DECISION 4/2022 Athens, 27-01-2022 Prot. No.: 222 The Personal Data Protection Authority met, at the invitation of its President, in an extraordinary meeting via video conference on 30-11-2021 following the meetings of the 16 -11-2021 and 23-11-2021, in order to examine the case mentioned in the history of the present. Konstantinos Menudakos, President of the Authority and regular members Spyridon Vlachopoulos as rapporteur, Konstantinos Lambrinoudakis also as rapporteur and Charalambos Anthopoulos were present. At the meeting, without the right to vote, were present, by order of the President, the audit specialists Konstantinos Limniotis, Georgia Panagopoulou, George Roussopoulos and Haris Symeonidou, as assistants to the rapporteur, and Irini Papageorgopoulou, an employee of the Department of Administrative Affairs, as secretary. The Authority took into account the following: The company COSMOTE MOBILE TELECOMMUNICATIONS S.A. (hereinafter COSMOTE) submitted to the Authority, based on article 12 par. 5 of Law 3471/2006 and Regulation (EU) 611/2013, the no. prot. C/EIS/6133/10-09-2020, notification of personal data breach incident, which was supplemented with the no. prot. C/EIS/6882/09-10-2020 document. The company issued a related public announcement about the incident in question1. Following the above, the Authority sent the no. prot. G/EXE/6882-1/20-10-2020 and G/EXE/491/27-01-2021 documents to COSMOTE for clarification. The company provided its answers and the requested data with no. prot. ... and ... its documents respectively (no. prot. 1 see https://www.cosmote.gr/cs/otegroup/gr/enhmerosh-cosmote-14_10_2020.html 1 Kifisias Ave. 1-3, 11523 Athens T: 210 6475 600 E: conta ct@dpa.gr www.dpa.gr Authority: G/EIS/7679/9-11-2020 and G/EIS/2042/23-03-2021). From these documents it emerged that the investigation of the incident, in terms of the applied security measures, had to include the company Hellenic Telecommunications Agency S.A. (hereafter OTE). The companies COSMOTE and OTE were invited to a hearing, before the Authority, with the no. prot. G/EXE/1062/12-04-2021 and G/EXE/1063/12-04-2021 documents of the Authority respectively. The meeting of the Authority, which took place via video conference on 4-23-2021, was attended by Irini Nikolaidis, Legal Advisor of OTE Group with AMDSA, A, ... Director ... of OTE Group, B, Director of ... OTE Group with AMDSA ..., Eleni Gerutsi, Lawyer with AMDSA ..., C, Director of ... OTE Group and D, Data Protection Officer of OTE Group. At the meeting in question, the representatives of the companies presented their views on the incident, but also on more specific questions raised in this regard and the legality of processing the personal data that was the subject of the incident, for all of which the two companies submitted to the Authority, after the hearing, memoranda within the set deadline (Authority prot. no.: C/EIS/3381/24-05-2021 and C/EIS/3382/24-05-2021 for COSMOTE and OTE respectively). From all of the above documents, regarding the incident, the following emerges: In ...2020, it was noticed by the

administrators of the companies' systems, through an automated notification message, that the data storage disk of a server exceeded the capacity limit. After investigation, a file of size 30 GB, called ..., was found stored on this server, which contained subscriber call data for the period 1/9/2020 - 5/9/2020. Also, it was established that from time ... a.m. until ... am of ...2020 there was a 30GB network data traffic between the server and an external internet address (IP address), which belongs to a Lithuanian hosting provider. 2 From the analysis of the log files made by COSMOTE, it emerged that from the same IP address an online piracy (hacking) had taken place on ...2020 on a website, which was hosted on OTE's infrastructure. The hacker managed to gain administrative access, using the password of an OTE administrator, which had come into the hacker's possession in the past, following an incident of leaking passwords of the LinkedIn social networking application. The hacker then managed to run queries on COSMOTE's Big Data system, from which he extracted the file …. It also emerged that to the aforementioned Lithuanian IP address, another four (4) significant data transfers (greater than 1GB) had been made from COSMOTE servers, specifically on …2020 (37GB, 2.4GB and 8.5GB) and on …2020 (6.1 GB). It was not possible to identify the type of data transmitted through this traffic. The leaked file contained subscriber call data for the period 1-9-2020 – 5-9-2020 with the following details: Telephone number A – Telephone number B, base station coordinates, International Mobile Equipment ID Identity IMEI), International Mobile Subscriber Identity (IMSI), timestamp, call duration, provider indicator, subscriber plan, age, gender, average revenue per user (ARPU). The various sets of calls, contained in the above file, include a different combination of the above data. The file comes from the 'BigStreamer' bulk data system. In particular, the data concerned: I. Traffic data, including base station coordinates, for 4,792,869 unique COSMOTE subscribers. Of these, the file additionally contained simple personal data (Age, Gender, Financial plan, ARPU) for 4,239,213 unique subscribers. 3 II. MSISDN2 / CLI3 6,939,656 users of other domestic fixed & mobile operators who called or were called by COSMOTE subscribers. III. The MSISDN, IMEI, IMSI and base station coordinates for 281,403 roaming subscribers who made calls over COSMOTE's mobile network. The initial point from which the incident originated, from a security point of view, was the installation of malicious software (a Bruteforce attack tool) on a server belonging to OTE. According to COSMOTE it is not a system, which is intended or may host personal customer data. The description of the intrusion method is described in the confidential annex A of the decision. The estimated causes of the incident according to COSMOTE are reflected in the confidential annex B of the decision. During the meeting of the Authority and the hearing of the companies COSMOTE and OTE on 23-4-2021, specific questions were raised by the Authority in relation to the processing activities related to the

incident. The companies in accordance with the documents and memoranda mentioned above indicate the following: In the Big Streamer system, for a period of three (3) months, call records of mobile phone subscribers are stored and maintained for two purposes. The first purpose is to serve the requests of subscribers who are experiencing problems/breakdowns in the mobile telephony network such as e.g. no connection, poor signal quality, failed calls, etc. Data retention for three months was deemed necessary in order to assess the repeatability and nature of network problems experienced by 2 Mobile Station International Subscriber Directory Number 3 Caller identification – caller identification 4 mobile phone subscribers in a representative and sufficient period of time. The data file in question (hereinafter also "simple") is kept for the above period of time and is subject to further processing for the purpose of executing the contract with the subscribers (article 5 par. 2 sub. b Law 3471/2006 in conjunction with article 6 par. 1 subsection b of the GDPR) and specifically the provision of electronic communications services, which according to the current regulatory framework must have specific quality characteristics. One of the essential features of the contractually provided services of COSMOTE, as defined by regulations and incorporated in the General Terms of Service that subscribers sign when concluding their connection contract with the company's network, are fault management services. In particular, fault management is a function that is at the core of the provided telecommunications services, in the sense that the subscriber, connected to his provider's network, looks forward to the provision of a service with specific quality characteristics, as determined in particular by the regulatory framework of the GDPR. The company refers in this regard to page 12 of the Guidelines 2/2019 of the European Data Protection Board (hereinafter, GDPR) for the processing of personal data in accordance with article 6 par.1point b), in the context of providing online services to data subjects, where the following is expressly stated: "Although the controller may consider that the processing is necessary for the contractual purpose, it is important to carefully consider the perspective of the average data subject data in order to ensure that there is a genuine mutual understanding of the contractual purpose'. COSMOTE also notes that the obligation of the providers to have effective fault management procedures in order to provide their services uninterrupted and in a quality manner is foreseen by the decision no. 834/2/2017 of the National Telecommunications and Posts Commission (EETT) Gazette 4262/6-12-5 2017 - entitled "Regulation of General Permits" (hereinafter the Regulation of General Permits4) as well as from Decision No. 488/82/2008 of EETT entitled "Code of Ethics for the Provision of Electronic Communications Services to Consumers" - Official Gazette 1505B/30-7-2008 (hereinafter the Code of Ethics5). Furthermore, the obligations stemming from the aforementioned regulatory framework are incorporated into the COSMOTE subscriber contract and constitute contractual terms governing the

