

No. Fac.: 11.17.001.010.064 Leakage of personal data of a citizen to a third party Decision I refer to a complaint submitted to my Office, on April 11, 2022, by Mr. XXX (hereinafter the "Complainant"), against the Cyprus Electricity Authority (hereinafter the "Complaint"), regarding the leakage of his personal data to a third party. After examining the complaint, based on the powers conferred on me by Articles 57 and 58 of Regulation (EU) 2016/679 on the protection of natural persons against the processing of personal data and on the free movement of such data (hereinafter the " Regulation"), I note the following:

Incidents of the Case Positions of the Complainant 2. Complainant claims the following: 2.1. He owns a portion of land on which the Defendant intended to install an overhead or underground power line. The Complainant, as a legal obligation, drew up a relevant notice to the Complainant, dated January 20, 2022, requesting his consent for the installation of the line. 2.2. The aforementioned consent form, dated January 20, 2022, was not served, nor was it sent to the Complainant, but an Officer of the Defendant delivered it to his neighbor. 2.3. According to the Complainant, his neighbor, who is also the applicant (hereinafter the "Applicant"), invited him and his wife (as owners of the land) to his house and asked them to sign the form, hiding from them the exact position of the pile and the number of wires. According to the complaint, dated April 11, 2022, 2.4. The consent form has been shared with our Office. It contains the following personal data of the Complainant: ☐ Name ☐ Address ☐ No. Sheet/Plan, No. Plot, Location, Share – ownership status of the land. 2.5. As the Complainant clarifies, the form was irregularly given to his neighbor, as it states that it was personally delivered to him by the Officer of the Court on January 20, 2022, which did not happen. 2.6. The same consent form was post-dated to the Complainant's postal address on February 11, 2022. 2.7. On March 18, 2022, by email to XXX of the Complainant (hereinafter "XXX"), the Complainant complained about the said incident and the leakage of his personal data to a third party. 2.8. XXX informed the Complainant of the receipt of his complaint on the same day. 2.9. The Complainant sent a second letter, on the above matter, on April 6, 2022, to XXX of Cathy. 2.10. The Complainant sent a letter related to the above matter to XXX of the Defendant, on April 11, 2022, who informed him that the study has been modified and his plot is ultimately not affected. 3. Subsequently, the Complainant sent a second letter to my Office, dated May 4, 2022, in which he brought to my attention, among others, the following: 3.1. He received the Defendant's reply, dated April 18, 2022, with which he was informed of her positions regarding his complaint. 3.2. He highlighted specific provisions of the Electricity Development Law (Chap. 171), which determine the procedures that the Defendant must follow. He states that "When there is a procedure, it must be followed. If it is not followed, some must be punished. And the one who did not observe it, and his manager who did not make sure that his subordinate observed it. And in

fact after informing him of the misconduct." 3.3. He denied any relationship with the Applicant and his neighbor and stated that he does not believe there is any justification for the leak under investigation. 2 screenshot (dated January 27, 2022) with a plan in which I note that the letter dated April 11, 2022 to Ms. XXX, XXX's responses dated March 18, 2022 and April 18, the consent form dated January 20, 2022, the complaint dated March 18, 2022 and the reminder of that date 4. below: A. included notes for removal and/or movement of a pole, B. C. April 6, 2022 to XXX, D. E. 2022, and F. annexes to the Electricity Development Law (CHAP. 171). 4.1. The letters I received include positions and opinions of the Complainant, which relate to the correct procedure for drawing up a study and/or request for the movement of piles, which I will not examine, as they do not touch my responsibilities, since they do not relate to illegal processing of personal data. Positions of the Defendant on the complaint 5. In my letter dated April 20, 2022, I informed the Defendant of the allegations of the Complainant, asked for her positions and asked her specific questions regarding the incident. 6. informed, among others, about the following: 6.1. the Court, following a citizen's request, prepared a study for the purpose of moving the network, 6.2. the above move would affect the Complainant, 6.3. on January 20, 2022, the relevant consent forms were given to an Officer of the Complainant who was present during the on-site visit of her researcher, to ensure the consent of all affected persons, 6.4. the Officer gave, as he mentioned in a meeting with the head of the day. 9 May 2022, sealed file with the consent form, to the Applicant, after he assured him that he is a relative and neighbor of the Complainant and could help locate him. 6.5. the Complainant accepts that the specific act of her employee was wrong, By letter dated May 11, 2022, the Complainant with 3 It was noted that the Officer also followed the correct procedure, 6.6. the Officer realized his mistake, apologized and stated that he will not repeat something similar, 6.7. received XXX from his supervisor (XXX) and will attend mandatory specialized training on personal data and the process of obtaining consent, 6.8. the Court's Officer justified his action by stating that the Applicant knew the Complainant personally, knew where he lived, their houses were next to each other and parallel, and knew that the Complainant was a co-owner of the lot affected by the move. 7. mailing the consent form to the Complainant. 8. As the Complainant has also mentioned, on March 18, 2022, he submitted a relevant complaint to the Defendant, complaining about the leakage of his personal data. 8.1. XXX confirmed on the same day, March 18, 2022, the receipt of the complaint and launched a first investigation into the incident. On April 18, 2022, the Complainant's procedure (D-DD-102) and the legal basis of the processing of his personal data for the purposes of said procedure were sent and explained to the Complainant. With regard to his complaint, the stages followed by the Court regarding the consent form were noted and, among other things, it

