Athens, 02-12-2022 Prot. No.: 3092 DECISION 38/2022 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. Initially, the following were submitted: a) Complaint No. C/EIS/4807/10-7-2020, b) Complaint No. C/EIS/7103/16-10-2020, 7255/22-10-2020, C/EIS/7299/23-10-2020, C/EIS/7300/23-10-2020 of incidents of violation. and G/EIS/7301/23-10-2020 notices The Authority, in the context of the examination of these cases, sent to the mobile telephony service provider Vodafone - PANAFON S.A.E.T. (hereinafter "data controller" or "Vodafone") the document no. prot. 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. G/EIS/8392/07-12-2020 according to which the measures implemented by the company for the effective identification of subscribers in cases of issuing a new or replacement SIM card SIM card are divided into 4 time periods. 1st period: Policies applied by the company until April 2020. During this period, the procedures followed by the company are as follows: (a) In the event that the relevant request is submitted in person by the subscriber, within the company's store, it is carried out by the competent officials to verify the identity of the applicant. In particular: a. During the process of identifying the applicant, only

identity cards/passports are accepted and not original supporting copies thereof (nor certified copies). (slip b. It is checked that the applicant who appeared is the same as the one shown in the photo of the identification document. c. It is checked in each case that the age estimated by the employees of the person who appeared/applicant matches the age of birth indicated on the identification document. d. It is checked and verified that the number of the supporting identification document and the date of birth written on it are identical with the corresponding data, which exist in the company's systems. e. The supporting document is carefully checked for any signs of forgery. (b) In the event that the a relevant request is submitted within the company's store by a third party using an authorization from the subscriber, similarly, the competent employees conduct face-to-face checks. In particular: a. It is checked that the authorization provided is special (and not general) and that it explicitly states that it provides the authorized the right to request the replacement of the SIM card of a specific MSISDN. b. It is checked that the details of the authorizer/delegate listed in the authorization match: o The details of the authorizer (name, surname, identification document number, date of birth, etc.) of the presented ID/passport). c. It is checked that the authorization provided is still valid (the authorization can be used only once and is valid for 6 months from the date of its signature) and that both the documents provided (authorization and identification document of the authorized person) do not show signs of forgery. and by lawyers. The authorization is required to bear an original visa of the authorizer's signature from any public or municipal authority, from a bank, from notaries In the case of electronic authorization (issued through gov.gr using Taxisnet codes) the authenticity of the electronic authorization is confirmed by entering https ://dilosi.services.gov.gr/ * either using the verification code of the document, or using the QR code. (c) In the event that the relevant request is submitted to the company's call center, the competent employees will similarly carry out close checks. In particular: a. Initially, the applicant is identified by phone and informed that he will need to go to a company store in order to process his request. b. In the event that the applicant informs that he does not wish or is unable to go to any of the company's stores either due to the special conditions of the coronavirus pandemic (COVID19) or because there is no company store operating in his area, the stated reasons for replacing the SIM will be examined and he will be informed the applicant that it is possible to send a non-activated SIM card by registered mail via a courier company. Also, the applicant is informed that in this case only he (by showing proof of identity) will be able to receive the sent non-activated SIM card from the responsible employee of the courier company. 2nd period: Policies applied by the company from April 2020 to October 2020 After the above incidents of violation were identified, i.e. in April 2020, the company proceeded with amendments to the existing procedures for replacing a SIM card by a subscriber. In particular, from

27/04/2020, the above procedures were amended, namely: a. The step of telephone communication with the requesting subscriber / SIM holder was established in order to confirm the submitted request in the cases of request through authorization in stores and request through call center. b. The obligation of the requesting subscriber to complete (via gov.gr) a relevant declaration and send either the declaration or the issued code, in order to check this in the case of a request via a call center, was established. c. In non-personal appearances, the obligation to send the SIM card via registered mail was established and no other SIM card that the subscriber may have is activated. Also, the activation process is done over the phone, in the connection for which the replacement of the SIM card is requested. Along with the aforementioned amendments, the following additional measures were taken: a. The managers and employees of the company's call center were informed and trained with a clear indication of the attention they must show to the risks posed by the SIM replacement process and the consequent need for full compliance and application of the above procedures. b. Relevant informational material was posted on the internal website (intranet) of the company's stores, with a clear indication of the attention they must show to the risks posed by the SIM replacement process and the consequent need for full compliance and application of the above procedures. 3rd period: Policies implemented by the company from November 2020 to July 2021 Despite the above new policies, which came into force in April 2020, new incidents were also observed, due to which the applied policies were improved again to combat this particular fraud. In particular, from 30-10-2020 the provision of the possibility was stopped replacement sim cards from the company's call center (with applicants to directed to one of the company's stores). In the event that the visit by the subscriber to a store of the company was not possible, the replacement of the sim card is carried out only by sending the new sim card by registered letter to the requesting subscriber and by simultaneously sending an informative SMS to the telephone number to which the replacement request. Furthermore, on 10-11-2020 the sim card replacement process at the company's stores was also optimized through the provision of an additional security step. In particular, the confirmatory outgoing call to the telephone number concerning the request to replace a sim card (which was only carried out in cases of a request with authorization) was also extended to the cases of a request submitted in person by the owner of the telephone number in question. 4th period: Additional measures implemented after July 2021 The company established additional measures, which are the following: (a) no possibility to change a card through digital channels in case of loss or theft and service only from stores and (b) after when the SIM card is replaced, incoming sms is blocked for a period of 2 hours. With the document number C/EXE/701/15-03-2022, the Authority called the company before it at its meeting on Wednesday 22-03-2022, to provide further clarifications and to

