Athens, 06-04-2023 Prot. No. 851 A P O F A S H 16/2023 (Department) The Personal Data Protection Authority met at the invitation of its President via video conference on Wednesday, March 15, 2023 at 10.00 a.m. m., in order to examine the case referred to in the present history. The Deputy President of the Authority, Georgios Batzalexis, who was unable to attend the President of the Authority, Constantinos Menoudakos, and the alternate members of the Authority, Maria Psalla and Demosthenes Vougioukas, appeared in place of Grigorios Tsolia and Konstantinos Lambrinoudakis, who, although legally summoned, did not attend due to being unable to attend, as and the alternate member of the Authority, Nikolaos Livos, as rapporteur without voting rights. Present without the right to vote were the legal auditor - lawyer Anastasia Tritaki, as assistant rapporteur, and the employee of the administrative affairs department Irini Papageorgopoulou, as secretary. of ordinary members of The Authority took into account the following: With the no. Authority Prot. C/EIS/5888/18-09-2021 complaint to the Authority against the Independent Public Revenue Authority (A.A.D.E.) - D.O.Y. X, A complained before the Authority that he received a tax payment notice from the D.O.Y. X by simple letter to his home address. According to the complainant's claims, the sending of the tax payment notice by letter was done without a legal reason, as the complainant had made a payment on the same day 1-3 Kifisias Ave., 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr 1 of the debt attributed to him on the day of the issuance of the liquidation note, while further, according to the complainant, the notification was sent by simple letter without any prior information to him. The complainant complains that the mail folder was subsequently breached in his apartment building, revealing his income details to third parties. The Authority, in the context of examining the above complaint, with the no. prot. C/EXE/2140/27-09-2021 her document, called the A.A.D.E., as well as the D.O.Y. X, to state their views on it. With the no. prot. … (under Authority no. prot. G/EIS/8236/23-06-2022, under 4) relat.) document, notified to the Independent Support Department of the Data Protection Officer, the General Directorate of Tax Administration of the A.A .NOT. informed the Authority that the notification of acts issued by the Tax Administration to natural persons takes place in accordance with the provisions of article 5 par. 2 of Law 4174/2013 (Tax Procedure Code), a) electronically in accordance with the provisions of law 3979/2011 or to the account of the said person or his legal representative or his tax representative in the information system of the Tax Administration, which is followed by an electronic notification to his declared e-mail address, b) by registered letter to the last declared postal address of residence or professional establishment of the person in question, or c) by service on the person in question, according to the provisions of the Code of Administrative Procedure, only if service is not possible in another way. In particular, however, in par. 4 of the same article it is defined that the documents that are of an

informational nature or for the acts of administrative determination of tax (of article 32 of Law 4174/2013), can be notified by simple letter, following a decision of the Secretary General. Furthermore, the General Directorate of Tax Administration of A.A.D.E. pointed out that the regulatory 2 provisions related to the issuance and notification of the acts of administrative or corrective determination of income tax (articles 32 and 34 of Law 4174/2013), are included in the decisions of the Governor of A.A.D.E. which are issued annually and define the type and content of the personal income tax return for each tax year. In this case, the ... decision of the Governor A.A.D.E. regarding the type and content of the personal income tax return for the tax year 2020, provides that in cases where the tax determination acts are issued by the competent D.O.Y., these are notified to those submitting the corresponding return in accordance with the provisions of a' of paragraph 2 of article 5 of the Tax Procedure Code (by electronic notification). In addition, with the above document, it was brought to the attention of the Authority that the General Directorate of Tax Administration of A.A.D.E. sent on 21/2/2021 to all D.O.Y. of the territory instructions related to the notification of the documents to the taxpayers, so that these are done via electronic notification (posting on the personalized information with simultaneous sending of an electronic message), by registered letter, or by service (not by simple letter). Furthermore, with the no. first... (under Authority's first no. C/EIS/8428/01-07-2022) document, the D.O.Y. X brought the following to the attention of the Authority: that following the ... income tax declaration for the tax year, the D.O.Y. X invited the complainant to provide the necessary supporting documents in order to complete the liquidation of the statement. The complainant submitted the supporting documents on 22/06/2021, and following the relevant audit, the act of administrative assessment of tax was issued with notification number ..., which was sent to the complainant by simple letter immediately after its issuance. In order to complete the relevant file, the Authority sent to the General Directorate of Tax Administration of A.A.D.E. the no. Authority Prot. C/EXE/2265/13-09-2022 document with which he requested the presentation of the instructions, which according to the provisions contained in no. Prot. ... (under No. Prot. Authority G/EIS/8236/23-06-2022), the General Directorate of Tax Administration sent to all D.O.Y. of the territory on 2/21/2021 regarding the manner of notification of documents to taxpayers. With the no. first ... (under Authority's first no. 3 C/EIS/10558/29-09-2022) its document to the Authority, the General Directorate of Tax Administration notified the Authority of the 24/2/2021 electronic mail message to the Tax Regions of the A.A.D.E., with which, among other things, it was referred to no. prot. ATYYPD 0000119 EX 2020/21.01.2020 document of the Independent Support Department of the Data Protection Officer by which it was pointed out to the services of A.A.D.E. the risk from the use of envelopes with a large window/window,

