Athens, 15-02-2022 Prot. No.: 433 DECISION 61/2021 The Personal Data Protection Authority met as a Department by teleconference on Wednesday, February 17, 2021, following the invitation of its President, in order to examine the case referred to in history of the present. The Deputy President, Georgios Batzalexis, who was obstructing the President of the Authority, Constantinos Menoudakos, and the alternate members Evangelos Papakonstantinou, as rapporteur, and Grigoris Tsolias, in place of the regular members Konstantinos Lambrinoudakis and Charalambos Anthopoulos, who, although legally summoned in writing, did not attend due to obstruction. The meeting was attended, by order of the President, Leonidas Roussos, expert scientist - auditor as assistant rapporteur. Irini Papageorgopoulou, an employee of the Administrative Department, attended as Secretary. The Authority took into account the following: The complaint No. C/EIS/7720/10-11-2019 of A was submitted to the Authority, which concerns the violation of his right of access as a data subject by the PORT AUTHORITY HERACLEIOU S.A. (hereinafter, "controller" or "ALL"). According to the complaint, the complainant requested on … with the application No. … via e-mail to be given information in writing 1 Kifisias Ave. 1-3, 11523 Athens T: 210 6475 600 E: contact@dpa. gr www.dpa.gr regarding the content of recorded material from the cameras of the Port Authority of Heraklion regarding a recorded traffic accident involving the I.X. of the complainant and another I.X. at … . To the complainant's specific request, the company responded with document No. ... and refused the transmission of visual material from the camera, citing procedures to investigate the terms and conditions for the legal framework compatible placement and recording through the video surveillance system in the context of compliance with the General Data Protection Regulation. In addition, the company stated that it is willing to comply with any judicial or prosecutorial order, if requested specifically and with reasons as to the permissibility and legality of the use by public authorities of the relevant evidence. The complainant again addressed via e-mail to the data controller on … and submitted a request with reference no. 11 of Directive 1/2011 of the Authority. On … he re-e-mailed the controller as he had not yet responded to his request. It is noted by the complainant that the relevant visual material from the cameras is necessary in order for him to prove the sole fault of the other I.X. in the car accident that took place on ... at ... the port of Heraklion and to claim compensation for the material damage suffered by his car from the competent insurance company. The Authority, in the context of examining the said complaint, sent to ΟΛΗ the document No. prot. C/EX/749/30-01-2020 informing him of the submitted complaint and asking for his opinions on the complainants . At the same time, he invited him to immediately consider the complainant's requests, satisfying the right to access the material from the video surveillance system, but without receiving a response from the data controller. Subsequently, the Authority invited

the data controller to a hearing, during which the said complaint was discussed, with document No. C/EX/7471/30-10-2020. At the meeting of 26-11-2020, B was legally present, as a representative of the complainant, who presented his views orally. Subsequently, the complainant was given a deadline and filed the memorandum No. G/EIS/8565/14-12-2020 on time. 2 In the aforementioned memorandum, the complainant claims that the reason he did not satisfy the subject's right concerned the long period of time that elapsed between the incident and the exercise of the said right (37 days later), while according to a relevant document of the company that supports the systems of OLI SA the data in the camera recorder are only kept for 6 days. He also invokes Directive 1/2011 of the Authority, according to which, "relevant information cannot be provided after 15 days", with the result that he cannot satisfy this specific right. In conclusion, according to the memorandum, the complainant should have been aware of the applicable law or asked about the incident the next day, not 37 days later. The Authority, after considering the evidence on the file, the hearing and the submitted memorandum after hearing the rapporteur and the clarifications of the assistant rapporteur, who then withdrew before the conference and decision, and after thorough discussion, CONSIDERED BY LAW 1. It follows from the provisions of Articles 51 and 55 of the General Data Protection Regulation (EU) 2016/679 (hereinafter "GDPR") and Article 9 of Law 4624/2019 (Government Gazette A´ 137) that the Authority has authority