present the views in detail of infringement incidents and related complaints. In addition, with the above call, the company was informed that clarifications are also required regarding the no. first G/EIS/5508/19-07-17 and G/EIS/2224/31-03-2021 complaints, concerning the same issue, and for which the company was informed with no. prot. G/EXE/1614/29-06-2021 and G/EXE/9729/04-12-2018, respectively, documents of the Authority and to which he responded with the no. prot. G/EIS/234/14-01-2019, G/EIS/4721/15-07-

2021 memos, respectively. The company appeared and submitted a postponement request, which was accepted and the examination of the case was postponed to the meeting of 3-5-2022, during which Emmanuel Chalkiadakis, Lawyer, AM ... ..., Apostolos Vorras, Lawyer, appeared for the company. AM ..., Emmanouil Dimogerontakis, Lawyer, AM ... ... and A, Data Protection Officer of the company and who supported what she had set out in writing in the above document, but also received a deadline for submitting a memorandum, which she filed with No. prot. C/EIS/7738/06-06-2022 email message. Following this memorandum, the company submitted additional information on 7/6/2022. process identification With the above, the company reports that since February 2018, a preliminary check of customer service procedures, including subscribers, had been carried out. This assessment was carried out in the context of an initial risk assessment in the context of which the relevant processing activities, the information systems involved, the type of personal data, the legal basis of the processing, as well as the technical and organizational measures taken for the ensuring an adequate level of personal data protection. From the prepared study, it was found that the technical and organizational measures applied to ensure the security of the customer identity verification procedure, are extremely effective, since no SIM swap incident had been detected until February 2020. In the memorandum it is noted that the first SIM swap incidents in the Company were detected in the month of February, i.e. they coincided with the beginning of the covid-19 pandemic and the imposed restrictive measures, which resulted, among other things, in the rapid increase in banking transactions and phenomena of electronic fraud. In the context of dealing with the phenomenon of SIM swap fraud, in March 2020, the company prepared an analytical impact assessment study as well as taking additional measures to deal with the phenomenon. It is noted that the following were taken into account for the preparation of this specific study: The new methodology of electronic fraud, which indirectly affected the increase in the risk for the rights of subjects in the context of the SIM card replacement process (through: a. the increase in the probability of occurrence of the risk, b. of the indirect increase in the severity of the effects for the data subjects) The results of the working meetings with the Vodafone Group's Data Privacy team, in the context of which SIM swap fraud incidents found in other

countries abroad were discussed. Also, in the context of the specific meetings, the methodology of the criminal actions was analyzed and an early evaluation of the potential additional security measures that could be adopted was carried out. The results from the analysis of international bibliographic reports on incidents of SIM swap fraud, which take place on a global scale. The incidents of violation of personal data of the company's subscribers by malicious persons who took advantage of the SIM card replacement possibility pretending to be either the owner of the SIM card or someone authorized by the legitimate subscriber. The increase in banking transactions and the phenomena of electronic fraud combined with the spread of the covid-19 pandemic and the related restrictive measures. As a result of this particular study, the following measures were taken: Adding further safeguards to the authorized SIM card replacement process. i. ii. the confirmation of the authenticity of the electronic authorization (issued through gov.gr using the Taxisnet codes) by entering https://dilosi.services.gov.gr/ either using the verification code of the document or using the QR code. the telephone communication with the requesting subscriber/SIM owner, for which a replacement is requested, should be carried out on the subscriber's contact telephone number, which has been declared by the latter and is stored in the company's systems, in the event that the telephone number for which the request is made SIM replacement is disabled. Adding further safeguards to the call center SIM card replacement process. After completing the phone identification, the requesting subscriber is asked to complete the process in a Company store. Alternatively, the possibility of sending a non-activated SIM card via courier. Only the applicant with proof of identity can receive it, while activation is suggested to be done by phone, once the following steps are completed: i. ii. iii. sending a relevant declaration (via gov.gr) or the issued code, in order to check it, a call from the requesting subscriber/SIM owner to the Company's call center (without hiding the phone number) and complete identification, a call from the company to requesting subscriber/SIM holder in order to confirm the submitted request. The above telephone communication will be carried out on the telephone number for which the SIM replacement is requested and in the event that this is deactivated on the subscriber's telephone number, which has been declared by the latter and exists in the Company's systems. Especially for prepaid subscribers, if the phone for which the SIM replacement is requested is switched off (and there is no other contact phone in the company's systems) it is recommended that the applicant provide information in relation to when the last airtime renewal was carried out and the amount it concerned. In October 2020, the company again updated its Impact Assessment Study from 2/3/2020. In particular, it recommended the adoption of additional security measures regarding the SIM card replacement process by the requesting subscriber/SIM owner, which were finally adopted and implemented. In particular, he recommended:

