Athens, 20-02-2023 Prot. No.: 435 DECISION 7/2023 (Department) The Personal Data Protection Authority met, at the invitation of its President, in a regular meeting in the composition of the Department at its headquarters on 25/01/ 2023, in order to examine the case referred to in the present history. The meeting was attended by teleconference by Georgios Batzalexis, Deputy President, in the absence of the President of the Authority, Konstantinos Menoudakos, and was attended by the alternate member Christos Papatheodorou, as rapporteur, as well as the alternate members Demosthenes Vougioukas and Maria Psalla, in place of the regular members Konstantinos Lambrinoudakis and Grigorio Tsolia who did not attend due to disability although they were legally summoned in writing. The meeting was attended, by order of the President without the right to vote, by experts Haris Symeonidou, legal auditor and Georgios Rousopoulos, IT auditor, as assistant rapporteurs and Irini Papageorgopoulou, an employee of the Authority's administrative affairs department, as secretary. The Authority took into account the following: With the no. prot. C/EIS/7558/18-11-2021 complaint by A (hereinafter the complainant), directed against the company Vodafone - PANAFON S.A.E.T. (hereinafter the complainant), complaining of non-fulfillment of the right to access recorded conversations, as well as a data breach incident. Specifically, according to the complaint and its supplementary documents, upon the complainant's request for access to her recorded telephone conversations with representatives of the complained company, which, as stated, was submitted in the manner indicated to her by the telephone service center of the complained and in the context of disputing the subscription plan sold to the complainant by telephone (converting the number ... from a prepaid mobile to a prepaid plan), was sent by company I-CALL SUPPORT & GROWTH IKE at the complainant's home address and delivered to her on …, upon presentation of her police ID for identification purposes, a folder containing a CD with recorded conversations of a third party with the complainant and not the complainant's conversations. As the complainant states, the conversation includes a lot of personal data of the third person in question (name, surname, tax number, identity number, date of birth, residential address, etc.). Further, according to the complaint, the complainant telephoned the complainant to inform the complainant of the erroneous shipment immediately after hearing the CD, asking for the latter's assurance that her own personal data had not been sent to another customer. However, as he reports, he did not receive any response in this regard. And according to the complainant's letter from ... to the Consumer Advocate, to whom the complainant also appealed (see C/EIS/1532/01-02-
2022 supplementary document), the complainant, among others, expressed her views on the above-complained incident (incorrect CD shipment). The Authority, in the context of examining the above complaint, with no. prot. C/EX/441/16-02-2022

her document, invited the complainant to state her views on the complainants, clarifying in particular, a) if, in what way and at what time the complainant exercised her right of access to the her recorded conversations, as well as if, in what way and at what time the complainant responded to this request, b) if the complainant was informed by the complainant, immediately after she received the CD in question, that, as she states, conversations of a third party were sent to her, as well as whether the complainant investigated whether the reported incident occurred and what was the result of any actions she took on it, c) if the complainant reported the incident to the Authority in accordance with Article 33 GDPR and in its announcement to the data subject concerned in accordance with Article 34 GDPR, justifying in each case its response and d) what is its relationship with the company I-CALL SUPPORT & GROWTH IKE and what is the role of each of the two in relation to the processing personal data of subscribers. The complainant in her reply from … (with Authority no. C/EIS/3253/04-03-2022) supports the following: That the complainant submitted the request for notification of a recorded call from …, and in accordance with the practice followed by the complained about the satisfaction of the right of access to recorded calls made by cooperating companies, responsible in this case for retrieving and sending the recorded call to the data subject was the company "I-CALL SUPPORT & GROWTH IKE" (hereinafter "I- CALL"), to which the request was forwarded for processing. That then, as per the relevant affidavit of the complainant (which she submits as Ref. 2), I-CALL delivered the recorded call on CD to the complainant by registered letter (courier) on …, therefore it follows that the complainant's request was satisfied , legally and within the prescribed period. That after receiving the recorded call, the complainant addressed the complainant claiming that she did not receive the call that concerned her, but the call of a third subscriber and that subsequently the complainant contacted I-CALL directly, in order to investigate this claim of the complainant . That subsequently I-CALL, with its response from ..., informed the complainant that "it tried to contact the complainant, which was not possible", while also in the context of the complainant's report to the Consumer Advocate, the complainant received the same answer from I-CALL, that is, it had not been able to locate the complainant, which is why it had not proceeded with further actions. The complainant underlines her strong belief that the complainant's claim about sending a recorded call to a third party subscriber is not true, which she bases on the following facts: A) that I-CALL, which was responsible for recording, retrieving and sending the recorded call to complainant insists that there is no indication of wrongful sending of recorded material, B) that already upon receipt of the recorded call, the complainant reserved for any lawful use, a fact which proves her prior willingness to engage in litigation in general with the complainant, C) that according to the information that the complainant has received from I-CALL, the latter has repeatedly tried