and at the same time requested the Tax Regions to provide instructions to the D.O.Y. of their competence regarding the notification of documents to taxpayers, highlighting as a preferable solution the electronic notification of documents, while in the case of sending documents by letter, envelopes without a box/window should be used. Furthermore, with the above document, the General Directorate of Tax Administration communicated to the Authority the previous email message from 12/16/2020 to the Tax Regions of the A.A.D.E., with which it informed about the D .ORG. A. 1133075/ 13.11.2020 (Government Gazette B' 5173/ 23-11-2020) decision of the Governor of AADE, according to which the Head of D.O.Y is authorized to electronically sign certificates, attestations and other certificates etc. documents issued by the Tax Administration in order to post them in the taxpayer's MyTAXISNet personal electronic mailbox through the application of electronic notification, also requesting the provision of relevant instructions from the Tax Regions to the D.O.Y. of their competence. After examining the details of the file, the Authority sent letter no. Authority Prot. C/EX/ 3112/05-12-2022 summons for hearing to the complained A.A.D.E., the Autonomous Data Protection Officer Support Department A.A.D.E. and the D.O.Y. X, as well as the no. Authority letter C/EX/ 3110/05-12-2022 to the complainant, in order to attend, via teleconference, a hearing before the Department of the Authority on Wednesday, December 14, 2022 at 10:00 a.m. At the meeting in question, which took place via video conference, the complainant A attended, while on behalf of the complainant the following attended: a) B, employee 4 of the Independent Support Department of the General Directorate of Tax Administration, b) C, Deputy Head D.O .Y X, c) D, Employee of the Department of Compliance and Relations with Taxpayers of D.O.Y X and d) E, Data Protection Officer A.A.D.E.. Both parties, after developing their opinions orally , received during this meeting a deadline to submit written memoranda to further support their claims. Following these, the Office of the Governor of A.A.D.E. submitted on time on 09/01/2023 the no. Prot. ... (No. Prot. Authority C/EIS/99/09-01-2023) memorandum, while the complainant did not provide a memorandum. During the above hearing of 14-12-2022, but also with the no. first ... (no. first Authority C/EIS/99/09-01-2023) following the hearing of the memorandum, the complainant further argued that a) ensuring the privacy of communications must be a concern and responsibility not only of postal service providers but also of users who , among other things, they must have installed a mailbox, in accordance with what the Building Architect specifies Regulation (see article 32 Y.A. 3046/304/1989 -Government Gazette 59/D` 3.2.1989), in which the distributor must place ordinary mail; in this case, the complainant had not taken the necessary self-protection measures (placing a letterbox) to ensure on the one hand the privacy of his postal communication and on the other hand the protection of his personal data, b) the simple postal letter was and continues to be to

