Athens, 31-10-2022 Prot. No.: 2734 DECISION 60/2022 The Personal Data Protection Authority convened at the invitation of its President in a videoconference meeting on Wednesday 06.08.2022 at 09:00, in order to examine the case referred to in the history of the present. The President of the Authority, Constantinos Menudakos, and the alternate members, Demosthenes Vougioukas, rapporteur, and Nikolaos Livos, were present in place of regular members, Constantinos Lambrinoudakis and Charalambos Anthopoulos, respectively, who, although legally summoned in writing, did not attend due to disability. Present, without the right to vote, were Panagiotis Tsopelas and Georgia Panagopoulou, auditors, as assistant rapporteurs and Irini Papageorgopoulou, employee of the administrative affairs department, as secretary. of The Authority took into account the following: Submitted to the Authority with no. prot. C/EIS/7204/20-10-2020 application of A, with which the applicant requests the review of the 31/20201 decision of the Authority issued on her with no. prot. C/EIS/2527/02-04-2019 of her complaint. 1 Based on its 31/2020 decision, the Authority had rejected as unfounded the complaint No. C/EIS/2989/19-4-2019 against the controller and subject "COMPLAINT FOR VIDEO SURVEILLANCE SYSTEM - B OE", reserving to investigate it further regarding the legality of installation and operation of the remaining cameras (remaining stores and premises of the controller). The reasoning behind the decision was that, on the one hand, the conditions of Articles 5 and 6 of the GDPR and Directive 1/2011 of the Authority are met and, on the other hand, that based on the scope of coverage as reflected in the image sample submitted by the data controller, it is established that, for the store in which the treatment requester worked, the absolutely necessary image data is collected to achieve the intended processing purpose, which cannot be achieved by milder and equally effective means. 1 Kifissias Ave. 1-3, 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr By decision 31/2020, the Authority reserved the right to further investigate the video surveillance system of the company "B OE" (hereinafter "controller") regarding the legality of the installation and operation of the cameras in the stores and facilities of the controller. The applicant with no. prot. C/EIS/7204/20-10-2020 and C/EIS/2241/31-03-2021, documents requested that her complaint be reviewed for the purpose of remedying the 31/2020 Decision, citing, among other things, the following : 1. The purpose of the processing exceeded what the data controller states in this regard, namely "(..) monitoring is limited as far as possible to the minimum areas that are important for the intended purposes of video surveillance and specifically the safety of persons and of goods and the avoidance of criminal actions (..)". In particular, the applicant claims that through the video surveillance system "(..) the performance, behavior, external appearance or tardiness of employees were monitored and supervised"(..), providing as evidence of the claim in question, inter alia, photographic material and electronic messages (items

1,4,5,6,7,8). 2. There were more than one cameras in the store on … street, contrary to what is stated in the table on page 13 of the memorandum with no. Prot. of Authority C/EIS/1955/13-03-2020 of the data controller, in order to document this claim, relevant evidence is provided, such as photographic material, e-mails and an excerpt of an affidavit before the Athens Magistrate's Court of a former employee in a shop of the data controller processing. 3. The cameras were installed before 2018 when the notification obligation of Article 6 of Law 2472/1997 still applied without the relevant information being submitted to the Authority. In this regard, the applicant refers to an excerpt from an affidavit before the Athens Magistrates' Court (no. 2637/27-02-

