Athens, 02-12-2022 Prot. No.: 3093 DECISION 39/2022 The Personal Data Protection Authority met in Plenary composition, via teleconference, on Tuesday 07-21-2022, at the invitation of its President, in order to examine the case referred to in the history of the present. The President of the Authority, Konstantinos Menudakos and the regular members of the Authority, Konstantinos Lambrinoudakis, as rapporteur, Spyridon Vlachopoulos, Charalambos Anthopoulos, Christos Kalloniatis, Aikaterini Iliadou and the alternate member Maria Psalla were present, in place of the regular member Grigorio Tsolia, who although was legally summoned in writing, did not attend due to disability. The meeting was attended by Spyridon Papastergiou and Leonidas Roussos, Specialist Scientists, Informatics, as assistant rapporteurs and by order of the President, Irini Papageorgopoulou as Secretary, employee of the Authority's administrative affairs department. The Authority took into account the following: A set of complaints and notifications of incidents of personal data breach related to incidents of unauthorized replacement of a subscriber's sim card (sim swap) as well as other procedures (e.g. call diversion, issuance of new phone numbers) were submitted to the Authority) from third parties, not the owners of said links. More specifically, initially, those with no. prot. C/EIS/2649/13-04-2020, C/EIS/2662/14-04-2020, C/EIS/2806/24-04-2020, C/EIS/3127/08-05-2020, C/EIS/2896/27-04-2020, C/EIS/2663/14-04-2020, C/EIS/3012/04-05-2020, C/EIS/3128/08-05-2020, C/ IES/3209/12-05-2020, C/EIS/3910/09-06-2020, C/EIS/4584/02-07-2020, C/EIS/5368/31-07-2020, C/EIS/ 6471/24-09-2020, G/EIS/7485/2-11-2020 complaints and notifications of incidents of violation. C/EIS/3142/11-05-2020, C/EIS//3244/13-05-2020, C/EIS/4348/23-06-2020, C/EIS/4653/03-07-2020, C /EIS/5468/05-08-2020, G/EIS/7233/21-10-2020, G/EIS/3143/11-05-2020, G/EIS/3246/13-05-2020, G/EIS /4436/26-06-2020, C/EIS/5173/03-07-2020, C/EIS/5590/11-08-2020, C/EIS/7254/22-10-2020, The Authority, in the context of the examination of these cases, sent to the mobile telephony services company COSMOTE KINITES TELEPIKOINONES S.A. & OTE TELEPHONES S.A. (hereinafter "Cosmote" or "data controller") the letter No. C/EX/7774/11 -11-2020 document, in which her opinions were requested regarding the relevant complaints, the notified incidents of violation and also the general way of dealing with the issues in question. Specifically, it was requested: a) A description of the policies that were applied regarding the process of canceling and replacing a SIM card by a subscriber, before the relevant incidents of violation were established. b) Description of the changes/amendments made to said policies and procedures after the above incidents of violation were identified. c) Description of the policies and relevant instructions currently applied by subscriber service points for the SIM card cancellation and replacement process. d) Disclosure if they have found other similar incidents after the implementation of the new policies and beyond those that have been submitted to

the Authority. The company responded to the above issues with document No. C/EIS/8858/28-12-2020. According to this, the measures applied per time period are as follows. 1st period: Policies applied by the company until April 2020 During this period for the replacement of a SIM card in the company's branches, the applicable procedure provided for the following: a. In case of physical presence of the subscriber in the store, presentation of original proof of identity. b. In the event that a third person appeared at the store to request the replacement of the card on behalf of the subscriber, it was required to show the subscriber's authorization to the third person with a certificate of the original signature of the customer from KEP or the Police Department, as well as the presentation of the authorized person's original identity document . A copy of the authorization was kept on file for evidence purposes. 2nd period: Policies applied by the company from April 2020 to October 2020 In particular from 8.4.2020, SIM card replacement requests are only served with the physical presence of the subscriber in the store. Requests submitted to the store by a third party authorized by the subscriber are not completed. In the case of a request submitted by a third party on behalf of the subscriber, the request is handled by the Customer Service over the phone, as follows: The employee of the branch network contacts the Customer Service by phone and reports that an authorization from a third party has been presented. The replacement of the card for this case is carried out in accordance with the existing procedure of Customer Service and not by the network of stores. Specifically, the following security measures are applied: Telephone identification of the subscriber of the telephone connection for which there is a request to replace a SIM card is carried out in order to confirm the request. If the request is indeed confirmed, the SIM card is sent to the subscriber via courier and then activated. 3rd period: Policies applied by the company after October 2020 Specifically, from 19.10.2020 the following information message is sent to the mobile number of the customer for which there is a request to replace a SIM card "For the mobile number 697XXXXXXXX you have requested the replacement of a sim card . In the event that the application was not made by you, contact 13888 immediately" With the document No. G/EXE/700/15-03-2022, the Authority called the company before it at its meeting on Wednesday 22-03 -2022, in order to provide further clarifications and, in addition, to present in detail its views on the infringement incidents and related ones, with no. proc. , for which she had already submitted her opinions, with no. prot. C/EIS/8867/18- 12-2019, C/EIS/4369/01-07-2021, C/EIS/5007/29-07-2021 and C/EIS/6908/26-10-2021 memos , respectively, on which clarifications were required, as well as for item no. first G/EIS/1771/10-03-21 complaint. The company attended and submitted a postponement request, which was accepted and the examination of the case was postponed to the meeting of 3-5-2022, at which A, Deputy Director of OTE Group Sales Networks Support & Training, B, Deputy Director

