No. Fax: 11.17.001.009.088 February 15, 2022 BY HAND DECISION Complaint for breach of personal data Mr. XXXXXX Facts Based on the duties and powers conferred on me by Articles 33(5) and 55(1) of the General Protection Regulation Given (EU) 2016/679, hereinafter "the Regulation", I issue the following decision: A. 2.1. A complaint was filed with my Office on May 7, 2021, by Mr. XXXXX (hereinafter the "complainant") against the Municipality of Strovolos (hereinafter the "Professor"). 2.2. Specifically and as stated in the complaint, an employee of the Student, collected, recording screenshots, and communicated to an unauthorized third party five forms/photos that have been printed on June 10, 2020, from the Student's Registry concerning to the complainant and the possession permit for XXXXX. In particular, the screenshots in question were shared with a lawyer in the context of filing a supplementary affidavit during legal proceedings, in which the complainant is not involved. The complainant claims that the said processing of his data was done "without having been asked or given his consent, and without any judicial or other warrant justifying the specific act by anyone." 2.3. The complainant provided my Office with the screenshots in question. More specifically, the first three documents titled "XXXXXX", include information XXXXXX, postal address and date of registration) in the street where the complainant lives. Also, in the fourth document entitled "Details of the Dealer", the name, ID number and postal address of the complainant appear. The last document entitled "TRADING XXXXXX", includes a list of the trading owners (name and postal address), in the specific street. 2.4. On September 8, 2021, based on my duty to examine complaints, pursuant to Article 57(1)(f) of the Regulation, an electronic message was sent on my behalf to the Defendant's Data Protection Officer (hereinafter the "DPO") , by which he was informed of the complaint in question and was called upon to inform me, until September 29, 2021, regarding the positions on the allegations of the complainant. More specifically, it was requested, by the above date, that you: "a) inform us about the legal basis for processing the personal data of the complainant, regarding the collection and notification of said forms by the Registry of the Municipality of Strovolos, b) inform us for the procedure followed in order to collect and share with an unauthorized third party the forms from the Registry of the Municipality of Strovolos and c) inform us by whom the request for access to the registry of the Municipality of Strovolos was made." 2.5. My Office did not receive a response to the above email within the deadline I set, and therefore on September 30, 2021, a reminder was made after telephone communication. 2.6. On October 05, 2021, following a written request from the Ministry of Internal Affairs, the aforementioned screenshots were provided, for the purpose of investigating the complaint in question, on behalf of the Defendant. 2.7. On October 14, 2021, an electronic letter was sent to the Defendant granting an exclusive deadline until October 26, 2021 for information regarding the

questions raised by an electronic message from my Office dated September 08, 2021. 2.8. On October 21, 2021, my Office received by e-mail a reply letter, of the same date, with No. Fac. 15.24.001.001.036, from the Municipal Secretary of the Defendant, in which, among other things, the following are mentioned: (a) The Defendant confirms that the request was made verbally by the lawyer Mr. XXXXXX to the employee in question How about. (b) The lawyer in question told the Defendant's employee that the disclosure of the complainant's data was "necessary for the purposes of administration of justice based on Article 5 of Law 125(I)/2018". Thus, the Defendant's employee acted voluntarily in his attempt, as he reported to the Defendant, to contribute to the case. (c) The Defendant clarifies that no written request was ever made to the Defendant by said attorney to follow the pre-established procedure for responding to such requests, but neither was a request made under the Right of Access to Public Sector information. (d) The Defendant clarifies that, at the request of lawyers, it is the policy of the Defendant that documents containing personal data are disclosed to lawyers in the event that a relevant Court Order has previously been issued. (e) The Defendant notes that the procedure followed for the collection and notification of the forms is not the appropriate procedure contained in the Defendant's data protection system. The employee in question confirmed to the Defendant that the lawyer approached him a year ago and verbally requested specific information from the Defendant's Record. (f) The Defendant admits that the employee in question recorded screenshots and without informing his supervisor or the DPO communicated them to the lawyer via fax. 2.9. Following the incident, the Defendant has taken the following actions: (a) The Defendant, following its breach response plan, has confirmed with the Defendant's IT Officer that Complainant 2's data was printed by said employee and then the DPA informed electronically all the relevant supervisors about the incident. (b) The incident was recorded and recommendations, regarding the third party notification process, were re-sent to all staff, including the employee in question. (c) The Defendant notes that he has already proceeded with an administrative investigation into the incident in question and disciplinary proceedings are expected against the specific employee. (d) A special confidentiality clause has been communicated with relevant information to all staff and recommendations and advice regarding the protection of personal data are communicated at regular intervals. (e) The Defendant intensifies the trainings and briefings of the staff regarding notifications to third parties, on the occasion of the incident in question. (f) Furthermore, the Defendant informs that there was already planned training by the Ministry of Foreign Affairs, regarding personal data breaches and the related procedures of the Defendant. 2.10. On November 03, 2021, I issued a prima facie Decision against the Defendant, with which the Defendant was requested to state the reasons why they believe that no corrective measure or administrative sanction