was stated that "the applicant (...) assured the EAC employee that the affected owners are his relatives and that they would grant the their consent and indeed, since he knew who they were, he could help track them down. The EAC cannot know whether the applicant, knowing that you are a co-owner, approached you of his own free will to obtain consent." The Defendant noted that her response to the Complainant was sent prior to her employee's admission, on May 9, 2022, of the incorrect service of the consent form on the Applicant. Consequently, it was not clear whether the Complainant's allegations were true.

9. She attached the complaint to her electronic letter to my Office, dated May 11, 2022, Personal data breach notification form, which included the following: 9.1. On May 9, 2022, the Accused was informed by the Officer himself, that a consent form with personal data of the Complainant was delivered to the Applicant, in a closed file. 4 9.2. As noted in the Notification, the Applicant was a relative and neighbor of the Complainant, and was privy to the personal data contained in the form. 9.3. The service of the form on a third party is not provided for by the relevant procedure of the Court and was a mistake. 9.4. The Officer who carried out this act received XXX from his supervisor and XXX, apologized and stated that he will not do it again. He will also attend mandatory specialized training on personal data and the process of obtaining consent. 9.5. The complaint alleging the act was submitted to the Defendant on March 18, 2022 by the Complainant, but the Officer involved had not initially admitted the act, so there was no knowledge but possible suspicion of the wrongful act. 9.6. The reasons for causing the incident were human error, trusting the wrong person, the need to quickly serve the customer and inform the concerned owner. 9.7. The data related to the incident are, as they are mentioned above, the Name, the Address, the No. Sheet/Plan, No. Lot, Location, Share – ownership status of the land. 9.8. The incident concerns a letter and affects a data subject, namely the Complainant. 9.9. During the incident there was a relevant procedure D-DD-102 on the basis of which the actions to be taken by the Officer were determined. Also, the Professor had organized staff trainings, posted a Personal Data Protection Policy and provides frequent updates on personal data issues to her employees. 9.10. The Prosecutor considers that a possible consequence of the incident is the breach of confidentiality, although as she states the person who received the form (the Applicant) knew the data contained in it as he is a neighbor and relative of the Complainant. 9.11. The seriousness of the possible consequences is judged to be negligible, because the data was known to the person disclosed. It is assumed that there are no consequences to the personal liberties of the Complainant or any material or mental damage. 9.12. After the incident, there was written and telephone communication with relevant Officers and Managers, a video conference, pressure to admit the leak, XXX and the imposition of mandatory training on personal data. 5 9.13. The Judge considers that the