a large extent a widespread and universally accepted way of communication (and by extension circulation of personal data) both of the State with citizens and between individuals, and the use of ordinary mail as a way of communicating documents from the public administration to the citizen is not a practice in itself capable of endangering the security of the data of citizens, c) that in the case under consideration it is obvious that, if the complainant had received, as he should have, the necessary means of self-protection or if the illegal act of the third party had not intervened, i.e. the violation of the complainant's correspondence, as 5 exactly describes it himself, there would not have been a risk to the security of the taxpayer's personal data, as his settlement note was in a closed envelope, it had been sent to the postal address declared by the complainant himself, while only the name and surname were written on the envelope address of the taxpayer, i.e. exclusively and only the absolutely necessary information for the safe delivery of the letter to its recipient, d) from the year 2021 (for income declarations of natural persons from the tax year 2020) it is provided as the exclusive way of notification of acts of administrative determination of income tax (clearance notes) the electronic sending to taxpayers; specifically, A.1118/2021 (Government Gazette B' 2226/27-5-2021) and A.1034/2022 (Government Gazette B' 1098/11-3-2022) decisions of the Governor of A.A.D.E. regarding the type and content of the personal income tax return for tax years 2020 and 2021 respectively, provide that in cases where the tax determination acts are issued by the competent D.O.Y. (and not automatically by the system), these are notified to the submitters of the corresponding declaration, in accordance with the provisions of paragraph a of paragraph 2 of article 5 of the Tax Procedure Code (electronic notification), and it is worth noting that the Tax Administration made this change in the way of sending the administrative tax determination acts issued by the D.O.Y. (clearance notes) following the opinion of the Independent Support Department of the Data Protection Officer with a view to the protection of the personal data of taxpayers, e) there was no intention to transmit the complainant's personal data to a third party. In addition, it was pointed out the adoption of technical and organizational measures to comply with the provisions for the protection of personal data, the establishment of the Independent Data Protection Officer Support Department, the preparation of the manual "Questions and answers manual for the familiarization of A.A.D. employees .E. with the General Regulation for Data Protection 6" on behalf of the Independent Support Department of the Data Protection Officer which was posted and communicated to all employees of A.A.D.E., as well as training on matters of security and personal data protection character which was included in the mandatory basic training of the new employees of A.A.D.E.. The Authority, after examining the elements of the file and what emerged from the hearing before it and the parties' memoranda, after hearing the rapporteur

and the clarifications from the assistant rapporteur, who were present without the right to vote, after a thorough discussion, CONSIDERED IN ACCORDANCE WITH THE LAW 1. Because of the provisions of articles 51 and 55 of the General Data Protection Regulation (Regulation 2016/679) and article 9 of Law 4624/2019 (Government Gazette A´ 137) it follows that the Authority has the authority to supervise the implementation of the provisions of the GDPR, Law 4624/2019 and other regulations concerning the protection of the individual from the processing of personal data. In particular, from the provisions of articles 57 par.1 item. f of the GDPR and 13 par. 1 item g´ of Law 4624/2019 it follows that the Authority has the authority to deal with A's complaint against the Independent Public Revenue Authority - D.O.Y. X, since the complaint under 1) relates to non-automated processing (storage and disposal by means of a simple letter) of personal data, including in a filing system within the meaning of article 4 par. 2) and 6) GDPR, therefore this is a processing subject to the regulatory scope of articles 2 par. 1 of the GDPR and 2 of Law 4624/2019. 2. Since, with regard to the determination of the data controller, it is pointed out that in accordance with the provisions of article 4 para. 7 GDPR, as data controller means "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and manner of processing personal data; when the purposes and manner of 7 of this processing are determined by the law of the Union or the law of a Member State, the controller or the specific criteria for his appointment may be provided by the law of the Union or the law of a Member State". According to the Guidelines 07/2020 of the GDPR regarding the concepts of the controller and the processor1, the functional criterion is essential for determining the controller. In cases where the law establishes an obligation or imposes on an entity the duty to collect and process specific data, the purpose of the processing is often determined by law and the controller is usually designated by law to achieve that purpose, that of public duty. In this case, the legislation implicitly identifies the controller. More generally, legislation may also impose an obligation on public or private entities to retain or provide specific data. The entities in question are generally considered responsible for processing with regard to the processing deemed necessary for the fulfillment of the specific obligation2. In the public administration, the concept of the data controller presupposes to a certain extent an independent organizational structure, while the functional criterion is concluded in principle with the powers conferred by law on a specific authority, service or legal entity under public law, which should also in practice exercised by their bodies3. With reference to the hierarchical structure of public sector services, it is pointed out that from the provision of article 4 par. 7) sec. b GDPR, the designation of a particular authority, agency or organization as a data controller is not excluded, as long as it is stipulated that when the purposes and manner of processing are determined by