should be imposed and further to notify me of the particulars of the employee in question. 2.11. The Defendant, in a letter dated November 24, 2021, considers that there are no reasons and/or facts for the imposition of sanctions for the complaint under discussion. Further, it claims that, "the background data on which the Commissioner bases her prima facie findings is flawed as it contains allegations that are not facts". In support of this claim, among other things, the following is stated: (a) Pursuant to Defendant's policy, upon request of attorneys, documents containing personal data are disclosed only upon production of a relevant court order. Every request that is sent to the Professor, based on the relevant procedures, is archived by the Central Archive and handled on a need-to-know basis. For matters concerning personal data, the Office of the Ombudsman is informed, which immediately sends its own opinions and contributes to the handling of each case separately. (b) In the present case, the request of said lawyer was not formally submitted to the Defendant, except through the employee's telephone conversations with the lawyer, and as a result the Defendant was not in a position to know of its existence specific request to respond accordingly. (c) The employee in question acted voluntarily, arbitrarily, without implementing the express instructions contained in the relevant circulars of the Defendant and without first informing and/or consulting the DPO, in violation of the express policy and procedure of the Defendant which has been communicated to all employees of the Professor and for which the employee received training. (d) After a related administrative examination by the Defendant, the employee in question stated that he did not act maliciously and/or fraudulently, as he believed that the lawyer in question was an associate of the Defendant and believed that he was obligated to in notification 3 for the purpose of issuing a court decision, in accordance with article 5 of Law 125 (I)/2018, following relevant representations and statements of the lawyer in question. (e) The employee in question did not check through his supervisor and/or through the Defendant whether the lawyer in question was a partner-lawyer of the Defendant, which is not the case. (f) The employee printed the information in question through the print screen function (snapshots/screen print) via the Defendant's computer and faxed them to said attorney. (g) The Defendant notes that the screenshots in question were sent without any cover letter, in violation of the Defendant's standing procedure. Consequently, the Defendant did not have any possibility of timely information about the actions of the employee in question. (h) The printing of the data was possible, because the employee in question has access to the specific file and the ability to print, as part of his duties, as a member of the Defendant's prevention team. (i) The Defendant confirms that he has taken all necessary actions to investigate the incident and conduct disciplinary proceedings against the specific employee of the Defendant, after the incident was reported. Furthermore, the Defendant proceeds to report the lawyer in

question to the Cyprus Bar Association. (j) It is the position of the Defendant that he bears no responsibility for the specific incident, as the facts have shown. (k) In response to the First Instance Decision dated 03/11/2021, the Defendant states that, "the Commissioner's reference in paragraph 6.4.2 p. 9 of the Letter, namely: "However, there is an admission that there are appropriate means to identify such violations with the help of the Informatics Officer of the Municipality. Therefore, the Municipality did not exercise sufficient supervision, based on article 32.4 of the Regulation", does not find the Municipality compliant, is acrossafe and does not respond to the facts of the incident/complaint under consideration." (l) Furthermore, the Defendant claims that, "the reference of the Commissioner in paragraph 6.4.3 that she took into account that in 2018 a decision was issued against the Municipality with an administrative fine, and that this reinforces the fact that the Municipality continues not to exercises sufficient control/supervision, according to the position of the Municipality, establishes prejudice of the Commissioner against the Municipality and damages the principle of equality and objectivity of the Commissioner." (m) The Defendant informed me that the Defendant's employee in question is Mr. XXXXXX. 2.12. In addition, the Professor informed me of the measures he is taking to comply with the Regulation, such as: (a) Procedure for responding to data sharing requests, policy and procedures applied in the Municipality (b) General staff information, information and trainings for provisions of the Regulation, Guidance Guide for staff, (c) Personal Data Protection System (document – organizational and technical measures, physical security measures), (d) Policy for the use of information equipment and electronic communication media (e) Circulars for information of staff, (f) Taking physical and technical security measures, 4 (g) Instructions to IT Officer, regarding user roles and levels of access to the server, (h) Responsibilities of Prevention Team members. 2.13. Furthermore, the Defendant took a series of actions to deal with a possible future violation, considering options that will strengthen the Defendant's technical and organizational measures, following the suggestions made in the First Instance Decision dated 03/11/2021, as follows: (a) the deactivation of the function of printing screenshots (screenshots) is studied in connection with the daily conduct of the Professor's work, (b) the Professor studies with the heads of the departments and his advisers ways to limit and avoid present incidents in the future by taking the necessary measures in the context of the proper operation of the Defendant and the fulfillment of all his statutory duties, (c) The Defendant thoroughly examined the installation of the software DLP, which conducts audits of printer reporting reports. However, he is unable to proceed with the installation of the said software, due to costs and limited resources, (d) Before the notification of the said complaint, the Defendant examined the levels of access, specifically to data, which is considered a special category, with the aim of update the accesses and limit

