Athens, 26-10-2022 Prot. No.: 2713 DECISION 57/2022 (Department) The Personal Data Protection Authority met, at the invitation of its President, in a regular meeting in the composition of the Department at its headquarters on 28/07/ 2022, in order to examine the case referred to in the history of the present. The meeting was attended by teleconference by Georgios Batzalexis, Deputy President, in the absence of the President of the Authority, Konstantinos Menoudakos, and attended by Konstantinos Lambrinoudakis, regular member, as rapporteur, Demosthenes Vougioukas, alternate member, and Maria Psalla, alternate member in place of regular member Grigorio Tsolias, who did not attend due to disability although he was legally summoned in writing. Haris Symeonidou and Georgia Panagopoulou, special scientists - auditors, as assistant rapporteurs and Irini Papageorgopoulou, employee of the Authority's administrative affairs department, as secretary, attended the meeting, by order of the President without the right to vote. The Authority took into account the following: With the no. prot. C/EIS/4872/21-07-2022 her complaint, A complains about illegal and non-transparent collection of personal data (face photo) by the company Cosmote. In particular, according to the above related complaint, during the complainant's communication with the complained-about company, for the purpose of concluding a contract, she was suggested to choose the electronic address for registering her information via 1-3 Kifisias Ave., 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr https://onboarding.cosmote.gr/ so that the certification process as a new customer is easier and shorter. According to the complainant, she was asked to take a photo of her face on the spot, so that her photo could be registered, without having previously been given the opportunity to be informed about the relevant processing. The complainant states that she refused to proceed with the relevant procedure and asked to send a photocopy of her identity card, while she then referred to the text "UPDATE REGARDING THE PROCESSING OF YOUR PERSONAL DATA THROUGH THE WEBSITE (https://onboarding.cosmote.gr)", which it attaches to its complaint, which however does not mention the face photo in the types of data that Cosmote collects and processes, nor the purpose of the relevant processing. Attached to the complaint is a screenshot of a mobile device screen (screenshot) from the address in question, which shows the following instructions to the user for taking a photo of himself: "(...) place your face in the center of the mobile screen at a distance of 25 -30 cm without glasses, hold the camera steady and take a photo (selfie)". The Authority, in the context of examining the above complaint, with no. prot. C/EXE/2190/01-10-2021 its document, invited the complained company to present its views on the complained within 15 days. In its response, Cosmote was asked to clarify in particular: a) whether it has collected facial image data of its customers with the above-described procedure, through the address (https://onboarding.cosmote.gr/) and how many subjects

this concerns processing, b) what is the purpose and legal basis of the above-described processing of personal data and how are the subjects informed about the specific processing, in accordance with Article 13 GDPR, c) if facial recognition techniques are used, describe the techniques them and any processors. With the no. prot. C/EIS/7613/19-11-2021 her response document, the complainant replied to the Authority that indeed, during the communication of the complainant with OTE for the purpose of concluding a contract, she was offered the option of identification and sending the necessary supporting documents documents through the https://onboarding.cosmote.gr platform and through the following process ("digital on-boarding"): a) sending via sms a unique PIN number for the prospective subscriber's access to digital onboarding, b) opening the hyperlink of https://onboarding.cosmote.gr by entering the PIN by the prospective customer, c) display of text regarding the choice of the prospective subscriber to consent to the taking of his photo (selfie) and the sending of the necessary documents for the purpose of verifying and verifying his identity, d) if he declares his consent, taking a photo, e) sending supporting documents, f) reading, saving and digitally signing the application, g) verifying identity and supporting documents. With reference to the use of the photo of the prospective subscriber for the purpose of his identification, the complainant notes that a separate screen is inserted (attached as ADDENDUM 1) with which the user is informed of the purpose of processing the above data, which is verification and verification of the identity and his consent is requested with a non-default check-box. According to the complainant, the informative text accompanying the choice of consent ("consent text") gives the prospective subscriber the necessary information in a concise manner. It is noted that, according to the image provided, next to the check-box the following is stated: "The photo will be used to verify and verify the identity. More information here. I have been informed and I consent to the use of my biometric data, related to the image of my face, for the purpose of ascertaining and verifying my identity." According to the complainant, at this point the prospective subscriber is directed to a more detailed text regarding the use of data resulting from the taking of the photo in real time (which is attached as ADDENDUM 2). In this text, in which both Cosmote and OTE appear as controllers, it is stated that "if you do not consent to the processing of your biometric data in accordance with this paragraph it will not be possible to complete our transaction electronically and you should contact in another channel of the OTE Group (e.g. store) by presenting the appropriate supporting documents", as well as that "If you change your mind before the completion of your application, we can stop the whole process and show you the alternatives ways to complete your request". During this response, OTE keeps in its file as proof of identification only the result of the processing and not the photo or video itself, from which the identification was derived. According to the complainant, in order

