Athens, 02-11-2022 Prot. No.: 2778 DECISION 58/2022 (Department) The Personal Data Protection Authority met as a Department following the invitation of its President in a meeting via video conference on 28.07.2022, in order to examine the case referred to in the history of the present. The Deputy President, Georgios Batzalexis, obstructing the President of the Authority, Constantinos Menoudakos, the regular member of the Authority, Grigoris Tsolias, as rapporteur and the alternate member Demosthenes Vougioukas, in place of the regular member Konstantinos Lambrinoudakis, who although legally summoned, appeared. in writing, did not attend due to disability. Present, without the right to vote, were Anastasia Kaniklidou, specialist scientist - lawyer, as assistant rapporteur and Irini Papageorgopoulou, employee of the administrative affairs department, as secretary. The Authority took into account the following: With his complaint No. C/EIS/2015/22-03-2021, A (hereinafter "the complainant"), complains to the Independent Public Revenue Authority (IAD .E) (hereinafter the "complainant") for violation of the provisions of the legislation on personal data (breach of security), as well as for wrongful satisfaction of the right to information. In particular, according to the complaint, the complainant received during the two previous years the settlement note of his tax return in a file that did not meet the specifications and security requirements of EETT and ADA. E., and in particular in a file with a window/box, in such a way that information of a sensitive nature, such as his total declared income, has been leaked to an unspecified number of people. As the complainant claims, the error in question concerns either the selection of the pre-configured envelopes or occurred during the encapsulation of the content by A.A.D.E or, finally, by the postal service provider, i.e. ELTA. Subsequently, on ... he sent a request to A.A.D.E., with which he requested an explanation from the latter as the Data Controller for the said violation of the security of his personal data. In addition, the complainant, invoking article 13 of the GDPR, requested full information from A.A.D.E.: i) about the processing of his personal data (with more specific reference to the identity of all those responsible, performing and sub-performing the processing of his personal data and their contact details, as well as any third parties to which his data had been made public, including the name and contact details of the recipients), as well as ii) for the role of ELTA S.A. in said processing of his personal data and the possible existence of a contract between ELTA S.A. and of A.A.D.E. pursuant to Article 28 of the GDPR. Finally, in view of the imminent receipt of a new settlement statement, the complainant objected to the processing of his personal data in this way, so that the incident would not be repeated. On his above request, on ... as the complainant claims, he received a response from the complainant, although according to his claims, the latter did not satisfactorily answer his questions and in particular his question regarding the role of A.A.D. .E and ELTA SA. in said processing. The Authority, in the

context of examining the above complaint, with the no. prot. C/EXE/995/05-04-2021 her document, informed the complainant and the Independent Data Protection Officer Support Department of the complainant about the complaint and invited them to express their views on it. In response to the above document of the Authority, was submitted under no. ... (and with no. prot. APD C/EIS/2686/20-4-2021) response of the Independent Data Protection Officer Support Department of A.A.D.E. In the above response it is understood that, following the complaint submitted by the taxpayer (current complainant) 2 through the electronic platform of the Taxpayer Service Center, the Independent Data Protection Officer Support Department of the complainant sent a document to the Director General of Tax Administration in which suggested that for data protection reasons electronic notification of documents to citizens should be chosen and that "the files in question should be destroyed". Subsequently, the complainant notified the data breach to the Authority (with protocol no. C/EIS/874/04-02-2021 notification) but did not make an announcement to the data subject, since she was already aware of this. Subsequently, as stated in the above response, on ..., the Independent Data Protection Officer Support Department of AADE responded to the taxpayer-complainant, satisfying, according to his claims, his right to information. With reference to the claim of the complainant that the right to information exercised by him under Article 13 of the GDPR was not satisfied, especially with regard to the role of A.A.D.E and ELTA S.A. in the said processing, as the Independent Support Department of the Data Protection Officer of A.A.D.E claims, responded to the complainant's request by informing him of all the information required under the GDPR, and the requested further information (signing an agreement of article 28 of the GDPR between A.A.D.E and ELTA) are not the subject of the right to information according to articles 13 and 14 GDPR. Following the above, a supplementary notification of a data breach was submitted according to Article 33 GDPR (with Authority protocol number C/EIS/2163/30-03-2021). intermediaries With regard to the claim of the complainant that his personal data (specifically the annual gross income) was leaked to employees of A.A.D.E., persons, including his neighbors, the Autonomous Data Protection Officer Support Department of A.A.D.E. D.E claims with his above response that there was no documented violation of his personal data, given that the complainant's unspecified number of income tax returns for 3 tax years 2017 and 2018 were both cleared on ..., the files containing them were sent at the same time and received by their recipient, complainant, inviolable/sealed. Furthermore, in accordance with the above response of the Independent Data Protection Officer Support Department of A.A.D.E. the complainant does not cite any specific incident from which it can be deduced that a specific third party became aware of his personal data, while the employees of A.A.D.E. processed the personal data of the complainant in