provision of telecommunications services. In particular, the following are mentioned in articles 5.4 to 5.9 of the General Terms of Service: "5.4. (…) The coverage provided by COSMOTE through its network is indicated on its website wwvv.cosmote.gr. COSMOTE will offer the 4 In particular, Cosmote points out that according to article 2.1.14 c of the Regulation of General Licenses the following applies: "The provider must apply procedures for immediate examination of the requests and complaints of the users regarding the order , the installation, initiation, termination, pricing and generally the quality of the public network and electronic communications services provided to the public. Also, he must inform EETT, upon its request, regarding all the above requests and complaints which have been submitted to them under signatures...". Case d' of the same article above states the following: "The provider is obliged, within a reasonable time, to take all necessary measures to facilitate and assist users in solving problems related to the operation of the public network and electronic services communications provided to the public'. In addition, articles 2.1.17 b) and c) of the General License Regulation provide for the following: " .... The unjustified interruption of the network and electronic communications services to users also gives rise to the right to compensation for them... c): In particular, in the event that the availability of the network and the provided electronic communications services is lower than the quality of service that the person is obliged to provide in accordance with the provisions of the General Licenses or with the special rights to use radio frequencies or numbers assigned to him or with the conditions of the contract as well as in the case of damage that is not due to the fault of the subscriber or a third party and leads to the interruption of the provision of electronic communications services to the subscriber, except in cases of force majeure, the provider must credit the subscriber (…) ». Finally, article 3.1.8. of the Regulation of General Licenses entitled "Customer Service Departments" provides for the obligation of providers to have a toll-free fault reporting number and the following is stated verbatim: "Especially for fault issues, the service line operates at least 16 hours a day without charge (both for calls in-network as well as for out-of-network calls) from Monday to Saturday". 5 In particular, Cosmote points out that article 5 par.1 of the Code of Ethics specifically provides for the following regarding the minimum consumer information: "1. The provider ensures that it has appropriate consumer information systems in place at each stage of service provision and especially during pre-contractual consumer information, so that it is possible to provide complete, accurate and clear information to the consumer at least about the following: (…) ii) characteristics of the service it provides, iii) quality of service provided, iv) availability of the service, (…), vii) Maintenance and technical support". In addition, article 9 par. 4 of the Code of Ethics states the following: "The service provider ensures that its personnel, who are involved in servicing consumers, redressing their problems and providing

technical support, are sufficiently trained (…) . Especially in cases of damage, the staff provides accurate and comprehensible information to the consumer about the nature of the damage, (…) and provides accurate information about the time and course of repairing the damage". 6 Services twenty-four (24) hours a day seven (7) days a week, without interruption, except for a period of time, which shall not exceed a total of six (6) hours per month, if such interruption is absolutely necessary for the execution of the necessary maintenance work (…). 5.5. (…) in case of interruption of the provision of Services to the Subscriber, through no fault of the latter, for a continuous period of time longer than two (2) hours and fifteen (15) minutes or for a period of time exceeding six (6) hours in any continuous period period of thirty (30) days, (…), the Subscriber will have the right to request in writing the credit of the part of the fixed fee corresponding to the period of the interruption, even if the interruption is due to an event beyond the control of COSMOTE" . COSMOTE states that, from the above, it follows that its obligation based on the current regulatory framework, but also a constituent element of the provided telecommunications services, is to deal with the problems of the network as a whole and also at the subscriber level through the organization and operation of effective fault management procedures. Damage management is a function that can reasonably be expected by its subscribers to be an integral part of the service provided, while it is connected to the basic service in such a way that any provision of it after consent, as a value-added service, constitutes, according to the claims of COSMOTE, defective fulfillment of its contractual obligations based on the regulatory framework. COSMOTE also notes that the closeness of the relationship between the fault management process and the provision of telecommunications services, so that the process in question cannot be offered to its subscribers as a value-added service, also results from the fact that subscribers declare their faults by phone toll-free. COSMOTE also states that according to recital 18 of Directive 2002/58/EC, examples of value-added services include "consulting services for cheaper packages of offers, road guidance services, services that provide traffic information, weather forecast and tourist information, i.e. services which are ecologically distant from the basic service of providing electronic e-commerce services". 7 In relation to the issue of whether the execution of the contract as a legal basis for processing is in accordance with Law 3471/2006, COSMOTE states the following: In article 5 par. 2 of Law 3471/2006 entitled "Processing Rules ", the legal bases for processing personal data in the field of electronic communications are specified, namely: "a) the consent of the subscriber or user after being informed and b) the processing is necessary for the execution of a contract, in which the subscriber or user is contracting party, or for taking measures during the pre-contractual stage, at the request of the subscriber". In article 6 par. 2, 3 and 4 of Law 3471/2006, the processing rules regarding traffic data and location

data are further specified, in particular in the cases of subscriber billing and connection payment (for traffic data) and for the provision of services added value after informing and consenting the subscriber (for location data). According to COSMOTE, the provisions of Article 6 specifically regulate these cases of movement and location data processing (i.e. processing for the purpose of billing and payment of connections, as well as processing for the provision of value-added services) and do not repeal provision of article 5 par. 2 of Law 3471/2006, which, in case of contrary interpretation, has no reason to exist. COSMOTE points out that article 6 par. 2 and par. 3 of Law 3471/2006 should be interpreted in the light of the more general interpretative rules of article 5 par. 2 of Law 3471/2006, taking into account the explanatory statement of Law 3471/2006, where the following are mentioned: "Article 5 repeats the general guiding and interpretive principles of protectionof personal data and privacy, with the necessary modifications and adaptations in relation to electronic communications and the use of traffic data. The cases that establish the legality of the processing (consent and contract) are enumerated and the principle of proportionality is specified, with an emphasis on the dimension of necessity. In addition, the possibility of providers to process traffic and location data for fault management purposes is mentioned, as noted by COSMOTE, and 8 in recital no. 29 of Directive 2002/58/EC, according to which: "The service provider may to process traffic data relating to subscribers and users when required in individual cases in order to detect technical malfunctions or errors in the transmission of communications. The service provider may also process traffic data required for billing in order to detect and terminate fraud involving the unpaid use of electronic communications services.' COSMOTE states that from the said recital it follows that Directive 2002/58/EC allows the processing of movement and location data not only for the transmission of the communication, but also for the process of identifying any errors that occurred during the transmission of the communication – so the process of fault management, which is carried out by processing movement and location data at a time slightly later than transmission, could not be treated differently, in the sense that there is no overriding objective reason for treating the two processes differently from a data protection point of view (referring also to CJEU Decision C-119/12 Josef Probst v mr. nexnet GmbH6). According to COSMOTE, the Greek legislator, when incorporating Directive 2002/58/EC into national law and taking into account that during integration EU countries are required to achieve a specific result but it is 6 In paragraph 14 of the said decision it is stated: "The referring court considers that Article 6(2) and (5) of Directive 2002/58 is crucial for the interpretation of Article 97(1) TKG. On the one hand, it underlines that the concept of "billing", which constitutes one of the purposes for the achievement of which Article 6, paragraphs 2 and 5, of the said Directive allows the processing of movement data, does not

necessarily include the collection of invoiced prices. However, it considers that there is no objective reason for the different treatment, from the point of view of personal data protection, invoicing and collection of claims. On the other hand, based on Article 6, paragraph 5, of the said directive, the processing of movement data must be limited to persons who act "under the supervision" of the provider of the public network and the publicly available electronic communications service (hereinafter: service provider). According to the requesting court, it cannot be deduced from this concept whether the service provider should have exclusively, throughout the processing of the data, even in each specific case, the possibility of determining the use of the data or whether general regulations are sufficient on the observance of the confidentiality of telecommunications and the protection of data, such as those agreed in this case with the contractual clauses, as well as the possibility of deleting or returning the data upon request". 9 free to choose the way to achieve this result, took care to allow the processing of movement and location data in accordance with article 5 par. 1 and 2 of Law 3471/2006, among others, in the event that said processing is necessary for the execution of the contract between provider and subscriber. Which functions are necessary for the performance of the contract is specified in detail in the applicable regulatory framework for telecommunications, as discussed above. COSMOTE also states that the German Legislator has chosen a similar way of achieving an equivalent result of protection of movement and location data, even expressly providing for the process of damage management as a legal reason for processing said data (making a relevant reference to Article 100 of the Telecommunications Act, which incorporates , among others, and Directive 2002/58/EC), while also making reference to what is foreseen in the draft of the new Regulation for the protection of privacy in electronic communications. COSMOTE states that the period of three months regarding the maintenance of the simple personal data file was chosen based on the experience of its executives involved in fault management, as it was found that critical information in the fault management process is the identification of the time point at which the problem started reported by the subscriber, in order to determine whether this problem can be related to specific events known to have affected network performance. Examples of such events are work involving base station software upgrades, base station replacements/extensions and interference. Also, there are frequent cases of subscribers who face problems with the quality of services after changing devices. In all cases, it is especially important to be able to ascertain whether the specific problems reported by the subscriber can be related to any of these events. COSMOTE also adds that it is not rare that the subscriber himself is late in contacting the company's Customer Service and reports a service quality problem in these cases, it is useful to have sufficient history so that the problems can be investigated of them and the correlation with