attended for the company Residential Customer Service & Sales OTE – COSMOTE, Eleni Geroutsi, Lawyer, AM ... and C, Data Protection Officer of the OTE Group and who answered the questions that were put to her, while reiterating what the company had stated in the above document her. In addition, the company argued that the examination of the cases by the Authority violates the principle of pending litigation and the principle of ne bis in idem, since the company was also controlled for many of the above incidents by the Authority for Ensuring the Privacy of Communications (hereinafter "ADAE"), for many of which ADAE Decisions and/or Conclusions have been issued, while in two of these cases ADAE has imposed on the company an administrative fine of 30,000 euros and 50,000 euros respectively. The company received a deadline for the submission of a memorandum, which it submitted with the no. prot. C/EIS/7531/30-05-2022 e-mail message, in which he attaches the Findings and Decisions of the IAEA in relation to twenty-five (25) incidents of violation, but also provides clarifications regarding the policies that were applied in each period from the company. He adds that during the 3rd period a security code (one time password - otp) is also sent to the customer via SMS, in order to complete the activation of the new SIM card. He adds that, from 8-2-2021, in the case of submitting a replacement sim card in stores, the old card will be completely blocked for 6 hours and then the new one will be activated with incoming sms blocked for 18 hours, while if this is done in the service customers, the blocking of the old card is permanent. In the case of a telephone replacement request, information is given on the identification details which are verified and include the full name, VAT number, VAT number, father's name, date of birth, billing address and the collection point where the last bill was paid . In the case of non-response to the confirming outgoing call from customer service by the "applicant" to the information entered in the system or in the event that the latter has no other connection to the company's network, then he is informed that he must go to a store for completion of the request. According to the said memorandum the process of identifying the subscriber when activating call forwarding has been strengthened since March 2021, as the subscriber is guided to perform the diversion himself from his device, if available, otherwise the verification process described above is followed . In the event that the subscriber has forwarding activated on the connection where the confirmation call is to be made, then it is recommended to remove it, send a signature email request and finally his transition to a store. The company, with its above memorandum, also stated that it re-evaluates on a regular and extraordinary basis the level of security of the existing measures, as it did in the above cases, as well as that it applies a procedure for assessing the security risks of information systems, while in the immediate future it is going to apply a similar procedure also regarding the security and protection of personal data processed by the company. He also invokes the need for immediate and quick service

to subscribers, pointing out that the blocking of the new card entails the interruption of the services provided and could only be implemented repressively and indeed after the appearance of a sufficient volume of incidents and not preventively, as the aim is to balancing security with speed and quality of service. Moreover, it is argued that similar incidents had not occurred previously and this proves the adequacy of the existing measures, until then. However, it is claimed that the barrier measure was pre-decided, but due to complex technical implementation was delayed. The company maintains, moreover, that as a large part of the fraud is carried out with the presentation of false documents, its employees do not have the competence to judge about the forgery, which belongs to the judicial authorities. Finally, he invokes the statement of the ADAE on its incompetence regarding such controls. Finally, the company stated that since October 2020, no other similar incident has occurred. In conclusion, the company invokes the principle of proportionality and leniency with regard to the sanctions imposed by the Anti-Corruption Commission, asserts that it has disclosed all the incidents as it should, that there was no malice, that it took measures, but also the circumstances of the frauds in question amid anti-pandemic measures. The Authority, after examining all the elements of the file and referring to those distributed during the hearing, after hearing the rapporteur and the clarifications of the assistant rapporteurs and after a thorough discussion, DECIDED IN ACCORDANCE WITH THE LAW 1. From the provisions of Articles 51 and 55 of General Data Protection Regulation (Regulation (EU) 2016/679 - hereinafter, GDPR) 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. 2. According to article 4 par. 1 of the 7th Protocol of the European Convention on Human Rights (ECHR), which was ratified by the first article of Law 1705/1987 (Government Gazette 89 A`) , "no one may be prosecuted or convicted by the courts of the same State for an offense for which he has already been acquitted or convicted by an irrevocable decision in accordance with the law and criminal procedure of that State." With this provision, the non bis in idem principle is established, which, as is firmly accepted by the jurisprudence of the ECtHR, the ECtHR and the SC, applies not only to criminal sanctions but also in cases where the relevant legislation provides for the imposition serious administrative penalties, such as large fines. A basic condition for the application of the non bis in idem principle, according to the Jurisprudence of the SC, is that a sanction has been imposed in the context of an administrative procedure, which has been finalized, either due to the non-exercise of an appeal or due to the rejection of the exercised appeal (StE 951 /2018, Supreme Court 4309/2015). In this case, as it appears from the memorandum of the complained company, the ADAE imposed sanctions