to supervise the implementation of the provisions of the GDPR, this law and other regulations concerning the protection of the individual from the processing of personal data. 2. Article 5 of the GDPR defines the processing principles governing the processing of personal data. Specifically, it is defined in paragraph 1 that personal data, among others: "a) are processed lawfully and legitimately in a transparent manner in relation to the subject of the data ("legality, objectivity, transparency"), b) are collected for specified, explicit and legitimate purposes and are not further processed in a manner incompatible with these purposes (…), c) are appropriate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimization") d) are accurate and, when necessary, updated, e) kept in a form that allows the identification of the data subjects only for the time required for the purposes of the data processing...('limitation of the storage period')'. 3 3. According to the provisions, from the provision of article 5 par. 2 of the GDPR it follows that the data controller bears the responsibility and must be able to prove his compliance with the principles of processing established in paragraph 1 of the article 5. As already judged by the Authority1, with the GDPR a new model of compliance was adopted, the central point of which is the principle of accountability in the context of which the controller is obliged to plan, implement and generally take the necessary measures and policies, in order the processing of the data is in accordance with the relevant legislative provisions. In addition,

the data controller is burdened with the further duty to prove himself and at all times his compliance with the principles of article 5 par. 1 GDPR. It is no coincidence that the GDPR includes accountability (Article 5 para. 2 GDPR) in the regulation of the principles (Article 5 para. 1 GDPR) governing the processing, giving it the function of a compliance mechanism, essentially reversing the "burden of proof" as to the legality of the processing (and in general the observance of the principles of article 5 par. 1 GDPR), shifting it to the controller,2 so that it can be validly argued that he bears the burden of invoking and proving the legality of processing3. Thus, it constitutes the obligation of the data controller, on the one hand, to take the necessary measures on his own in order to comply with the requirements of the GDPR, and on the other hand, to demonstrate his compliance at all times, without even requiring the Authority, in the context of research - of its audit powers, to submit individual – specialized questions and requests to establish compliance (APD 43/2019 sc. 9). 4. According to article 15 par. 1, 3 and 4 of the 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 so, the right to access the personal data and the following information: [...] 2. […] 3. The controller shall provide a copy of the personal data being processed. [...]". 1 See Authority decision 26/2019, sc. 8, 44/19 sk. 19 available on its website. 2 Relatedly see L. Mitrou, The principle of Accountability in Obligations of the controller [G. Giannopoulos, L. Mitrou, G. Tsolias], Collected Volume L. Kotsali – K. Menoudakou "The GDPR, Legal Dimension and Practical Application", 2nd ed. Law Library, 2021, p. 265 ff. 3 P. de Hert , V. Papakonstantinou, D. Wright and S. Gutwirth, The proposed Regulation and the construction of a principles-driven system for individual data protection, p. 141. 4In the context of the above right, it is pointed out that the data subject should have the right to access personal data collected and the concern and be able to exercise said right fluently and at reasonably regular intervals, in order to be aware of and verify the legality of the processing (see p. s. 63 GDPR). Therefore, in order to satisfy the right of access, it is not necessary to invoke a legitimate interest, since this exists and forms the basis of the subject's right of access to obtain knowledge of information concerning him and which have been registered in a filing system maintained by the data controller, so in order to realize the basic principle of the law for the protection of personal data, which consists in the transparency of the processing as a condition for any further control of its legality on the part of the data subject4. Similarly, it is not required to invoke the reasons why the data subject wishes to exercise the right of access. Besides, it should be pointed out that the satisfaction of the right of access is universal, i.e. it concerns all the information concerning the data subject and furthermore, it does not only require invoking the reasons why the data subject wishes to exercise said right, as discussed above, but neither mediation5. 5.

