

Athens, 11-03-2022 Prot. No. 655 DECISION 14/2022 (Department) The Personal Data Protection Authority met as a Department by teleconference on Tuesday 02-08-2022, at the invitation of its President, following the 01-12-2021 of its regular meeting, in order to examine the case referred to in the history of the present. Georgios Batzalexis, Deputy President and regular members Spyridon Vlachopoulos, as rapporteur, Charalambos Anthopoulos and Konstantinos Lambrinoudakis were present. The meeting was attended, by order of the President, without the right to vote, Eleni Kapralou, special scientist-auditor, as assistant rapporteur. Irini Papageorgopoulou, an employee of the Administrative Department, attended as secretary. The Authority took into account the following: A, a resident of [area X], with no. first of the Authority C/EIS/5975/20-09-2021 his document submitted to the Authority a complaint against the Municipality of Chios, for sending a mail folder (which probably concerns a municipal summons), on the outside of which are written and made visible by third parties more personal data than what the complainant claims is necessary to identify him as a recipient and send the mail. In particular, as can be seen from the complaint in question and the document attached to it, the complainant complains about the fact that he received mail from the complainant in the common mail area of the apartment building where he lives and that the external shipping envelope contains the VAT number, the D. O.Y and his identity card number, information which he claims became known to third parties, and whose use is possible for his identification. In the context of examining the said complaint, the Authority with no. prot. C/EX/2147/27- 09-2021 her document, forwarded the complaint with the attached relevant documents to the complained Municipality of Chios and the Data Protection Officer B, whom she invited to report in writing within fifteen (15) days from upon receipt of the document, their views on the complainants, attaching to the answer every element relevant to the case and in particular, as they make known to the Authority the following: a) What procedure is followed by the ... Service of the Municipality when sending letters, regarding the protection of personal data and what procedure was followed in the case of the complainant and b) What are the technical and organizational measures taken in this case to secure the data from prohibited dissemination or access. The complained-about Municipality responded to the Authority's document in question with no. prot. C/EIS/6598/13-10-2021 his document on the subject "Response to A's complaint", in which he stated that during the process of issuing individual notices using a financial program, the wrong print form was mistakenly used with as a result of its issuance and sending to Mr. A, as well as accepting that the said individual notice lists information such as the VAT number, the identity card number and the D.O.Y. Furthermore, in the same above-mentioned document, the complainant claims that apparently during the sending of the notices and due to the large

volume of letters and also the heavy workload, the error in the specific letter was not noticed and that it is a standard practice of the ... Service when issuing said notices is that these data are not printed, as well as that in the Municipality of Chios, the organizational and technical measures provided for in article 11 of the P.D. 75/2020. Based on the aforementioned, A and the Municipality of Chios were legally summoned by the Authority, with documents No. C/EX/2645/22-11-2021 and C/EX/2644/22-11-2021, respectively, in a hearing before her at the Department's meeting on 01-12-2021, to provide further clarifications and thoroughly state their views on the above. At the meeting of 01-12-2021, A was legally present in person and Irini Moniou, lawyer of the Municipality, represented the Municipality of Chios, with, C, Head of the Municipality of Chios, D, Head of the Department, as well as B, Data Protection Officer of the Municipality. During the hearing, the aforementioned presented their views orally and requested and received a deadline to submit a memorandum. Subsequently, A and the Municipality of Chios submitted, in a timely manner, relevant memoranda under Authority No. C/EIS/8180/15-12-2021 and C/EIS/8139/13-12-2021, respectively. Among other things, the following are noted in said memorandums: On the one hand, the Municipality of Chios claims in its memorandum that the printing in question is due to an error (printing error) and is not the usual practice, it is the only case, given that they have that the necessary organizational and technical measures are taken by the Municipality to protect the personal data of the debtors of the Municipality of Chios, as well as that the computer software that carries this data has undergone encryption and has been equipped with the appropriate antivirus systems, while access to only a specially authorized employee of ... has a file. In fact, according to the claims of the Municipality, there was no intention from the beginning to transmit the personal data to a third party. Finally, he requests that the case in question be dealt with leniently and that no sanction be imposed against the Municipality, taking into account that it was a low-level violation, which took place by accident and affected one person, namely the complainant, that the violation did not receive country by fraud and does not take place in the other cases, where the duty of diligence required by law is observed, that the degree of responsibility of the data controller is particularly low, taking into account the technical and organizational measures applied by the Municipality of Chios pursuant to articles 25 and 32, that to date no administrative sanction has been imposed by the Authority against the Municipality of Chios, that there was recognition of the error from the outset and an admission that it was due to an oversight, that the categories of personal data affected by the violation do not concern personal data of articles 9 and 10 GDPR, as well as that the Municipality as a data controller did not obtain a financial benefit, nor did it cause material personal injury to the data subject. On the other hand, complainant A states in his memorandum that the complainant