for the user to press the "Continue" button and proceed to the next steps, which are taking a photo (selfie) and sending the identification documents, it is necessary to obtain consent and select the relevant check-box . In this case, upon the complainant's response, complainant A gave her consent in accordance with the above, the proof of which is attached (as ATTACHMENT 3), however she chose along the way to discontinue the procedure. With reference to the Authority's specific questions, OTE replied that it has identified a total of 1,532 subscribers through the aforementioned digital onboarding process. The purpose of the above-described processing is the electronic identification of prospective subscribers, the legal basis is the consent of the subjects, while the data subjects are informed through the summary text of the consent in the relevant check-box (SYN.1), as well as in more detail through the text which is available at the hyperlink (LINK 2). These texts are more specific updates regarding the processing of biometric data of prospective subscribers for the purpose of their consent and ultimately their secure remote identification. For the electronic identification process, biometric data is used, resulting from taking a photo in real time (real time selfie) and facial features in order to confirm the authenticity of the photo and identify the natural person. The use of the photo in real time provides the possibility of verifying if the person requesting a transaction is indeed the same as the person appearing on the presented identification document (ID card or passport, etc.) providing security to its transactions. In particular, according to the company, the following procedure is followed for electronic identification: Taking a Snapshot of the Face of the user being identified (selfie) Taking an identification document Confirmation of identification of the Snapshot of the User's Face (selfie) with the person depicted in the identification document Verification that the identification document belongs in the accepted and valid identification documents Authenticity check using technologies such as image processing, visual characteristics detection, document type image matching, ID verification. The process in question is described in a relevant presentation, which is attached by the complainant (SYN.4) and, as it states, was implemented on behalf of the companies OTE and COSMOTE by the company IntelliSolutions Information Services S.A, which is based in Kallithea and is the Processor on behalf of the two companies. Finally, the complainant states that in the (general) informative text regarding the processing of personal website https://onboarding.cosmote.gr (privacy notice) and which A attached to her complaint, was added (after the notification of the complaint to the company) the more specific information regarding the process of obtaining consent for the processing of biometric data (which is attached as ATTACHMENT 5). data use according to Subsequently, the Authority with no. prot. C/EXE/809/30-03-2022 and C/EXE/810/30-3-2022 summons invited the involved parties to a hearing before the Department of the Authority via video