them to the data that is necessary, only for the exercise of the duties of the employees. However, the Professor emphasizes that various gaps related to the design and development of the computerized system have been identified, as it is not possible to separate access to forms of the system as well as to give specific roles based on tasks. On the contrary, with regard to the external reports of the prints of the employees of the Defendant, each employee has access to his own reports and not to reports of another department. 2.14. In summary, the Defendant cites the following mitigating factors, which "should in no way be construed as admissions by the Defendant of any responsibility": (a) type of personal data and possible consequences for the data subject (the data in question do not constitute special category data and the number of recipients was small), (b) lack of malice on the part of the Defendant, (c) number of affected subjects and the degree of damage suffered by them, (d) the complainant had not made a direct complaint to Cath. 2.15. In relation to the above and in support of his positions, the Professor sent: (a) the Professor's Personal Data Protection Policy, (b) an instructional guide, containing information and informative material about the Regulation, 5 (c) samples of letters, concerning staff information about personal data, (d) letter dated 18/11/2019 to a law firm where, following a request for disclosure of personal data of third parties, the Defendant responded by requesting the legal basis and clarifying that all processing of personal data is carried out based on the provisions of the Regulation, (e) circular to the staff dated 24/10/2019, regarding personal data protection practices, (f) list of implemented actions for the year 2020. 3.1. On December 02, 2021, my Office sent an email to the employee in question, requesting his position regarding the complaint in question. 3.2. On January 04, 2022, the said employee responded with an electronic message, in which his positions are essentially the same as those of the Defendant, regarding his responsibilities, regarding the sharing of said screenshots with an unauthorized third party atom. He further informed me that he has already been "heavily punished" by the Defendant, demoting him from the position of head of the group of workers, which he held, and by extension cutting off his corresponding allowance of approximately 85 euros per month. 3.3. The responsibilities of the employee in question, as a separate controller, in the complaint under reference is the subject of an independent case/complaint against him. B. 4.1. Article 4(1) of the Regulation defines that "personal data" is "any information concerning an identified or identifiable natural person (data subject)". 4.2. In Article 4(2), processing is defined as "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 collection, registration, organization, structuring, the storage, adaptation or alteration, retrieval, retrieval of information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, limitation, deletion or destruction”. 4.3.