Union law or the law of a Member State, the 1 EDPB, Guidelines 07/ 2020 on the concepts of controller and processor in the GDPR, Version 2.0, Adopted on 07 July 2021, https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf 2 As above, par. 24. 3 See and Decision 98/2013 of the Authority, available at: https://www.dpa.gr/sites/default/files/2019-10/apofash_98_2013_anonym.pdf 8 controller or the special criteria for his appointment may be provided by the Union law or the law of a Member State. However, if such a special regulation is not contained, then it is accepted that the mere granting to the existing body of the authority to sign would not be sufficient to make it a distinct controller, if it is not accompanied by a corresponding division of powers, establishing the independence of the authorized body to determine the purpose and means of processing, as required by article 4 par. 7) sec. a' GDPR.4 3. Because, in this case, according to the provisions of article 1 of no. no. D.ORG.A 1125859 EX2020 (Government Gazette B´ 4738/26.10.2020) "Organization of the Independent Public Revenue Authority (A.A.D.E.)" (hereinafter A.A.D.E.) "1. The Independent Public Revenue Authority (A.A.D.E), hereinafter Authority or A.A.D.E, which was established with the provisions of paragraph 1 of article 1 of Chapter A` of Part One Law 4389/2016 "Emergency Provisions for the Implementation of the Agreement on Fiscal Goals and Structural Reforms and Other Provisions" (A' 94), based in Athens, is an Independent Administrative Authority without legal personality. 2. Mission of A.A.D.E. is the determination, certification and collection of tax, customs and other public revenues, which are related to the scope of its competences. 3. A.A.D.E. enjoys functional independence, administrative and financial autonomy and is not subject to control or supervision by government bodies, state agencies or other administrative authorities except for parliamentary control, in accordance with the provisions of the Rules of Procedure of the Parliament and with the procedure defined in the provisions of article 4 of Law 4389/2016.(...)". Furthermore, from article 48 of the Organization of AADE, which concerns the Public Financial Services (P.O.Y.) as Regional Services, it follows that the P.O.Y. X is a regional service of AADE that falls under the General Directorate of Tax Administration and does not have an independent legal personality. 5 4 See in Kon/no N. Christodoulou, Personal Data Law, 2nd edition, Law Library, par. 209-211, p. 66. 5 See and Decision 54/2021 of the Authority, available at: https://www.dpa.gr/sites/default/files/2022- 01/54_2021%20anonym.pdf 9 Furthermore, in accordance with the provisions of article 1 paragraph 1 of Decision No. A. 1118 of the Governor of A.A.D.E. "Type and content of the personal income tax return for tax year 2020, the other forms and supporting documents submitted with it" (Government Gazette B' 2226/27-05-2021): "1. The annual income tax returns for the tax year 2020, of those liable under paragraph 1 of

article 67 of Law 4172/2013, must be submitted, using an electronic method of communication via the internet, by the date set by the relevant provisions (…)", while according to par. 13 of the same article above "In the above cases of paragraphs 3, 7, 8, 10, 11 and 12 where the declarations are cleared and the Tax Determination Deeds are issued by the competent D.O.Y., these are notified to the submitters of the corresponding declaration by the D.O.Y. liquidation of the statement, in accordance with the provisions of case a' of paragraph 2 of article 5 of the KFD (Law 4174/2013)." (by electronic notification). Finally, it is taken into account that the notification of the acts by the competent D.O.Y. takes place following instructions which are disseminated according to the rules of the vertical hierarchy of the tax administration. From the above it is concluded that D.O.Y. X, from which the tax assessment deed was sent by simple letter to the complainant, organically, based on the legislative framework, falls under the A.A.D.E. to taxpayers, the competent local D.O.Y. act, in accordance with the Decision and Instructions of the Governor of the A.A.D.E..6 6 Contrary to the Authority's Decision 98/2013 (see above under 8), it was decided that the General Secretariat of Information Systems is an independent service with fiscal autonomy, a special accounting display of its budget in the state, a special organizational unit with its own bureaucratic organization, which corresponds directly with the public services and the governed and issues settlement notes for the determination of tax and fiscal obligations addressed to the debtors. And from the overview of the statutory powers of the G.G.P.S., it is concluded that as a public service it determines, for the first time, essential elements of the method of processing that are linked to the security of the processing, i.e. it sets the objectives of data security, plans , implements and controls the technical and organizational security measures, determines the required financial, human, etc. resources, without additionally providing for its control by another agency. 10 4. Because, according to the provisions of article 5 par. 1 of the GDPR regarding the principles that should govern the processing of data, personal data “(…) f) are processed in a way that guarantees the appropriate security of personal data, including its protection against unauthorized or unlawful processing and accidental loss, destruction or damage, by using appropriate technical or organizational measures ("integrity and confidentiality").", Furthermore, in accordance with the provisions of provision of article 4 par. 12 GDPR, a personal data breach is defined as "the breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed". A breach can potentially have various significant adverse consequences for persons, which can lead to physical, material or moral harm. The GDPR explains that this harm can include loss of control over their personal data, limitation of their rights, discrimination, misuse or identity theft, financial loss, unlawful de-pseudonymisation, damage to reputation and loss of