conference on 6/4/2022, in order to present their views on the case. Because the complainant initially did not present any contract between Cosmote or OTE and the aforementioned company IntelliSolutions Information Services S.A., which it characterizes as performing the processing, with the no. prot. C/EXE/809/30-03-2022 Summons, the summoned company was requested to provide before the hearing the documents necessary to document the legality based on the principle of accountability (contract according to article 28 par. 3 GDPR , GDPR according to article 35 GDPR, activity record according to article 30 GDPR etc.). During the meeting of 6/4/2022 the complainant requested the postponement of the debate, a request that was accepted and the debate was postponed to 11/5/2022, with the obligation to provide the above requested documents by 12/4/2022. With her document C/EIS/6066/15-04-2022, the complainant sent the following documents to the Authority: 1) Excerpt of the activity file (SYN.1) 2) Impact Assessment Study, which consists of the following files: a. System categorization questionnaire in terms of security and data protection (SYN.2). b. Questionnaire for initial assessment of data protection issues (Initial Consultation Guide), which is answered during the planning phase of changes in information systems (SYN.3). c. Documentation of security and data protection of the system (SYN.4). d. Compliance (Statement of Compliance) of the System (SYN.5) with data protection and security requirements and measures. 3) Personal data processing delegation agreement with the Processor (SYN. 7) During the meeting on 11/5/2022, the complainant A and on behalf of the complained company, B, Customer onboarding digital Transformation Manager, Eleni attended the meeting on 11/5/2022 Gerutsi, attorney-at-law (…) and C, Data Protection Officer of the OTE Group. During the hearing, the parties developed their views, received a deadline and filed within the deadline, while the OTE SA company no. prot. G/EIS/7733/06-06-2022 memorandum, while the complainant no. prot. G/EIS/7749/06-06-2022 memorandum. The complainant, both during the hearing and with her memorandum, argued that she did not receive sufficient and detailed information before proceeding to the stage of photographing her face, at which point she stopped the process, as well as that if she had indeed proceeded to photograph her face having read "misleadingly", as she states, the incomplete terms of personal data management of the accused, she would have filed a lawsuit, because, as she claims, she did not receive transparent and clear information about the collection and processing of her personal data in a complete text and not "in fragments in various hyperlinks that complement each other as was done in this case." In addition, the complainant stated that although the complainant stated that it only retains the result of the identification of the person dealing, it is not clearly stated anywhere that the third partner company IntelliSolutions does not store / manage / share or sell the result of the processing that includes identification of the characteristics of the person facial

data that are unique to each person such as fingerprints, i.e. the biometric data of subscribers. The complainant, both during the hearing and in her memorandum, stated firstly that the company OTE SA is responsible for the processing complained of, because the complaint concerns a request for landline portability through the digital onboarding process and for this reason the company OTE SA (hereinafter "company") provided the under no. prot. C/EIS/7613/19-11-2021 and C/EIS/6066/15- 04-2022 her opinions and submitted C/EIS/7733/06-06-2022 memorandum. According to what the company reports, in an effort to modernize and improve its services, it decided to launch in June 2020 the possibility of "Digital onboarding", which concerns the remote electronic identification of its prospective subscribers in a modern and secure way and using artificial technology Artificial Intelligence (AI) and biometric data analysis, which is currently available on fixed telephony and only to serve portability requests. As the representatives of the company stated, this is a digital process that aims to satisfy a subscriber's request to transfer his connection to OTE, following a telephone call, as soon as possible. In particular, before the said procedure was adopted, after the telephone request for landline portability, a folder with supporting documents (identification document and signed contract) had to be sent by courier to the company, while in this way the documents are submitted entirely electronically, so that don't waste time. The use of biometric methods is used to automatically compare the applicant's real-time photo (selfie) with the photo of the identification document through personal data, and only the result of the comparison is kept, not the photo of the applicant. The company claims that during the planning of the possibility of identification through digital onboarding, it recognized the need to prepare an Impact Assessment Study regarding the protection of personal data according to article 35 par. 1 GDPR, which it submitted with G/EIS/6066/15 -04-2022 document, while for the purpose of informing the subjects a detailed information text regarding the processing of the https://onboarding.cosmote.gr platform was posted, as well as an information and consent text regarding the use of biometric data, which were attached in C/EIS/7613/19-11-2021 its opinion document. The company describes the process of electronic identification, sending supporting documents and signing the necessary documents in the context of serving a portability request through digital onboarding, which includes sending a PIN code via sms which the subscriber fills in on the onboarding.cosmote.gr page where a hyperlink appears (link) entitled "Data Protection" which leads to the informative text on the processing of personal data through the platform in question. Then, after filling in the code, the message "Welcome to Digital Document Management" appears on the screen, and the following is mentioned: "To complete your request, you will need to follow the following procedure in the next steps: - Download actions and sending a photo (selfie) - Actions to send