to contact the complainant to investigate the incident to no avail and D) that with the reply letter from ... of the complainant to the Consumer Advocate (which she attaches as Ref. 3) urgently requested the complainant, in case her claim is true, to return the recorded material, so that the complainant is informed and able to take all the necessary actions based on its obligations under the current legislation on personal data, while the complainant had not responded to this request for the presentation of the CD up to the day of the response. With regard to the obligations under articles 33 and 34 of the GDPR, the complainant claims that the evaluation and management of security breach incidents by the Data Controller requires the data controller to be aware of the facts that may constitute a security incident, as well as the evaluation of the facts, in order to initially establish whether a security incident exists and, in the event that it does, to assess whether the conditions for its notification to the competent supervisory authority and the data subject are met, as well as to take the necessary measures to mitigate the risk for the data subjects. Invoking the under no. 18/2018 OE guidelines29, according to which "...a data controller should be considered to have acquired 'knowledge' when said data controller has a reasonable degree of certainty that a security incident has occurred which results in them being personal data at risk", the complainant argues that in this case, due to the nature of the incident, a necessary condition for the relevant evaluation is the prior presentation by the complainant of the CD sent to her with the recorded conversation, which she has not happen, because the complainant, as stated, has not responded to the complainant's repeated attempts to investigate the incident, as a result of which she is unable to assess the existence or non-existence of a security incident within the meaning of Articles 33 and 34 GDPR, as well as whether the conditions for submitting a notification to the Authority and to any affected data subject are met. begets promotion ofof its telecommunications products and services, and since it acts as

I was performing the Processing on behalf of, signed between them or by

03-23-2018 personal data processing delegation contract, which,

as it states, it includes all the terms of article 28 GDPR.

Subsequently, the complainant with G/EIS/3645/09-03-2022 supplementary

document communicated to the Authority its history recorded from ...

of her conversation with a representative of the complained-about company, which she received at

continue to her e-mail. Here is a relevant excerpt:

X: Good evening! My name is X and you are logged in

in the Card program/Debit card group!

X : I have read the conversation you had with Tobi

our digital assistant.

X: it's yours to submit a request. I did and requested all conversations with

details. The store informed me that because I am in doubt, no

I am charged. After 10 days they did not call me to inform me that the cd is there

ready. let's make an appointment to pick it up at my house. After 20

X : I immediately check the request for the recorded call

don't worry at all.

: days + after I called you again as I had not received the cd. You sent me

the cd. The details (my name and phone number) in the envelope were correct but

You sent me another person's file. You have inadvertently made me a member of the staff

data

: name, address, identity, afm.

X : After a check I made on your record

it appears that on ... the recorded communication was initiated as I correctly

you said but in the content it is a different owner?

X : What I can do for you to you

serve immediately and in the first year I will forward immediately and in the first year to

section of our offers to check it and inform you to receive it

correct.

X: Within 1 day you will have received it.

X : We are sorry for the mistake of the mission I have undertaken

I get the right one.

: I wonder if you shared my details with

third!!! In parallel, you sent me a note that a value account has been issued...!!

I called again and asked for immediate cancellation of the card, the

my transcript, to write off my debt immediately

X : I fully understand your displeasure and certainly

I will pass your comments internally as they are very important and help us

we are getting better, however your personal information has not been given to a third party.

X : My name is X whatever you need

you can request me via Live Chat.

: how can you if you are sure that my details have not been given to you

alon?

: rather?

X : Seen in sending the request.

: I am sure dear Mr. X that you are good at your job.

X : In summary, I would like to inform you, that I have

forward for review the request made, so that it can be completed immediately and in the first place

time!

X : Rest assured that your issue will be resolved immediately.

: I would like the lady from whom I received the information to be informed

your own negligence

X : As soon as possible.

X: I have already informed her from here.

: It hasn't been solved for a month now. And I have called several times, and I have

goes 4 times to your store.