Because according to article 12 GDPR "1. The controller shall take appropriate measures to provide the data subject […] with any communication under Articles 15 […] 2. The controller shall facilitate the exercise of the data subjects' rights provided for in Articles 15 […] 3 .The controller shall 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. […] 4. If the controller does not act on the data subject's request, the controller shall inform the data subject, without delay and at the latest within one month of receiving the 4 See indicative APD 2/2020, 23/2020, 16/2017, 98/2014, 149/2014, 72/2013 and 71/2013. 5 See APD 16/2017. 5 of the request, for the reasons why he did not act and for the possibility of submitting a complaint to a supervisory authority and bringing legal action." Furthermore, for the more specific case of video surveillance systems, in 6. article 13 paragraph 1 of Directive 1/2011 of the Authority regarding the use of video surveillance systems for the protection of persons and goods it is provided that "The data controller has an obligation to grant within fifteen (15) days from the submission of the relevant application a copy of the part of the image signal registration where the subject of the data is recorded or a printed series of snapshots from the recorded images or, accordingly, to inform the interested person in writing within the same period of time either that it is not depicted or that the relevant part of the record has been corrupted. Alternatively, if the data subject also agrees, the controller can simply display, directly, the above section. To this end, the data subject must indicate the exact time and place he was found within the range of the cameras. When granting a copy of an image, the controller must cover the image of third parties (e.g. by blurring part of the image), since their right to privacy may be violated. In the case of simple demonstration, covering the image of third parties is not necessary." It should be noted that the period of fifteen (15) days, which is provided for in article 13 paragraph 1 of Directive 1/2011 of the Authority, after the implementation of the GDPR has been extended to thirty days. 7. According to article 8 of Directive 1/2011 ("Compliance period"): "1. The data must be kept for a specific period of time in view of the intended purpose of processing each time. In any case, as long as the taking of stored images or the taking done in real time does not result in the occurrence of an event deviating from the intended purpose, the data must be destroyed within fifteen (15) working days at the latest, subject to more specific provisions of the existing legislation that apply to specific categories of processors (e.g. casinos) or if otherwise specified in this Directive. 2. In the event of an incident (e.g. theft, robbery, beating) against the person or property of

the controller, he is allowed to keep the images in which the specific incident is recorded in a separate file for 30 days. 3. If the incident concerns a third party, the controller is allowed to keep the images for 3 months.' 8. Before the implementation of the General Regulation (EU) 2016/679 for the protection of natural persons against the processing of personal data and for the free movement of such data (hereinafter, the Regulation), which has been in force since May 25 2018, regarding the issue of the use of video surveillance systems for the purpose of protecting persons and goods, the Authority had issued Directive 1/2011 (available on its website www.dpa.gr), which must be interpreted in accordance with the new provisions of the Regulation. This applies in particular to the obligations of the controller included in chapter C' thereof (articles 10 to 13). For example, data controllers no longer have the obligation to notify the Authority6 of the processing, but must ensure that the enhanced rights provided for in the Regulation are met. In this case, as it appears from the data of the 9th case file, the complainant invoking his status as the subject of the personal data (image data) concerning him and identifying him as the driver of a car with a visible registration number who was involved in a traffic accident and which were recorded by the video surveillance system of OLI legally exercised on ... the according to art. 15 GDPR right of access by which he requested to be informed about a series of information concerning his person regarding a traffic incident that had taken place on … . OLI initially responded to the above request with his letter from ..., within the deadline, refusing to grant the right of access citing on the one hand the ongoing process of compliance with the requirements of the GDPR and the investigation of the legality of the operation of the video recording system, on the other hand, that he is willing to comply with a court or prosecutorial order to release the material. From the above, it is established that OLI on ... had at its disposal the disputed material which included the complainant's personal data and had not yet deleted it. The Authority comes to this conclusion as, firstly, if OLI had deleted the image data at the time of submitting the access request, it would have informed the applicant of the fact of the deletion and there would have been no need to invoke the ongoing compliance process, nor the need issuance of a judicial or prosecutorial order. In addition, from the same answer, the Authority finds that the image data in question was kept in the OLI system and had not been deleted, but due to the implementation of the General Protection Regulation 6 See and the Authority's announcement regarding the abolition of record keeping/editing notices and the granting of licenses (Decision 46/2018). 