the event that caused them so that fault management actions can be routed. The second purpose is to derive statistical conclusions, which are used for the optimal design of the mobile network. Specifically, call data was enriched on a daily basis with simple personal data (specifically: ARPU, financial plan, age and gender). This file is henceforth referred to as "enriched". The specific file is then anonymized7. For example, depending on the demographic characteristics of the subscribers served by a specific base station and the revenue of each base station, the planning of the network upgrade in the specific area from 3G to 4G is initiated. Anonymization is performed using the SHA-2 algorithm in combination with a salt key, which changes every three months. To limit the risk of re-identification of anonymous data, their retention time is limited to 12 months. This time is considered necessary by the company, in order to draw correct conclusions about the use of the network, taking into account that the usage figures change significantly depending on the season (e.g. usage increases during tourist periods). According to COSMOTE, this process constitutes further processing compatible with the purpose for which the data was originally collected. Until the end of January 2021 ... this file was created after first enriching the first ("simple") file with personal data that do not belong to the special categories of Article 9 of the GDPR (ARPU, age and gender of the subscriber, type of contract). Then, in the new file, the identifiers of each subscriber (MSSDN, IMSI, IMEI) were anonymized. Following a re-evaluation of the above procedure for creating the second file, it was modified so that the simple personal data of the first file is no longer retained. In particular, the change implemented in the procedure 7 The use of this term when quoting COSMOTE's opinions is based on the company's memos 11 anonymization of the enriched file, in order to strengthen it, is as follows: Anonymization is carried out in the file of calls, as well as in the file containing simple personal data. The two above files are then combined to form the second file, which is used for statistical processing. This is essentially a process of combining two separate anonymous files, whose information is combined based on a unique value per (anonymous) subscriber, so that a valid match can be achieved. According to COSMOTE, the applied procedure makes the data anonymous, eliminating the possibility of re-identification of the file in the sense that: i) An irreversible mechanism is used toanonymization of the data, through hashing functions (SHA-256). ii) For greater security an additional key is used, which is changed periodically. iii) The retention time of anonymous data is limited. iv) Only authorized personnel have access to the anonymous data, as a result of which the risk of malicious re-identification of the data through the combination of anonymous and named data is eliminated, while the file in question is not available to third parties. v) In addition to applying a hash function to subscriber identifiers, measures are applied to protect the key. Specifically, the salt key is only accessible by the

system account that implements the anonymization process. vi) Log files are kept for access to the CEA (Customer Experience Analysis) application, which are checked on a daily basis and the necessity of access to subscriber data is confirmed, checking e.g. the existence of a relevant subscriber request in the CRM system (Customer Relations Management), as a result of which the risk of maliciously combining anonymous and named subscriber data with the aim of re-identifying the anonymous file is eliminated. vii) Finally, both named and anonymous data are encrypted at file system level (Hadoop Distributed File System) 12 and AES-CTR algorithm with 128 bit encryption key is used. In addition, when conducting the Impact Assessment Study (for which COSMOTE was specifically asked by the Authority whether it was prepared), data protection requirements regarding data anonymization / pseudonymization were taken into account. In its original submission the company had stated that in accordance with its internal procedures, the details of the processing carried out per system are recorded in the Data Protection Issues Initial Assessment Questionnaire as part of the documentation for the impact assessment. The resulting evaluation results are recorded. The Impact Assessment Study, the complete files of which have been submitted to the Authority (as well as the evaluation questionnaires), was carried out as part of the implementation of the anonymization process on 01/2019 and updated on 03/2020, while it has been approved by the Group's Data Protection Officer OTE. COSMOTE, in conclusion, notes that from all the above and based on common experience, it can be asserted with great certainty that all appropriate measures have been taken so that the anonymous file in question cannot be objectively re-identified, taking into account objective factors, such as costs and the time the re-identification process would require. However, it is a process that is periodically re-evaluated, in the context of upholding the principle of accountability. In relation to the legal basis for processing, COSMOTE states that the process of anonymizing movement and location data, when these are no longer necessary for the purposes of servicing the contract, is expressly provided for in article 6 par. 1 of Law 3471/2006. At the same time, as in any type of processing, in addition to the existence of an appropriate legal basis (in this case the existence of an explicit legislative provision), the obligation to observe the general principles governing the processing of personal data and in particular the principle of purpose limitation, which is declared in article 5 paragraph 1 paragraph b of the GDPR. Furthermore, as it claims, it took into account the relevant Article 29 Working Group Opinion (WP 5/2014 on anonymization techniques), 13 according to which the anonymization process is a case of "further processing", for the evaluation of which specific factors must be considered, such as: the relationship between the initial and further processing purposes, the reasonable expectations of the data subjects, the nature of the personal data and the possible consequences of

the further processing, as well as the measures taken by the controller to protect data. The result of said evaluation is, in COSMOTE's judgment, that the process of anonymizing subscribers' personal data for statistical analysis purposes to improve the network provided is a purpose compatible with the purpose for which the personal data was initially collected. Regarding the time period for keeping the enriched file, one year was chosen, in order to cover all seasons of the year, as the use of the network varies according to the season (e.g. due to tourism, travel on holidays) and the way this makes it possible to draw reliable conclusions about the optimization needs of the network. Access to the above files (simple and enriched) is given to competent COSMOTE personnel – specifically, users from customer service, network technical support users, users who design and implement the functionalities provided by the system, system administrators from the Network Department Planning & Analytics Systems - and the company Intracom, which provides system development and technical support services, as processors on behalf of COSMOTE. Responding to a related question raised by the Authority during the hearing, COSMOTE informed that it has an average of 4,700 (1,500 of which are coverage related) requests per month from its subscribers related to network failure issues, while the enriched file is used daily an average of 50 times, since it is used to draw statistical conclusions, which then contribute to more efficient network planning. COSMOTE also mentions indicative cases of using the anonymous file for the above purpose. 14 Finally, it states that the file with the branded data has been kept since 2015, while the enriched one has been kept since 2019. With regard to informing its subscribers, COSMOTE claims that they are informed about the processing of their personal data for the purposes of fault management through the text of the General Information on the Processing of Personal Data (Data Privacy Notice), which is attached to its General Terms of Service and is a part thereof. Through the text of the General Information, subscribers and prospective subscribers are provided with details regarding the processing of personal data carried out by the company for the purposes of servicing the contract, as well as for other purposes. In particular, in article 3 of the information text in question, the following are mentioned: "3. For what purposes do we process your personal data (lawful processing bases)? We process your data to serve your contract. In order to sign a contract for the provision of fixed or mobile services with OTE and/or COSMOTE and/or to submit an application with the aim of concluding it, it is necessary to provide us with your identity data (name, surname, address, VAT number, identity card number , contact information, etc.), which we will process. In addition, if you become our subscriber, it is necessary for us to process your traffic and location data (e.g. incoming and outgoing calls, location data, etc.) for the purpose of transmitting your communication to our network, billing you accordingly with the use of each service, as well as solving

problems and serving you. As part of the interconnection of our network for the purpose of transmission of communication, we may transfer your personal data to other networks of providers located within or outside the European Union. The processing in question, therefore, is carried out for the purpose of executing the contract between us and providing you with our telecommunication services or even at your request before signing the contract". Furthermore, with regard to the retention period of personal data, the following are included in article 5 of the information text in question: "5. How long will we keep your personal data? The personal data concerning your identity, those resulting from the use of the services, are kept for as long as you are an active subscriber to the OTE/ COSMOTE network. In the event of termination or expiration of your contracts, your data is retained in our systems for a period of fourteen (14) months, based on the regulatory requirement. […] Traffic data is retained for billing and contract servicing for one year. They may also be retained for other purposes after your contract ends, such as in the event of your debt or pending complaint in relation to the provision or pricing of our services, and for a period of time defined by applicable law. Location data is retained for three months for the purpose of resolution problems in our network and improving the service we offer you". Above in the same text, specifically in Article 1, the definition of movement and location data is provided (in a simple and comprehensible way for the average subscriber, as stated by COSMOTE). COSMOTE states that the above information meets the requirements of both articles 13 and 14 of the Regulation and the Guidelines of the Working Group of article 29 regarding transparency based on Regulation 2016/679 and specifically information is provided in a simple and clear manner, with written media and free. In addition, the information regarding the processing of personal data is immediately available on the COSMOTE8 website, while the text is available for those who wish to "download" it. Regarding informing subscribers about the use of the anonymous 8 On the website https://www.cosmot e.gr /c s/c osm ote /gr/dat aprivac ypolic y.ht ml 16 file, the text of the General Information regarding the processing of Personal Data by the companies OTE and COSMOTE (Data Privacy Notice) makes explicit reference to the anonymization process (Article 5 of the text), where the following are mentioned verbatim: "... Otherwise your data will be deleted with way that it is not technically possible to retrieve them or they will be anonymized. Anonymization is the application of practices to personal information that make it anonymous, so that it is no longer possible to identify you from that information. The use of anonymous data is extremely important to us, because it helps us draw useful conclusions regarding the use of our services and, at the same time, is a useful tool in the design of new services. It is thus provided in a simple and understandable way - as stated by COSMOTE - to the subscriber or prospective subscriber information regarding the anonymization of his data for