Complainant was angered by the submission of an application for the movement of the stake and submitted the complaint to my Office to facilitate the substance of his objection to the movement in question. 10. In her letter dated 11 May 2022, it was pointed out that Cyprus-wide training will be organized for all staff dealing with the Consent Process before the summer holidays, once the queries/topics for discussion have been collected first. Finally, the Complainant's correspondence with XXX, the letter dated April 5, 2022 from XXX to the Complainant and the Complainant's letter to Mr. XXX dated March 17, 2022, were attached. On June 3, 2022, my Office sent a second electronic 11. letter with additional clarifying questions in order to further investigate the incident. Specifically, the Complainant was asked about the following: 11.1. The technical and/or organizational measures it had put in place, in advance, in order to prevent any irregular actions by its employees regarding the delivery of the consent form and/or to check the consistency of its employees with the D-DD- procedure 102 which he has determined. 11.2. The stages that the Officer had to follow in relation to the service of the consent form, which were foreseen by the DD-DD-102 procedure. 11.3. Whether the consent form which was served to the Applicant and not to the Complainant, was returned by the Officer on the same day signed. That is, if field B.4. "Signature of receipt of EAC Form E-T-104, by holder/owner" which is included in the consent form and refers to the confirmation of its receipt by the holder/owner, was returned signed to Kathi on January 20, 2022, the date indicated on the form as the date of service. 11.4. Whether the specific process of giving and receiving consent is controlled by another competent employee (e.g. supervisor). 11.5. The penalty imposed on the Officer who committed the irregularity. 11.6. To what extent the employee had attended seminars on personal data and/or had received updates on them from the Client, before the incident. 12. that had been put to her, brought the following to my attention: On June 16, 2022, after studying the additional questions 6 12.1. "Letters of consent are always mailed in sealed envelopes. An envelope is not required in the service of the relevant forms, when they are given by hand to the person to whom the letter concerns. In this particular case, the relevant forms were given by an Officer of the Submissions Department to a fellow EAC Employee, in a closed envelope, which colleague delivered them to the applicant." 12.2. The complainant had been informed that the Applicant is a neighbor of the Complainant, they had known each other for some time and had generally good relations. The only affected lot owner, other than the Applicant, was the Complainant's lot, so it was felt that serving the former would complete the process more quickly. 12.3. All officers dealing with Process D-DD-102 are informed about it by their supervisor. 12.4. Relevant excerpt from Proceeding D-DD-102, "[...] After receiving the search certificate, the competent officer assigns the work, to officer XXX. He checks whether he has addresses in the search

certificate and whether they are correct. The check is done with the local authorities, with the telephone directory of A.TH.K., with the Authority's SAP program, with SATIKIN or IRIDA or with information it collects. He then writes the correct addresses and any telephone numbers he secured on the search certificate. He then plans and carries out an on-site investigation, if deemed necessary. He then registers all the information (names of owners, addresses, telephones, affected parcels, etc.) in the SATIKIN or IRIDA program and proceeds to print the forms E-DD-104 - Consent of the owner/owner of land or the form E-DD-111 - Consent form for cutting or pruning trees if it involves pruning, together with a registered letter E-DD-103 - Letter for consent of the owner/owner of land and together with a topographical plan sends them to the affected owners. In some cases, after sending the registered letter, if requested by the landowner, they arrange a meeting with the landowners for clarifications.[...]" 12.5. The consent form given to the Applicant in a sealed envelope to hand over to the Complainant was not returned to the Lady signed by the Complainant. 12.6. According to the DD-DD-102 procedure, the supervisor assigns the work to Officer XXX, who ensures the completion of the Procedure of securing the necessary Consent. 12.7. The supervisor has the responsibility of checking that the work is carried out correctly. 7 12.8. After the specific incident, a meeting was held with all XXX Officers of the Consent Procedure, in which the methodology to be followed was explained in detail in order to avoid similar incidents in the future. 12.9. XXX the imposition of a penalty on an employee of the Defendant presupposes the conduct of a Disciplinary Procedure in accordance with the provisions of the Cyprus Electricity Authority (Disciplinary Code) Regulations of 1985, as amended. It is noted that the penalties that may be imposed on an employee who is found to have committed a disciplinary offense of this nature include a reprimand and/or a severe reprimand. XXX because other measures were taken for the training of the employee in question, but also of all employees involved in this Procedure. 12.10. With reference to the 2 training seminars on personal data held in 2018 and 2019 at the Nicosia-Kyrenia-Morfos Regional Office, the specific Officer does not seem to have attended them, even though the invitation from the Human Resources Department explicitly stated that were mandatory for the staff. 12.11. Conducting seminars, around the end of September - beginning of October 2022, in the specialized training that the Distribution Department has requested for the Process in question. such 13. On July 20, 2022, I issued a prima facie Decision, in which I found, prima facie, a violation of Articles 5(1)(f), 24(1) and 32 of the Regulation. In the context of the right to a hearing granted to the Complainant, pursuant to Article 43 of the General Principles of the Administrative Law Law of 1999, Law 158(I)/1999, as amended, I requested that within six weeks of receiving the on the face of my Decision, Ms. submits the reasons and circumstances that I must take into account for the purposes of

