXX, Municipal Councilor DECISION OF THE COMMISSIONER FOR PROTECTION OF PERSONAL DATA SUBJECT: Complaint for violation of the GDPR On 3/15/2019 it was submitted to my Office by lawyer K.X. on behalf of its customers, XXXXXXXXXXXXXXXXX and XXXXXXXXXXXXXXXXXXXX (hereinafter "Complainants"), a complaint for illegal sharing/announcement of their personal data by unauthorized persons of the XXXXXXXXX Municipality. 1. Facts: 1.1. In particular, the lawyer of the Complainants states in his letter that his clients are workers in the Municipality XXXXXXXX and that on and/or around November 2018 they found that a directory in which their personal data, such as their names, jobs and salary, was listed, had been leaked and circulate both in public places (e.g. coffee shop) and in places used by employees of the Municipality XXXXXXXX (e.g. warehouses, canteens, etc.). 1.2. It is the claim of the Complainants' lawyer that this list is a confidential document, which was in the custody of the Municipality XXXXXXXXXXX and the administrative staff of the Municipality have access to it. 1.3. As a result of the leak, his clients have been damaged as the release of their data, and especially their payroll, has been commented on in the form of gossip and belittling, and even mockery, both by their neighbors and by their colleagues who work in other sectors of the business. Municipality and/or in other Municipalities. 1.4. Pursuant to Article 57(1)(f) of Regulation (EU) 2016/679 (hereinafter "GDPR 2016/679"), on 27/03/2019 via email, my Office informed the Municipality XXXXXXXX of the allegations of Complainant and asked for his own opinions and positions on the matter. Positions of Municipality XXXXXXXXXX: 1.5. The lawyer of the Municipality of XXXXXXXXXXXXXXXXX, responded with an electronic message dated 3/6/2019, in which, among other things, the following are mentioned: 1.6. On 29/8/2018, a session of the Administrative Committee of the Municipality was held, where the Mayor, among other issues, informed the members of the Administrative Committee about the process of joining the Water Supply Department of the Municipality XXXXXXXXX to the Larnaca Water Supply Council (hereinafter "SYL"). The two complainants are employees of the Water Supply Department of the Municipality of XXXXXXXXXXXXXXXX. Following the session, the list of Municipality employees who will join/move to SYL was discussed. The list in question was prepared by the Municipal Treasurer and reproduced in seven (7) copies, which were delivered to the Mayor in a sealed envelope. Each councilor who took part in the session of the Administrative Committee, officially received a copy of the list. 1.7. On 5/9/2018, a new session of the Management Committee was held, during which, in addition to other matters discussed, the Mayor expressed his displeasure that the list had been leaked between 29/8/2018 and 31 /8/2018, to people outside the Administrative Committee and more specifically to the workers of the Water Supply