confidentiality of personal data of a nature protected by professional secrecy, etc. (see also paragraphs 85 and 75 GDPR). Further, in the Article 29 Working Party Opinion 3/2014 on personal data breach notification, any personal data breach is examined based on three classic security criteria: an "availability breach" will correspond to an accidental or unlawful destruction or loss of personal data; the "breach of integrity" in the alteration of personal data, and the "breach of privacy" in unauthorized disclosure of personal data or access to it7. Finally, in the Article 29 Working Party Guidelines on personal data breach notification 7 Article 29 Working Party, Opinion 03/2014 on personal data breach notification, available at: http://ec.europa.eu/ justice/article-29/documentation/opinionrecommendation/files/2014/wp213_en.pdf, p. 5. 11 character under Regulation 2016/6798 it is clarified that "(...) unauthorized or illegal processing may include the disclosure of personal data to (or access by) recipients who are not authorized to receive the data (or have access to it) or any other form of processing that violates the GDPR"9. Therefore, one of the types of personal data breach is that which is categorized based on the security principle of "confidentiality", when unauthorized access to personal data is found ("confidentiality breach"). 5. Because, in the considered complaint, taking into account all the elements of the case file, the hearing procedure and the submitted memoranda, the Authority considers that the complained processing of the sending of the tax assessment act by means of a simple letter constitutes, in accordance with the in the above considerations, breach of confidentiality (privacy), since, although the complainant had the possibility by law to take the appropriate technical and organizational measures, so that during her communication with the citizens their data would not be put at risk, she did not complied with the applicable security policy, with the result that unauthorized persons gain access to and learn about the data of the complainant, in violation of the provision of article 5 par. 1 item. f) GDPR on the obligation to observe the principle of data integrity and confidentiality10. Besides, and from the amendment of the directives of A.A.D.E. regarding the method of sending the acts of administrative determination of tax issued by the D.O.Y., a modification pointed out by the complainant and decided, according to her claims, following the opinion of the Independent 8 Working Group of Article 29, Guidelines on the notification of personal data breaches under Regulation 2016/679, WP250rev.01, ed. 3 October 207, as rev. February 6, 2018, available at: https://www.dpa.gr/sites/default/files/2020-05/wp250rev01_el.pdf 9 As above, p. 7. 10 See in this regard, Decisions 47/2009, 14/2022 and 58/2022 of the Authority, available on its website. 12 of the Data Protection Officer Support Department with a view to, among other things, the protection of taxpayers' personal data, the risk to which taxpayers' personal data are exposed through the notification of the above actions in alternative ways is acknowledged. 6. Because, in order for personal data to be

lawfully processed, i.e. processing in accordance with the requirements of the GDPR, the conditions for applying and observing the principles of article 5 par. 1 GDPR11 must be met cumulatively. The existence of a legal basis in accordance with Article 6 GDPR does not exempt the data controller from the obligation to comply with the principles enshrined in Article 5 paragraph 1 GDPR. In the event that any of the principles provided for in article 5 para. 1 of the GDPR are violated, the processing in question is considered illegal and subject to the provisions of the GDPR, and the examination of the conditions for applying the legal bases of article 6 GDPR12 is omitted. Thus, the illegal collection and processing of personal data in violation of the principles of Article 5 GDPR is not cured by the existence of a legitimate purpose and legal basis (cf. GDPR 38/2004, GDPR 43/2019). In addition, however, it is mentioned that according to the provisions of article 6 par.1 GDPR regarding the legality of processing: "1. The processing is lawful only if and as long as at least one of the following conditions applies: (…) c) the processing is necessary to comply with a legal obligation of the controller, (…) e) the processing is necessary for the fulfillment of 11 DIE, C- 496/17, Deutsche Post AG v Hauptzollamt Köln1, 16 January 2019, SC 57. 12 Compare CoE 517/2018 para. 12: "[...] in order for personal data to be lawfully processed, it is required in any case that the conditions of article 4 para. 1 of Law 2472/1997 are cumulatively met , which, among other things, stipulates that the data must be collected and processed in a legitimate and legal manner, for clear and legal purposes... As long as the conditions of article 4 par. 1 of Law 2472/1997 (lawful collection and data processing for clear and legitimate purposes), it is further examined whether the conditions of the provision of article 5 par. 2 of Law 2472/1997 [legal bases] are also met. Also, cf. SC in Plenary 2285/2001 par. 10: "[...] Only if the above basic conditions are met, the provisions of articles 5 and 7 of Law 2472/1997 apply, which impose as a further additional, in principle, condition of legal processing of personal data of a specific person, his consent". 13 of a duty performed in the public interest or in the exercise of public authority assigned to the controller,(...)" . As admitted by the complainant with no. prot. ... (under no. prot. Authority C/EIS/8236/23-06-2022) document of the General Directorate of Tax Administration regarding the notification of acts of the tax administration to taxpayers, article 5 of Law 4174/2013 (Government Gazette A' 170, Tax Procedure Code), as it was in force at the time of the events and is still in force states that: "1. The notification of acts issued, in accordance with the Code, by the Tax Administration to a taxpayer or another person, is done in writing or electronically. 2. If the act concerns a natural person, notification is made if: a) it is notified electronically, in accordance with the relevant provisions of Law 3979/2011 or to the account of the said person or his legal representative or his tax representative in the information system of the Tax Administration, which is followed by an electronic