acknowledges that a violation has occurred, that the specific incident is not isolated, and regarding the preventive measures taken by the Municipality states that the planning for the protection of personal data requires the existence of a separate form, with the absolutely necessary data isolated for all letters sent, an appropriate measure and not overly burdensome for the Municipality. Finally, he invokes the seriousness of the breach in question, claiming that the data made visible to third parties can be used to identify him, e.g. in transactions with banking institutions, without however claiming that he has actually suffered loss or damage. The Authority after examining the above complaint, the other elements of the file, the hearing of the parties involved, and after hearing the proposal of the rapporteur, after a thorough discussion, DECIDED IN ACCORDANCE WITH THE LAW 1. Because, according to a. 2 par. 1 of the GDPR "This Regulation applies to, in whole or in part, the automated processing of personal data, as well as to the non-automated processing of such data which are included or are to be included in a filing system", while, according to article 4 paragraph 1 of the GDPR as processing of personal data means "any act or series of acts carried out with or without the use of automated means, on personal data or sets of personal data, such as the collection, registration, organization, the structuring, storage, adaptation or alteration, retrieval, retrieval of information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, restriction, deletion or destruction" . Further, in a. 5 par. 1 para. b, c and f of the GDPR it is defined that: "Personal data: (...) b) are collected for specified, explicit and legal purposes and are not further processed in a manner incompatible with the purposes them ("purpose limitation") c) are appropriate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimization") (...) f) 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 damage, using appropriate confidentiality". technical or organizational measures ("integrity and Because these provisions establish as fundamental conditions for the legality of any processing of personal data, as well as for the legality of the establishment and operation of each file, the principles of the purpose of the processing and the proportionality of the data always in relation to the purpose of the processing. Because any processing of personal data, which is done beyond the intended purpose or which is not appropriate and necessary for its achievement, is not legal. Because personal data to be legally processed should be relevant, appropriate and no more than is required each time in view of the purpose of the processing. Because the controller must take the organizational and technical measures for data security from prohibited dissemination or access (art. 25 and 32 GDPR).

Because, according to article 58 par. 2 of the GDPR "Each control authority has the following corrective powers: (...) b) to address reprimands to the controller or to the processor when processing operations have violated its provisions of this regulation (...)".

2. Because, in this case, the following occurred:

The ... Service of the Municipality of Chios sent the complainant a letter, which he keeps as controller in his file, in a mail folder, in a way that does not meets the conditions of legal processing set by the GDPR.

In particular, in the shipping envelope except for his name and address complainant-recipient, the VAT number, the D.O.Y and the card number are also indicated of his identity, as a result of which they can access them illegally and third parties (e.g. postman, neighbors, etc.).

Because the above - except for the name and postal address - reported personal details of the complainant appearing in the file mission are not relevant, convenient and depending on the purpose served by specific processing. The ... Service of the Municipality of Chios as responsible for the processing of personal details of the respective debtor, he should send him the... certificate in a mail envelope, on the outside of which and on the transparent- visible to all - window, only the data necessary for the mission will be listed of the file to the recipient and his identification, i.e. name, surname and address.

Furthermore, because, as it follows from the above and the Authority has already judged in its previous decision (with no. 47/2009) admissible elements for sending a file only the recipient's name and address are irrefutable.

Because, with this specific shipping method, the provisions of article 5 are violated par. 1, para. b, c and f of the GDPR on the obligation to observe the principle of limitation purpose, data minimization and integrity and confidentiality;

and personal data of the debtors are disclosed in this way to non-third parties

authorized persons.

3. Because, further, the representatives of the Municipality assured the Authority that the said violation constitutes an isolated case of violation, and it is not the usual practice to are sent to the debtors the ... certifications in this way, and indeed that to shipping envelopes according to the Municipality's standard policy, only the name, the surname and postal address of the debtor and no other information.

Because after an ex officio inspection by the Authority, no other complaint has been submitted against the Municipality of Chios until today.

FOR THOSE REASONS

The Authority addresses to the complained controller, Municipality of Chios, a reprimand for the violations of article 5 par. 1, para. b, c and f of the GDPR.

The Deputy President

The Secretary

George Batzalexis

Irini Papageorgopoulou