Department of the Municipality themselves. In addition, the Mayor reminded all the members of the Administrative Committee, the duty of confidentiality and privacy that the members of the Municipal Council have, in relation to the communication of confidential documents and information to unauthorized persons. 1.8. At the session in question, you admitted that you gave a copy of the list to a third person, but without, as you stated, having a bad intention, since "those on the list knew that they would be transferred to SYL". 1.9. Following your admission, the Municipality proceeded with an internal investigation where it was found that the list was given by you to the Foreman of the Water Supply Department of the Municipality XXXXXXXXXX, who in turn forwarded the information of the list to the workers/employees of his department. In the list in question, information was written about the people who would join the SYL, such as name, date of employment, position scale, scale level in which the employee is and salary details. 1.10 On 18/6/2019, the lawyer of the Municipality XXXXXXXXX, sent via e-mail, an excerpt of the minutes of the session dated 5/9/2018 of the Administrative Committee of the Municipality, in which your statement of admission is recorded, that is, you gave a copy of the list to a third person, since according to your claim everyone who was on the list knew that they would be transferred to SYL. 1.11. Pursuant to Article 57(1)(f) of Regulation (EU) 2016/679 (hereinafter "GDPR 2016/679"), on 19/06/2019, my Office informed you about the allegations of both the Complainants and the Municipality XXXXXXXX and asked for your own opinions and positions on the matter. Your Positions 1.12. In your letter dated 7/18/2019, you state that you do not disagree with the position of the Municipality XXXXXXXXXX and that with good intentions you gave the Supervisor of the specific Department the list, for internal use, since you knew that all the information contained in said list was known to those affected and interested. 1.13. Specifically, as you mention, the list had recorded those transferred to SYL, who knew about their transfer, as well as their specialties and salaries, information known to each other, since they have been working together for years and know each other's information elsewhere. 1.14. You repeat, that the list in question was given without bad intention and without knowing that there is any violation, since the specific information was known to all those affected and was given internally to the Municipality. 1.15. Pursuant to Article 57(1)(f) of Regulation (EU) 2016/679 on 16/07/2019, my Office informed the Superintendent I.K. about the allegations of the complainants and the Municipality XXXXXXXXX and requested his own views and positions on the matter. 2 Foreman Positions XXXXXXXXX 1.16. The Foreman XXXXXXXXXXX with a letter dated 30/7/2019, confirmed the promotion of the list to the existing employees of his Department, presenting as an excuse that the data of the list were already known to those affected. He did not have any bad intention or purpose to harm those affected by his act and moreover his own data was also included in the said list. 1.17.

On 05/08/2019 I sent you a letter stating that based on the data in front of me and the legal analysis thereof, I judged prima facie a violation of Articles 4, 5, 6 and 32 of GDPR 2016/679 and called you, in the context of right to be heard, to submit your positions and opinions regarding possible violations on your part of these provisions, as well as for what reasons you believe that any corrective measure or administrative fine should not be imposed on you based on the powers granted to me by the articles 58 and 83 of GDPR 2016/679 and article 24(b) of Law 125(I)/2018, within 4 weeks from the date of receipt of the letter. Your Positions after the prima facie decision 1.18. In your reply, 03/9/2019, regarding the prima facie decision dated 05/8/2019, state that in your opinion, Articles 4, 5, 6 and 32 of GDPR 2016/679 were not violated by the act you to give internally to the Superintendent of the Water Supply Department, a document, which contained information that was known to all those affected. 1.19. The document was provided in good faith for the internal information of the Overseer, contained information already known to the Overseer and was provided for his own use only. 1.20. Finally, as you mention, you do not know the new GDPR legislation in depth, but you are available for further information so that you do not fall into a similar incident. 2. Legal aspect: 2.1. In article 4. par. 1 of the GDPR it states that personal data is "any information concerning an identified or identifiable natural person ("data subject"); an identifiable natural person is one whose identity can be ascertained, directly or indirectly indirectly, in particular by reference to an identifier such as a name, an identity number, location data, an online identifier or one or more factors that characterize the physical, physiological, genetic, psychological, economic, cultural or social identity of the data subject due to a natural person" while in article 4 paragraph 2 it is stated that personal data processing concerns "any act or series of acts carried out with or without the use of automated means, on personal data or sets of personal data, such as the collection, registration , organizing, structuring, storing, adapting or changing, retrieving, searching for information, the use, disclosure by transmission, dissemination or any other form of disposal, association or combination, restriction, deletion or destruction". In article 4. par. 7 it is mentioned as a data controller "the natural or legal person, i public authority, or agency or other entity that, alone or jointly with others, determine the purposes and manner of processing personal data" and in Article 4. par. 11 of GDPR 2016/679 the term consent is defined "as any indication voluntary, free, specific, explicit and fully aware, by which the data subject expresses that he agrees, by statement or by a clear positive action, to be the object of processing the personal data concerning him;...". In Article 4, paragraph 12, a breach of personal data is defined as: "a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise submitted to processing,"…… 2.2. Additionally, Article