notification to his declared e-mail address, b) sent by registered letter to the last declared postal address of residence or business establishment of the person in question, or c) delivered to the person in question, according to the provisions of the Code Administrative Procedure, only if it is not possible to serve in another way. The notification according to the Code of Administrative Procedure, according to the previous paragraph, is considered legal, as long as it is made at the address of residence or business establishment of the person in question last declared to the Tax Administration. (…) 4. By decision of the Secretary General, documents of an informative nature or acts of tax determination of Article 32 of this Code may be notified by simple letter.", while according to Article 32 of the KFD as it was in force at the time of the events and is in force "1. In cases where, according to current tax legislation, the tax return does not constitute a direct assessment of tax, the Tax Administration issues an act of administrative assessment of tax." Furthermore, in accordance with the provisions of article 1 par. 1 of Decision No. A. 1118 of the Governor of A.A.D.E. "Type and content of the income tax return of 14 natural persons for tax year 2020, the other forms and supporting documents submitted with it" (Government Gazette B' 2226/27-05-2021): "1. The annual income tax returns for the tax year 2020, of those liable under paragraph 1 of article 67 of Law 4172/2013, must be submitted, using an electronic method of communication via the internet, by the date set by the relevant provisions (…)", while according to par. 13 of the same article above "In the above cases of paragraphs 3, 7, 8, 10, 11 and 12 where the declarations are cleared and the Tax Determination Deeds are issued by the competent D.O.Y., these are notified to the submitters of the corresponding declaration by the D.O.Y. liquidation of the statement, in accordance with the provisions of case a' of paragraph 2 of article 5 of the KFD (Law 4174/2013)." (by electronic notification). 7. Since, in this case, the act of determining the tax of the complainant concerned the tax year 2020, it is concluded that the accused, did not have to notify the act of determining the tax to the complainant by means of a simple letter according to article 6 par. 1 item. c), but on the contrary, based on the provision of article 1 par. 13 of Decision No. A. 1118 of the Governor of A.A.D.E., obliged to its exclusive electronic notification. The existence of an express contrary provision issued by a higher hierarchical body also leads to the logical necessity of excluding the assistance of the condition of article 6 par. 1 item. e) on the fulfillment of a duty performed in the public interest or in the exercise of public authority. Consequently, by sending the tax assessment act to the complainant by means of a simple letter, despite the existence of a contrary legislative provision, the complainant processed his data without the assistance of the legal basis of Article 6 GDPR. 8. Because, with the entry into force of the GDPR, a new model of compliance was adopted, the central dimension of which is the principle of accountability. (Article 5 para. 2 GDPR: "The controller is