Further, in Article 4(7), a data controller is defined as anyone (the natural or legal person, public authority, agency or other body) who, "alone or jointly with another, determine the purposes and manner of data processing of a personal nature". 4.4. Article 4(10) defines as a third party, "any natural or legal person, public authority, agency or body, with the exception of the data subject, the responsible Legal framework 6 of processing, the processor and the persons who, under the direct supervision of the controller or processor, are authorized to process the personal data". 4.5. Article 4(11) provides that consent means "any indication of will, free, specific, explicit and fully informed, by which the data subject expresses that he agrees, by statement or by a clear positive action, to be the subject of processing personal data relating to it." 4.6. In Article 4(12) personal data breach is defined as "the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed ». 4.7. The Principles governing the processing of personal data are defined in Article 5(1) of the Regulation. In subsection (a) of this Article it is provided that, personal data must be "lawfully and legitimately processed in a transparent manner in relation to the data subject ("lawfulness, objectivity and transparency")". Also, in subsection (b) of the same Article it is stated that personal data must be "collected for specified, explicit and lawful purposes and not further processed in a manner incompatible with these purposes ("purpose limitation")". Furthermore, in subsection (f) of this Article it is provided that, personal data must be "processed in a way that guarantees the appropriate security of personal data, including their protection from unauthorized or illegal processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality"). 4.8. Article 6(1) of the Regulation, which concerns the legality of the processing, 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 personal data of its nature for one or more specific purposes, b) the processing is necessary for the performance of a contract to which the data subject is a party or to take measures at the request of the data subject prior to the conclusion of a contract, c) the processing is necessary for compliance with a legal obligation of the controller, d) the processing is necessary to safeguard a vital interest of the data subject or another natural person, e) the processing is necessary for the fulfillment of a task performed in the public interest or against the exercise of public authority assigned to the controller, f) the processing is necessary for the purposes of the legal interests pursued by the controller or a third party, unless these interests are overridden by the interest or the fundamental rights and freedoms of the data subject 7 that require the protection of personal data, in particular if the data subject data is a child. Item f) of the first paragraph does not apply to the processing carried out by public authorities in the

exercise of their duties." 4.9. In Article 6(4) of the Regulation 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 constitutes 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 others: 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 was collected, in particular with regard to the relationship between data subjects and the controller, c) the nature of the personal data ra, 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 intended further processing for the data subjects, e) the existence of appropriate guarantees, which may include encryption or pseudonymization." In Recital 50 of the Preamble of the Regulation it is explained that, "The processing of personal data for purposes other than those for which the personal data were originally collected should only be allowed if the processing is compatible with the purposes for which the personal data character 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 for further processing to be considered compatible and lawful. 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 8 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 data of a personal nature; the consequences of the intended further processing for the data subjects; and the existence of appropriate safeguards for both the initial and the intended acts of further processing". 4.10. Article 24(1)

of the Regulation states that it is the responsibility of the controller, in this case the Defendant, such as, "taking into account the nature, scope, context and purposes of the processing, as well as the risks of different possibility occurrence and seriousness for the rights and freedoms of natural persons, ... implements 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." 4.11. Article 29 of the Regulation, which concerns processing under the supervision of the controller or processor, states that, "... any person acting under the supervision of the controller or processor, who has access to personal data , processes said data only on the instructions of the controller, unless obliged to do so by Union or Member State law.' 4.12. Also, based on Article 32(1) regarding processing security, it provides that, "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 seriousness for the rights and freedoms of natural persons, the controller and the processor implement appropriate technical and organizational measures in order to ensure the appropriate level of security against the risks…". 4.13. According to paragraph (4) of the same Article, the data controller, in this case, the Defendant must take "measures to ensure that any natural person acting under the supervision of the data controller or the processor who has access to personal data processes them only on the instructions of the data controller…" 4.14. Based on Article 58(2), the Commissioner has all of the following corrective powers: "a) to issue warnings to the data controller or processor that intended processing operations are likely to violate the provisions of this regulation, b) to issue reprimands to the controller or processor when processing operations have violated provisions of this regulation, c) to instruct the controller or processor to comply with the requests of the data subject to exercise his rights in accordance with this regulation, 9 d) to instruct the controller or the processor to make the processing operations compliant with the provisions of this regulation, if necessary, in a specific way and within a certain period, e) to instruct the controller to announce the data breach of a personal nature to the data subject, f) to impose a temporary or definitive restriction, including the prohibition of the processing, g) to give an order to correct or delete personal data or limit the processing pursuant to articles 16, 17 and 18 and an order to notify these actions to recipients to whom the personal data was disclosed pursuant to article 17 paragraph 2 and article 19, h) withdraw the certification or order the certification body to withdraw a certificate issued in accordance with articles 42 and 43 or order the certification body not to issue certification, if the certification requirements are not met or are no longer met, i) to impose an administrative fine pursuant to article 83, in addition to or instead of the measures referred to in this