2019), by the controller's ex-wife and store worker, in which she states that she knew there were cameras inside 2 of the stores for security reasons. The above, combined with the fact that the witness worked at the controller's company until October 2016, leads, according to the applicant, to the conclusion that there was a video surveillance system in operation at the controller's premises before 2018. It is pointed out that in the memorandum of the controller with no. prot. C/EIS/1955/13-03-2020, it is stated that the installation of the cameras started in 2017. 4. The cameras recorded sound. An electronic message sent by the data controller through the Viber application as well as a reference to an excerpt of a deposition before the Single-Member Court of First Instance of Athens are provided as documentary evidence of the claim in question. 5. The data controller and the relevant legislation were not indicated on the information boards. Photographic material is enclosed as proof of said report (item 16). 6. In support of her allegations, she provided a video clip that has been sent to the complainant's mobile phone through the Viber application in the context of the investigation of the incident of the loss of an anti-theft magnet, regarding which the data controller in the memorandum no. prot. C/EIS/1955/13-03-2020 had quoted a laboratory analysis by a special expert which questioned its authenticity based on specific technical findings. 7. The Authority issued a decision even though it was aware of the pending trial of the same case before the Single Member Court of First Instance of Athens, of which it was aware from the memorandum with no. authority letter C/EIS/1955/13-03-

2020 of the controller. Furthermore, the applicant refers to the Decision of the Single-Member Court of First Instance of Athens with number ... against which she states that she has filed an appeal. In said decision, it is stated, among other things, that the claim of the plaintiff (in this case, the treatment requester) that "(..) n defendant (in this case, the data controller) did not comply with the legal conditions required to be observed 3 in the case of the installation of a system with the possibility recording audio data in violation of the principle of proportionality as it could achieve its purpose, preventing incidents of theft by installing a

simple camera at the entrance of the shop (..) is rejected as substantively unfounded'. Subsequently, the Authority, after examining the data of the applicant submitted with the treatment application and in connection with the relevant reservation of decision 31/2020 for further investigation, carried out on 19/11/2021 a surprise on-site inspection at the store of the data controller on the street ... at ... after the no. prot. C/EXE/2559/11-11-2021 order of the President of the Authority and drew it up with no. prot. C/EIS/8149/14-12-2021 conclusion of administrative control. Through the access given by the technical manager of the controller, the capture fields, event logs, recorded video recordings and system configuration were checked by the shop in question via a remote connection to the other recorders and for the craft facilities. of the controller in … . Subsequently, the Authority with no. prot. C/EXE/2951/20-12-2021 and C/EXE/2952/20-12-2021 documents, invited the treatment requester and the data controller to attend a meeting of the Authority's Department on 09/02/2022 . During the hearing on 09/02/2022, C, Legal Representative of company B and Ilias Tomaidis, lawyer from Thessaloniki (...), as well as the complainant A, her husband D and A's lawyer Maria appeared on behalf of the complainant Long with ... . Both parties, after orally developing their opinions, received during this meeting a deadline for presenting memoranda to further support their claims and the complainant submitted them in a timely manner with no. prot. G/EIS/2777/25-02-2022 and G/EIS/2809/28-02-2022 her memoranda, while the complainant no. prot. C/EIS/2775/25-02-2022 and C/EIS/2776/25-02-
2022 memoranda, with which they submitted, among other things, the following: 4 In particular, the applicant, through her attorney, submitted to the Authority a supplementary memorandum, in which she included video recording material which, according to her claims, confirms the fact that the video surveillance system of editor record audio. As additional evidence, she also submitted two photos sent to her cell phone via the Viber app, which were dated to match the date and time she claims the anti-theft magnet was lost. For the material in question, the controller has submitted a laboratory analysis (see point 6 p. 4) which the treatment requester disputes on the procedure and findings and cites the TEE code of ethics, claiming that based on this the expert, appointed by the controller should have invited both parties to show him their mobile phones and answer any questions they may have so that a complete and correct analysis documented with a correct conclusion can be completed.Finally, the applicant states that it should be taken into account that its installer video surveillance system of the controller, does not hold the two legal licenses required (category b) (law YP.ARITH.B707/2008) and has not issued a license to operate a private business providing security services, as the law stipulates. And the data controller, regarding the no. prot. C/EIS/7204/20- 10-2020 request for treatment, during the above hearing of 09-02-2022, but also with the - timely filed - after