against it only in two cases (D, E), against which the complained party already states that she intends to appeal before the competent Court. imposition of a finalized sanction on behalf of the ADAE, which prevents the examination of the complaints in question by the Authority, in application of the non bis in idem principle. Regardless of this, the violations examined in this case constitute an infringement of a legal good other than that affected by the violations, for which sanctions have been imposed on the company by the ADAE and which concern exclusively the implementation or non-implementation of the policies of those in charge, as the case may be. Therefore, no processing (no. 12 par. 3 sec. c n. 3471/06) and not, in addition, to the effectiveness of the measures described in them and which are followed based on them and which in the end, even though they were implemented, were not sufficient to prevent the identified incidents breaches of subscriber data. ... Therefore, and for this reason, the non bis in idem principle is not applicable in this case according to the recent Jurisprudence of the Supreme Court (see Supreme Court 433/2021, 1771/2019, 3473/2017), which accepts that it is possible to impose two administrative sanctions on the same offender for the same facts by different administrative bodies or independent administrative authorities if their imposition aims to protect particularly important and different legal goods because any impossibility of imposing one of the two administrative sanctions in application of the non bis in idem principle, since one of them has already been imposed and finalized, it would render inactive the obligation that different state bodies have under the Constitution to protect the victims of their individual rights (StE 433/2021, 3473/2017) and that this principle neither prohibits the cumulative imposition of sanctions by invoking provisions that are in fact conceptually confluent nor imposes "unity of procedure" (una via), and, precisely for this reason, cannot be considered to prohibit the imposition of such sanctions by different authorities with independent and independent procedures (StE 1771/2019). 3. According to Article 4 of the GDPR, personal data is defined as "any information relating to an identified or identifiable natural person" and a data controller is defined as "the natural or legal person, public authority, agency or other entity that, alone or jointly with others, determine the purposes and manner of processing personal data; where the purposes and manner of such processing are determined by Union law or the law of a Member State, the controller or the specific criteria for appointing may be provided for by the law of the Union or the law of a Member State", while the processor is defined as "the natural or legal person, public authority, agency or other entity that processes personal data on behalf of the controller". 4. The same article defines a personal data breach as "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". 5. According to article 5 paragraph 3 of the GDPR the data

controller bears the responsibility and must be able to prove his compliance with the principles of processing established in paragraph 1 of the same article, which include legality, objectivity and transparency of processing in accordance with article 5 par. 1 item a' and the confidentiality and integrity of the data in accordance with article article 5 par. 1 item f'). In other words, with the GDPR, a compliance model was adopted with the central pillar being the principle of accountability in question, i.e. the controller is obliged to design, implement and generally take the necessary measures and policies, in order for the data processing to be in accordance with the relevant legislative provisions and, in addition, must prove himself and at all times his compliance with the principles of article 5 par. 1 GDPR. 6. According to article 12, paragraph 5, of Law 3471/06 "in the event of a breach of personal data, the provider of publicly available electronic communications services shall immediately notify the A.P. of the breach. D. E.G. ….. The notification … shall include, at a minimum, a description of the nature of the personal data breach and the points of contact from which more information can be obtained. It also describes the consequences of the breach and the measures proposed or taken by the body to address the breach." 7. According to article 12 par. 1 of the above law, "the provider of funds to the public of electronic communications services must take the appropriate technical and organizational measures, in order to protect the security of its services, as well as the security of the public network electronic communications. These measures, if necessary, are taken together with the provider of the public electronic communications network, and must guarantee a level of security commensurate with the existing risk, taking into account the most recent technical possibilities on the one hand and the cost of implementation on the other their.". 8. In accordance with Article 12 paragraph 3 of Law 3471/06, "... with the measures of this article as a minimum: a) it is ensured that access to personnel datacharacter can only be legally authorized personnel
approved purposes, b) stored or transmitted are protected
personal data from accidental or unlawful destruction, by accident
loss or alteration and from unauthorized or unlawful processing,
including storage, access or disclosure and c)
the implementation of a security policy in relation to processing is ensured
personal data.".
9. According to paragraph 6 of the same article, "when the data breach
of a personal nature may adversely affect the data

personal nature or the private life of the subscriber or another person, o

operator immediately informs the affected subscriber of this violation

or the affected interest. The update of the previous paragraph includes

a minimum description of the nature of the personal data breach

character and the points of contact from which they can be obtained

more information, as well as recommendations that may limit

potential adverse effects of the personal data breach

character."