any administrative sanction. I also called on her, within the same deadline, to inform me about her turnover for the financial year 2021 and about the number of people she employs. 14. By letter dated August 30, 2022, the Defendant submitted the reasons and circumstances that she considers should be taken into account for the purposes of imposing an administrative sanction, pursuant to Article 58(2) of the Regulation. It also noted its turnover for the year 2021 and the number of employees. The following was noted in said letter: 15. 15.1. Full admission and remorse of Kathy in relation to the incident. 15.2. The incident concerns a letter and affects a data subject. 8 15.3. The leak of the data through the delivery of a letter in a sealed envelope happened only once, and then the form was delivered in the usual way by registered letter. 15.4. The consent form included only simple personal data. 15.5. The leak was due to negligence and there was no indication of ulterior motive or malice. 15.6. To mitigate the damage, the Defendant sent the consent form by registered mail, communicated with the Complainant in writing and verbally, apologized, prepared a new study and made a decision such that the Complainant would not be affected by the network move. 15.7. The Complainant, after the incident, regularly informs her staff who handle the delivery of the letters. 15.8. Kathy is solely responsible for hand delivering the letters and consent forms. They are delivered by trained employees. 15.9. It is the position of the Prosecutor that, as far as she knows, there were no previous violations by the Consent Department. 15.10. She adopted my suggestions and states that she is always at the disposal of my Office. 15.11. The procedure for pile moves/removals will be reviewed. 15.12. After being informed about the submission of the Complaint to my Office, the Lady sent a Personal Data Breach Notification form. 15.13. There was a relevant procedure of the Distribution System Manager Directorate, in which the actions to be taken by the Operator were determined. The said procedure is under review by the competent Directorate. Queries and suggestions have been collected from each Regional Office and a workshop will be organized to correct the process and forms. 15.14. All Kathy's staff have been trained in relation to personal data. Kathy is rescheduling trainings within September-October 2022 for all staff. 15.15. Kathy has adopted a Personal Data Protection Policy which she has posted on her website and online portal for the information of all staff. 15.16. Updates its staff periodically on personal data issues (last updated 2/8/22). of the relevant forms for delivery 9 15.17. The Defendant considers that the incident cannot cause any consequence to the detriment of the Complainant's personal freedoms or any other material or spiritual damage. Legal Framework 16. Below I list the Legal Framework on which I have based my Reasoning and Conclusion. Any marking in the text is my own. 17. Pursuant to article 31 of the Electricity Law (CHAP. 170) " 31.-(1) Contractors may install any electric line either above or below ground through any land, other than land covered with buildings,

it is understood that before from laying any such line through any land the contractors shall deliver to the owner and occupier of the land, or if the owner and occupier are not known, post on the land by notice board, notice of their intention together with a description of the lines intended to be placed; and if, within fourteen days after the service or posting of the notice, the owner and occupier fail to give their consent, or if they attach to their consent any terms or conditions to which the contractors object, the Prefect after first consulting the competent local authority administration may give his consent to the laying of such lines, either unconditionally or subject to such terms and conditions as he deems just. (2) Nothing in the preceding subsection shall authorize or enable contractors to construct or place any electric line or other works in, through or upon any building or on any land covered with buildings, without the consent of the owner and owner thereof, provided that any bracing or any other support of an overhead line or any support or upright required for the sole purpose of securing the support of an overhead line may be placed on any land or building with the consent of the Parish after having previously consulted the competent authority local authority if in his opinion the owner and occupier unreasonably withhold their consent, and the Prefect after first consulting the competent local authority shall determine the amount of the compensation or the annual rent or both, which shall be paid by the contractors to the owner and occupier or to the owner or occupier as the case may be. 10 (3) Subject to the provisions of subsection (4), if the owner or occupier of any land on which any electric line has been placed requires that the position of that electric line be changed, the Prefect, after first consulting with the competent local administration authority, may written notice, to require the contractors to change the position of the electric line in compliance with the conditions which, in case of failure to reach an agreement between the parties, may be decided by the Council of Ministers whose decision is final. (4) If compensation has been paid in connection with the laying of any electric line through any land to the person requiring that the position of such line be removed or to his predecessor in title such person shall offer to the contractors such sum as may be necessary to defray the expenses of removal or removal and no further or other compensation shall be paid by the contractors in respect of such removal or removal: Provided that where any such electric line has been constructed for a period exceeding five years and in the opinion of the Cabinet the position of the line causes undue inconvenience or late development, the Council of Ministers may determine by whom and in what proportions the costs of the move or removal will be paid, and the decision of the Council of Ministers on this is final. (5) Contractors, after first securing approval from the relevant Department, may cut or remove from each side of any proposed or existing electric line all trees and bushes that may obstruct or may obstruct the construction or proper operation of any such line." 18. Based on recital 74 of the Preamble of the