the hearing his memorandum with no. prot. C/EIS/2775/25-02-2022 argued that: The applicant for treatment, after her voluntary departure from the company, has filed numerous lawsuits against him. The allegations of the applicant for the treatment regarding the illegal installation of a video surveillance system have been rejected as unfounded with the no. ... decision of the Single Member Court of First Instance of Athens. The applicant for treatment with the aim of misleading the Authority relied on electronic messages and Minutes of the Session of the Single Member Court of First Instance of Athens (see point 4.2 p. 7) which related to a video surveillance system that was installed in the home of the owner of the data controller for his personal use and not in the 5 business they worked for. The video submitted by the applicant for treatment to the Authority is edited based on an informative note of laboratory analysis by the expert. The video surveillance system is not programmed to record audio. With regard to the text messages that the treatment applicant has submitted to the Authority in the form of screenshots, she reserves their authenticity. Nevertheless, he considers that even if they were authentic, it does not follow from their content that workers were monitored through the video surveillance system. There was never a second camera installed in the store of ... that the complainant was working as she claims. In this regard, it is pointed out that since no renovation, partial or total, has been done in the store since 2017, traces of the installation in question could be seen when the Authority's surprise on-site inspection was carried out. Regarding the no. prot. C/EIS/8149/14-12-2021 conclusion of the Authority's administrative control the data controller, during the above hearing of 09/02/2022, but also with the - timely filed - after the hearing his memorandum with no. prot. C/EIS/2776/25-02-2022 argued that: The purpose of processing the video surveillance system in the facilities of the unit of ... is the safety of the equipment from damage/destruction/malfunctions/theft but also the protection of the workers themselves . The workplace camera does not cover the whole area but the points where the machines and the fire safety system are located, there is no monitoring in recreation or rest areas and the faces and hands of the workers are not recorded to determine which workers are in the area. The use of a non-automated process for deleting video surveillance data beyond fifteen days is due to a limitation of the system that determines the duration of the cyclic recording in combination with the exhaustion of the physical capacity of the hard drives and not the number of recording days. Therefore, given that the storage means of the system in question have a physical storage capacity of more than fifteen days, this particular methodology cannot be applied. The reason for exceeding the 6 time of fifteen days in the store of ... is due to a technical problem of the telecommunications network for which the Internet service provider is responsible. In order to document this claim, the data controller submitted the document no. first ... certificate of the OTE SA group. The browser used

belongs to Microsoft, one of the largest software development companies in the world. Newer versions of other browsers do not provide the ability to view live camera downloads or play old videos. The "https" and "sttp" protocols are not compatible with the communication methods of the company's recording systems, as a result of which it is impossible to use them when accessing them. The security of access is fully ensured through all unique and confidential user authentication elements, which are known to the controller and the processor. The Authority, after examining the elements of the file and after listening to the rapporteurs 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. The installation and operation of video surveillance systems by downloading or image or sound recording through the collection, preservation, storage, access and transmission of personal data, constitute as individual acts of processing, interference with the individual rights to respect for private life according to art. 9 S., 7 XTHDEE2 and 8 ECHR as well as the protection of personal data according to art. 9A S., 8 ESDA and 8 XTHDEE3, as decided by the Authority with its Opinion No. 3/2020. 2 CJEU Digital Rights Ireland para. 29. 3 CJEU Digital Rights Ireland para. 38. 7 2. In accordance with Guidelines 3/2019 of the EDPS regarding the processing of personal data through video devices4, in order to assess the legality of the installation and operation of the video surveillance system must cumulatively meet the conditions of articles 5 and 6 par. 1 GDPR and the legality of the processing must be documented internally before the installation and operation of the system and in fact when determining the purpose of the processing may need a relevant rating for each camera separately, depending on where it is placed. In particular, these Guidelines define the following: "a (...) 5. Video surveillance is not necessary by definition if there are other means to achieve the underlying purpose. Otherwise, there is a risk that the cultural norms will be changed and therefore the lack of privacy will be established as a general principle (…)". b "(...) 20. The legal interest must actually exist and concern a present matter (ie the interest must not be fictitious or hypothetical). There must be an actual risk situation – such as damage or serious past events – before surveillance can begin. (…)". c. "(...) 24. Personal data should be appropriate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimization"), see Article 5(1)(c). Before installing a video surveillance system, the controller should always thoroughly consider whether this measure is, firstly, appropriate to achieve the desired objective and, secondly, sufficient and necessary to achieve its purposes. Video surveillance measures should only be chosen if the purpose of the processing could not reasonably be fulfilled by other means, which infringe to a lesser extent the fundamental rights and freedoms of the data subject." 3. According to article 27 par. 7 of Law 4624/2019 "The processing of personal data through