the purposes of drawing statistical conclusions and developing new services. Regarding the role of COSMOTE in the configuration of the copy server mentioned in the confidential Appendix A, the company states that OTE and COSMOTE operate on a case-by-case basis as independent or joint controllers, as it is possible that the personal data stored on the said server may concern systems of OTE or COSMOTE or even both companies, with the result that they jointly or independently define the purposes and means of data processing, as well as the applied security measures. The two companies, despite the request of the Authority during the hearing, did not provide any evidence from which the definition of roles and the distribution of responsibilities between them can be derived, such as an agreement based on Article 26 GDPR in case of joint control or controller and processor contract based on Article 28 GDPR. Given the functional integration of the two companies, common infrastructure, systems and human resources are used, while common policies, procedures and technical and organizational measures are applied. This fact, according to COSMOTE, does not automatically make the two companies jointly 17 Controllers of Processing, as the mere use of common systems does not always make the parties involved jointly Controllers of Processing (COSMOTE refers in this regard to the Guidelines 07/2020 of the GDPR for the concepts of controllers and processors). Finally, he points out that each company is responsible for taking appropriate measures to protect the personal data it processes. In this particular case, since the incident concerns the breach of COSMOTE subscriber data, it states that COSMOTE was responsible for taking the appropriate security measures, which immediately after the occurrence of the incident, took measures so that network access is no longer possible in its data. COSMOTE reports that apart from the fact that the infrastructure used by the attacker (hacker) to attack COSMOTE belongs to OTE, no other involvement of the organization in the incident is found. Accordingly, OTE maintains that its only involvement with the incident is that this infrastructure was the attacker's entry point, even though the company had taken appropriate measures. The infrastructure in question had been categorized as a system that does not host or process personal data, but adequate security measures were in place at the time of the incident, based on the policies outlined in the memo. OTE maintains that no access to its subscribers' or customers' data has been detected which would constitute a data breach and that improvements were immediately made to the configuration of the infrastructure. This system was interconnected with a central common (both companies) server, whose network configuration allowed access to COSMOTE data. The Authority, after examining all the elements of the file and after hearing the rapporteurs and assistant rapporteurs, who (assistants) withdrew after the discussion of the case and before the conference, after a thorough discussion, DECIDED ACCORDING TO THE LAW 18 1. According to

article 4 par. 1 of the GDPR, personal data is defined as any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one whose identity can be ascertained, directly or indirectly, in particular by reference to an identifier identity, such as name, ID number, location data, online identifier or one or more factors that characterize the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person. 2. Furthermore, according to article 4 par. 5 of the GDPR, pseudonymisation is defined as the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as said additional information is kept separate and subject to technical and organizational measures in order ensure that they cannot be attributed to an identified or identifiable natural person. It is pointed out that, according to recital 26 of the Regulation, personal data that has been pseudonymised, which could be attributed to a natural person by the use of supplementary information, should be considered information relating to an identifiable natural person. In the same recital it is stated that the principles of data protection should be applied to any information which concerns an identified or identifiable natural person, and also that in order to judge whether a natural person is identifiable, all means should be taken into account which are reasonably likely to be used, such as its separation, either by the controller or by a third party to directly or indirectly verify the identity of the natural person. In order to determine whether any means is reasonably likely to be used to verify the identity of the natural person, all objective factors, such as the cost and time required for identification, should be taken into account, taking into account the technology that is available at the time of 19 processing and technology developments. Data protection principles should therefore not apply to anonymous information, i.e. information that does not relate to an identified or identifiable natural person or to personal data that has been made anonymous in such a way that the identity of the data subject cannot or will not be can now be ascertained. 3. According to Article 5 of the GDPR, fundamental principles for the legal processing of personal data are, according to paragraph 1 thereof: a) the principle of transparency of processing ("the data is processed lawfully and legitimately in a transparent manner in relation to the data subject"), b) the principle of purpose limitation ("the data are collected for specified, explicit and lawful purposes and are not further processed in a manner incompatible with these purposes; the further processing for archiving purposes to the public interest or purposes of scientific or historical research or statistical purposes is not considered incompatible with the original purposes according to Article 89 paragraph 1), c) the principle of data minimization ("the data are appropriate, relevant and limited to what is necessary for the purposes for processed', d) the principle of accuracy ('the data are accurate and, when necessary, update tai· must all

reasonable steps are taken to promptly delete or correct of personal data which are inaccurate, in relation to the purposes of the processing), e) the principle of limitation of storage time ("the data are kept in a form that allows the identification of the data subjects only for the period necessary for the purposes of the processing of personal data; personal data may be stored for longer periods, as long as the personal data will only be processed for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, in accordance with article 89 paragraph 1 and as long as the appropriate technical and organizational measures required by this regulation are applied to ensure the 20 rights and freedoms of the data subject), f) the principle of confidentiality and integrity ("the data are processed in a way that guarantees the appropriate security of n personal data, including their protection from unauthorized or illegal processing and accidental loss, destruction or damage, by using appropriate technical or organizational measures". 4. Furthermore, according to article 5 paragraph 2 of the GDPR the controller bears the responsibility and must be able to prove his compliance with the processing principles established in paragraph 1 of the same article. In other words, with the GDPR a compliance model was adopted with the central pillar of this principle of accountability, according to which the data 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 be able to prove himself and at any time his compliance with the principles of article 5 par. 1 GDPR. 5. Any processing of personal data is lawful only if at least one of the conditions set out in Article 6, paragraph 1 of the GDPR applies, such as: "(...) b) the processing is necessary for the execution of a contract of which the subject of the data is a contracting party or to take measures at the request of the data subject prior to the conclusion of a contract, (…), f) the processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, unless against the interests these are overridden by the interest or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular if the data subject is a child". If one of the above conditions is met, then this constitutes the legal basis for the processing. Furthermore, in paragraph 4 of the same article it is stated: "When the processing for a purpose other than that for which the personal data have been collected is not based on the consent of the data subject or on the law of the Union or the law of a Member State which constitutes necessary and proportionate measure in a democratic society to ensure the purposes referred to in Article 23 paragraph 1, the controller, in order to ascertain whether the processing for another purpose is compatible with the purpose for which the personal data are initially collected , takes into account, among other things: a) any relationship between the purposes for which the personal data have been

collected and the purposes of the intended further processing, b) the context in which the personal data were collected, in particular with regard to the relationship between of the data subjects and the controller, c) the nature of the personal data character, in particular for the special categories of personal data processed, in accordance with Article 9, or whether personal data related to criminal convictions and offenses are processed, in accordance with Article 10, d) the possible consequences of intended further processing for the data subjects, e) the existence of appropriate guarantees, which may include encryption or pseudonymisation". 6. With reference to the principle of processing transparency, the GDPR imposes specific obligations on data controllers regarding the information they must provide to data subjects. In particular, according to article 12 par. 1 of the GDPR, the data controller takes the appropriate measures to provide the data subject with any information referred to in article 13 - which specifically mentions that "when personal data concerning a subject of the data are collected from the data subject, the data controller, when receiving the personal data, provides the data subject with all of the following information: a) the identity and contact details of the data controller and, where applicable, of his representative controller, b) the contact details of the data protection officer, as the case may be, c) the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing, d) if the processing is based on Article 6 paragraph 1 point f), the legal interests pursued by the data controller or from a third party, e) the recipients or categories of recipients of the personal data, if any (…)" (see par. 1 of article 13 of the GDPR). Furthermore, in paragraph 2 of the same article, it is stated that "in addition to the information referred to in paragraph 1, the controller, when receiving the personal data, provides the data subject with the following additional information that is necessary to ensure fair and transparent processing: a) the period for which the personal data will be stored or, when this is impossible, the criteria that determine the period in question, b) the existence of the right to submit a request to the data controller for access and correction or deletion of personal data or restriction of processing concerning the data subject or right to object to processing, as well as right to data portability, c) when the processing is based on article 6 paragraph 1 letter a) or article 9 paragraph 2 letter a), the existence of the right to withdraw his consent at any time, without prejudice the legality of the processing based on consent before its withdrawal, d) the right to submit a complaint to a supervisory authority, e) whether the provision of personal data is a legal or contractual obligation or a requirement for the conclusion of a contract, as well as whether the subject of the data is required to provide the personal data and what possible consequences the non-provision of such data would have, f) the existence of automated decision-making, including profiling, referred to in article 22 paragraphs 1 and 4 and, at least in the cases these, important information about the