5(1)(b) of the GDPR states, among other things, "1. The personal data: ……. b) are collected for specified, explicit and legal purposes and are not further processed in a manner incompatible with these purposes; …….»……., 2.3. Article 6 of the GDPR sets out the circumstances in which a processing becomes lawful. In the absence of another legal basis (Article 6(1)(b) to (f), the communication of the data concerning the Complainants should be based on their consent. Article 6(1)(a) of the GDPR, among other things, provides that the processing is lawful only if and as long as at least one of the following conditions applies:……. a) the data subject has consented to the processing of his personal data for one or more specific purposes…….”…… 2.3. 1. In paragraph (4) of Article 6 of the GDPR it is explained that "When the processing for a purpose other than that for which the personal data have been collected is not based on the consent of the data subject or on the law of the Union or the law of a Member State which is a necessary and proportionate measure in a democratic society to ensure the purposes referred to in Article 23 paragraph 1, the controller, in order to ascertain whether the processing for another purpose is compatible with the purpose for which the personal data are initially collected , takes into account, among other things: a) any relationship between the purposes for which the personal data have been collected and the purposes of the intended further processing, b) the context in which the personal data were collected, in particular with regard to the relationship between of the data subjects and the controller, c) the nature of the personal data of nature, in particular for the special categories of personal data processed, in accordance with Article 9, or whether personal data related to criminal convictions and offenses are processed, in accordance with Article 10, d) the possible consequences of the intended further processing for the data subjects, e) the existence of appropriate guarantees, which may include encryption or pseudonymisation". 2.4. Recital 50 of the GDPR's Preamble explains that "The processing of personal data for purposes other than those for which the personal data were originally collected should only be permitted if the processing is compatible with the purposes for which the personal data were were originally collected. In this case, a legal basis separate from that which allowed the collection of the personal data is not required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of public authority delegated to the controller, Union or Member State law may determine and determine the tasks and purposes for which to be considered compatible and lawful for further processing. Further processing for archiving purposes in the public interest, for the purposes of scientific or historical research or for statistical purposes should be considered a compatible lawful act of processing. The legal basis provided by Union or Member State law for the processing of personal data may also constitute the legal basis for further processing. In order to ascertain whether the purpose of the further

processing is compatible with the purpose of the initial collection of the personal data, the controller, if it meets all the requirements for the lawfulness of the initial processing, should take into account, among others: any links between of these purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of the data subject based on his relationship with the controller regarding their further use; the nature of the personal data character; the consequences of the intended further processing for the data subjects; and the existence of appropriate safeguards for both the initial and the intended further processing acts". 2.5. According to Article 32 of the GDPR concerning the security of processing: "1. Taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and freedoms of natural persons, the controller and the executor the processing implement appropriate technical and organizational measures in order to ensure the appropriate level of security against risks, including, among others, as appropriate: a) the pseudonymization and encryption of personal data, b) the ability to ensure confidentiality, integrity, availability and reliability of processing systems and services on an ongoing basis, c) the possibility of restoring the availability and access to personal data in a timely manner in the event of a physical or technical event, d) a procedure for the regular testing, assessment and evaluation of efficiency being the technical and organizational measures to ensure the security of the processing. 2. When assessing the appropriate level of security, particular consideration shall be given to the risks deriving from processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise submitted to processing. 3. Compliance with an approved code of conduct as referred to in article 40 or an approved certification mechanism as referred to in article 42 may be used as evidence of compliance with the requirements of paragraph 1 of this article. 4. The controller and the processor shall take measures to ensure that any natural person acting under the supervision of the controller or the processor who has access to personal data processes it only on the instructions of the controller, unless required to do so by Union or Member State law." 2.6. Additionally, Recitals 74 and 83 of the Preamble of the GDPR state, among other things, that the controller should be required to implement appropriate and effective measures and be able to demonstrate the compliance of the processing activities with the GDPR, including the effectiveness of meters. 2.7. Such measures should take into account the nature, context, scope and purposes of the processing and the risk to the rights and freedoms of natural persons. To maintain security and avoid processing in breach of this Regulation, the controller or processor should assess the risks involved in the