: please how can I get a copy of our conversation

X : No other action is needed from you

I guarantee you will get the correct recording and your issue will be resolved.

Given the above, the Authority, with relevant calls, called them

involved in the board of the Department of the Authority on 02-11-2022,

in order to express their views on the case.

During the meeting, the complainant was also present on her behalf

of the accused company, the attorneys-at-law of Emmanuel Chalkiadakis

(…), Apostolos Vorras (…), Emmanuel Dimogerontakis (…) and Konstantina –

Maria Karopoulou (…) and B, Data Protection Officer of the company.

During the meeting the invitees were given a deadline and then n

Complainant timely filed under no. prot. G/EIS/11924/21-11-2022

her memorandum document, while the complainant did not file a memorandum.

During the hearing, the complainant repeated what was mentioned in

her complaint, stressing that no one contacted her on her behalf

of the complained-of company to receive the CD which had been delivered to it by it

I-Call, that for the first time this was requested through her letter from ...

reported to the Consumer Ombudsman (see C/EIS/1532/01-02-2022

supplementary document), which, however, did not specify in which store or at

which address should the CD be delivered to? The complainant both at

hearing as well as with her memorandum she argued that I was executing her

processing

I-Call has received the categorical assurance that in

complainant was sent the correct recording as well as that after her report

that she has received another client's conversations, repeated attempts were made

of telephone communication with the complainant, to which she did not answer

and thus it was not possible to confirm the accuracy of her claim. THE

the complainant also emphasizes that the complainant did not provide either the

itself neither in I-CALL nor in any of the Authorities in which

appealed, the disputed CD, despite the fact that a person in the capacity, the

knowledge and her age could easily do so, finding for

example the address of the company from its website. According to

defendant Vodafone, from the facts stated above

it follows that on the one hand the complainant's right of access to

her recorded call has been upheld as no evidence has been provided

on the contrary, on the other hand, the complainant has not received knowledge of the incident

data breach with a sufficient degree of certainty to assess it with

based on articles 33 and 34 GDPR. It should be noted that in the context of the hearing

the representatives of the complainant were asked by the rapporteur why

they did not act themselves by sending a courier to the complainant's house to

receive and review the CD. The complainant replied that for the reason

this was addressed to the complainant both by phone and in writing.

Finally, as part of the hearing, the complainant was asked to present

the relevant Policy it has for the management of incidents of infringement

personal data as well as clarify which actions were taken by

the moment he became aware of the complainant's allegation. The complainant

with her memorandum she submitted, among other things, (Ref. 7) the Management Process

Incidents of Data Breach (document “P-047 Manage Information &

Cyber Security, Data Privacy, Fraud & Service Affecting Network Unavailability

Incidents"), which describes how to manage security incidents.

The analysis of appropriate actions

after receiving notice of

incident, includes (step 1)1 immediate forwarding of notifications

(alerts) received to the competent department (Incidents Management Dept. Lead

– IMDL) and their timely evaluation, in order to confirm or not

existence of an incident of violation (step 3)2.

The Authority, after examining the elements of the file and after hearing him

rapporteur and the clarifications from the assistant rapporteur, who attended without

right to vote, after thorough discussion,

THOUGHT ACCORDING TO THE LAW

1. From the provisions of articles 51 and 55 of the General Protection Regulation

Data (Regulation (EU) 2016/679 – hereinafter GDPR) and Article 9 of the law

4624/2019 (Government Gazette A' 137) it follows that the Authority has the authority to supervise the

application of the provisions of the GDPR, this law and other regulations that

concern 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 pc. g' of Law 4624/2019 it follows that the Authority has the authority to take action

of A's complaint against Vodafone – PANAFON A.E.T. and exercise,

1 "An incoming alert is identified by a monitoring system and forwarded accordingly (i.e. via e-mail).

Incidents Management Dept. Leads (IMDL) receive the alert from system monitoring sources (i.e.

Vodafone Group, GSM Association, local/Group SIEM system, DLP, Fraud system, etc.) and are

responsible to timely pick it up. The Security Incident Lead (SIL) should be informed, supervise, and

ensure that all alerts are timely picked-up. Go to step 3" (Ref. 7: 3 Flowchart Analysis, p. 16).