documents (e.g. proof of identity). The photo will be used for identity verification and verification. More information here. I have been informed and consent to the use of my biometric data, related to the image of my face, for the purpose of ascertaining and verifying my identity." According to the company, the subscriber is invited to be informed about the processing of his biometric data through the text available via a hyperlink (link) by clicking on the word "here"). He states, however, that after submitting the complaint in question, he found that it had not been fully understood by the complainant that there were two information texts, i.e. a) an information text on the processing of personal data regarding the entire process through the digital onboarding website and b) a text of consent regarding the use specifically of biometric data. For this reason, the company declares that it has made changes to the text of the (general) information (attached as Add. 5 to G/EIS/7613/19-11-2021 document), so that it contains an explicit reference to the consent text. This text states, among other things, that "using real-time photography is made possible through technologies such as machine learning, artificial intelligence (AI) and biometrics, combined with human review to verify if the person requesting a transaction is indeed the same as the person appearing on the presented identification document (ID card or passport etc.) providing security to our transactions. […] In order to confirm the checks of the result using the above technologies, COSMOTE and/or OTE may additionally use a specialized representative to check the data of the digital analysis and the final identification". However, as the company's representatives explained during the hearing, human intervention refers only to the control of identification documents and other documents attached to the application and not to the process of matching the person depicted in the photograph (selfie) with the person appearing in the identification document, which (matching) takes place entirely automatically, using artificial intelligence technology. According to the company, the process cannot proceed if the user does not select ("tick") the icon with which he expresses his consent to the processing of his biometric data. In the event that the electronic process is interrupted, the subscriber is indicated with alternative ways of completing his request, as was done in the case of the complainant. Furthermore, the company maintains that it keeps in its file as proof of identification only the result of the processing, i.e. whether the prospective subscriber was finally identified or not, and not the photo itself from which the identification was derived, stating at the same time that "the photo is deleted without possibility of recovery after 30 days from the submission of the request" (p. 11 of the memorandum). It further argues that the subscriber's information was "from the outset complete and easily accessible for the subscriber, given that during the first stage of the process there was a prominent link labeled Data Protection through which the prospective subscriber could easily access the set of information", while immediately afterwards it

points out that "with regard to the processing of biometric data, the relevant field through which the subscriber's consent was requested, contained a hyperlink ("More information here"), through which the prospective subscriber is led to a detailed text information regarding the processing of his biometric data for the purpose of providing free and fully informed consent, [...] on the occasion of A's complaint was added from 11/19/2021 to the information text regarding the processing of the website (https://onboarding .cosmote.gr), paragraph regarding the processing of biometric data". of personal data through The Authority, after examining the elements of the file, after hearing the rapporteur and the clarifications from the assistant rapporteurs, who were present without the right to vote, after a thorough discussion, DECIDED IN ACCORDANCE WITH THE LAW 1. From the provisions of the articles 51 and 55 of the General Data Protection Regulation (Regulation (EU) 2016/679 – hereinafter, GDPR) and Article 9 of Law 4624/2019 (Government Gazette A´ 137) it follows that the Authority has the authority to supervise the implementation of the provisions of the GDPR , of this law and other regulations concerning the protection of the individual from the processing of personal data. In particular, from the provisions of articles 57 par. 1 item f of the GDPR and 13 par. 1 item g´ of Law 4624/2019 it follows that the Authority has the authority to deal with A's complaint and to exercise, respectively, the powers granted to it by the provisions of Articles 58 of the GDPR and 15 of Law 4624/2019. 2. According to article 5 par. 1 a) GDPR "1. Personal data: a) are processed lawfully and legitimately in a transparent manner in relation to the data subject ("legality, objectivity and transparency"). In addition, according to the fundamental principle of accountability (art. 5 para. 2 GDPR) the controller bears responsibility and is able to demonstrate compliance with paragraph 1. 3. As "biometric data", defined by art. 4 No. 14 GDPR, the "personal data resulting from special technical processing linked to physical, biological or behavioral characteristics of a natural person and which allow or confirm the indisputable identification of said natural person, such as facial images or fingerprint data". Biometric methods mean the techniques of certifying the identity of natural persons through the analysis of their fixed characteristics. Biometric methods can be classified into two categories: i. techniques based on the analysis of physical or genetic characteristics (such as fingerprints, palm geometry, pupil analysis, facial features, DNA) and ii. in techniques based on behavioral analysis (such as signature, voice, typing style). Biometric data are included in the special categories of personal data, which in principle are prohibited to be subject to processing, according to article 9 par. 1 GDPR. Paragraph 2 of the same article provides for the exceptions to the above prohibition (thus providing the permitted legal bases for the processing of special categories of data), the first of which is the express consent of the subject: "Paragraph 1 does not apply in the following cases : a) the data subject has provided express consent to the