processing and implement measures to mitigate those risks, such as through encryption. These measures should ensure an appropriate level of security, which includes confidentiality, taking into account the latest developments and the costs of the application 5 in relation to the risks and the nature of the personal data to be protected. 3. Rationale: 3.1. After a previous investigation, we found that the Department of Water Supply of the Municipality XXXXXXXXXX will be abolished and its workers/employees will be transferred to SYL. The interested parties were aware of the procedure and were aware of their transfer to SYL. 3.2. In this case, there is an admission that you gave a copy of the list to the Foreman of the Water Supply Department of the Municipality XXXXXXXXXX. Then the Foreman forwarded the said list to the workers of his Department, the details ofwhich, together with his own, are included in the list under reference.

3.3. Your acknowledgment that you have given a copy of the directory to a third party exists recorded in the minutes of the session dated 5/9/2018 of the Administrative Committee of of the Municipality XXXXXXXXXX and as an excuse for your act, you stated that all those who were in the list they knew that their move to SYL was imminent.

3.4. Furthermore, in your letter dated 7/18/2019, which responded to his letter of my office dated 19/6/2019, you confirmed that you yourself gave the Overseer the list under reference, acting as you state in good faith if all the concerned and affected, knew about their movement and rest items listed in said list. This fact has made you separate data controller with all the resulting obligations under the GDPR.

3.5. Even if it is accepted that the information concerning the Complainants, art many are known to their colleagues, however this does not give you the right to them you are sharing this information without their consent.

3.6. The full name of the employees who would be transferred to SYL was so well known to the directly interested parties as well as to other employees, both of the Municipality XXXXXXXXXX, as well as of SYL. The data mentioned in the reference list and concern for employees are the following: a) full name, b) position title, scale position, scale step in which it is located and date of placement in it and c)

salary details.

3.7. All employees of the Municipality XXXXXXXXXXX are included in the organizational chart. In the organizational chart refers to the duties performed by each employee as well as to specialty of each of them. Therefore, for these facts, both the Complainants as much as other persons have knowledge. The recruitment date is known to be observed hierarchy in each Department and by extension also in the Water Supply Department.

3.8. In the Pan-Cypriot Collective Agreement of Labor Personnel of Municipalities, signed on 5/12/2017 between the Union of Municipalities, including the Municipality XXXXXXXXXXXX and of the Federation of Associations of Semi-State Organizations OHO-SEK and the Syntechnia Parastatal, Municipal and Community Employees of Cyprus PEO, article 14 entitled Payroll/Rises, it states “Granted automatically to workers any general increase or any percentage increase will be agreed between the Ministry Finance and Trade Unions, for Municipalities (including similar ones benefits). The salary scales of the working staff of the Municipalities are shown in Annex 2, of the Convention.

3.8.1. In Appendix 2, the basic salary of each year and grade is detailed employee. In addition, there are clarifications for the position scale, i.e. D6 is a worker

dog cars (such as the Complainant XXXXXXXXX) and D7 working driver (except crawlers) (like Complainant XXXXXXXXX).

3.9. From the above, it follows that the identity of the Complainants can directly be ascertained and identified, as the conditions of Article 4 of the GDPR for face identification.

3.10. The data referred to in this catalog were collected for a specified, express purpose and legitimate purpose, namely to be taken into account in the proceedings of the Administrative session Committee of the XXXXXXXXXX Municipality, held on 29/8/2018 in the matter

concerned the process of joining the Water Supply Department of the Municipality XXXXXXXXX to

SYL and the employees who will join/transfer to SYL from the Municipality XXXXXXXXXX.