the context of the exercise of their duties, bound by the duty of confidentiality and tax confidentiality. And the employees of ELTA S.A. processed the personal data in the context of the performance of their duties, bound by the duty of confidentiality. Subsequently, the Authority with nos. C/EXE/678/14-03-2022 and C/EXE/679/14-03-2022 documents it invited the complainant and the AADE with the indication that the Independent Support Department of the Data Protection Officer should also attend, respectively, as presented at a meeting of the Authority on Wednesday 23.03.2022. At this meeting, the examination of the case was postponed to 04.05.2022 at the request of the complainant. The new meeting was attended by Augustinos Kogievinas (AM/...) and Apostolos Vorras (AM/...), attorneys-at-law of the complainant, while B, an employee of the Independent Support Department of the General Directorate of Tax Administration, attended on behalf of the complainant, while C also attended , Data Protection Officer of AADE. During this meeting, those present, after developing their views, were given a deadline to submit written memoranda until 27.05.2022. Following this, the parties submitted their relevant memoranda on time, namely the complainant from ... with the no. protocol G/EIS/ 7534/30.05.2022 his document, and the Office of the Governor of AADE the under no. prot.: ... (and with APD protocol number C/EIS/7521/27.05.2022 document). The complainant, both at the hearing and in his pleadings, supported the allegations in his complaint, reiterating that: 4 (a) The files in question were sent to his former distribution point, ... and remained exposed to public view, for a long period of time , ... (b) AADE did not respond to his request to define the roles between ELTA and AADE and therefore violated the obligation of Article 13 GDPR. (c) The personal data leaked to an unspecified number of people was of a sensitive nature, taking into account the type of information, ... and the possible impact. (d) This is not an isolated incident, but repeated negligent behavior by AADE. The complainant, both during the hearing and with the memorandum, reiterated the positions supported by the Independent Support Department of the Data Protection Officer of the complainant with the Authority's protocol number C/EIS/2686/20-4-2021 document and specifically made the following allegations: (a) Personal income tax returns are generally submitted by taxpayers electronically, through their Taxisnet account and the myAADE digital portal, are cleared electronically and are notified electronically to taxpayers, while only in exceptional cases where the liquidation of the personal income tax return cannot be carried out electronically, as in the present case, a manual liquidation and notification of the act of administrative tax determination is carried out by the competent DOU. (b) During the period in question, DOU ... did not carry out a mass dispatch of settlement notes, and the incorrect placement of the settlement notes is an isolated incident, due to human error. (c) The handling of the complaint was completely appropriate, and after the incident, the General Directorate of

Tax Administration sent to all the D.O.Y of the territory the instruction to use envelopes without a box/window in the correspondence with the citizens, subsequently no order was given to 5 all Services of the D.O.Y. to discontinue the supply of windowed/slotted envelopes. (d) From the year 2021, electronic sending to taxpayers is now provided as the exclusive way of notifying the acts of administrative determination of income tax (clearance notes). The Authority, after examining the elements of the file, after hearing the rapporteur and the clarifications from the assistant rapporteur, who was present without the right to vote, after a thorough discussion, DECIDED IN ACCORDANCE WITH THE LAW 1. Because, from 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, this law 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 AADE as, in this case, automated processing of personal data took place, subject to the protective scope of the legislation on the protection of personal data (articles 2 para. 1 GDPR and 2 Law 4624/2019). 2. Since, article 5 par. 1 item in the GDPR provides that personal data: "are processed in a way that guarantees the appropriate security of personal data, including their protection against unauthorized or unlawful processing and accidental loss, destruction or deterioration, using appropriate techniques or organizational measures ("integrity and confidentiality"). Furthermore, according to the provision of article 24 par. 1 GDPR: "1. Taking into account the nature, scope, context and purposes of the processing, as well as the 6 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. The measures in question are reviewed and updated when deemed necessary", while according to Article 32 GDPR regarding the security of the processing: "1. Taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and freedoms of natural persons, the controller and the executor the processing implement appropriate technical and organizational measures in order to ensure the appropriate level of security against risks, including, among others, as the case may be: (…) b) the ability to ensure the confidentiality, integrity, availability and reliability of the systems and processing services on an ongoing basis (…). 2. When assessing the appropriate level of security, particular account shall be taken of the risks deriving from the processing,