Regulation, "The responsibility and obligation to compensate the data controller should be established for any processing of personal data carried out by the data controller or on behalf of the data controller. In particular, the controller should be required to implement appropriate and effective measures and be able to demonstrate the compliance of the processing activities with the effectiveness of the measures. Such measures should take into account the nature, context, scope and purposes of the processing, including the regulation, present 11 and the risk to the rights and freedoms of natural persons. According to recital 83 of the Preamble of the Regulation, "To 19. maintain security and avoid processing in violation of this regulation, the controller or processor should assess the risks involved in the processing and implements measures to mitigate such risks, such as through encryption. Such measures should ensure an appropriate level of security, which includes confidentiality, taking into account the latest developments and the cost of implementation in relation to the risks and the nature of the personal data to be protected. In the data security risk assessment, attention should be paid to the risks arising from the processing of personal data, such as the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or were otherwise processed which could lead to physical, material or non-material damage." 20. Pursuant to recital 87 of the Preamble, "It should be ascertained whether all appropriate technological protection measures and organizational measures have been put in place for the immediate detection of any breach of personal data and the immediate notification of the supervisory authority and the subject of the data. It should be established that the notification was made without undue delay, taking into account in particular the nature and seriousness of the personal data breach, as well as its consequences and adverse results for the data subject. Such disclosure may lead to intervention by the supervisory authority, in accordance with its duties and powers set out in this regulation." 21. Based on Article 4 of the Regulation, "1) "personal data": 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 , in particular by reference to an identifier such as a name, to an ID number, to location data, to online identifier or to one or more factors 12 Pursuant to Article 5 of the Regulation, which attribute to the physical, physiological, genetic, psychological, economic, cultural or social identity of the natural person in question, 2) "processing": any act or series of operations performed, with or without the use of automated means, on personal data or sets of personal data, such as collection, registration, organization, structuring, storage, adaptation or alteration, retrieval, retrieval information, use, communication by transmission, dissemination or any other form of disposal, association or combination, limitation, deletion or destruction" 22. "1. The personal



data: (...) f) are processed in a way that guarantees the appropriate security of the personal data, including their protection against unauthorized or illegal processing and accidental loss, destruction or damage, using appropriate techniques or organizational measures ("integrity and confidentiality"). 2. The controller shall be responsible and able to demonstrate compliance with paragraph 1 ("accountability")." 23. Pursuant to Article 9 of the Regulation, "1. The processing of personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or membership in a trade union is prohibited, as well as the processing of genetic data, biometric data for the purpose of indisputable identification of a person, data concerning the health or data concerning a natural person's sex life or sexual orientation." 24. Based on Article 24(1) of the Regulation, "Taking into account 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 implements 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 deemed necessary." 25. Pursuant to Article 32 of the Regulation, "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 to the rights and freedoms of natural persons, the controller and the processors 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 privacy, integrity, the availability and reliability of processing systems and services on an ongoing basis, c) the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical event, d) a process for regular testing, assessment and evaluation the effectiveness of 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 the law of the Union or the member state" 26. According to Article 57 of the Regulation,

"1. Without prejudice to the other tasks set out in this regulation, each supervisory authority in its territory: (...) f) handle the complaints submitted by the data subject or by a body or organization or association in accordance with Article 80 and investigate, in appropriate measure, the subject of the complaint and informs the complainant of the progress and outcome of the investigation within a reasonable period of time, in particular if further investigation or coordination with another supervisory authority is required" 14 27. Based on paragraph 2 of Article 58 of Regulation, the Personal Data Protection Commissioner has all the following corrective powers: "a) to issue warnings to the data controller or to the processor that intended processing operations are likely to violate the provisions of this regulation, b) to address reprimands to the data controller or to the processor when processing operations have violated the provisions of this regulation, c) instruct the controller or the processor to comply with the requests of the data subject to exercise his rights in accordance with this regulation, d ) to instruct the data 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 data controller to announce the personal data breach nature to the data subject, f) to impose a temporary or definitive restriction, including the prohibition of processing, g) to order the correction or deletion of personal data or the restriction of processing pursuant to articles 16, 17 and 18 and an order to notify these actions to recipients to whom personal data have been disclosed pursuant to Article 17(2) and Article 19, h) to withdraw the certification or to order the certification body to withdraw a certificate issued in accordance with Articles 42 and 43 or to order the certification body not to issue a certification, if the certification requirements are not met or 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 order to suspend the flow of data to a recipient in a third country or an international organization." 28. Based on Article 83 of the Regulation, "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(2)(a) to (h) and Article 58(2)(j). When making a decision regarding the imposition of an administrative fine, 15 as well as regarding the amount of the administrative fine for each individual case, the following are duly taken into account: a) the nature, gravity and duration of the violation, 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 intent or negligence that caused the breach, c) any actions taken by the controller or processor to mitigate the damage they suffered the data subjects, d) the degree of responsibility of the controller or 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 supervisory authority to remedy the breach and limit its possible adverse effects, g) the categories of personal data affected by the breach, h) the way in which the supervisory authority was informed of the breach, in particular if and to what extent the data controller or processor notified the violation, i) in case the measures referred to in Article 58 paragraph 2 were previously ordered against the data controller or processor involved in relation to the same object, compliance with said measures, j) compliance with approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42 and k) any other aggravating or mitigating factor resulting from the circumstances of the specific case, such as financial benefits gained or losses avoided, directly or indirectly, by 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 16 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 enterprises, up to 4 % of the total worldwide annual turnover of the previous financial year, 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 data subjects in accordance with Articles 12 to 22, c) the transfer of personal data to a recipient in a third country or to an international organization in accordance with articles 44 to 49, d) any obligations under the law of the Member State established pursuant to chapter IX, e) non-compliance to order or to temporarily or permanently limit the processing or to suspend the flow of data imposed by the supervisory authority pursuant to Article 58 paragraph 2 or not to provide access in violation of Article 58 paragraph 1."