The clear indication to the managers and employees of the company's stores about the care they must show during the identification process, given that the use of a protective mask makes it difficult to check the identity. The addition of an additional security barrier during the SIM card replacement process by the requesting subscriber/ SIM owner, within the company's store: a confirmatory outgoing call to the telephone number concerning the SIM card replacement request. Removal of the ability to replace a SIM card through the company's call center (customer service department). Applicants must visit a company store and submit their request in person. Alternatively, it is recommended to send the new SIM card only by registered letter with a parallel sending of an informative SMS to the telephone number to which the replacement request concerns. Finally, in June 2021, the company again updated its 2/3/2020 Impact Assessment Study resulting in the adoption and implementation of the following measures: Addition of additional safeguards during the SIM card replacement process: i. ii. sending a consent message (SMS consent) to the number for which the SIM card replacement request was made, in order for the requesting subscriber/SIM holder to confirm the request, after the completion of each SIM card replacement request automatic activation of incoming SMS blocking for a period of two ( 2) hours. Also, in August 2021, the company extended the duration of the blocking of incoming SMS from two (2) to four (4) hours, a measure that is still in effect today. At the same time, the company points out that it has already implemented a set of training, information and awareness actions for its staff. In particular, it is reported that the company from the beginning of 2020 started the implementation procedures: a) Staff information and awareness program and b) Staff training program in the new procedures. Regarding the incidents of violation for which the company was summoned to a hearing, clarifications were given for fourteen (14) of the examined cases. In particular, the following were highlighted: The complaint No. C/EIS/4807/10-7-2020 is related to the incident notified to the Authority with No. C/EIS/7103/16-10 -2020 breach notification. For five (5) incidents which are included in No. C/EIS/7103/16-10-2020 notification of an incident of violation, the company has been called to provide data, which it has provided to the ADAE. Subsequently, a hearing has taken place before the Court of Human Rights and the issuance of a decision is pending. For three (3) incidents which are included in No. C/EIS/7103/16-10-2020 notification of an incident of violation, the company has been called to provide data, which it has provided to the ADAE. A possible summons of the company to a hearing is pending. For the notification of violation No. C/EIS/7255/22-10-2020, the company has been called to provide data, which it has provided to the ADAE. A possible summons of the company to a hearing is pending. For the notification of violation No. C/EIS/7299/23-10-2020, the company has been called to provide data, which it has provided to the