in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, transmitted, stored or otherwise processed. (…) 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'. It follows from the above that one of the requirements of the GDPR is that, by using appropriate technical and organizational measures, personal data is processed in a way that guarantees the appropriate security of personal data, including its protection from unlawful processing . personal data that 7 3. Because, subsequently, in accordance with the provisions of article 4 par. 12 GDPR defines a personal data breach as "the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed". This definition is explained in terms of “unauthorized or unlawful processing” in the Article 29 Group Guidelines on the notification of personal data breaches under Regulation 2016/679 “(…) Finally, unauthorized or unlawful processing may includes 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"1. 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"). 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). 4. As a result of the above, in the considered complaint, taking into account the information contained in the immediately preceding considerations of the present, all the elements of the case file, the hearing procedure and the submitted memoranda, the Authority considers that the complained processing of 1 See page 7, Article 29 Panel Guidelines on the notification of personal data breaches under Regulation 2016/679 WP250rev.01 from 03.10.2017, as finally revised and issued on 6 February 2018, available at http://ec .europa.eu/justice/dataprotection/index_en.htm. 8 of sending the settlement notes in an envelope with a window/window from where the complainant's personal data were visible, more than what is necessary for sending the envelopes and identifying the recipient, recommends, based on information security principles in accordance with Opinion 3/2014 of article 29 on the notification of a personal data breach2 and the Guidelines of article 29 on the notification of personal data breaches pursuant

to Regulation 2016/6793, breach of confidentiality (privacy)4, i.e. potential unauthorized disclosure and receipt of knowledge by unauthorized persons in violation of the provision of article 5 par. 1, paragraph f of the GDPR regarding the obligation to observe the principle of data integrity and confidentiality as well as the requirements of article 32 GDPR, since AADE owed, in fulfillment of the obligation to receive appropriate techniques and organizational measures, within the framework of an appropriate security policy by AADE as data controller, to ensure privacy/confidentiality both when printing and wrapping the settlement notes, and when sending them to taxpayers. keeping the In addition, the reference of the Independent Data Protection Officer Support Department of A.A.D.E. to the obligation of users of postal services to safeguard the privacy of letters, in accordance with article 32 of the Building Regulation of the Ministry of Environment, Spatial Planning and Public Works) to take self-protection measures by installing a mailbox with a lock, in which the distributor must place ordinary mail, as well as the provisions on tax confidentiality (no. 26 of Law 4174/2013) or the duty of confidentiality (Y.A.3046/ 304/1989 2 Opinion 03/2014 on personal data breach notification http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf, p. 5 3 WP250rev.01 of 03.10.2017, as finally revised and issued on 6 February 2018, available on the website http://ec.europa.eu/justice/data-protection/index_el.htm 4 See in this regard the Authority's decision 47/2009, with the which sent a warning to the IKA, because in the mailing envelopes of the pension notices there was a transparent window through which personal data was visible in the notice, as well as the Authority's decision 14/2022. 9 of the employees of AADE in the context of the performance of their duties (no. 26 Law 3528/2007), no influence is exerted on the independent obligations of the controller regarding the security of the processing, as expressly specified in articles 5 (1) (f) , 24 and 32 GDPR. Specifically, with the GDPR, a new compliance model was adopted, the central dimension of which is the principle of accountability, in the context of which the data controller is obliged to plan, implement and generally take the necessary measures and policies in order to process the data to be 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. Therefore, the