2 A competent Incidents Management Dept. Lead (IMDL) conducts a fist-level evaluation of the alert/

event received, following the defined incident types reference table (Section 1.8 – Incident Types), the

classification levels (Annex A) and considering if the alert/event relates to Vodafone Greece systems or

network, or if the required countermeasures are already in place. In order to ensure that

countermeasures are in place Subject Matter Experts (SME) may be consulted. In case the alert is

received on the Security_Incidents.gr@vodafone.com, all the Incidents Management Dept. Leads

(IMDL) in coordination with the other recipients of this email address (i.e. Subject Matter Experts) will

make all the above-mentioned actions/decisions. In case of non-working hours, this process will be

conducted by NOC/ NITO working on shift. The Security Incident Lead (SIL) should be informed,

supervise, and ensure that all alerts/events are being timely evaluated. - If the alert is evaluated as "Not-Applicable" or "False Positive" then go to step 4 - If the alert is evaluated as "Applicable" or "True Positive" then go to step 16" (Ref. 7: 3 Flowchart Analysis, pp. 16-17 ). respectively, the powers granted to it by the provisions of articles 58 of the GDPR and 15 of law 4624/2019. 2. Article 5 par. 1 of the General Regulation (EU) 2016/679 for the protection of natural persons against the processing of personal data (hereinafter GDPR) sets out the principles that must govern a processing. According to article 5 par. 1 a) and f) GDPR "1. Personal data: a) are processed lawfully and legitimately in a transparent manner in relation to the data subject ("legality, objectivity and transparency"), [...] f) are processed in a way that guarantees appropriate data security of a personal nature, including their protection from unauthorized or illegal processing and accidental loss, destruction or damage, by using appropriate technical or organizational measures ("integrity and confidentiality")", while as pointed out in the Preamble of the Regulation, "The data personal data should be processed in a way that ensures the appropriate protection and confidentiality of personal data, including to prevent any unauthorized access to such personal data and the equipment used to process it or the use thereof of the personal data and the equipment in question" (App. Sk. 39 in fine). Furthermore, according to the principle of accountability which is expressly defined in the second paragraph of the same article and constitutes a cornerstone of the GDPR, the data controller "bears the responsibility and is able to demonstrate compliance with paragraph 1 ("accountability")". This principle entails the obligation of the controller to be able to demonstrate compliance with the principles of art. 5 par. 1. 3. According to article 15 par. 1 and 3 GDPR "1. The data subject has the right to receive from the controller confirmation as to whether or not the personal data concerning him is being processed and, if so, the right to access the personal data and the following information: [...] 3. The controller provides a copy of the personal data being processed. […] If the data subject submits the request by electronic means and unless the data subject requests otherwise, the information shall be provided in a commonly used electronic format." In addition, according to article 12 GDPR "1. The controller shall take appropriate measures to provide the data subject […] with any communication under Articles 15 […] 2. The controller shall facilitate the exercise of the data subjects' rights provided for in Articles 15 […] 3 .The controller shall provide the data subject with information on the action taken upon request pursuant to articles 15 to 22 without delay and in any case within one month of receipt of the request. This deadline may be extended by a further two months if necessary, taking into account the complexity of the request and the number of requests. The data controller shall inform the data subject of said extension within one month of receipt of the request, as well as of the reasons for the delay. […] 4. If the data controller