7 Data no. 679/2016 from 25.5.2018 in accordance with article 99, there were doubts as to the legality of their retention, which is why reference is made to "[…] a process of investigating the terms and conditions for the placement and registration compatible with the legal framework through video recording system at OLI S.A.…. We are prepared to comply with any

judicial or prosecutorial order....as to the permissibility and legality of the use by public authorities of the relevant evidence." The more specific reference to "permissible and lawful use by public authorities of the relevant evidence" proves that the complainant's image data, along with of course all other image data included in the system and relating to other natural persons, was retained indefinitely and the ALL maintained doubts, both about the legality of the system's operation, and about the legality of maintaining them or not. It should also be pointed out that while OLI, as data controller, should have complied with the requirements of the GDPR in relation to the legal operation of the video recording system from 25.5.2018, however, eighteen (18) months later, on... , time of response to the complainant, was still in compliance process, by his express admission. 10. With his application from ... to ALL, the complainant once again exercised the right to access his personal data and additionally requested the retention and non-deletion of the disputed material, while on ... he repeated his requests noting that he did not receive any response. Indeed , OLI did not respond at all to the following, ofinitially, requests of the complainant. OLI, with its 10-12-2020 hearing memorandum to the Authority, argued for the first time and only before the Authority (without ever informing the complainant) that at the time of submitting the complainant's first request for access to the requested personal data had already been deleted given that according to the relevant document of the company that supports the cameras they are kept for six (6) days, while according to Directive 1/2011 of the Authority no data can be given after the lapse of 15 days. 11. From all of the above it follows that OLI violated the provisions of articles 15 par. 1 in combination with art. 12 par. 1, 2 GDPR. In particular, OLI as data controller had to respond, even if negatively, to the request of the complainant as a data subject regarding whether it has collected and maintains his personal data (StE 2627/2017 and APDPX 43/2019). ALL instead of responding with his letter from ... that he no longer has the recordings of the image data due to their deletion after the six (6) day period during which the personal data was kept in the video recording system, according to what later argued in his pleading before the Authority, he ultimately responded to the complainant that he is in the process of complying and that he is willing to comply with a court or prosecutorial order to release the material. If ALL had deleted the image data within six (6) days of the collection and recording of the material, it would have responded to the complainant that it was objectively unable to satisfy its right of access as according to its internal policy it would have already been deleted, in accordance and with what was accepted above in no. 10 thought. It was therefore established that what OLI first claimed in its memorandum before the Authority did not correspond to reality and that at the time of submitting the first request for access to the complainant's personal data, he had not deleted his personal data, but instead kept it and therefore without legal reason

did not answer the complainant if he keeps his personal data, nor did he provide him with access to them, without any legal case and without invoking against the complainant any legal reason for refusing to satisfy his right of access. Similarly, OLI did not respond to the complainant's two (2) subsequent access requests, to which he did not provide any response. Therefore, it is established that OLI violated the complainant's right of access according to art. 15 par. 1 in combination with art. 12 par. 1, 2 GDPR and 13 par. 1 of Directive 1/2011. 