ADAE. Subsequently, the company has been summoned to a hearing before the ADAE with a deadline for submitting a memorandum on 07-08-2022. For the notification No. C/EIS/7300/23-10-2020 of an incident of violation, the company has been called to provide information, which it has provided to the ADAE. Subsequently, a hearing has taken place before the Court of Human Rights and the issuance of a decision is pending. For the notification No. C/EIS/7301/23-10-2020 of an incident of violation, the company has been called to provide information, which it has provided to the ADAE. Subsequently, a hearing took place and we were served with the ADAE's decision, which imposes an administrative sanction on the company. The one with no. Prot. C/EIS/5508/19-07-17 complaint does not constitute an incident of SIM swap fraud. In this case, there was fraud in the context of entering into a new contract with the company. The methodology differs substantially from the other cases. The case is already being examined by the Greek Justice. In summary, it is stated that: for six (6) incidents a hearing has taken place before the ADAE and the issuance of a decision is pending, for four (4) incidents, the company has been summoned to provide information, which it has provided to the ADAE. A possible summons of the company to a hearing is pending, for one (1) incident, a summons of the company to a hearing before the ADAE has taken place with a closing date for submitting a memorandum on 07-08-2022, for one (1) incident, the decision of the ADAE has been served , which imposes an administrative penalty on the company, one complaint does not constitute an incident of SIM swap fraud, and one complaint relates to a reported breach incident. In addition, the company states that from the above facts, in combination with the relevant information contained in the notifications, it follows that in most of the cases the Company's then applicable procedure was correctly followed by the competent employees. Despite this, the miscreants managed to complete the illegal operations by presenting fake documents. Only in two cases is it found that the company's procedures were not faithfully applied, as the additional security measure that had been taken at the time of the incident by the company, namely the measure of "phone communication with the requesting subscriber/SIM holder for the for which a replacement is requested to be carried out on the subscriber's contact phone number, which has been declared by the latter and is stored in the company's systems, in the event that the telephone number for which the SIM replacement is requested is deactivated." For the rest, in all other cases the security measures and procedures that had been established and implemented at that time were observed. The company notes that the malicious actors acted systematically, premeditated and organized, by presenting and using fake documents in most cases, as a result of which they exceeded the organizational security measures and the reasonable suspicions of the company's employees. In addition, it is stated that the arousal of suspicion is not to be expected with respect to the average

employee of the provision of mobile telephony services, since, despite his relevant training, he is objectively less familiar with fraudulent representations as to the identity of persons appearing as policyholders. Much more, it is considered as unexpected to cause corresponding suspicions to the employees of the company, when those appearing: a) had full knowledge of the personal data/personal details of the subscriber, which they reported to employees of the Company, b) presented fake identity documents. Finally, the company raises an issue regarding the application of the ne bis in idem principle, as some of the incidents are already being controlled by the Communications Privacy Authority (hereinafter "ADAE"). In particular, the company refers to the decision 122/2012 of the APDPH regarding the application of this principle in cases of imposition of sanctions by two administrative authorities for these facts. In particular: "On this matter, the Authority, by majority, judges that when for these (or essentially similar) facts, which involve an infringement of these or various legal goods, and which refer to the guilty persons (identity of acts and offenders), the first competent authority has taken and issued a decision, and its judgment is on the substance of the case, then it is not possible for the second competent authority to take over their judgment for the possible imposition of sanctions. Therefore, in this particular case, if the ESR has been taken over and judges on the substance of facts, which are the content of a television or radio broadcast, which may also constitute an infringement of the right to the protection of personal data, then the APDPH when called upon to take over as a second competent body, it is not possible to exercise its sanctioning authority by carrying out a relevant investigation, establishing the violation and imposing sanctions, but it is obliged to proceed with the finding that for these (or substantially similar) facts there is a substantive judgment of the ESR and must to refrain from examining these factual incidents. Although in the opinion of three members the ne bis in idem principle does not simply cover the coincidence of these facts and guilty persons (identity of act and offense) but is only applied in the event that these facts constitute an infringement of this legal good and the these purposes of protecting society as a whole, and therefore since the Authority's mission is to protect personal data, as such and not the personality in general, it still retains the authority to impose sanctions even though the ESR, during the control of radio and television broadcasts, has the authority to impose sanctions for insulting respect for human dignity and personality in general." The company states that corresponding jurisprudential positions have also been formulated in decisions of the Council of State [Decision 1091/2015 (StE Section D'- Referral to a Seven-member Panel), which is identical with the opinion of the majority of the APDPH, as well as Decision 2797/ 2015 (StE Section D'), which follows the opinion of the minority of the APDPH]. Therefore, given the special nature of the case in question and its individual aspects, the company finds that there is an

identity of the objective nature of the incidents examined by the two authorities, both by the APDPH and by the ADAE, and there is a complete identification of the facts regarding the scope of control of the two Authorities as incidents of violation in the light of the application of this legislation (Law 3471/2006 article 12 paragraph 5, as amended and in force) and for this reason the company raises its concern regarding the application of the ne bis in idem principle. In addition, it finds that the possible imposition of sanctions by the above Authorities against the company would not be possible based on the general principle of administrative law on non-imposition of cumulative administrative sanctions for the same act (ne bis in idem). 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, 4309/2015). In this case, as it appears from the memorandum of the complained company, the ADAE has imposed sanctions against it only in two cases (B, C), against which the complained party already states that she intends to appeal before the competent Court. Therefore, there is no case of imposing a finalized sanction on the part 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 exclusively concern the implementation or