does not act on the data subject's request, the data controller shall inform the data subject, without delay and at the latest within one month of receipt of the request, of the reasons for not acting and for the possibility of submitting a complaint to a supervisory authority and taking legal action". Given the above, it follows that the subject's right of access to the personal data concerning him is established with the main purpose of ensuring the subject of the accuracy and legality of the processing of his data. Therefore, in order to satisfy the right of access, it is not necessary to invoke a legitimate interest, since this exists and forms the basis of the subject's right of access to obtain knowledge of information concerning him and which has been registered in a file kept by the data controller, so that to implement the basic principle of the law for the protection of personal data, which consists in the transparency of the processing as a condition for any further control of its legality on the part of the data subject3. 4. 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 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 can demonstrate that the processing is carried out in accordance with this regulation. The measures in question are reviewed and updated when deemed necessary", while in accordance with the provisions of paragraphs 1 and 2 of article 32 GDPR for 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, where appropriate: a) the pseudonymization and encryption of personal data, b) the ability to ensure confidentiality, integrity, availability and reliability of processing systems and services on an ongoing basis, c) the possibility of restoring the availability and access to personal data in a timely manner in the event of a physical or technical event, d) a procedure for the regular testing, assessment and evaluation of 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 See indicative APD 2/2020, 23/2020, 16/2017, 98/2014, 149/2014, 72/2013 and 71/2013, likewise. 5. According to article 4 no. 12 GDPR as a personal data breach means "a 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". According to the Working Group Guidelines of Article 29 of Directive 95/46/EC (currently European Data Protection Board - EDPB) dated 06-02-2018 on Personal data breach notification ("Guidelines on Personal data breach notification under Regulation 2016 /679" WP 250 rev. 1) one of the types of personal data breach is the one 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). 6. Incidents of data breach must be notified to the Authority within 72 hours from the moment the data controller becomes aware of them, in accordance with article 33 par. 1 GDPR: "1. In the event of a personal data breach, the controller shall notify the supervisory authority competent in accordance with Article 55 without delay and, if possible, within 72 hours of becoming aware of the personal data breach, unless the breach of personal data may not cause a risk to the rights and freedoms of natural persons. When the notification to the supervisory authority is not made within 72 hours, it is accompanied by a justification for the delay.". The notification must have the minimum content referred to in paragraph 3 of article 33 GDPR, while according to paragraph 5 of the same article "The data controller shall document each personal data breach, consisting of the facts concerning the personal data breach, the consequences and the corrective measures taken. Such documentation shall enable the supervisory authority to verify compliance with this Article.' With regard to the time when the Data Controller became aware of the incident, the above-mentioned OG29 (wp 250) states the following: "As detailed above, the GDPR requires, in the event of a breach, the Data Controller to notify the breach without delay and , if possible, within 72 hours of becoming aware of the fact. This may raise the question of when a controller can be deemed to acquire "knowledge" of a breach. OE29 considers that a controller should be deemed to have acquired “knowledge” when that controller has a reasonable degree of certainty that a security incident has occurred which results in personal data being compromised. However, as mentioned above, the GDPR requires the data controller to implement all appropriate technical protection measures and organizational measures to immediately detect any breach and immediately inform the supervisory authority and the data subjects. It also states that notification should be found to be delayed, taking into account in particular the nature and seriousness of the data breach, as well as its consequences and adverse results for the data subject. In this

way, the controller is subject to the obligation to ensure that it becomes "aware" of any breaches in time to be able to take appropriate action. The exact point in time at which a controller can be deemed to acquire "knowledge" of a particular breach will depend on the circumstances of the particular breach. In some cases, it will be relatively clear from the outset that a breach has occurred, while in others it may take some time to establish whether personal data has been unreasonably compromised. However, the emphasis should be on taking timely action to investigate an incident to determine whether personal data has been breached and, if so, to take remedial action and make a disclosure, if required." 7. In addition, the violation must also be announced to the data subject, as the case may be and in accordance with the provisions of article 34 par. 1 and 2 GDPR: "1. When the personal data breach may put the rights and freedoms of natural persons at high risk, the data controller shall immediately notify the data subject of the personal 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)". 8. In the case under consideration, from the information in the file and after the hearing, the following emerged: In satisfaction of her request for access to her recorded conversations with the call center of the complained-about company, the complainant received on ... via courier sent from her processing I-CALL a CD which, although outwardly stating her own information, contained the recorded conversations of another person. Regarding the incident in question, the complainant was informed, as data controller, initially on … by the complainant through the Live Chat application, then in the context of the latter's report to the Consumer Advocate and finally, in the context of the present complaint to the Authority , which was communicated to her on …. However, her reaction was limited to a) her email communication with the I-CALL processor on … ("The subscriber has come back and claims that she was sent a recording of another subscriber. Can you please investigate this so that the subscriber?"), from which he was informed on ... that "we have called the subscriber ... so that she could inform us about this and give her the necessary clarifications, but she did not answer us" (note that the said response from I-CALL differs from Vodafone's claim cited in the memorandum that on ... I-CALL "stated that there is no indication of incorrect sending of recorded material", while no documentation is provided in relation to the cited attempts to call the complainant) and b) in the ... written letter to the complainant asking her to return the material. From the above facts it appears that the complainant did not actively investigate the possible incident brought to her attention, but transferred the burden of responsibility for gathering the relevant information to the complainant. The complainant, as the data controller, could easily find out if it had actually been sent to the complainant's conversation (and to whom), instead of