processing of such personal data for one or more specific purposes, unless the law of the Union or a Member State provides that the prohibition referred to in paragraph 1 cannot be lifted by the data subject, [...]'. 4. A valid consent according to the GDPR must meet on the one hand the conditions of the definition of the concept of consent (Article 4 para. 11 GDPR) and on the other hand the additional conditions of Article 7 GDPR, according to which: "1 . When the processing is based on consent, the controller is able to prove that the data subject consented to the processing of the personal data. […] 3. The data subject has the right to withdraw his consent at any time. Withdrawal of consent does not affect the lawfulness of processing that was based on consent prior to its withdrawal. Before giving consent, the data subject is informed accordingly. Withdrawing consent is as easy as giving it. [...]". 5. Furthermore, in order to ensure the principle of transparency of processing, Article 12 para. 1 GDPR states that: "The data controller shall take appropriate measures to provide the data subject with any information referred to in Articles 13 and 14 and any communication in the context of Articles 15 to 22 and Article 34 regarding processing in a concise, transparent, comprehensible and easily accessible form, using clear and simple wording, in particular when it comes to information specifically addressed to children." Mandatory information provided is provided for in Article 13 GDPR for the case where the data is collected by the subject and in Article 14 GDPR for the case where the data has not been collected by the subject. The information, according to the same article, is provided during the collection of the data. 6. According to Article 28 GDPR, "When processing is to be carried out on behalf of a data controller, the data controller shall only use processors who provide sufficient assurances for the implementation of appropriate technical and organizational measures, in such a way that the processing meets the requirements of this regulation and to ensure the protection of the rights of the data subject", and paragraph 3 of the same article provides for the minimum content of the contract or other legal act, which must bind the processor in relation to the person in charge processing. According to the GDPR Guidelines 07/2020 on the concepts of controller and processor in the GDPR, the controller determines the purposes and means of processing, i.e. the reason and manner of processing. The controller must make the decisions concerning both the ends and the means. However, decisions concerning some more practical aspects of the application ("material means") may be taken by the processor. The controller does not need to actually have access to the data being processed to be considered a controller. The processor is the natural or legal person, public authority, agency or other entity that processes personal data on behalf of the controller. In order to identify an entity as a processor, two basic conditions apply: that it is a separate entity in relation to the data controller and that it processes personal data on behalf of the data controller. The processor must not process the data in any other way, except