obligations in question as described above are independent obligations of the data controller that do not cease to apply due to the possible provision of other obligations in different areas of law such as the referenced Building Regulation or the provisions on tax confidentiality or the duty of confidentiality of the employees of A .A.D.E in the context of exercising their duties. 5. The Authority, in relation to the established violation of the principle of article 5 par. 1 item. f of the GDPR in conjunction with Article 32 of the GDPR for the reported processing, considers that there is a case to exercise the corrective powers of Article 58 para. 2 item i and 83 of the GDPR (imposition of a fine), with regard to the above violations, and that based on the circumstances established, and an effective, proportionate and dissuasive administrative fine should be imposed in accordance with article 83 of the GDPR in accordance with 10 of the Guidelines for the "application and determination of administrative fines for the purposes of regulation 2016/ 679 of the working group of Article 29". When evaluating the data, in order to choose the appropriate corrective measure, the Authority takes into account the fact that the complainant violated the principle of confidentiality provided for in Article 5, paragraph 1, point f of the GDPR, that is, she violated a fundamental principle of the GDPR for the protection of personal data (article 83 par. 5 item a' of the GDPR), and in addition the criteria for measuring the fine defined in article 83 par. 2 of the GDPR that apply to this case, and in particular: i) ii) iii) iv) v) The fact that the specific security breach did not take on a broader nature (Article 83 par. 2 letter a' GDPR). The fact that A.A.D.E accepts that the specific violation was due to human error (article 83 par. 2 letter b GDPR). The fact that A.A.D.E could not take actions to mitigate the damage suffered by the data subject (article 83 par. 2 letter c of the GDPR). The fact that A.A.D.E must take technical and organizational measures pursuant to articles 25 and 32 of the GDPR to ensure confidentiality at all stages of the processing (article 83 par. 2 item d' of the GDPR). The fact that a special category of personal data of the complainant was not affected by the violation established above (Article 83 par. 2 letter g GDPR). 6. Because, Article 33 para. 1 GDPR provides: "In the event of a personal data breach, the data controller shall immediately and, if possible, within 72 hours of becoming aware of the personal data breach notify the supervisory authority competent in accordance with Article 55, unless the breach of personal data is not likely to cause a risk to the rights and freedoms of natural persons. Where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a justification for the 11 delay.' And according to Guidelines 1/2021 on examples of disclosure of personal data breaches5 "the role of human error in personal data breaches should be highlighted, as its presence is not unusual". 7. Because in this case, from all the elements of the case file, it appears that the complainant made a notification of a data breach (submitting it with the Authority's protocol number C/EIS/874/04-02-

2021 personal data breach notification form and then the supplementary one with the Authority's protocol number C/EIS/2163/30-03-2021). As the AADE does not mention in the form for submitting notification of a personal data breach, but also in the no. APD C/EIS/7521/27.05.2022) memorandum, the incident in question is due to human error. protocol: ... protocol number (and with 8. Because Article 34 GDPR provides: "1. When the breach of personal data may put the rights and freedoms of natural persons at high risk, the data controller shall immediately notify the data breach 2. The notification to the data subject referred to in paragraph 1 of this article clearly describes the nature of the personal data breach and contains at least the information and measures referred to in article 33 paragraph 3 items b), c) and d). 3. The notification to the data subject referred to in paragraph 1 is not required if any of the following conditions are met: a) the controller has implemented appropriate technical and organizational protection measures, and these measures have been applied to the personal data affected by the breach nature, mainly measures that make the personal data unintelligible to those who do not have permission to access them, such as encryption, b) the controller subsequently took measures that 5 See Guidelines 1/2021 on examples of notification of personal data breaches as issued on 14 December 2021, page 19. 12 ensure that the high risk referred to in paragraph 1 to the rights and freedoms of data subjects is no longer likely to occur , c) requires disproportionate efforts. In this case, a public announcement is made instead or there is a similar measure by which the data subjects are informed in an equally effective way (…)". In addition, OE 29 in the Guidelines on the notification of personal data breaches pursuant to Regulation 2016/679, taking into account Recital 86 of the GDPR, underlines, among other things, (p. 23-24) that: "Data controllers shall they must remember that notification to the supervisory authority is mandatory, unless it is unlikely that a risk to the rights and freedoms of persons will be created as a result of the breach. In addition, when the rights and freedoms of individuals may be at high risk as a result of a breach, individuals must also be informed. The threshold for reporting a breach to persons is therefore higher than for notification to supervisory authorities and, consequently, not all breaches will require notification to persons, which protects them from unnecessary burden fatigue notifications. The GDPR states that notification of a breach to individuals should be made "immediately", i.e. as soon as possible. The main objective of the notice to persons is to provide specific information about the actions they should take to protect themselves. As stated above, depending on the nature of the breach and the risk posed, timely notification will help persons to takeactions to protect themselves from any negative consequences of the breach".

In the present case, as can be seen from the above

response of the Independent Protection Officer Support Department

Data, the incident was not announced to the data subject because

"the data subject himself informed A.A.D.E about the potential

incident of breach of his personal data, and was therefore already taking place

knowing this". The Authority considers that, although there was a risk to the rights and

the freedoms of the complainant, there was no obligation to announce it

9.

13

infringement to the complainant, taking into account the objective of the communication

of the data, as it is analyzed in the Guidelines regarding the

notification of personal data breaches pursuant to

regulation 2016/679, but also recital 86 of the GDPR, among others,

(pp 23-24), which consists in providing the subjects with specific

information about the actions they must take so that

to be protected, as the further actions it could take

data subject (which, it should be noted, was already known to him

incident and had already objected to the processing of his personal data

data in the aforementioned manner) to protect against any

negative consequences of the breach were limited.