responsible and is able to demonstrate compliance with paragraph 1 ("accountability")."), in the context of which the 15 controller is required to design, implement and in general to take the necessary measures and policies so that the processing of the data is in accordance with the relevant legislative provisions. In addition, the data controller is burdened with the further duty to prove by himself and at all times the compliance with the principles of article 5 par. 1 of the GDPR. Thus, it constitutes an obligation of the data controller on the one hand to take the necessary measures on his own in order to comply with the requirements of the GDPR and on the other hand, to demonstrate at all times his above compliance. Moreover, under the GDPR, security is one of the basic principles governing the processing of personal data, while its more general responsibility for determining the appropriate technical and organizational measures in order to ensure and be able to prove the legality of a processing originates and from article 24 GDPR. 9. Because, according to Article 24 para. 1 GDPR, the controller, "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, implements appropriate technical and organizational measures in order to ensure and be able to prove that the processing is carried out in accordance with the GDPR", while "the measures in question are reviewed and updated when deemed necessary". In addition, Article 32 GDPR regarding the security of processing provides: "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 against risks, a level of security including, among others, as the case may be: (…) b) the ability to ensure the privacy, integrity, availability and reliability of the 16 systems and of processing services on an ongoing basis (…). 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. (…) 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 them only on his instructions controller, unless required to do so by Union or Member State law'. 10. Because, according to (before the implementation of the GDPR) Opinion 3/2010 of the Article 29 Working Group on the principle of accountability13, appropriate accountability measures to comply with the principles of Article 5 par.1 GDPR can include the following non exhaustive list of measures: establishment of internalprocesses before creating new processing

operations, establishing written and binding data protection policies available to data subjects, mapping processes, maintaining a list of all data processing operations, appointing a data protection officer and other persons with responsibility for data protection, providing appropriate education and training to employees in data protection, establishing procedures for handling requests for access, rectification and erasure, which must be transparent to data subjects, establishing an internal complaint handling mechanism, establishing internal procedures for the effective management and reporting of security breaches, conducting an impact assessment on the 13 Article 29 Working Party, Opinion 3/2010 on the principle of accountability (WP 173), ed. 13-

7-2010 pp. 13-14, available at:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf 17 privacy in special cases, application and supervision of verification procedures to ensure that all measures are not only envisaged as procedures, but are implemented and operated in practice (internal or external audits, etc.). Furthermore, the Authority, in the context of the implementation of the GDPR, has already referred to the controller's obligations regarding security and his more general responsibility for the determination of appropriate technical and organizational measures, proposing "appropriate" measures which may be documented in individual procedures or in more general security policies14, clarifying that "in any case, before defining the security measures to be adopted, the correct assessment of the risks and their possible consequences15 for the data subjects takes precedence...the implemented measures must be submitted to periodic, at least, revision, but also to be demonstrably validated by the management of the controller or processor16. Taking the required security measures must take into account a number of parameters, while as mandated by the principle of accountability and determined by the provisions of article 24 par. 2 GDPR, appropriate policies must be applied, depending on the processing activities17. 11. Because, from the above, it follows that the use of appropriate technical and organizational measures is required in order for personal data to be processed in a way that guarantees the appropriate security of personal data, including their protection from illegal processing and a key feature of any of a data security policy is to provide the ability, when possible, to prevent a breach and, should it hopefully occur, to respond in a timely manner. In this case it is pointed out that the issuance and notification to the competent D.O.Y. of the relevant Decision A.1118/2021 14 www.dpa.gr/ "Security" section 15 See and G. Roussopoulou, special scientist APDPH, "Processing security and notification of incidents of violation" in EKDDDA Report "GDPR: the new landscape and the obligations of the public administration", Athens, January 2018, pp. 20 ff. available