closed-circuit visual recording within workplaces, whether they are publicly accessible or not, is only permitted if 4 https://edpb.europa .eu/our-worktools/ourdocuments/guidelines/guidelines-32019-processing- personal-data-through-video_en 8 is necessary for the protection of persons and goods. Data collected through closed-circuit visual recording may not be used as a criterion for evaluating employee performance. Employees are informed in writing, either in writing or in electronic form, about the installation and operation of closed-circuit visual recording within the workplaces. 4. The Authority has issued Directive No. 1/2011 on the issue of the use of video surveillance systems for the purpose of protecting persons and goods, the provisions of which must be applied in conjunction with the provisions of the GDPR and Law 4624 /2019, which defines GDPR implementation measures. This applies in particular to the obligations of the controller included in chapter C' thereof (articles 10 to 13 of Directive 1/2011). For example, data controllers no longer have an obligation to notify the Authority5 of the processing, but must take the necessary measures to comply with the requirements of the GDPR and ensure the satisfaction of the enhanced rights provided for by the GDPR. 5. According to article 7 of Directive 1/2011 of the Authority, the application of the principle of proportionality is of particular importance in the cases of operation of video surveillance systems in workplaces. The system should not be used for the surveillance of workers within these premises, except in specific exceptional cases where this is justified by the nature and working conditions and is necessary for the protection of health and safety. worker safety or the protection of critical workplaces (eg military factories, banks, high-risk facilities). Also, in special areas, such as areas with electro-mechanical installations, the shift manager or safety officer can monitor high-risk machine operators in real time, in order to intervene immediately if a safety incident occurs. In any case, the data collected through a video surveillance system is not allowed 5 See and the Authority's announcement regarding the abolition of record keeping/editing notices and the granting of licenses (decision 46/2018). 9 be used as exclusive criteria for evaluating the behavior and efficiency of employees (see Directive no. 115/2001 on the processing of personal data of employees, section E', par. 6 – 8). 6. In accordance with Article 32 of the GDPR 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 the natural persons, the controller and the processor implement appropriate technical and organizational measures in order to ensure an appropriate level of security against risks. 7. As can be seen from the data in the case file, the complained company has the role of controller for the processing of personal data carried out through the video surveillance system. 8. During the on-site inspection, it was found that in the shop of … on the

