Athens, 20-06-2022 Prot. No.: 1493 DECISION 23/2022 (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 10/05/ 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 opposition to the President of the Authority, Constantinos Menoudakos, and regular members Charalambos Anthopoulos, Spyridon Vlachopoulos and Konstantinos Lambrinoudakis attended as rapporteur. At the meeting, by order of the President without the right to vote, Haris Symeonidou, special scientist - auditor, attended as assistant rapporteur and Irini Papageorgopoulou, employee of the Authority's administrative affairs department, as secretary. The Authority took into account the following: With the no. prot. C/EIS/6446/23-09-2020 complaint by A (hereinafter the complainant), directed against the Wind store [area] X and in total against the company WIND Hellas Telecommunications SA (hereinafter the complainant), which is subscriber, complaining about a security gap during the process of renewing his contract and not being satisfied with his right of access to his data. In particular, according to the above related complaint, on 29/07/2020 the complainant went to the Wind store in [area] ... and asked to renew his connection plan for the landline number ... . The complainant states that during the contract renewal process Kifisias Ave. 1-3, 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr he was not asked for any identification document, no document was submitted to him to sign , either physical or electronic, while the employees, after handing him a form entitled "Permanent Renewal Contract" with blank fields for customer signature, signature and partner seal, assured him, as he states, that the renewal in this way is valid. Subsequently, the complainant submitted electronically on the same day (29/07/2020) both to the store in [region] X and to the Data Protection Officer of the complainant, via e-mail, a request for access to the recorded visual material from the store's cameras , for the duration of his stay there, while he repeated his question about the validity of the renewal of his contract. Furthermore, the complainant, with his supplementary report under no. prot. C/EIS/5750/25-08-2020 notified the Authority of the 24/8/2020 response received from the Complainant's Written Communication Department, with which his company stated that verbal confirmation of the name and A .F.M. of the complainant, and no identification documents were requested as the employees of the Wind [area] X store know him by sight, and due to a temporary system problem it was not possible to digitally sign the contract. In relation to the visual material from the cameras, the complainant referred the complainant to her partner, B, who runs the store in question under the franchise regime. The complainant in his supplementary document to the Authority argued that, contrary to what was stated in the complainant's reply, the employee who served him was new and was seeing

him for the first time, while the only information the complainant gave him was the number his phone. In addition, he complains about the fact that he was not informed in time about the systemic problem that prevented him from signing, while regarding his right of access to the recorded material from the cameras, he states that he sent a relevant request via e-mail to the complainant's address ...@windstores.gr B, on 29/07/2020. The Authority, in the context of examining the above complaint, with no. prot. C/EX/5346-1/16-10-2020 her document, which was communicated to the owner of the store [area] X, invited the complainant to state her views on the complainants, specifying in particular the following: a) which is the more general policy provided by the complainant regarding the contract renewal process by a subscriber, in case of his physical presence in a store, b) if this procedure was followed in the case of the complainant, c) if and how the complainant responded to the request of the complainant's access to the recorded visual material that concerns him and is related to the transaction in question, which was exercised with the complainant's 29-07-2020 electronic message to the complainant and to the Wind store [region] X. The complainant with the from 17-11-2020 her response (with Authority no. C/EIS/7904/17-11-2020) first of all refers to her letter from 24-08-2020 to the complainant, in which she argued that thehis identification at the [area] X store had been "properly" carried out with confirmation of his VAT number, while no identification document was requested, as the complainant was "known and recognizable by the employees of the [area] X store, who serve him regularly". However, as the complainant states, the renewal of contracts with the subscriber's personal presence in a physical store, according to its official instructions, takes place after presenting an identity document and comparing its details with the subscriber's card. After agreeing to the services provided, the subscriber signs digitally via tablet and receives his renewal contract and summary offer. According to the complainant, signing via tablet in this case was not possible, as the system that supports the relevant function was blocked, but the complainant was informed about this and received a copy of his contract as proof. Furthermore, although the issue of signing the contract is primarily subject to the provisions of the EETT General License Regulation and consumer protection law, the complainant stated that she provided the complainant with the possibility of immediate withdrawal, sending him the relevant form with detailed instructions on 27-08 -2020, however the complainant did not withdraw from his contract. Finally, regarding the complainant's right of access to the recorded visual material from the cameras of store [area] X, the complainant again referred to her partner, B, who runs the store under a franchise regime. At the same time, with his letter dated 18-11-2020 to the complainant, which was communicated to the Authority (prot. no. C/EIS/7922/18-11-2020) the owner of the shop [area] X, B, also argued that the complainant during his visit was served by a salesperson who knows him, due to

his regular visits to the store, both himself and his wife, that after the complainant's verbal agreement on the features of his program, the salesperson confirmed from new the details of the complainant by mentioning his VAT number, thus completing the identification, and that during the stage of electronic signatures, the computer with the installed software got stuck and in order not to delay customer service, the seller printed a copy of the contract without the addition of digital signatures. Regarding the visual material from the cameras requested by the complainant, the complainant stated that "unfortunately there is no longer a copy due to irreversible damage caused to the hard drive that held the files". Subsequently, with the no. prot. C/EIS/7939/19-11-2020 his document to the Authority, the complainant stuck to his initial complaints and argued that the complainant's answer is false, as the employee was new and did not know him, no verbal confirmation was made of his details and no identification and for this reason he immediately requested the material from the store and from the YPD of the complained company. Subsequently, the Authority, with no. prot. C/EX/2290/12-10-2021 and C/EX/2301/13-10-2021 Summons it invited the involved parties to a hearing at the meeting of the Authority's department on 19-10-2021 and, after adjournment to 10-