logic followed, as well as the importance and intended consequences of said processing for the data subject". Furthermore, in paragraph 3 of the same article it is stated that "When the data controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the data controller provides the 23 data subject, before said further processing, information for this purpose and any other necessary information, as referred to in paragraph 2". 7. In accordance with Article 24 para. 1 of the GDPR, the controller, 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 the natural persons, implements appropriate technical and organizational measures in order to ensure and be able to demonstrate that the processing is carried out in accordance with the GDPR, while also these measures are reviewed and updated when deemed necessary. Furthermore, according to Article 32 of the GDPR, "taking into account the latest developments, the costs 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 liberties of natural persons, the controller and processor apply appropriate technical and organizational measures to ensure an appropriate level of security against risks, including, inter alia, where: (…) d) procedures for regular testing, assessment and evaluationthe effectiveness of the technical and organizational measures to ensure the security of the processing". Furthermore, in paragraph 2 thereof, it is stated that "when assessing the appropriate level of security, the risks deriving from the processing are taken into account, in particular from accidental or illegal destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed'. 8. According to Article 25 para. 1 of the GDPR, where the principle of data protection by design is described, "taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of different probability of occurrence and severity to the rights and 24 freedoms of natural persons from the processing, the controller effectively implements, both at the time of determining the means of processing and at the time of processing, appropriate technical and organizational measures, such as pseudonymisation, designed to implement data protection principles, such as data minimisation, and to incorporate the necessary safeguards into the processing in such a way as to meet the requirements of this Regulation and to protect the rights of data subjects ». The above applies to any processing of personal data. Furthermore, according to Article 35 of the GDPR, "when a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, may entail a high risk to the rights and freedoms of the natural persons, the controller shall, before processing, assess the impact of the planned

processing operations on the protection of personal data". 9. In article 2 par. 3 and 4 of Law 3471/2006, which incorporates Directive 2002/58/EC into the national legal order, the concepts of traffic data and location data are defined respectively. In particular: "(...) 3. "traffic data": the data processed for the purposes of transmitting a communication on an electronic communications network or charging for it. 4. "location data": the data processed in an electronic communications network or by an electronic communications service and indicating the geographic location of the terminal equipment of the user of a publicly available electronic communications service. 10. Articles 5 and 6 of the same law establish special conditions for the legality of processing personal data in the context of the provision and use of electronic communications services, which include mobile telephony services in accordance with article 2 paragraph 8 of the law. Specifically: According to article 5 of Law 3471/2006 ("Processing Rules"), "1. The processing of personal data, including movement and location data, must be limited to the measure absolutely necessary to serve its purposes. 2. The processing of personal data is permitted only if: ... b) the processing is necessary for the execution of a contract, to which the subscriber or user is a contracting party, or for taking measures during the pre-contractual stage, at the request of the subscriber. (…) 4. The design and selection of technical means and information systems, as well as the equipment for providing electronic communications services available to the public, must be done with the basic criterion of processing as little personal data as possible". Furthermore, according to article 6 of Law 3471/2006 ("Traffic and location data"), "1. Traffic data concerning subscribers and users, which are processed and stored by the provider of a public network or publicly available electronic communications service, are destroyed or rendered anonymous upon termination of the communication, subject to Law 3917/2011 (A`22), as well as paragraphs 2 to 6 of this article. 2. In order to charge subscribers and pay for connections, if necessary, the provider of a public network or publicly available electronic communications services is allowed to process traffic data. The provider of electronic communications services informs the subscriber about the type of traffic data being processed, as well as about the duration of the processing. This processing for the purpose of billing and payment is permitted for a period of time that cannot exceed twelve (12) months from the date of communication, unless the bill has been disputed or unpaid. In this case, processing is permitted until the dispute is irrevocably resolved. The transmission of traffic data to another provider of a public network or a publicly available electronic communications service is permitted for the purpose of charging for the services provided, provided that the subscriber or user is informed in a clear and appropriate manner, in writing or by electronic means, when drawing up 26 the contract or before transmission. Similarly, the transmission of the necessary traffic data and personal data relating to the

contract with the sole purpose of collecting the bill is permitted, provided that the subscriber or user is informed in a clear and convenient manner, in writing or by electronic means, during drawing up the contract or before the transfer....” 11. With reference to the security of processing, article 12 of Law 3471/2006 states that: "1. 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 electronic communications network. These measures, if necessary, are taken jointly 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. (…) 3. (…) with the measures of this article as a minimum: a) it is ensured that only authorized personnel can have access to personal data for legally approved purposes, b) the stored or transmitted personal data is 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. Relevant special provisions, as well as Regulations of Independent Authorities, are still valid. (…) 5. In the event of a breach of personal data, the provider of publicly available electronic communications services shall immediately notify the AP of the breach. D. E.G. and in A. D. S.A.. (…) 6. 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 or the affected party of this breach atom. (…)" 27 12. According to Recital 10 of Directive 2002/58/EC, in the field of electronic communications, Directive 95/46/EC applies in particular to all issues concerning the protection of fundamental rights and freedoms that are not expressly covered by the provisions of this Directive, including the obligations of the controller and individual rights. Furthermore, Article 95 of the GDPR states that the Regulation does not impose additional obligations in relation to the Directive in question. 13. The EDPS issued Opinion 5/2019 on the interaction between Directive 2002/58/EC on the protection of privacy in the field of electronic communications (hereinafter referred to as the "Directive") and the GDPR, in particular with regard to competence, duties and powers of data protection authorities. In fact, in par. 39 of the said Opinion it is mentioned that article 6 of the Directive, which concerns the processing of "traffic data", is an example of a case in which the provisions of the GDPR are "specialized". Usually, the processing of personal data can be justified on the basis of each of the legitimate grounds listed in Article 6 of the GDPR. However, the full range of possiblelegal reasons provided for in Article 6 of the GDPR cannot be applied by the electronic communications service provider to the processing of

traffic data, because Article 6 of the Directive expressly limits the cases in which it is possible to process traffic data, including personal data. In this case, the more specific provisions of the Directive on the protection of privacy in electronic communications must prevail over the more general provisions of the GDPR. However, Article 6 of the Directive does not limit the application of other provisions of the GDPR, such as the rights of the data subject. Also, the requirement that the processing of personal data must be lawful and legitimate (Article 5(1)(a) GDPR) is not negated. In paragraph 45 of the said Opinion it is stated that when there are special provisions governing a specific processing act or a set of processing acts, the special provisions (lex specialis) should be applied, while, in all the other 28 cases (i.e. when there are no special provisions governing a specific processing operation or a set of processing operations) the general rule (lex generalis) applies. Recital 173 of the GDPR confirms that, with regard to the processing of personal data to which the specific obligations of the Directive do not apply, the GDPR continues to apply: "in all matters concerning the protection of fundamental rights and freedoms against the processing of personal data nature and which are not subject to the specific obligations that have the same objective, as described in Directive 2002/58/EC of the European Parliament and of the Council, including the obligations of the controller and the rights of natural persons". This recital repeats what is already provided for in recital 10 of the Directive, which states that: "In the field of electronic communications, Directive 95/46/EC [already Regulation (EU) 2016/679] applies in particular to all issues concerning the protection of fundamental rights and freedoms not expressly covered by the provisions of this Directive, including the obligations of the controller and individual rights.' Opinion 5/2019 of the EDPS states as an example that a provider of a public communications network or a publicly available electronic communications service must comply with national rules transposing Article 6(2) of the Traffic Data Directive when processing data necessary for the purposes of billing subscribers and interconnection payments. Due to the absence of specific provisions for the protection of privacy in electronic communications regarding, for example, the right of access, the provisions of the GDPR apply. Similarly, recital 32 of the Directive confirms that when the provider of an electronic communications service or value-added service subcontracts to another body the processing of personal data necessary for the provision of these services, this subcontracting and the subsequent processing of the data should comply fully to the requirements regarding 29 controllers and processors, as already defined in the GDPR. 14. In this particular case, a file of personal data kept by COSMOTE was leaked to unknown third parties in 2020, due to a successful security attack carried out. Consequently, an incident of personal data breach arises, which concerns subscribers of the company, but also subscriber details of other telecommunication providers for those who,