paragraph, depending on the circumstances of each individual case, j) to give an order to suspend the circulation of data to a recipient in a third country or an international organization." 4.15. Furthermore, Article 83 of the Regulation, which concerns the general conditions for imposing administrative fines, provides that, "1. Each supervisory authority shall ensure that the imposition of administrative fines in accordance with this article against violations of this regulation referred to in paragraphs 4, 5 and 6 is effective, proportionate and dissuasive in each individual case. 2. Administrative fines, depending on the circumstances of each individual case, are imposed in addition to or instead of the measures referred to in Article 58 paragraph 2 points a) to h) and Article 58 paragraph 2 point j). When deciding on the imposition of an administrative fine, as well as on the amount of the administrative fine for each individual case, the following shall be duly taken into account: a) the nature, gravity and duration of the infringement, taking into account the nature, extent or purpose of the relevant processing, as well as the number of data subjects affected by the breach and the degree of damage they suffered, b) the fraud or negligence that caused the breach, c) any actions taken by the controller or the processor to mitigate the damage suffered by the data subjects, d) the degree of responsibility of the controller or the processor, taking into account the technical and organizational measures they apply pursuant to articles 25 and 32, e) any relevant previous violations of the controller or processor, f) the degree of cooperation with the control authority to remedy the violation as well as the limitation of its possible adverse effects, g) the categories of personal data affected by the breach, 10h) the way in which the supervisory authority was informed of the breach, in particular if and to what extent the data controller or the processor notified the violation, i) in case the measures referred to in Article 58 paragraph 2 were previously ordered against the controller involved or the processor in relation to the same object, the compliance with said measures, j) the observance approved codes of conduct in accordance with article 40 or approved certification mechanisms in accordance with article 42 and k) any other aggravating or mitigating factor resulting from the circumstances of the specific case, such as the financial benefits obtained or losses avoided, directly or indirectly, from the violation. 3. In the event that the controller or processor, for the same or related processing operations, violates several provisions of this regulation, the total amount of the administrative fine does not exceed the amount set for the most serious violation. 4. Violations of the following provisions shall attract, in accordance with paragraph 2, administrative fines of up to EUR 10 000 000 or, in the case of undertakings, up to 2 % of the total worldwide annual turnover of the previous financial year, whichever is higher: a) the obligations of the controller and the processor in accordance with Articles 8, 11, 25 to 39 and 42 and 43, b) the obligations of the certification body in accordance with Articles 42 and 43, c) the obligations of the monitoring

body in accordance with Article 41 paragraph 4. 5. Violations of the following provisions shall attract, in accordance with paragraph 2, administrative fines of up to EUR 20 000 000 or, in the case of undertakings, up to 4 % of the total global annual turnover of the previous financial year, depending whichever is higher: a) the basic principles for the processing, including the conditions applicable to the authorization, in accordance with articles 5, 6, 7 and 9, b) the rights of the subjects of the data in accordance with Articles 12 to 22, c) the transmission of personal data to a recipient in a third country or an international organization in accordance with Articles 44 to 49, d) any obligations under the law of the Member State which are established pursuant of chapter IX, e) non-compliance with an order or temporary or permanent restriction of processing or suspension of data circulation imposed by the supervisory authority pursuant to article 58 paragraph 2 or failure to provide access in violation of article 58 paragraph 1. 6. The failure to comply with an order of the supervisory authority as referred to in Article 58 paragraph 2 shall attract, in accordance with paragraph 2 of this Article, administrative fines of up to EUR 20 000 000 or, in the case of undertakings, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. 7. Without prejudice to the corrective powers of the supervisory authorities in accordance with Article 58(2), each Member State may determine the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that member state. 11 Recital 8. The exercise by a supervisory authority of its powers under this Article shall be subject to due process safeguards under Union and Member State law, including effective judicial review and due process. 9. Where the legal system of the Member State does not provide for the imposition of administrative fines, this article may be applied in such a way that the enforcement procedure is initiated by the competent supervisory authority and enforced by the competent national courts, while ensuring that the because legal remedies are effective and have an equivalent effect to the administrative fines imposed by the supervisory authorities. In any event, the fines imposed are effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt in accordance with this paragraph by 25 May 2018 and, without delay, any subsequent amending law or amendment thereof.' 4.16. According to article 32(3) of Law 125(I)/2018, "an administrative fine imposed on a public authority or public body and related to non-profit activities may not exceed two hundred thousand euros (€200,000)." C. 5.1.1. In this case, the complainant has stated that the collection and sharing of the screenshots from the Defendant's Registry to an unauthorized third party was done without obtaining his consent and without securing any judicial or other warrant, which to be able to justify the said processing of his data. 5.1.2. In addition, in this case there is the admission of the Defendant and the employee in question that the latter acted