In accordance with article 32 of Part X, of the Laws of 2018 and 2022 on the Protection of 29. Natural Persons Against the Processing of Personal Data and the Free Movement of such Data (hereinafter "Law 125(I)/2018") :

"32.-(1) In compliance with the provisions of article 83 of the Regulation, the Commissioner imposes an administrative fine. (2) In case of failure to pay the administrative fine referred to in subsection (1), this is collected as a civil debt owed to the Republic. (3) An administrative fine imposed on a public authority or public body and related to

activities of a non-profit nature may not exceed two hundred thousand euros (€200,000)." Rationale 17 30. First of all, I would like to point out that the illegal act of the Defendant's Officer, namely the statement on the consent form that it was personally delivered by him to the owner/owner of the land (i.e. the Complainant) which in fact it had not been done, I will not look into it as it is not within my remit. However, I will examine, based on my powers, the result of the Officer's act, namely the unauthorized disclosure of the Complainant's personal data to a third party and the Defendant's inability to locate it. According to Article 4 of the Regulation, the use or dissemination or 31. any form of disposal of personal data constitutes processing. Therefore, serving the consent form constitutes processing. The Complainant, as the person identified by the processing of the personal data included in the consent form, is the subject of the data. The Complainant, specifying the purpose and manner of processing the Complainant's personal data, constitutes the data controller. 32. Based on article 31 of the Electricity Law (CHAP. 170), the procedure for the service of the consent form is specific, and in no case does it provide for its service to a third party other than the owner. Therefore, she has admitted that serving the form on the Applicant and not the Complainant was wrong and has also filed a relevant Notice of Violation about the incident with my Office. 33. Each processor is obliged, based on Article 24 of the Regulation, to apply the appropriate measures in order to be able to check and therefore ensure that any processing it carries out is in accordance with the Regulation. These include the measures that the data controller has taken in order to prove that the processing carried out is legal. I note that, during the investigation of the Complainant's complaint dated 18 March 2022 to XXX, the Defendant was unable to ascertain whether there was any infringement, therefore she was unable to ascertain and prove whether the processing she had carried out was in all respects legal and met the provisions of the Regulation. 34. This is also noted by the Defendant herself, since she states in her electronic letter to my Office dated May 11, 2022, that "(...) the response to the Complainant was made after the first investigation of the complaint/complaint when it was not yet clear that his claims about the 18 leak were true." He points out that "After yesterday's meeting and extensive discussion both with the relevant Directors and the supervisor of the colleague who had given the file to the Applicant, it became clear that the file with the letter and the consent form was indeed given through a third party, who did not is processing. The colleague was scared and initially did not want to speak, because he feels that he trusted the wrong person, namely the Applicant (...)" 34.1. I point out that the Defendant could have established whether the consent form was served to the owner, if she had established a procedure in advance that would allow her to do so. This position of mine is supported by the fact that on the consent form there is a field in which the landowner signs his receipt by the Officer.