during the disputed period, had electronic communication with COSMOTE subscribers, and falls under the notification obligation of article 12 par. 5 of Law 3471/2006, as the company did. Furthermore, as COSMOTE considered that the breach may have adverse effects on the personal data or privacy of subscribers or other individuals, it proceeded to inform the affected subscribers and individuals, as required by paragraph 6 of the same article. 15. Before considering processing security issues, it is necessary to assess the legality of the processing activities served by the leaked file originating from the "Big Streamer" bulk data system. The primary processing purpose is to use location and movement data for fault management purposes. According to COSMOTE, the "execution of a contract" according to article 5 par. 2b of Law 3471/2006 in combination with 6 par. 1b of the GDPR is mentioned as the legal basis for this processing. The documentation presented by the company lies in the fact that, from the existing institutional framework (which is extensively analyzed in its memos), COSMOTE has an obligation when providing its services to have specific quality characteristics and effective fault management procedures. Therefore, fault management is a function that can reasonably be expected by its subscribers to be an integral part of the service provided, while the relevance of the relationship between the fault management process and the provision of telecommunications services is such that the process in question cannot be offered to its subscribers as a value-added service. Regarding the fact that article 6 of Law 3471/2006 places restrictions on the processing of 30 location and movement data, COSMOTE argues that paragraphs 2 and 3 of article 6 of this law should be interpreted in the light of the more general interpretations rules of article 5 par. 2 of the same law and that the provisions of article 6 specifically regulate these cases of traffic and location data processing (i.e. processing for the purpose of billing and payment of interconnections, as well as processing for the provision of additional services value) and do not repeal the provision of article 5 par. 2, which, in the event of a contrary interpretation, according to COSMOTE has no reason to exist. The processing of personal data in the field of electronic communications is regulated by Law 3471/2006, which must be interpreted in the light of Directive 2002/58/EC which it incorporated into Greek law, as explained through its explanatory notes and interpreted by the decisions of the CJEU. The purpose of damage management is closely linked to the contractual relationship between provider and subscriber and its pricing, as follows from recital no. 29 of the Directive, according to which "The service provider may process traffic data concerning subscribers and users when required in individual cases in order to detect technical faults or errors in the transmission of communications. [...]". However, as expressly stated in recital No. 30 "[t]he systems for the provision of electronic communication networks and services should be designed in such a way as to limit the amount of personal data

required to the minimum possible", in accordance also and with the principle of data minimization (art. 5 par. 1 letter c) GDPR). Furthermore, the CJEU has judged9 that the principle of confidentiality of communications enshrined in Directive 2002/58/EC includes, among other things, as follows from its article 5, paragraph 1, second subparagraph, the prohibition, in principle, of the storage of related to electronic communications of traffic data from persons other than users, without the 9 See judgment in joint cases C 203/15 and C 698/15 - Tele2 Sverige AB v Watson, paragraphs 82-87. 31 consent of the users concerned. Excluded are only legally authorized persons, in accordance with Article 15, paragraph 1, of this directive, and technical storage which is necessary for the transmission of communication. Therefore, and as confirmed by recitals 22 and 26 of the Directive, the processing and storage of traffic data is permitted under Article 6 of this Directive only to the extent and for the required duration for the pricing of the services, their commercial promotion or the provision of value-added services (Decision C-203/15 and C-698/15 - Tele2 Sverige AB/Watson, §85-86), but also for the purposes of identifying technical faults or errors in individual cases only, as it follows from recital 29, as mentioned above. Consequently, this is how article 610 of the Directive must be interpreted, as well as article 6 of Greek Law 3471/2006. It should also be noted that the obligations for quality in the provision of services to subscribers which are determined by the relevant EETT regulations and codes code of conduct do not impose nor do they state that universal observance is required in advance for a specific period of time of all location and movement data without exception for the purposes of fault management. The goal of quality service provision does not presuppose 10 In particular, in article 6 of the Directive the following are mentioned: "1. Traffic data relating to subscribers and users, which is processed and stored by the provider of a public network or publicly available electronic communications service, must be deleted or made anonymous when it is no longer necessary for the purpose of transmitting a communication, with without prejudice to paragraphs 2, 3 and 5 of this article and article 15 paragraph 1". 2. Traffic data necessary for billing subscribers and payment for connections may be processed. Such processing is permitted only until the end of the time period within which the account may be legally disputed or payment sought. 3. For the commercial promotion of electronic communications services or for the provision of value-added services, the provider of publicly available electronic communications services may process the data referred to in paragraph 1 to the required extent and for the required duration for this service or commercial promotion, provided that the subscriber or user to whom they concern gives their prior consent. Users or subscribers must be given the possibility to withdraw their consent to the processing of traffic data at any time. 4. The service provider must inform the subscriber or user about the type of traffic data processed and the duration of such

processing for the purposes referred to in paragraph 2 and, before consent is granted, about the purposes referred to in paragraph 3". 32 such extensive processing. Taking into account the above, for the purpose of fault management it would only be permissible to keep a limited subset of traffic data, in individual cases, to the extent and for the time required to identify specific technical faults or specific errors, while there is no legal basis in which could support the observance of all the movement data for three months, as in the case under consideration. Moreover, the processing in question began, as COSMOTE reports, in 2015 - a fact which suggests that for all the previous years of the company's operation, during which the same legal framework was also in force that obliges the company to provide services with specific quality characteristics , the intended purposes - including damage management - could be achieved without said processing. 16. In this regard, COSMOTE prepared an impact assessment for the processing in question regarding the protection of personal data (hereafter, DPA). Although the impact assessment in question was based on an ICO11 methodology which consists in answering specific questions, from which answers it is demonstrated, among other things, the necessity of the processing in relation to the resulting risks, it does not appear that this methodology was applied against the right way since the answers provided by COSMOTE, as controller, are not documented and, therefore, do not demonstrate that all risks have been considered (indicative example: in a question "Is it possible to achieve the purpose without the specific processing?" ” the answer is given “No, it is not possible to serve the subscriber's fault management requests without the processing of the specific personal data”). According to article 35 paragraph 7 of the GDPR, the GDPR must contain at least specific elements, including an assessment of the necessity and proportionality of the processing operations in relation to the purposes. Therefore, the GDPR prefers the detailed examination of the processing operations during the preparation of the GDPR. Each 11 UK Information Commissioner – The UK Data Protection Supervisory Authority 33 judgment contained therein must be substantiated and each response properly reasoned. Consequently, there is a violation of article 35 paragraph 7 of the GDPR, as the content of the GDPR is not sufficient, especially in terms of assessing the necessity and proportionality of the processing. 17. Regarding the transparency obligations in relation to damage management, although there was information to the subscribers about the processing in question, the information in question cannot be characterized as accurate and complete because the information is not clear as to the purpose of the processing in relation to the retention time (in this case 90 days), regardless of the fact that, according to what is stated in the previous paragraph, it was not legal to retain all the data for three months. In the information text, for the traffic data the purpose is indirectly mentioned as "service of the contract", without making it clear that