passively waiting for the CD in question to be delivered by the complainant, on her own initiative and at her own expense, to a Vodafone store or at its headquarters. Besides, the complainant had been informed that "no further action" is needed from her and to "keep quiet", as can be seen from her recorded conversation via Live Chat on ..., which she provided. In addition, the complainant contacted the processor after several days (…), as it emerged from the electronic mail she provided, and not immediately upon receiving the initial information about a possible incident (…), despite the fact that in the relevant Procedure Management of Data Breach Incidents that it presented with its memorandum (Ref. 7) includes the obligation to immediately forward and evaluate the notifications (alerts) received, by the competent department (Incidents Management Dept. Lead - IMDL), in order to confirm the existence or of a non-incident of violation and the consequent compliance with its obligations as a data controller, vis-à-vis the Authority and the data subjects. Furthermore, the Complainant did not send the correct file to the Complainant, in order to satisfy her right of access to her recorded conversations, despite assurances to the contrary via Live Chat on … ("within 1 day you will have received it. We apologize for the wrong shipment, I have taken it upon myself to receive the correct one"). 9. Following the above, from the data in the file and following the hearing, the Authority finds on behalf of the complained Vodafone, as data controller: a) violation of Article 15 GDPR, as it did not prove (in accordance with the principle of accountability) that satisfied the complainant's right of access to the requested recorded call, given that the latter disputed the content of the CD she received and Vodafone did not take any action in this regard (e.g. resending the correct file). b) violation of article 33 GDPR, because despite having an indication of a data breach incident, Vodafone did not actively investigate the incident and did not notify it to the Authority, but on the one hand was satisfied with the response of the I-CALL processor that it did not find the complainant on the phone, on the other hand, after the lapse of several months and after the complainant appealed to the Consumer Ombudsman, with a document communicated to the complainant, he invited her to return the CD, passively waiting for him to confirm whether it happened or not breach incident. Given the small probable risk to the rights and freedoms of the third affected subject, the Authority does not find a violation of Article 34 GDPR. 10. Based on the above, the Authority considers that there is a case to exercise its corrective powers according to article 58 para. 2 c) GDPR (order to satisfy a right) and 58 para. 2 i) and 83 GDPR (imposition of a fine) regarding the violations identified above. To determine the sanction, the Authority takes into account the criteria for measuring the fine defined in article 83 par. 2 of the GDPR that are applicable in this case. In particular, the following are taken into account: a) The nature, gravity and duration of the violation: It is taken into account that the violation of the subject's right falls under the provisions of article 83 par. 5 GDPR,

therefore incurs as a maximum penalty the amount of 20 million euros or 4% of the total global annual turnover of the previous financial year, depending on which is higher. The processing related to the violation in question is not directly related to the basic activity of the complained business (providing telecommunications services). b) The fact that in this case the violations affect two data subjects.c) The degree of responsibility of the complainant, which although has taken appropriate organizational measures and has established relevant policies for the managementof data breach incidents, it did not appear that he put them into practice

in this case.

d) The fact that the complainant was given on behalf of the complainant

incorrect information on ... regarding the satisfaction of the right

access ("within 1 day you will have received the correct recording") but

and regarding the required actions on its part regarding the investigation

of the potential breach ("no further action is required

from you"), however, in the context of the hearing, the complainant transferred her

responsibility for investigating the potential incident rests with the complainant.

e) The fact that the complainant did not take steps to investigate it

incident and satisfaction of the complainant's right nor according to

during the examination of the case by the Authority.

f) The fact that the Authority has, as a data controller

reprimands the past for not satisfying a right of access to

two more cases (decisions 46/2022 and 19/2022).

g) The fact that the defendant had a turnover of 907,300,000 euros in the year 2021,

according to the balance sheet published on its website.

FOR THOSE REASONS

THE BEGINNING

A. He gives an order to the company Vodafone – PANAFON A.E.T. as responsible

processing, based on article 58 par. 2 sec. c) GDPR, to immediately satisfy the

exercised on ... the complainant's right of access to recordings

her conversations, by sending the correct files.

B. Imposes, on the company Vodafone - PANAFON A.E.T. as responsible

processing, based on article 58 par. 2 sec. i) of the GDPR, administrative fine

in the amount of forty thousand (€40,000) euros, for his established violations

right of access of the complainant under Article 15 GDPR and

obligation to notify an incident of violation based on article 33 GDPR.

The Secretary

The president

George Batzalexis

Irini Papageorgopoulou