Therefore, there are several ways that the relevant finding could be achieved, for example the following: □ the form would be delivered in duplicate to the owner and the Officer would return one of the two forms with the receipt field filled in, □ a relevant clipping of the form concerning its delivery should be returned to the offices of Ms. I note that, the receiving field is separate from the field where the landowner gives his consent for the placement/movement of the power line. Therefore, completing the receipt does not require the consent of the owner. 34.2. Therefore, if the Defendant had defined a specific procedure in advance, in which the actions to be taken by the staff were determined, she would have been able to determine whether the form was delivered to the owner, in which case to check and/or to establish any violation. In order to verify that similar measures, such as those I describe 35. above, had not been taken by the Defendant, I requested and reviewed the excerpts related to the incident from the DD-DD-102 specified procedure. I have also considered XXX's comments regarding the implementation of the procedure in question. Apart from noting that the consent form is placed in a sealed envelope if not hand-delivered to the landowner, and that overall responsibility for checking the completion of the work rests with the supervisor, points which do not appear to be included in the process in question, I did not find that any other measure had been taken which would have prevented and/or detected the violation after the fact. 36. It therefore follows that the Defendant had not taken the appropriate measures so that she would be able to establish, and at the same time prove, whether the processing she carried out was in accordance with the provisions of the Regulation, since as she herself has states that he was not in a position to establish the violation of the Officer, if the latter did not admit his mistake on May 9, 2022. 37. In the Notification form, the Defendant noted human error, trust in wrong person and the need for quick service. In addition and according to the data I have before me, the incident is due, to a large extent, to the fact that the Defendant had not defined specific procedures and measures based on which the staff would carry out the service. Procedures which would be able to prevent any error, prevent illegal processing and/or detect any error if it has been made. 38. Therefore, I find a violation of Article 24(1) of the Regulation, since the Defendant had not implemented in advance, appropriate technical and organizational measures, to ensure that the processing under investigation was in accordance with the Regulation. Nor had he implemented measures to be able to detect and/or verify any violation. 39. I emphasize that the Defendant's position according to which, if there was no admission by the employee about the incorrect service of the consent form, he could not have established any violation, not only does not mitigate the violation, but constitutes in itself a violation of the Regulation . 40. Based on recital 87 of the Preamble of the Regulation, v the investigation of an incident should ascertain whether appropriate measures have

been put in place to immediately detect any violation. In the present case, the violation was not detected by the Defendant during the investigation of the complaint, it was confirmed only after the admission of the error by the Officer himself. As a result of this, was the insufficient and complete response sent to the Complainant by the Client, dated April 18, 2022, regarding his complaint, but also the 20 late submission of the Notification of the Incident of Violation to my Office on May 11, 2022. In Disclosure of the incident, it was reported that although the 41. complaint had been submitted to the Defendant on March 18, 2022 in writing, initially the Officer had not admitted his mistake and thus there was no knowledge but possible suspicion of the incorrect service of the consent form . In other words, the Defendant was unable to establish whether the Complainant's claim was indeed true. In the Notification, it is stated verbatim that "(...)the manner of delivery of the original letter could not otherwise be established, unless the third party or EAC employee himself corroborated the allegations", thus confirming my above positions. 42. I also note that the Defendant must implement appropriate technical and organizational measures in order to ensure the appropriate level of security, taking into account the risks that may arise from the processing of personal data. The defendant had not implemented the appropriate measures in advance in order to prevent the unauthorized disclosure of the consent form, whether these related to further training of the staff, or to control of the actions of the staff by their superiors. As a result of this, a violation of Article 32 of the Regulation, but also a violation of integrity and confidentiality, as stated in Article 5(1)(f) of the Regulation, as the Complainant's personal data were processed in a way that allowed unauthorized and/or illegal processing. 43. I notice that, although the Defendant, as she mentioned, had made frequent updates to her staff about the personal data, before the incident, these were not enough to prevent the incident. A fact that Kathy recognizes as she points out that she will carry out additional training for the protection of personal data. 44. From the clarifying questions I asked, it was confirmed that the Officer who made the mistake had never attended any seminar/training related to personal data. I note that staff training and seminars fall under the organizational measures taken by a data controller, which, as the Regulation provides, must be appropriate so that its provisions are met. I consider it necessary that the staff, who in the performance of the tasks of principle 21 process personal data in any way, receive the appropriate updates and attend trainings, so that they are aware of and understand their obligations under the Regulation. 45. I emphasize that the Defendant has recognized the sole responsibility she bears for the incident, and has indicated her full admission and remorse. He has also emphasized that the Officer's act was due to negligence and not malice/ulterior motive. As the sole person responsible for the incident, she bears sole responsibility for training and informing her staff, so that their actions do not violate the provisions