for damage management reasons the data is kept for three months, while for the location data the same purpose is more specifically mentioned as "solving problems in the network and service improvement". In fact, COSMOTE keeps data of both its subscribers and subscribers of third-party providers, which in terms of data related to calls are collected directly from these persons when using its telephony services, so article 13 of the GDPR is applicable, while regarding the location data, it is collected by the provider itself, so Article 14 of the GDPR is applicable. Consequently, there is a violation of the principle of transparency (no. 5 par. 1 a) GDPR) and articles 13 and 14 of the GDPR due to unclear and incomplete information. 18. The second processing purpose is the processing of both the traffic and location data file as well as the other personal data of the subscribers (enriched file) in order to draw statistical conclusions for network development purposes. As can be seen from the case file, this file serves a purpose which can, in principle, be achieved by using anonymized data. In addition, COSMOTE advocates this, which states that it performs anonymization, for this purpose, as it is foreseen to be done after the end of the communication based on article 6 par. 1 of Law 3471/2006. However, in relation to COSMOTE's process for anonymization, the following emerges: At the time of the incident and earlier, the file was kept, in non-anonymized form for a period of three months, after which the anonymization process followed. During the quarter, enriched data was not in anonymized (nor pseudonymized) form. After all, this is the file that the leak is about. Therefore, apart from the fact that there is no legal basis for the creation and maintenance for the purpose of drawing statistical conclusions of the original, non-enriched ("simple") personal data file as described above, there is no legal basis for the creation and maintenance either of the enriched, non-anonymized file since, for the purposes of the enriched file, it should be in an anonymized form. The GDPR actually provides, in article 5 par. 1 item. b' of the GDPR regarding the principle of purpose limitation, that further processing for statistical purposes is not considered incompatible with the original purposes, but refers in relation to what is defined in article 89 paragraph 1, where there is an explicit reference to the fact that " the processing (…) for statistical purposes is subject to appropriate guarantees, (…), regarding the rights and freedoms of the data subject (…). These guarantees ensure that the technical and organizational measures are in place, in particular to ensure compliance with the principle of data minimization. Such measures may include the use of pseudonyms, as long as such purposes can be fulfilled in this way. To the extent that said purposes can be fulfilled by further processing which does not allow or no longer allows the identification of data subjects, said purposes are fulfilled in this way.' The reference to a compatible purpose does not establish a legal basis for the processing of traffic data, which could only be based on article 6 of Law 3471/2006, as developed in previous considerations.

Besides, COSMOTE, recognizing that it is not necessary to keep the enriched file in a non-anonymized form, has modified its procedures from January 2021 so that this (new type) enriched 35 file no longer contains, at any time, the direct identification data of each subscriber (MSSDN, IMSI, IMEI). However, even after thethis modification, the processing is carried out by combining the traffic data of each subscriber with their commercial information (subscriber tariff plan, age, gender, ARPU), so even if it is considered that anonymization is actually carried out, the anonymization is preceded by a data correlation process, which constitutes processing without a legal basis, which takes place in violation of articles 5 and 6 of Law 3471/2006. 19. From the analysis of the procedure for the anonymization of the data, both that which was in force during the period in question, but also the improved one - according to the above - which was applied afterwards, it follows that the data which are ultimately used for the second purpose are pseudonymized and not anonymized. According to this method, a cryptographic hash function is applied to the identifying information of each subscriber using a secret key ("salt"), which is kept separately and protected. The "salt" changes every three months. COSMOTE holds the secret key and also knows the IDs of its subscribers, so it can at any time, for the period of the quarter in which the salt has not been destroyed, match each hash value (appearing in the - supposedly anonymized - file) with the corresponding subscriber ID. In the new method that COSMOTE has been implementing since January 2021, the company is able to properly merge two files that it qualifies as anonymized, due to the fact that each of its subscribers corresponds to a unique hash value in the two files. But COSMOTE itself in its documents, regarding the documentation of the effectiveness of the process, refers to "limitation of the risk of re-identification of anonymized data", which also indicates that it is pseudonymization and not anonymization. Consequently, the processing in question constitutes pseudonymisation, within the meaning of article 4 para. 5 of the GDPR, where the additional information that allows identification and needs protection 36 consists of the secret key ("salt"), which indeed, based on COSMOTE's description, is kept separately and is subject to technical and organizational security measures. So, the data in question is personal data and not anonymous, so for the said enriched file GDPR12 applies, according to the provisions of which this way of processing does not lead to legal processing, since the data remains personal and not anonymous. Therefore, it follows that the applied anonymization process of the "enriched" file, both before January 2021 (after the quarter) and after, does not ensure the anonymity of the data kept, but only the keeping of personal data in a pseudonymized form. This constitutes a violation of Article 25 para. 1 of the GDPR by COSMOTE as appropriate technical and organizational measures were not implemented at the time of the determination of the means of processing and at the time of processing, to

ensure the proper implementation of an anonymization process. 20. Furthermore, there was no information to the data subjects about this processing (i.e. keeping the enriched file, in non-anonymized/pseudonymized form). In the text of the update there is a reference to the retention of data for three months in order to improve the service, without this update implying the retention of all categories of traffic data (including location data) included in the file nor their combination with other personal data (such as gender, age, subscriber plan, ARPU) for the purpose of extracting statistics and optimizing the network. It is pointed out that, even if it is considered that the purpose of the statistical processing of the above data for the optimization of the network is 12 It is also noted that even if the secret key (salt) were deleted directly, in which case it would not be permissible to recover the original identifiers of users from the new, irreversible, identifier, it does not automatically follow that the data in question is anonymized. Taking into account the amount of information for each entry of this file, Cosmote as controller should investigate whether it is indeed not possible to identify a user taking into account all reasonable means available to someone who will have access to the due to record, Such an analysis/valuation does not appear to have been done. 37 compatible purpose of further processing, for which a separate legal basis is not required from that which allowed the initial collection of the data, in any case the obligation to inform the subjects according to articles 13 par. 3 and 14 par. 4 of the GDPR must be respected, where it is stipulated that the controller must provide the data subject, before further processing, with information about the new purpose and other necessary information. In this case, the information provided is not complete. Specifically, in the text of the provider's General Information on the Processing of Personal Data, the following is mentioned: "(...) Otherwise, your data will be deleted in a way that it is not technically possible to recover it or it will be anonymized. Anonymization is the application of practices to personal information that renders it invalid, so that it is no longer possible to identify your identity from this information. The use of anonymous data is extremely important for us, because it helps us to draw useful conclusions regarding the use of our services and, at the same time, it is a useful tool in the design of service websites". In addition to COSMOTE referring to anonymization, which, as mentioned above, is not accurate, it appears from the text that this anonymization (as characterized by COSMOTE) only takes place when the subscriber's contract with COSMOTE is terminated in any way – while , after all, it applies to all active subscribers, those who use the roaming network and those who receive calls from subscribers. Therefore, from the above, there is a violation of the principle of transparency (no. 5 par. 1 subsection a' GDPR) and articles 13 and 14 of the GDPR due to unclear and incomplete information. 21. From the examination of the elements of the file, vulnerabilities arise in relation to the security measures, which were exploited

directly or indirectly by the attacker during the incident. These vulnerabilities are developed in detail in the confidential annex C of the decision. A total of six vulnerabilities are identified, the first of which concerns a system that is not related to the processing activities in question – however, due in particular to incorrect settings in the inner network connections, this 38 first vulnerability was the springboard for the attacker. In the other vulnerabilities, it is established that COSMOTE is the controller in relation to the two intended purposes of the file that was the subject of the incident. Regarding security measures, it is noted that COSMOTE's responsibility is not exclusive. The security measures are taken, in practice, jointly with OTE. This results from the analysis of the vulnerabilities of the policies and related arrangements that led to the breach of security in relation to the processing in question. The determination of security measures rests with OTE, to a large extent, in relation to vulnerabilities numbered 2 (to a large extent), 3 (to a large extent), 4 (to a large extent as it relates to OTE personnel) and to a lesser extent (but not negligible) in vulnerabilities 5 and 6 which are more related to COSMOTE's processing activities. As regards the taking of security measures, as their determination essentially belongs to both COSMOTE and OTE, with a degree of responsibility as described above, there is a violation of article 12 par. 1 of Law 3471/2006, as far as COSMOTE is concerned, while for OTE there is a violation of article 32 par. 1 of the GDPR. 22. The two companies maintain that they act together in terms of the systems, but independently of each other. This model of operation, in which the cooperation of the companies is unrecorded, at least in relation to security measures, is not in accordance with the principle of accountability of article 5 par. 2 of the GDPR. And this is because it does not appear which of the cooperating entities is responsible for the selection of the essential means of processing, and therefore it is not possible to prove the compliance of the entities in relation to the observance of the principle of integrity and confidentiality provided for in the article 5 par. 1 sec. f of the GDPR. The cooperation of the two bodies and the distribution of their responsibilities13 should be based either on 13 See and App. Sec. 79 GDPR: "The protection of the rights and freedoms of the subjects ofdata, as well as the responsibility and obligation to indemnify controllers and processors, including in relation to monitoring by supervisory authorities and measures of supervisory authorities, requires a clear division of responsibilities under this Regulation, including the case when which a responsible s 39 agreement14 based on Article 26 of the GDPR in the case of joint responsibility or in a contract or other legal act based on Article 28 in the case of delegation of processing. As it emerged during the hearing of the two companies, such agreements do not exist. 23. COSMOTE immediately notified the said incident of violation to the Authority, in accordance with the provisions of article 12 of Law 3471/2006, while it also proceeded, in a reasonable time, after the initial investigation and