street … there is one camera installed, as claimed by the data controller in his memorandum, and not two as claimed by the treatment applicant, and it cannot be established whether the camera referred to the applicant was established in the specific location in the past. 9. During the on-site inspection, it was further found that the audio capture capability from the cameras was disabled on all recording devices, and in the shop of … the camera did not have a built-in microphone and therefore hardware-level audio recording is not possible. 10. There is no possibility, from the video material submitted by the applicant, to establish the proof of the audio recording in the video surveillance system of the controller. Specifically, from the examination of the multimedia file submitted by the applicant with no. prot. C/EIS/2809/28-02-2022 its memorandum, the Authority found that the findings of the laboratory analysis of the material in question included in no. prot. C/EIS/1955/13-03-2020 memorandum of the controller. However, since the current analysis does not contain a comparison of the file in question with a counterpart extracted from the same equipment and since the Authority does not have the ability to produce such a file, since it does not have access to a camera and recording machine 10 of the same capabilities , it is not possible to draw conclusions about the authenticity or otherwise of the video recording file based on the findings of the laboratory analysis submitted by the controller. 11. In the store on the street ... in ... where the surprise spot check was carried out there were two information signs, one at the entrance of the store, which mentions the existence of a video surveillance system and one next to the cash register which is based on the standard of Directive 1/2011 of Principle. It cannot be ascertained whether the signs had a similar form in the past. 12. From the examination of the copies of the electronic messages submitted by the applicant for treatment, it cannot be established with certainty that the means of recording the mentioned conversation is the illegally installed camera and that the content of the message results from the processing of data from the video surveillance system. 13. The applicant's claim that the video surveillance system was installed before 2018 cannot be confirmed from the submitted data since a significant period of time has passed since that year. 14. The claim of the applicant regarding the importance of the fact that a relevant dispute was pending in the civil courts was for the procedure before the Authority, is unfounded because this fact does not prevent or suspend the exercise of the authority's competence (see the decision of the Supreme Court...) 15. Regarding the video surveillance system operating at the craft premises in …, the processing purpose stated by the controller could be achieved by milder and equally effective means, such as by placing cameras at the entrances/exits of the premises, or protecting workers from accidents by taking other technical and organizational measures. There are also strong reservations about whether the machines (sewing machines) being monitored

can be characterized as high risk. From the examination of the data it appears that the monitoring of the machines is not only done in real time by the shift manager or the security manager with the aim of immediate intervention if a security incident occurs, but also takes place the storage of the video material 11 to which he has access the owner of the complained company. The controller's claim that the persons working cannot be identified from the material in question is unfounded, given that the positions of the cameras combined with technical capabilities, such as digital zoom within the cameras' field of view, allow the identification of employees. Consequently, the operation of the video surveillance system in question violates article 5 par. 1 sec. a' and b' of the GDPR. 16. Furthermore, the manual deletion of the data of the video surveillance system after 15 days, which was found during the on-site inspection at the store of ..., constitutes a violation of article 5 par. 1 sub. e' of the GDPR since the data controller could have solved the mentioned problem of the limitation that exists in the recording devices in relation to the creation of a process of automatic deletion of the recorded data by taking technical measures (e.g. creating partitions of an appropriate size on the hard disks of the system or using another automated deletion methodology such as running a timer file deletion script). 17. Regarding the issue of security when accessing the transmitted data over the Internet, the controller's claim that the browser used to access the cameras is secure because it belongs to Microsoft is not true, because the manufacturer itself accepts that the browser in question has a security vulnerability6, is no longer supported by Microsoft, and is no longer receiving periodic security updates, having been replaced by Microsoft Edge software. Also, there are methodologies through which access to any web page can be done in an encrypted way regardless of its content and there are technical solutions available through which access could be done using the https protocol regardless of what limitations the said system. The 6

https://support.microsoft.com/en-us/topic/microsoft-security-advisory-vulnerability-in-internet-explorer-could-allow-remote-code-execution-fc5c609d-f9a9-909e-c227- 45ef70da6dff 12 entering the system through user authentication is only one of the parameters that protect against unauthorized access, while in this particular case there does not seem to be a controlled access process of the controller and the processor using user roles, as the users log into the system with admin credentials. In view of the above, it is established that the company has not taken the necessary technical and organizational measures for the security of the processing in violation of article 32 of the GDPR. 18. Based on the above, the Authority considers that for the processing concerning the operation of the video surveillance system in the store in ... and in the craft industry in ..., there is a case to exercise its corrective powers according to article 58 paragraph 2 of the GDPR in relation to the violations found.