Any further processing of them which is not consistent with the original purpose, constitutes

violation of Article 5(1)(b) of the GDPR. Your act of giving the directory to

Caretaker, even internally as you claim, for his own use, constitutes further

processing, which is not consistent with the original purpose.

3.11. Both the Complainants and the other persons mentioned in sub

directory reference did not consent to further processing of personal data

them and the unauthorized disclosure and/or distribution of said catalog without the

their consent, constitutes a violation of Article 6(1)(a) GDPR.

3.12. You, as a separate controller, did not take any measures to

protection of the personal data of the Complainants, mentioned in the list,

as provided for in Article 32 of the GDPR. Instead, you shared without

authorization of said list to the Overseer.

3.13. With regard to the Claimants' lawyer's claim that the list

circulated in public places (e.g. XXXXXXXXX's coffee shop) and in places where

used by employees of the Municipality XXXXXXXXXXXX (e.g. warehouses, canteens, etc.), this does not have

proved according to the evidence before us. The documented leak is from you

to the Overseer, a fact which you yourself admit. From now on,

anyone, including

of the Complainants themselves, may

used information contained in said directory.

3.14. The Complainants, according to their lawyer's letter, state that

found the directory leak in and/or around November 2018, that's almost three

(3) months after the City Council investigated the matter. His letter

of the Complainants' lawyer, is dated 29/1/2019 and was delivered to my Office

on 3/15/2019. The time elapsed since the actual date of the event, end

August 2018, until his termination in my Office is about seven (7) months.

3.15. The admission, that you gave the Overseer the list in question, with good

intention, as you state, and given that the personal data included

in the list were already known, it does not negate the fact that you disclosed without permission and

without consent, personal data of Complainants.

3.16. In addition, your claim that you do not know GDPR 2016/679 in depth does not constitute

justification. You also have an obligation as a citizen but more specifically as an official, that is

Municipal Councillor, be aware of the provisions of GDPR 2016/679 and protect the

rights of data subjects.

3.16.1. On and/or about 25/5/2018 it was placed in the mailboxes of the Primary School Members

Council, Administrative Note on the Subject: General Data Protection Regulation

(GDPR) in which it is stated, among other things, that "Personnel data

7

is

how

and which one

of our work.

Especially important

character we collect should be limited to what is necessary for processing

of

data

we transfer/share with third parties"….. Therefore, the Municipality XXXXXXXXXXX had already

inform the members of the Municipal Council, and therefore you, about its general provisions

GDPR.

3.17. In summary, you legally own the directory, since you are a member of the Admin

Committee of the Municipality XXXXXXXXXXXX, but it does not legalize you to share and/or to

make available and/or disclose said directory to a third party, even if that

person was the Foreman.

4. Conclusion/Conclusion:

4.1. Considering the above, I have come to the conclusion that the list and specifically the

content of the directory shared by you to the Superintendent, constitutes an infringement

of Articles 5(1)b and 6(1)(a) of GDPR 2016/679.

4.2. Taking into account the provisions of article 83 of the Regulation, which concerns

General Conditions for the imposition of administrative fines, when measuring the administrative

fine, I took into account, when calculating the penalty, the following mitigating factors (a

– c) and aggravating (d – e) factors:

(a) the fact that you immediately admitted the breach;

(b) the fact that the data contained in the catalog may be exported and with

other ways, accessible to third parties

(c) the time elapsed from the occurrence of the event until the complaint to the Office

my (7 months),

(d) the nature of the violation, which affects their personal and professional life

complainants,

(e) the extent and seriousness of the infringement;

Based on Article 58(2) GDPR 2016/679, I have the power to impose an administrative sanction on

Controller (i.e. you) for violation of the provisions of the Regulation,

including the sanctioning of the administrative fine pursuant to Article 83 thereof

Regulation and therefore I DECIDE to impose a fine of One Thousand Euros

(€1,000).

Irini Loizidou – Nikolaidou

Protection Commissioner

Personal Data

8