of the Regulation. Although according to the Defendant's positions, she had updated her staff at regular intervals, and had previously organized training in relation to the Regulation, as a result, as I note above, these are considered insufficient. 46. As I pointed out in the Rationale of my prima facie Decision, although the Professor recognized the necessity of organizing further training for her staff and as she mentioned she is planning seminars around the end of September - beginning of October, she did not mention anywhere, before the its issue, on July 20, 2022, that it will review and/or update the measures it has taken, so that it is able to ensure and be able to prove that the processing it carries out is in accordance with the Regulation. Following the issuance of my prima facie Decision and the analysis I provided in her Reasoning, the Court in her letter dated August 30, 2022, indicated that my suggestion for duplicate delivery of the consent form has been adopted. 47. According to the information I have received, the Lady did XXX to the Officer, without the imposition of any other penalty. As reported, additional measures were taken after the leak was discovered to prevent similar incidents in the future and to mitigate the impact on the Complainant. In particular, all XXX Officers attended a meeting where the methodology they must follow was explained in detail, and they will attend personal data related training through seminars. Also, as noted, the Officer realized his mistake, apologized and stated that he will not repeat a similar act in the future. Finally, regarding the movement of the network to which the consent form referred, a new study was prepared and a decision was made such that the Complainant was not affected by it. 22 48. I take into account that the personal data contained in the consent form do not fall into a special category of personal data as defined in Article 9 of the Regulation. I also take into account that the form was disclosed to only one person, ie the Applicant and not to an unlimited number of persons. Nevertheless, the Defendant had no reason to consider the Applicant trustworthy, as he has claimed, nor to consider that any intervention by him was impartial, nor that the wrong service would hasten any process. 49. The Defendant's claim that the Applicant knew the personal data included in the form cannot be proven, nor will it be examined. Even if the Applicant was aware of the personal data included in the form, the processing carried out is in no way legalized, nor does it change the violations I have identified. Similarly, I will not consider the position of Ms. that the Complainant was angered by the filing of the request to move the stake and filed the complaint with my Office for the purpose of facilitating the substance of his objection, as the reasons for filing the complaint do not affect, as can be seen from my findings above, but neither do they change the violations I have identified. 50. The Professor argued in the letter dated August 30, 2022, that as far as she knows, there were no previous violations by the Consent Department. A position which I cannot accept, as from what I have described above, Kathy was not in a position to check and establish whether the incident

was indeed an isolated one. The absence of previous complaints to my Office, of similar incidents, does not prove that such events had not occurred in the past. 51. Finally, in the same letter, the adoption of a Privacy Policy by the Defendant was highlighted as a mitigating factor. The purpose of the Privacy Policy is to inform data subjects about the processing of personal data carried out by the controller, its purpose, their rights and the measures taken by the latter to protect them. Therefore, although the adoption of a Privacy Policy by the Defendant is mandatory under the Regulation and is taken into positive consideration, its implementation does not mitigate the violations that I have identified. Conclusion 23 52. Based on the above findings and based on the powers granted to me by Articles 58 and 83 of Regulation (EU) 2016/679, I find a violation of Articles 5(1)(f), 24(1) and 32 of the Regulation. 53. Based on the provisions of Article 83 of the Regulation, insofar as they apply to this specific case, I take into account the following mitigating (1)-(8) and aggravating (9)-(14) factors: (1) (2) (3) (4) (5) (6) (7) (8) (9) the fact that the incident concerns a letter, affects a data subject, and the disclosure of the personal data contained in the form was made only to one person, the fact that the consent form does not include sensitive personal data, the taking of additional mitigation measures of the damage that the Complainant may suffer, the organization of staff training, the revision of the existing procedure, the full cooperation of the Defendant with my Office and the immediate adoption of my recommendation regarding the performance procedure, the absence of malice or intent violation on the part of the Defendant of the complaint, the non-existence of another, previous, related to the submitted complaint, incident on the part of the Defendant, the inadequacy of the existing form service process consents for prevention, but also detection/identification of violations of the Regulation,

(10) the fact that the Defendant discovered the infringement after it was sent regarding the letter of termination from my Office,

(11) the late submission of the Incident Notification form personal data breach,

(12) the Defendant's inability to fully investigate the complaint of the Complainant,

(13) the inadequacy of the briefings and training that the Defendant had already organized for its staff,



(14) the non-participation of all staff in personal matters

training data.

54. Having taken into account and considered-

24

(a) the applicable statutory basis for the proposed remedies

powers granted to me by Article 58(2) of the Regulation,

(b) the circumstances and factors that the Complainant raised

before me based on all existing correspondence,

(c) the above mitigating and aggravating factors.

I decided,

at my discretion and subject to the above provisions to impose on

According to the complaint, in its capacity as data controller,

Administrative Fine of €5,000 (five thousand euros), for the commission

breach of its obligations under Articles 5(1)(f), 24(1) and 32 of

Regulation (EU) 2016/679.

Irini Loizidou Nikolaidou Nicosia, September 21, 2022

Data Protection Commissioner

Personal Character

25