in accordance with the instructions of the controller. The controller's mandates may provide some discretion as to how best to serve the controller's interests, allowing the controller to choose the most appropriate technical and organizational means. However, the processor violates the GDPR if it goes beyond the instructions of the controller and begins to determine the same purposes and means of processing. In such a case the processor will be considered a controller with respect to the processing in question and may be subject to sanctions for exceeding the instructions of the controller (see summary CG 7/2020 ESPD, pp. 3-4). 7. According to Article 35 para. 1 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 rights and freedoms of natural persons, the controller carries out, before the processing, an assessment of the effects of the planned processing operations on the protection of personal data. The Authority, pursuant to paragraph 4 of article 35 GDPR, has drawn up and published a list of the types of processing operations that are subject to the requirement to carry out an impact assessment regarding data protection pursuant to paragraph 1 (decision APD 65/2018). Among these actions are the following: 1.2 Systematic data processing aimed at making automated decisions, which produce legal results regarding the data subjects or significantly affect the data subjects in a similar way and may lead to exclusion or discrimination against the data subjects of the natural person. Relevant examples are the automatic refusal of an online credit application or electronic recruitment practices without human intervention (ref. 71 of the GDPR) or the automatic refusal of insurance benefits. 1.3 Systematic processing of data that may prevent the subject from exercising his rights or using a service or contract, especially when taking into account data collected by third parties. Relevant examples are the case where a bank checks its customers using a creditworthiness database to decide whether to grant them a loan or not, the entry of the subject on a "black" list, such as the list of mobile phone providers (telenges), the registration of the subject in whistleblowing systems. 2.1 Large-scale processing of the special categories of data (including genetic and biometric data for the purpose of indisputable identification of a person) referred to in article 9 par. 1 and of the data referred to in article 10 of the GDPR. 3.1 Innovative use or implementation of new technologies or organizational solutions, which may include new forms of data collection and use, with a potentially high risk to the rights and freedoms of natural persons such as the combined use of fingerprints and facial recognition for enhanced physical access control, or mhealth applications or other "smart" applications, from which users are profiled (eg daily habits), or artificial intelligence applications or publicly accessible blockchain technologies that include personal data. 8. In the case under consideration, the following emerged from the information in the file: The company OTE

SA. implemented and made available to its subscribers the digital onboarding service in June 2020. The purpose of the service is the electronic identification of its prospective subscribers and at this stage only landline transfer requests are served through it. For the electronic identification of the subscriber, his biometric data is processed, which are obtained from the photo (real time selfie). Confirming the authenticity of the photo and matching it with the photo of the applicant's face takes place exclusively automatically, using artificial intelligence (AI) technology. The legal basis for the above processing of biometric data is the subscriber's consent, which is provided with the above described procedure. For the processing of biometric data, according to article 9 par. 2 a) GDPR, the provision of valid express consent, fully informed, after full and correct information and provided by indisputable means, should be ensured in every case. From the examination of the case, it emerged that at the time of the submission of the complaint and until 19/11/2021, the general information text regarding the website https://onboarding.cosmote.gr did not include information about the processing of biometric data. The relevant information of the subjects was provided until 19/11/2021 only via hyperlink at the stage just before the provision of the subject's consent. In this way, the information on data processing through the website was incomplete, to the extent that it was not easily accessible, as required by Article 12 para. 1 GDPR, while the general information on data processing on the digital onboarding platform was not complete. This lack also caused the complainant's concern and was the reason for submitting the present complaint. After all, the company also acknowledges that in the case of the complaint, the complainant did not realize that there was a second information text, the so-called "consent text", which included the information about the processing in question, which demonstrates a lack of transparency (the information was not visible and easily accessible, possibly also to other subjects, who may have provided consent without "full awareness"), at least until 19/11/2021. On the occasion of the complaint, from 19/11/2021 a paragraph on the processing of biometric data was added to the general information, so the specific deficiency was corrected. 9. In the special update on the processing of biometric data, which has now, due to the complaint, been added to the general update of the website (https://onboarding.cosmote.gr), it is stated, among other things, that the controller is "the COSMOTE company or OTE company". The general information provided to the subjects, at the time of the complaint, about the website https://onboarding.cosmote.gr, as attached to the complaint, stated that "The person responsible for processing personal data is the company COSMOTE MOBILE TELECOMMUNICATIONS SA ("COSMOTE"), with headquarters in Marousi Attica (99 Kifisias Avenue) with contact phone number 13888 for residential customers or 13818 for corporate customers". However, according to the company's memorandum after the hearing, the process of digital