10. Furthermore, in paragraph 7 of this article it is defined that "the information of

affected subscriber or affected individual for the data breach

of a personal nature is not necessary, if the body has proven against

satisfactory manner to the competent authorities, that it has implemented the appropriate

technological protection measures and that these measures were implemented for the

data related to the security breach. These technological measures

protection must, at a minimum, include secure encryption of

data so that unauthorized access is not possible. If the carrier

has not updated in accordance with paragraph 6 of this article,

the competent authorities, after examining its possible adverse effects

breach, they may ask him to do so."

11. Regarding the incidents of personal data breach that

have been recorded and listed in the Appendix, the following three arise

categories of incidents, in relation to the policies that were in place:

1. The current policy and measures related to it were not implemented

SIM card replacement procedure. Specifically, they have been recorded

nine (9) incidents for the 1st period, seven (7) incidents for the 2nd period

and two (2) incidents for the 3rd period.

2. The measures applied regarding customer authentication

during the process of replacing the SIM card was not sufficient to

prevent the exploitation of weaknesses in existing policy and

personal data breach. Specifically, nine (9) have been recorded

incidents for the 1st period, seven (7) incidents for the 2nd period and two

(2) incidents for the 3rd period.

3. The measures applied regarding customer authentication

during the process of servicing other service requests (e.g. diversion

calls, issuing new numbers

subscriber phones) were not

effectively to prevent the exploitation of weaknesses in

existing policy and the breach of personal data. Specifically,

one (1) incident recorded for 1st period, one (1) incident for

in the 2nd period and three (3) incidents for the 3rd period.

Considering the aforementioned categorization of incidents

the following are established:

I. From the analysis of the incidents belonging to the three categories (A, B and

C) it follows that the security measures applied to the respective

periods were not appropriate in order to ensure adequate

level the security of the services offered as well as its security

public electronic communications network (article 12, par. 1 of Law 3471/06).

It is noted that the security level must be proportional to

existing risk, taking into account one of the most recent

technical capabilities on the one hand and their implementation costs on the other.

Also despite the fact that the company seems to have acted in order to

address the approaches followed by the malicious and limit

the occurrence of relevant incidents, the review of applicable policies
and the adoption of the additional measures was not able to prevent it
appearance of new cases.
II. In addition, the existence of incidents that were exploited is established
weaknesses in the customer identification process in various services
(eg process of connecting one number to another, diversion process
calling from one number to another number, card replacement process
SIM). This fact raises additional security issues as well
of the services offered as well as the public electronics network
communications (article 12, par.1 of Law 3471/06).
III. From the evaluation of the incidents belonging to the first (A) category
it is found that there were cases where the policies that had been set the
corresponding periods were not applied (article 12, par.3, ed.c of Law 3471/06).
From the above findings, two (2) categories of violations emerge.
Specifically:
1. From the first and second findings (I, II above) it follows that the company
implemented at different periods of time policies which were incomplete
(article 12 par. 1, law 3471/2006).
2. From the third finding (III above) it follows that there were cases where
the applicable policies were not applied (article 12 par. 3 sub. c, law 3471/2006).
Also, cases (at least eight) were observed where the incidents did not
were notified to the Authority without delay (discrepancies were noted between the time
during which the incident became known to the controller and his
time of submitting its notification to the Authority, ranging from one to three
months).
Based on the above, the Authority unanimously judges that according to Article 12 of Law

3471/2006, the conditions for enforcement against those responsible are met

processing, based on the one hand, article 13 of Law 3471/2006, in combination with

article 21 par. 1 item b' of Law 2472/1997 and with Article 84 of Law 4624/2019,

and on the other hand, article 58 par. 2 sec. i' of the Regulation and article 15 par. 6 thereof

Law 4624/2019, of the administrative sanction, referred to in its operative part

present, which is judged to be proportional to the gravity of the violation.

FOR THOSE REASONS

It imposes on the company the effective, proportional and deterrent administrative

fine that is appropriate in the specific case according to

special circumstances thereof, amounting to one hundred and fifty thousand euros (150,000.00)

euros, for the violations of Article 12 of Law 3471/2006 found above.

The president

Kon/nos Menudakos

The Secretary

Irini Papageorgopoulou