voluntarily, without clarifying the status of the lawyer, without following the prescribed procedures of the Defendant and without consulting the superior of. 5.1.3. This act of the employee made him a separate controller with all the entailed obligations pursuant to the Regulation and this act is being investigated separately. 5.2.1. Firstly, I believe that the incident in question could have been prevented by disabling the ability to take screenshots, which is something the Professor is considering. However, from what has been put before me, the Defendant could not have avoided the disclosure of the said screenshots, since the printing of the said data is within the scope of the duties of the said employee, who acted arbitrarily, without following the proper procedures of the Professor and without consulting his supervisor. Furthermore, the fact that he sent the said data to the lawyer via facsimile and without a cover letter made it almost impossible for the Defendant to detect the violation. 12 5.2.2. Regarding paragraphs 2.9, 2.12 and 2.13 of this Decision, I believe that the Defendant took all the necessary actions and proved that he takes seriously the need to protect the data of his citizens. 5.3.1. As mentioned in the letter dated 24/11/2021 and to the claim that,“the background of facts on which the Commissioner bases the prima facie case its findings are highly insecure as it contains claims that are not events", I wish to clarify that, although it is not clear to whom The Defendant refers to "allegations", however the facts, i.e. her incidents case, presented in Annex A of my First Instance Decision date 03/11/2021 and which are described in detail, were never disputed by him Here you go.

5.3.2. Furthermore, in the same letter of Kath'ou it is stated that, "The mention of her Commissioner in paragraph 6.4.2 p. 9 of the Letter, namely: "Nevertheless there is the acknowledgment that there are appropriate means to identify such violations with the help of the Municipality's IT Officer. Therefore the Municipality did not exercise sufficient supervision, based on article 32.4 of the Regulation", he does not find him Municipality agreed, it is extremely safe and does not respond to the facts under consideration incident/complaint."

5.3.3. I consider it appropriate to mention that, in a letter dated 21/10/2021 states that, "the Municipality and according to its response plan to violations...

confirmed with the IT Officer that the data had been printed from the

specific user". Therefore, I stand by my opinion that there are suitable ones

means to identify such violations with the help of the Operator

Information technology. However, the fact that, the control of the weekdays is acceptable

of printing in an organization, such as Kat' th, which prints thousands of documents, is

difficult to do by the IT Officer.

5.3.4. Nevertheless, an enforceable administrative act could not be based on

speculation and unsubstantiated claims. The Decisions are based on allegations which

have been documented.

5.4.1. With reference to the position of the Prosecution that, evidence of prejudice on my part n

my reference to a previous Decision of 2018 with an administrative fine of €5,000

against the Defendant, I consider it appropriate to mention that, in accordance with Article 83(2) of

Regulation, "... When making a decision regarding the imposition of an administrative fine,

as well as regarding the amount of the administrative fine for each individual case,

duly taken into account … e) any relevant previous offenses of his

controller or processor". Therefore, there is

obligation to take into account previous violations of a similar nature

data controller, in this case the Professor. Therefore, the said

reference, in no way, establishes prejudice on my part towards him

Here you go.

D. Conclusion – Conclusion

13

Based on the provisions of Article 83 of the Regulation, insofar as they apply

in this particular case, I take into account the following mitigating factors (1-5)

factors:

(1) the taking of immediate compliance measures from the moment it was notified to the Professor

the initial finding,

(2) the examination for taking more effective organizational and technical measures to

compliance with the provisions of the Regulation,

(3) the fact that the Defendant had proceeded with an administrative investigation against the person in question

employee,

(4) the fact that the Defendant had filed a complaint against the person in question

lawyer to the Pancypriot Bar Association,

(5) the time that elapsed from the occurrence of the event to the denunciation to

My office (11 months).

Taking into account the appropriate and appropriate measures taken by the Municipality of Strovolos,

I consider that the taking of any corrective measure, i.e. enforcement, is not justified

administrative fine. But given the action of the employee in question

of the Municipality, I recommend that the Municipality of Strovolos immediately repeat the training of all

of the staff of the Municipality with regard to the provisions of the Regulation, which to

repeats at regular intervals.

Irini Loizidou Nikolaidou

Data Protection Commissioner

Personal Character

/A.D.