at www.ekdd. gr/images/seminaria/GDPR.pdf 16 www.dpa.gr/ "Security" section 17 See and Decisions 67/2018, 11/2022 of the Authority, available on its website. 18 of the Governor A.A.D.E. regarding the type and content of the personal income tax return for the tax year 2020, as well as related Directives, constitute in principle technical and organizational measures in accordance with the above. of Projects) take self-protection measures 12. Because, however, the complainant, as data controller, had to, in fulfillment of the obligation to take appropriate technical and organizational measures, in the context of an appropriate security policy, to ensure the observance of privacy/confidentiality also during the sending to the taxpayers, as the defective implementation of the above Decision and the relevant Directives, resulted, as predicted, in the violation of the principles of article 5 par. 1 item. f) GDPR, as well as the principles of article 6 GDPR. Besides, the reference of the complainant to the obligation of users of postal services to preserve the confidentiality of letters, in accordance with article 32 of the Building Regulations (Y.A. 3046/304/1989 of the Ministry of Environment, Spatial Planning and Public Affairs by installing a mailbox with a lock , in which the distributor must place the simple mail, has no influence on the independent obligations of the controller regarding the security of the processing, as expressly defined in articles 5 par. 1 letter f), 24 and 32 GDPR, as the said obligations as described above, are independent obligations of the data controller and do not cease to apply due to the possible provision of other obligations in different areas of law such as the referenced Building Regulation18. Consequently, sending the tax assessment document to the complainant by simple letter, despite the existence of a contrary legislative provision, constitutes a violation of the obligations of the data controller under Article 32 GDPR to implement the appropriate technical and organizational measures, while the data controller did not prove the its compliance in accordance with the principle of accountability of article 5 par. 2 GDPR. 18 See and Decision 58/2022 of the Authority, available on its website. 19 13. Because, following the above, from the elements of the file, and from what emerged from the hearing process and the submitted memoranda, the Authority finds a violation of articles 5 par. 1 item. f), 6 par. 1 item c), e) and 32 GDPR and considers that there is a case for exercising its corrective powers in accordance with article 58 par. 2 of the GDPR, as well as article 39 of Law 4624/2019, taking into account the Guidelines for the implementation and the determination of administrative fines for the purposes of regulation 2016/679 of the Working Group of Article 2919. When evaluating the data, in order to choose the appropriate and corrective measure, the Authority takes into account, based on the conditions of article 83 par. 2 GDPR , the following elements: "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 infringement and the degree of

damage they suffered" , therefore it is taken into account that the specific security breach did not take on a broader nature, while the complainant's statements do not directly indicate his material damage that can be attributed with certainty to the breach in question, (Article 83 par. 2 par. a). these, may be an indication of negligence (Article 83 par. 2 letter b) GDPR), "any actions taken by the controller or processor to mitigate the damage suffered by the data subjects", so it is taken into account that the complainant could not 19 Available at: https://www.dpa.gr/sites/default/files/2019-12/wp253_el.pdf Additionally taking into account the Guidelines 04/2022 for the calculation of administrative fines under GDPR of the European Data Protection Board from 12.05.2022 under public consultation, available at the link https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf 20 Available at: https://www.dpa.gr/sites/default/files/2019-12/wp253_en.pdf. 20 take actions to mitigate the damage suffered by the data subject (Article 83 par. 2 letter c) GDPR), "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", therefore it is taken into account that the complainant has taken certain technical and organizational measures pursuant to Articles 25 and 32 GDPR to ensure confidentiality, however she must take technical and organizational measures for all stages of processing (article 83 par. 2 letter d) GDPR), "any relevant previous violations of the controller or the processor", therefore the conclusions of Decisions 54/2021 and 58/2022 of the Authority21 are taken into account, as in accordance with the Guidelines of the Article 29 Working Group on the application and determination of administrative fines22, any type of infringement of the regulation, although different from the infringement examined in the particular case by the supervisory authority, may be "relevant" for the assessment, since it may to be indicative of a general lack of knowledge or disregard for the rules ondata protection, (article 83 par. 2 letter e) GDPR).

• "the categories of personal data affected by the breach",

therefore it is taken into account that the violation established above does not concern

special category of personal data of the complainant (Article 83

par. 2 item g) GDPR)

• "any other aggravating or mitigating factor arising from the circumstances

of the specific case, such as financial benefits obtained or losses

21 Available on the website of the Authority.

22 See Guidelines 04/2022 for the calculation of administrative fines under the GDPR

of the European Data Protection Board from 12.05.2022 under public consultation,

available at: https://edpb.europa.eu/system/files/2022-

05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf, p. 15:

"Supervisory authorities should take into account that, in this case, the scope of the assessment

it can be quite broad as well as any kind of violation of the regulation, although

different from the offense examined in the specific case by the supervisory authority,

it may be "relevant" to the assessment since it may be indicative of a more general one

lack of knowledge or disregard for data protection rules.", p. 15.

21

which were avoided, directly or indirectly, by the infringement.' is therefore taken

bearing in mind that the accused did not present any benefit from the case (article 83 par.

2 pcs. k) GDPR).

FOR THOSE REASONS

The beginning

finds that the complained processing of the assignment of the act

determination of tax by means of a simple letter constitutes a violation of articles 5 par.

1 pc. f), 6 par. 1 item c), e) and 32 GDPR and reprimands under article 58

par. 2 item b) GDPR to the complainant, for the reasons that are extensively analyzed

in the reasoning of the present.

The president

George Batzalexis

The Secretary

Irini Papageorgopoulou

22