12. It should be pointed out that while OLI claims that according to the relevant document of the company that supports the cameras, the image data is kept in the system for six (6) days and then deleted, however, it never presented it before the Authority , but neither provided relevant documentation of the legality of the operation of the video surveillance system in relation to the retention time of the data, e.g. by presenting the corresponding Video Surveillance System Installation and Operation Policy or Personal Data Preservation Policy pursuant to art. 24 GDPR, in the context of compliance with the principles of processing according to art. 5 para. 1 GDPR (in particular para. c' and e'), as he must according to art. 5 para. 2 GDPR based on his accountability obligation as data controller, without having to be requested by the Authority (see APD 43/2019 sc. 6). Based on the above, the Authority considers that there is a case to exercise its corrective powers in accordance with 13. article 58, paragraph 2 of the GDPR in relation to the established violation 9 and that it should, based on the circumstances established, be imposed, according to implementation of the provision of article 58 par. 2 sec. i of the GDPR, an effective, proportionate and dissuasive administrative fine according to article 83 of the GDPR, both to restore compliance and to punish illegal behavior7. Furthermore, the Authority took into account the criteria for measuring the fine that 14. are defined in article 83 par. 2 of the GDPR, paragraph 5 subsection b' for the violation of the rights of the subjects provided for by the same article and applicable to the present case, as well as the Guidelines for the application and determination of administrative fines for the purposes of Regulation 2016/679 issued on 03-10-2017 by the Article 29 Working Group (WP 253) in combination with the actual data of the case under consideration and in particular: i. ii. iii. iv. v. The fact that OLI failed to satisfy the complainant's right of access while knowingly retaining the requested image data in the system. The fact that OLI invoked the first and only before the Authority that at the time of submitting the access request it had deleted the complainant's image data while it was found that it had kept it and had not deleted it. The fact that while OLI, as data controller, should have complied with the requirements of the GDPR in relation to the legal operation of the video recording system from 25.5.2018, however, eighteen (18) months later, on ..., response time to complainant, was still in the compliance process, by his express admission. The fact that while the complainant, after the initial request to exercise the right of access, came back

two more times with a supplementary request for access and preservation - non-deletion of the data, nevertheless OLI never responded, even negatively. The fact that the non-satisfaction of the right of access in this case affected one (1) natural person as the subject of the personal data. 7 See OE 29, Guidelines and the application and determination of administrative fines for the purposes of Regulation 2016/679 WP253, p. 6 10 vi. vii. viii. ix. x. xi. xii. The fact that the violation of the right of access did not concern personal data under Articles 9 and 10 GDPR, according to the information brought to the attention of the Authority. The fact that the violation of the right of access is attributed to a conscious choice of OLI as while the image data of the complainant was knowingly kept in its systems, on the one hand it chose not to satisfy the right of access, on the other hand, it was invoked before the Authority with the hearing memorandum that the data in question had been deleted at the time the right of access was exercised, while it had not been deleted and was kept in its system. The fact that the violation of the provisions regarding the violation of the rights of the subjects fall under, in accordance with the provisions of article 83 par. 5 sec. 2nd GDPR, in the highest prescribed category of the classification system of administrative fines. OLI's lack of cooperation with the Authority as, on the one hand, it did not respond to the Authority's initial document, on the other hand, with its hearing memorandum it presented for the first time as a reason for denying the satisfaction of the complainant's right of access the alleged deletion of personal data the time of exercise of the right, when in fact the image data had not been deleted and was knowingly retained in his system. The absence of previous established violations of the complainant as a relevant audit shows that no administrative sanction has been imposed on her by the Authority to date. The fact that from the data brought to the attention of the Authority and based on which it established the violation of the GDPR, the data controller did not obtain a financial benefit, nor did it cause material damage to the complainant. The fact that according to the published financial statements of the company for the year from 01-01-2020 to 31-12-2020 the turnover of OLI amounted to the amount of 4,585,382 euros. Based on the above, the Authority unanimously judges that OLI S.A. should be imposed. as a data controller, the administrative sanction referred to in the ordinance, which 11 is judged to be proportional to the gravity of the violation. FOR THESE REASONS THE AUTHORITY IMPOSES the Heraklion Port Authority S.A. the effective, proportional and dissuasive administrative monetary fine appropriate to the specific case, according to the specific circumstances thereof, in the amount of thirty thousand (30,000.00) euros for the violations of articles 15 par. 1 cond. 12 par. 1, 2 GDPR and 13 par. 1 of Directive 1/2011 and in accordance with articles 58 par. 2 item. i' and 83 par. 5 item. II GDPR. The Deputy President Georgios Batzalexis The Secretary Irini Papageorgopoulou12