10. Because, finally, Article 13 GDPR provides with regard to the right

informing the data subject that: "1. When personnel data

character concerning the subject of the data collected by the

data subject, the controller, when receiving the

of personal data, provides the data subject with all

following information: a) his identity and contact details

controller and, where applicable, the controller's representative

processing, b) the contact details of the data protection officer,

where applicable, c) the processing purposes for which they are intended

the personal data, as well as the legal basis for it

processing, d) if the processing is based on Article 6 paragraph 1 point

f), the legal interests pursued by the controller or by

third, e) the recipients or categories of recipients of the personal data

character, if any, f) as the case may be, the intention of the person in charge

processing to transmit personal data to a third country or

international organization and the existence or absence of a Commission adequacy decision

or, when it comes to the transmissions referred to in article 46 or 47 or in

article 49 paragraph 1 second paragraph, reference to appropriate or suitable

guarantees and the means to obtain a copy thereof or where they were made available. 2.

In addition to the information referred to in paragraph 1, the person in charge

processing, when receiving the personal data, provides to

data subject the following additional information that is necessary for

ensuring fair and transparent processing: a) the time period for the

which the personal data will be stored or, when it is

impossible, the criteria that determine the interval in question, b) the existence

of the right to submit a request to the controller for access and

correction or deletion of personal data or limitation thereof

processing concerning the data subject or right of opposition

processing, as well as the right to data portability, c) when

the processing is based on Article 6(1)(a) or Article 9

paragraph 2 point a), the existence of the right to revoke the

his consent at any time, without prejudice to the legality of the processing which

was based on consent before its withdrawal, d) the right to submit

complaint to a supervisory authority, e) whether the provision of personnel data

character is a legal or contractual obligation or requirement for the conclusion

contract, as well as whether the data subject is obliged to

provides the personal data and what possible consequences will

had the failure to provide this data, f) the existence of automated download

decisions, including profiling, referred to

article 22 paragraphs 1 and 4 and, at least in these cases, important

information about the logic followed, as well as the meaning and

foreseen consequences of said processing for the subject of

data."

11. As a consequence of the above, taking into account the above

in the immediately preceding thoughts of the present and the elements of its file

case, the Guidelines 1/2022 of the European Council

Data Protection regarding the rights of the subjects of

data – right of access6 but also its Guidelines

group of article 29 on transparency based on regulation 2016/6797, h

6 See Guidelines 1/2022 on data subject rights - Right of access of the GDPR from 18.01.2022 under public

consultation, sc. 20 and sc. 110 available at https://edpb.europa.eu/our-work-

tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en

7 Guidelines of the Article 29 Group on Transparency under the Regulation

2016/679, WP 260 rev. 01, paragraph 29.

The Authority considers, in this case, that AADE as the controller, through it

of the answer he provided with the Autotelous document no

Data Protection Support Department to the complainant, satisfied it

right of information exercised by the complainant with his request from ..., regarding

the information he requested and indeed on time, i.e. before it expired

period of one month, in accordance with the provisions of article 12

par. 3 of the GDPR, given that he answered all the information required in

fulfilling the requirement of transparent information to the complainant,

even making reference to the existence of a Framework Agreement (under no. 5/13-03-

2018) for the provision of postal services to the Greek State

(ministries and decentralized administrations) with the contracting authority the General Directorate

of Public Contracts of the General Secretariat of Trade and Protection

Consumer of the Ministry of Economy and Development and Greek contractor

Post Offices S.A.

The Authority further considers that the additional information requested by

complainants (in relation to the role of ELTA in the said processing of

his personal data) are not included in the information he owes,

according to article 13 of the GDPR, the data controller must provide the data subject with

data, taking into account that the responsibility for the complained

breach of confidentiality of his financial/tax data with

A.A.D.E. is responsible for sending the disputed settlement note. as

data controller in accordance with the above provisions.

Based on the above, the Authority unanimously considers that it should be imposed on

denounced as a data controller, or referred to in the ordinance

administrative sanction, which is judged to be proportional to the gravity of the violations.

FOR THOSE REASONS

THE BEGINNING

It imposes on A.A.D.E. the effective, proportional and deterrent administrative

fine that is appropriate in the specific case, according to

more special circumstances thereof, amounting to eight thousand (8,000) euros for the above established violations of articles 5 par. 1 item f and 32 GDPR, according to with articles 58 par. 2 item i' and 83 par. 5 item 1 GDPR.

The Secretary

Irini Papageorgopoulou

The Deputy President

George Batzalexis