handling of the incident, to inform the its subscribers and other persons, as described in the history of the present. COSMOTE, together with OTE where necessary, took corrective measures for the security of the processing, in order to adequately address, at the discretion of the Authority and for this time, the vulnerabilities mentioned earlier. However, it is pointed out that the two companies must have and continuously implement a procedure for the regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure the security of the processing. 24. Based on the above, the Authority considers that there is a case to exercise the powers according to Article 13 par. 1 and 4 of Law 3471/2006, in conjunction with Article 21 of Law 2472/1997 and Article 84 of Law 4624/2019, powers for the established violations of Law 3471/2006, as well as its corrective powers according to article 58 par. 2 of the GDPR in relation to the established violations of the GDPR. To determine the penalties, the Authority takes into account the criteria for measuring the fine defined in article 83 par. 2, 4 item. a' and 5 of processing determines the purposes and means of processing together with other controllers or when a processing operation is carried out on behalf of a controller". 14 "...for the sake of legal certainty, even if there is no legal requirement in the GDPR for a contract or other legal act, the EDPB recommends that such arrangement be made in the form of a binding document such as a contract or other legal binding act under EU or Member State law to which the controllers are subject. This would provide certainty and could be used to demonstrate transparency and accountability. in case of non-compliance with the agreed allocation provided in the arrangement, its binding nature allows one controller to seek the liability of the other for what was stated in the agreement as falling under its responsibility. Also, in line with the accountability principle, the use of a contract or other legal act will allow joint controllers to demonstrate that they comply with the obligations imposed upon them by the GDPR" (Guidelines 7/2020 of the GDPR, § 173). Indeed, 40 pcs. a' and b' of the GDPR applicable to this case and the guidelines for the application and determination of administrative fines for the purposes of the GDPR, as well as the factual data of the case under consideration, and in particular the specific measurement criteria referred to in the previous consideration of each violation and the following measurement criteria concerning the whole of the activities, to the extent that they affect COSMOTE or OTE respectively: a) The nature of the violation concerning a GDPR right. b) That it is not personal data under articles 9 and 10 of the GDPR, but data subject to special confidentiality. c) That administrative sanctions have been imposed by the Authority on OTE in the past (see Decisions 1/2015, 31/2019, 34/2019). d) That the two companies fully cooperated with the Authority and that COSMOTE reported the incident. e) That the two companies took measures to contain and deal with the incident. f) From the data available on the internet which the group

has posted15, it appears that the turnover of the group amounted to 3.258 billion euros. Specifically, the Authority: A. Finds for COSMOTE: a) Violation of articles 5 and 6 of Law 3471/2006, as described in detail in paragraph number 15 hereof. For the sanction imposed, it is particularly taken into account that the said processing was intended to serve the subscribers, was done without malice and that the relevant institutional framework is difficult to interpret. It is pointed out that the purpose of processing damage management may be pursued in the future, as long as the conditions described in point number 15 are met. 41 b) Violation of article 35 paragraph 7 of the GDPR, as analyzed in paragraph 16 hereof. For the sanction imposed, it is also taken into account that the violation in question may result in a fine of up to 2% of the total global annual turnover of the previous financial year, in accordance with article 83 par. 4 GDPR. c) Violation of the principle of transparency (article 5 par. 1 a) GDPR) and articles 13 and 14 of the GDPR in relation to damage management, as analyzed in paragraph 17 hereof. For the sanction imposed, it is also taken into account that the violation in question may result in a fine of up to 4% of the total global annual turnover of the previous financial year and that there was information but it was incomplete. For the above infringements under items a', b' and c', the very long duration of the infringement (6 years) as well as the number of affected subscribers, users or natural persons, which in total, together with the subscribers or users, are also taken into account of other providers numbers many millions of persons (over 10,000,000 numbers). d) Violation of articles 5 and 6 of Law 3471/2006 on the legality of the processing of the extraction of statistical conclusions for the purposes of network development, as described in detail in point number 18 hereof. e) Violation of the principle of transparency (article 5 par. 1 a) GDPR) and articles 13 and 14 of the GDPR in relation to the enriched file, as analyzed in paragraph 20 hereof. For the sanction imposed, it is also taken into account that the violation in question may result in a fine of up to 4% of the total global annual turnover of the previous financial year. f) Violation of article 25 paragraph 1 of the GDPR in relation to the correct application of the anonymization process, as analyzed in paragraph 19 hereof. For the sanction imposed, it is also taken into account that the violation in question may result in a fine of up to 2% of the total global annual turnover of the previous financial year and that if it had been applied correctly and in time the 42 anonymization procedure would had limited the consequences of the incident. For the violations under points d', e' and f' above, the very long duration of the violation (6 years) is also taken into account, the number of affected subscribers, users or natural persons, which in total, together with the subscribers or users of other providers numbers many millions of persons (over 10,000,000 numbers) and that for a long time there was no pseudonym protection measure in the initial quarter after the calls. g) Violation of article 12 par. 1 of Law 3471/2006, as

described in detail in point number 21 of this. For the sanction imposed, it is also taken into account that the incident is attributed to negligence, it affected a very large number of subscribers, users of the provider and subscribers of other providers, the number of vulnerabilities and the degree to which they are attributed to COSMOTE, as described in the relevant annex of the decision, and that the security measures proved to be deficient for a long time. h) Violation of article 5 paragraph 2 in combination with articles 26 and 28 of the GDPR, as analyzed in paragraph 22 hereof. For the sanction imposed, it is also taken into account that the violation in question may result in a fine of up to 4% of the total global annual turnover of the previous financial year, that this violation has a long duration, as already from the beginning of application of the GDPR, the companies appeared under a single trade name and that it concerns all the natural persons who are subscribers of the 2 companies, but also that the violation is due to negligence due to the special relationship of the companies. B. Finds for OTE: Violation of article 32 of the GDPR and the incomplete adoption of security measures, as described in detail in paragraph number 21 of this.

imposed sanction is also taken into account that the infringement in question

may result in a fine of up to 2%

of total global annual turnover of the previous financial year

year, that the incident is attributed to negligence, affected a very large number

natural persons, the number of vulnerabilities and the degree to which they

attributed to OTE, as described in its relevant annex

decision, as well as that the security measures proved to be insufficient for

long time.

The Authority considers that, based on the circumstances established, the sanctions

fine mentioned in the operative part of the decision is the effective one,

proportionate and dissuasive measure both to restore compliance, as

and for the punishment of unlawful conduct.

The beginning:

FOR THOSE REASONS

 It imposes on COSMOTE MOBILE TELECOMMUNICATIONS S.A.

Sanction of cessation of processing and destruction of data, based on Art

21 paragraph e' of Law 2472/1997, for the violation described in paragraph 24,

point A. a).

Based on article 58 par. 2 sub. i of the GDPR, total fine

5,850,000 euros, which is distributed as follows:

 Sanction of a fine of 1,300,000 euros for the violation described

in paragraph 24, point A. b).

 Sanction of a fine of 650,000 euros for the violation described

in paragraph 24, point A. c).

 Sanction of a fine of 1,300,000 euros for the violation described

in paragraph 24, point A. e).

 Sanction of a fine of 1,300,000 euros for the violation described

in paragraph 24, point A. f).

 Sanction of a fine of 1,300,000 euros for the violation described

in paragraph 24, point A.h).

Based on article 21 par. e' of Law 2472/1997, the suspension sanction

processing and destruction of data, for the offense described

in paragraph 24, point A. d) and in paragraph 24, point A. g).

Based on article 21 paragraph b of Law 2472/1997, a total fine

150,000 euros for the violations described in paragraph 24, points A. d),

and A. g).

 It imposes a sanction on the Hellenic Telecommunications Organization SA

a fine of (3,250,000) euros based on article 58 par. 2 sec. his i

GDPR, for the breach of the GDPR which is described in point B of

paragraph 24 hereof.

The president

Konstantinos Menudakos

The Secretary

Irini Papageorgopoulou