non-implementation of the policies of the data controllers (no. 12 par. 3 para. c Law 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 of data breaches subscriber. ... 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 is aimed at the protection of particularly important and different legal assets because any failure to impose one of the two administrative sanctions under application of the non bis idem principle, as long as 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, it cannot be considered as prohibiting the imposition of sanctions those from different authorities with independent and autonomous 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 the 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 at. 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 body providing 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. According to article 12 par. 3 of Law 3471/06, "... with the measures of this article as a minimum: a) it is ensured that access to personal data can only be granted to authorized personnel for legally approved purposes, b ) stored or transmitted personal data are protected from accidental or unlawful destruction, accidental loss or alteration and from unauthorized or unlawful processing, including storage, access or disclosure and c) ensure the application of a security policy in relation to the processing of personal data .». 9. According to paragraph 6 of the same article, "when the breach of personal data may have adverse effects on the personal data or the private life of the subscriber or another person, the operator shall promptly inform the affected subscriber of this breach or the affected interest. The update of the previous paragraph includes, at a minimum, a description of the nature of the personal data breach and the contact points from which more information can be obtained, as well as recommendations that may limit possible adverse effects of the personal data breach." 10. Furthermore, in paragraph 7 of this article it is defined that "notifying the affected subscriber or the affected person of the breach of personal data is not necessary, if the operator has demonstrated to the satisfaction of the competent authorities that it has implemented the appropriate technological protection measures and that these measures were applied to the data concerned by the security breach. These technologicalprotective measures must, as a minimum, include safe

encryption of the data so that it is not possible to

authorized access. If the operator has not made an update

in accordance with paragraph 6 of this article, the competent authorities, since

consider the possible adverse effects of the breach, they may

ask him to do so."

11. Regarding incidents of personal data breach

recorded and listed in the Appendix arise the

following three categories of violations:

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

SIM card replacement procedure. Specifically, they have been recorded

three (3) incidents for the 1st period, three (3) incidents for the 2nd

period and 2 incidents for the 4th period.

B. The measures applied regarding the verification of identification of

of customers during the SIM card replacement process was not sufficient

to prevent the exploitation of weaknesses in existing policy

and the breach of personal data.

Specifically, they have

recorded eight (8) incidents for the 1st period and two (2) incidents

for the 2nd period.

C. The measures applied regarding the verification of identification of

customers during the process of serving requests for other services

(eg diverting calls, issuing new subscriber phone numbers) no

were effective in preventing the exploitation of weaknesses

to the existing policy and personal data breach.

Specifically, two (2) incidents have been recorded for the 2nd period, two

(2) incidents for the 3rd period and three (3) incidents for the 4th

period.

Considering the aforementioned categorization of incidents

the following are established:

I.

From the evaluation of the incidents belonging to the three categories (A,

B and C) it follows that the security measures applied to

corresponding periods of time were not appropriate in order to

ensure the safety of those offered at a sufficient level

services as well as the security of the public electronics network

communications (article 12, par.1 of Law 3471/06). It is noted that the level

security must be proportionate to the existing risk,

taking into account one of the most recent techniques

capabilities on the one hand and the cost of their implementation. In this case

case, despite the fact that the company seems to have acted on it

to counter the approaches taken by the malicious and to

limit the occurrence of related incidents, the review of

existing policies and the adoption of additional measures did not stand

capable of preventing the occurrence of new incidents.

Additionally it is found that incidents, which appear mainly

the 3rd and 4th time periods, are related to the exploitation of weaknesses in

customer identification process in various services (e.g.

process of connecting one number to another, process of diversion

call from one number to another number, process of replacing it

SIM card). This fact raises additional questions about the

security of both the services offered and the public

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

From the analysis of the incidents belonging to the first (1) category

it is judged that there were cases where the policies in force at

II.

III.

corresponding time periods were not applied (article 12, par. 3, sec. c

of Law 3471/06). It is noted that incidents of non-application of the existing

policy and applicable measures appear in all periods.

From the above findings, two categories of violations emerge.

Specifically:

1. From the first and second finding (I, II above) it follows that h

company implemented policies in the four consecutive time periods

which were incomplete (article 12 par. 1, law 3471/2006).

2. From the third finding (III above) it follows that there were cases

non-application of the applicable policies of the company (article 12 par. 3 sub. c,

Law 3471/2006).

Also, cases (at least five) were observed in which the

incidents were not promptly notified to the Authority (discrepancies were noted

between the time the incident became known to the person in charge

processing and the time of submission of its notification to the Authority, of

ranging from 2-3 months to even beyond the semester).

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

with the special circumstances thereof, amounting to one hundred and fifty thousand euros

(150,000.00) euros, for the aforementioned violations of article 12 of

Law 3471/2006.

The president

Mr. Menudakos

The Secretary

Irini Papageorgopoulou