11-2021, in order to present their views on the case. During the hearing, the parties developed their views and were given a deadline of 15 days (until 01-12-2021) to submit briefs. During the meeting of 10-11-2021, complainant A from the offices of the Authority attended via video conference, and on behalf of the complainant, her attorneys, Athina Hatzipavli ... and Chrysi Tzatha .... B, who runs the WIND [area] X store under franchise status, and his attorney, Ilias Spyrou, also appeared. The parties involved received, during this meeting, a deadline and submitted, the complainant the no. prot. C/EIS/7551/18-11-2021 memorandum, and the defendant Wind the no. prot. C/EIS/7889/02-12-2021 her memorandum and the complained owner of the Wind Shop [area] X, B, the C/EIS/7913/02-12-2021 memorandum. The complainant, both orally during the hearing and with his above-mentioned memorandum, supported what was stated in his complaint. The complainant Wind, during the hearing and with its memorandum, stated that it has established a correct and complete process for identifying its customers in the stores , which and provides, as well as ensuring the suitability of its store staff with a staff training system for personal data protection issues. He argued that the discrepancy in the identification process in this case, which took place only with the confirmation of A.F.M. of the complainant, can be justified "in the course of everyday business life" because the complainant was known and recognizable by the employees. Finally, he reiterated the claims that the issue of not signing the contract is related to consumer law, that he was finally granted both the contract and the terms of use and that there is no question of

damage to the complainant, since he did not dispute the transaction or withdraw from this without charge even though he was given this possibility, while regarding the issue of the complainant's access to the recorded material from the store's cameras, he reiterated that the store operating under a franchise system is responsible for processing this particular processing. The complained owner of the store, B, both in the context of the hearing and in his memorandum, argued that during the complainant's visit to the store [area] X to renew his fixed contract there were three (3) employees present, whom he knew personally and greeted upon his entry, as proof of this he does not provide responsible statements of the employees in question, while he was served by another employee who was in a probationary period of work and who was supervised and assisted by the others. In addition, it states that the A.F.M. number was used to identify the complainant, that the complainant never disputed the fact that he himself was present at the incident, nor did he suffer any damage, and that for technical reasons the contract was not possible to be printed at that time, yet it was given in the following days to the complainant, who neither disputed its validity nor retracted from it, although he was given an opportunity to do so gratuitously. Finally, regarding the complainant's request for access to the recorded material from the store's cameras, the owner of the store argued that due to a technical problem (detection of viruses) it was not possible to grant the relevant files to the complainant, as he replied on 28-11- 2020. During the hearing, B's lawyer admitted that he did not respond in time to the complainant's relevant access request. The Authority, after examining all the elements of the file and after listening to the rapporteur and the assistant rapporteur and after a thorough discussion, DECIDED IN ACCORDANCE WITH THE LAW 1. From the provisions of 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, this law and other regulations concerning the protection of 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 take charge of A's complaint against WIND Hellas Telecommunications SA 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 the provisions of article 15 par. 1, 3 and 4 GDPR: "1. The data subject has the right to receive from the controller confirmation as to whether or not the personal data concerning him is being processed and, if this is the case, the right to access the personal data […]. 3. The controller provides a copy of the personal data being processed. For additional copies that may be requested by the data subject, the controller may charge a reasonable fee for administrative costs. If the data

subject submits the request by electronic means and unless the data subject requests otherwise, the information is provided in a commonly used electronic format", while according to the provision of article 12 para. 3 GDPR: "The data controller provide the data subject with information on the action taken upon request pursuant to Articles 15 to 22 without delay and in any case within one month of receipt of the request. This deadline may be extended by a further two months if necessary, taking into account the complexity of the request and the number of requests. The data controller shall inform the data subject of said extension within one month of receipt of the request, as well as of the reasons for the delay. If the data subject makes the request by electronic means, the information shall be provided, if possible, by electronic means, unless the data subject requests otherwise.' The data controller must respond to the subject's request, responding (either positively or negatively) without delay and in any case within one month of receiving the request. As pointed out in the EDPB Guidelines 1/2022 on the right of access, the controller must react and, as a rule, provide the information of Article 14 without delay, or, in other words, as soon as possible (see EDPB Guidelines 1/2022 on data subject rights – Right of Access, §§155-157). the appropriate level of security against 3. Furthermore, according to article 32 GDPR par. 1 b), 2 and 4: "1. Taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and freedoms of natural persons, the controller and the executor the processing implement appropriate technical and organizational measures in order to ensure the risks, including, among others, as the case may be: [...] b) the ability to ensure the confidentiality, integrity, availability and reliability of processing systems and services on a continuous basis , […] 2. When assessing the appropriate level of security, particular account shall be taken of the risks arising from the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access transmitted, stored or otherwise submitted to processing.. […] 4. The person in charge of processing and the executor of the processing shall take measures to ensure that any natural person acting under the supervision of the controller or the processor who has access to personal data processes it only on the instructions of the controller, unless required to do so by the law of the Union or the Member State". personal data that 4. In addition, according to article 28 par. 3 GDPR "3. The processing by the processor is governed by a contract or other legal act governed by Union or Member State law, which binds the processor in relation to the controller and determines the object and duration of the processing, the nature and the purpose of the processing, the type of personal data and the categories of data subjects and the obligations and rights of the controller. The contract or other legal act in question provides in particular that the processor:

a) processes the personal data only on the basis of recorded instructions of the controller, including with regard to the transfer of personal data to a third country or international organization, unless obliged to to this end on the basis of Union law or the law of the Member State to which the processor is subject; in this case, the processor shall inform the controller of such legal requirement prior to processing, unless such law prohibits this type of information for serious reasons of public interest, c) takes all the required measures pursuant to article 32 [...]". 5. Finally, article 4 no. 7 defines the data controller as the natural or legal person, public authority, agency or other entity that, alone or jointly with others, determines the purposes and manner of personal data processing. Fundamental to the determination of the controller is the functional criterion. In other words, a controller is the one who takes decisions on certain critical elements of the processing, i.e., determines the purpose and/or the essential elements, at least, of the method of processing (cf. for the concept of the person responsible and performing the processing, Opinion 1/2010 of the EO of Article 29, in which it is mentioned, among other things, that the definition of the objectives and the method is equivalent to the definition, respectively, of the "why" and the "how" of certain processing activities, as well as paragraphs 25-27 of the Guidelines 07/2020 of the ESPD for the concepts of the person in chargeprocessor and the processor in the GDPR).

6. In the case under consideration, the following emerged from the information in the file:

The complained company, as controller of his data

complainant for the purpose of executing the supply contract between them

telecommunications services, has granted specific orders - instructions to

the stores, acting in this case as processors, for

the identification of subscribers in a physical store. According to the instructions

these provide without exception the presentation of an identification document in cases

entering into a new or amending an existing contract. Since

physical store subscriber identification process is related to

security of the processing of their personal data which is carried out

under the responsibility of the complained telecommunications service provider, h

this process is part of its technical and organizational security measures

Data Controller in accordance with Article 32 GDPR. In the context of the hearing

said instructions were requested, for documentation of

her claims

defendant, who with her memorandum presented the document "Procedure

identification of owners of telecommunication services", which it states that it has

disclose to all affiliated stores, and which includes the

identification of the subscriber by presenting an original identification document.

7. In this case, from the presented data it appears that indeed the

employees of the store knew the complainant by sight and

confirmed his identity using A.F.M. of, therefore no

a violation of article 32 par. 4 by the complained-about company is found

as Processor, nor violation of articles 28 par. 3 a) and 32 par. 4

by the store as processors. After all, the risk for the

subject in the case of the renewal of a fixed telephony contract is

low.

The question of the correct or incorrect procedure for renewing the fixed contract

telephony does not fall under the competence of the Authority.

It was further noted that the complainant submitted electronically on 29/7/2020

request for access pursuant to Article 15 GDPR to recorded visual material from

video surveillance system of store [area] X, both to

complained about company as well as to the store. Based on what is mentioned in

paragraph 4 and in accordance with the operational criterion, data controller

regarding the video surveillance system is the store, as well as in its context

franchise agreement the store owner retains the autonomy to

decides how to protect his store. In this case, the

owner of store B, as controller did not respond with

no way to the complainant's access request, except after the

intervention of the Authority. Specifically, on 28/11/2020, 4 months after submission

of the request, the controller rejected his access request

complainant on the grounds that the recorded material had been destroyed.

8. Following the above, from the information in the file and after the hearing

procedure, the Authority finds on behalf of the Wind store [region] X, as

controller regarding the video surveillance system, violation

of article 15 in conjunction with article 12 par. 3 GDPR and considers that

case to exercise the corrective actions according to articles 58 par. 2 i) and 83 GDPR

its powers (imposition of a fine) in respect of the above offence. For

determining the sanction, the Authority takes into account its measurement criteria

fine defined in article 83 par. 2 of the GDPR that apply to

present case.

In particular, particular consideration is given to:

a) The nature and gravity of the violation,

b) The fact that only one (1) subject was affected and did not suffer

financial cost

c) The fact that the violation on the part of the data controller does not

attributed to fraud

d) The lack of previous violations of the controller, and

h) The fact that special categories were not affected by the violation

personal data.

FOR THOSE REASONS

THE BEGINNING

It imposes on B, as data controller based on article 58 par. 2 subsection i

of the GDPR a fine of two thousand (€2,000) euros for the violation of the non

responding to the complainant's access request pursuant to Article 15 GDPR

within the period provided for by article 12 par. 3 GDPR.

The president

George Batzalexis

The Secretary

Irini Papageorgopoulou