onboarding initially and until today, currently concerns only requests for the portability of fixed telephony lines and therefore OTE S.A. is responsible for processing. and not Cosmote. Therefore, the information on this point regarding the data controller was incorrect. After the complaint, "the COSMOTE company or the OTE company" is mentioned as the controller. Given that the information provided must be clear and definitive, it should be clarified at this point that personal data processing through which of the above companies is responsible for processing in each case. Furthermore, in the specific update on biometric data processing that was initially provided only at the pre-consent stage and has now been added to the general update text, it is stated that “using real-time photography is enabled through technologies such as machine learning (machine learning), artificial intelligence (AI) and biometrics, combined with human review to verify if the person requesting a transaction is indeed the same as the person appearing on the presented identification document (police card identity card or passport etc.) providing security in our transactions. […] In order to confirm the checks of the result using the above technologies, COSMOTE and/or OTE may additionally use a specialized representative to check the elements of the digital analysis and the final identification”. However, as the company's representatives explained during the hearing, this is not the case in relation to the verification of the person's identity: human review only intervenes in relation to the validity of documents, while the establishment of identity through controlled processing takes place fully automated. At this point the information is unclear and should be corrected to avoid misinterpretation. Regarding the recipients of the data, the general information initially provided the following information: "Recipients of your personal data may be third-party companies with whom we cooperate for remote Online transactions using electronic signatures, between COSMOTE and its customers, namely the company IntelliSolutions Information Services S.A., which is based in El. 46 Venizelou, 176 76, Kallithea. In these cases, the third-party companies are processing on behalf of OTE, i.e. partners of OTE, who undertake the execution of a specific project following our instructions and applying the strict procedures of the OTE Group regarding the processing of your personal data". In the completed information text it is now stated that "Specifically for your identification through the use of biometric data we are cooperating withcompany IntelliSolutions Information Services SA...". Nevertheless, from listening
and the documents submitted by the company did not show that the
company IntelliSolutions is a recipient of biometric data, while it is not
it became clear which processing operations (of simple personal data)
are carried out by this company on behalf of OTE: With the no. first

C/EIS/6066/15-04-2022 OTE document an agreement was presented

processing of personal data entitled Agreement on Processing of Personal

Data on Behalf of a Controller, between OTE SA and the company IntelliSolutions

Information Services S.A., which however does not include processing

biometric data, but only technical support and implementation services

changes to the Digital Onboarding platform, while mentioning that the

processing takes place on the premises of the controller. Such as

the company then argued in its memorandum, “it was deemed not

processing of biometric data is entrusted to IntelliSolutions and for the reason

this biometric data was not included in its relevant annex

contract", noting that it is reviewing the said contract text. I will

it must be pointed out that according to the fundamental principle of accountability (art

5 para. 2 GDPR), the data controller should have known the exact role of

parties involved and be able to document their legitimacy

actions they have undertaken to carry out, before the start of it

processing. For this reason, it is established on behalf of the complainant

company's breach of the principle of accountability regarding the role of the third party

company IntelliSolutions Information Services S.A., while, for its purpose

compliance with GDPR requirements, should be clarified by

controller, if such third party is processing

biometric data on his behalf and, if necessary, to

modify the text of the contract between them and/or the text accordingly

informing the subjects.

FOR THOSE REASONS

THE BEGINNING

1. Address the complained company COSMOTE MOBILE TELECOMMUNICATIONS

S.A. according to article 57 par. 2 b) GDPR reprimand for the identified deficiencies and ambiguities in informing the subjects (article 5 par. 1 a' and 13 GDPR) and for the established violation of the principle of accountability (article 5 par. 2 GDPR) in in relation to the role of the company IntelliSolutions Information Services S.A. in sub crisis processing.

2. Address the complained company COSMOTE MOBILE TELECOMMUNICATIONS S.A. according to article 57 par. 2 d) GDPR order, to modify and complete appropriately the information text of the subjects, in accordance with those set forth in Thought 9 of this decision, for the purpose of its full compliance with the principle of processing transparency (article 5 par. 1 a' GDPR), informing regarding the Authority.

The president

George Batzalexis

The Secretary

Irini Papageorgopoulou