The Authority also considers that, based on the circumstances established, it should be imposed, pursuant to the provision of article 58 par. 2 sec. i of the GDPR the effective, proportional and dissuasive administrative fine according to article 83 of the GDPR both to restore compliance and to punish the illegal behavior regarding the operation of the video surveillance system in the industry in ... . 19. Furthermore, the Authority took into account the criteria for measuring the fine defined in article 83 par. 2 of the GDPR, paragraph 5 item. a' and b' of the same article that are applicable in this case and the Guidelines for the application and determination of administrative fines forpurposes of Regulation 2016/679 issued on 03-10-2017 by the Group Work of Article 29 (WP 253), as well as its actual data

case under consideration and in particular:

a) the nature, gravity and duration of the violation, in view of the nature of

extent or purpose of the relevant processing, as well as the number of

of data subjects affected by the breach and the degree of damage that

specifically suffered:

i. the fact that the controller has violated the provisions of Article 5

par. 1 sec. a' of the GDPR principles of legality, objectivity and

transparency, in addition to the principle of purpose limitation according to article 5

par. 1 sec. b', i.e. violated fundamental principles of the GDPR for protection

of personal data,

ii. the fact that the observance of the principles laid down by the provisions

of article 5 par. 1 sec. a' and b' of the GDPR are of capital importance,

primarily, the principle of legality, objectivity and transparency

so that if this is missing, the processing becomes illegal from the beginning,

even if the other processing principles have been observed. Similarly

of capital importance becomes the principle of limitation of purpose

as well as the principle of accountability in the context of the new model

of compliance introduced with the GDPR, where the burden of compliance and the

relevant responsibility rests with the data controller, who has

provided by the GDPR with the necessary compliance tools,

iii. the fact that the controller has failed to comply

with the orders of the processing authorities of article 5 par. 1 sec. a and b

GDPR also failed to document compliance

the legality of the video surveillance system,

iv. the fact that the violation of the above principles falls under the

provisions of article 83 par. 5 sec. a' of the GDPR in the higher provision

category of the classification system of administrative fines,

v. the fact that, from the elements brought to the Authority's attention, no

material damage occurred to the data subjects,

vi. the fact that the violation of the principles of article 5 par. 1 sec. a and b

it did not, based on the information brought to the Authority's attention, relate to data

personal nature of articles 9 and 10 of the GDPR, but it concerns

employees, who require special data protection

of a personal nature.

b) the fact that a relevant check shows that it has not been imposed on

reported company until today administrative sanction by the Authority.

c) the size of the company

Based on the above, the Authority unanimously considers that it should be imposed on

denounced company as controller or the one referred to in the ordinance

administrative sanction, which is considered proportional to the gravity of the violation.

FOR THOSE REASONS

The beginning

A. It imposes on the complained company with the name "B OE" the

effective, proportionate and dissuasive administrative fine which

appropriate in the specific case, according to the special circumstances

thereof, in the amount of ten thousand (10,000.00) euros for the above established

violations of articles 5 par. 1 sec. a' and b' regarding the system

of video surveillance in the industry in ..., for the reasons that are extensively analyzed in

paragraph 15, and gives an order as within one (1) month from its receipt

present, to remove the cameras from the craft in ..., informing

regarding the Authority.

B. Addresses a reprimand to the complained company with the name "B OE", as

controller, for violation of article 5 par. 1 sec. e' of the GDPR, for them

reasons elaborated in paragraph 16 and instructs him to receive all the

necessary technical and organizational measures to make it automated

deletion of data.

C. Addresses a reprimand to the complained company with the name "B OE", as

controller, for violation of Article 32 of the GDPR, and instructs,

for the reasons detailed in paragraph 17 to receive all the necessary technical and

organizational system adaptation measures.

D. Denies A's request for treatment for the reasons set forth at length

in paragraphs 9-14.

THE PRESIDENT

Konstantinos Menudakos

THE SECRETARY

Irini Papageorgopoulou