Athens, 26-08-2021 Prot. No.: 1947 DECISION 36/2021 (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 17/2/2021 and 10:00 a.m., in order to examine the case referred to in the present history. The meeting was attended by teleconference by Georgios Batzalexis, Deputy President, in opposition to the President of the Authority, Konstantinos Menoudakos, and the alternate members Evangelos Papakonstantinou and Grigorios Tsolias attended as rapporteur. They did not attend due to disability, although regular members Charalambos Anthopoulos and Konstantinos Lambrinoudakis were legally summoned in writing. The meeting was attended, by order of the President without the right to vote, by Haris Symeonidou, specialist scientist - auditor as assistant rapporteur and Irini Papageorgopoulou, employee of the Administrative Department of the Authority, as secretary. The Authority took into account the following: With no. prot. C/EIS/5208/24-07-2020 and C/EIS/6315/16-9-2020 his complaints to the Authority, A complains that the company Dixons South East Europe AEVE-KOTSOVOLOS (hereinafter "Company") and the National Bank of Greece (hereinafter "Bank"), respectively, do not satisfy the right of access to his personal data. In particular: I.A) According to the first complaint above, the complainant, after returning a product he had purchased from the Company in installments to his credit card, issued by the Bank, and after finding that the installments continued to be charged every month and to be credited the next, he complained about it to the Company and in communication he had with its representatives via Facebook, 1 Kifisias Ave. 1-3, 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr informed that a request to mature the installments has been submitted to the Bank. Following this, according to the complaint, on 6/26/2020 the complainant requested to be notified of the Company's request to the Bank regarding the discharge of his credit card installments. The response of the representatives of the Company was negative, on the grounds that "the communication that has been carried out with the bank constitutes an internal communication and it is not possible to share it". In the context of investigating the complaint, the Authority sent the no. prot. C/EX/5208-1/11-08-2020 letter to the Company, requesting its opinions on the reported facts, but also to clarify in particular, whether the complainant exercised, as he states, a right of access to data that concern, as well as whether and how the complained-about Company responded to his above-mentioned request, attaching in particular the complainant's request, so that it is clear what he requested, when and on what basis, the possible response of the Company, and any relevant with the item case. With the no. prot. C/EIS/6044/08-09-2020 (which was sent again in a more readable form with no. prot. C/EIS/6065/08-09-2020) its document to the Authority, the Company claimed the following : - After the product was returned by the complainant on

22/5/2020, the Company carried out all the necessary actions to debit the complainant's card, i.e. sent to the cooperating bank (Alpha Bank) that handles credit card transactions cards, the file with all the transactions of the day, so that she in turn can make the necessary entries by informing the issuing banks of the customers' cards, in accordance with the procedure provided for in the agreements between them. - The complainant, on 22/7/2020, contacted the Company via a message on Facebook stating that the total amount of the purchase had not been released to his card but the installments were offset monthly (i.e. that the charge for the canceled transaction was not deducted in total but a charge was made and automatic credit of each installment each month). The Company maintains that it replied to the complainant that all the necessary actions had been taken towards the liquidating Bank (Alpha Bank), and that the method of offsetting the canceled charge on his card does not depend on it but on his contract with the issuer Bank and its policy; therefore referred him to the bank that had issued his card. However, because the complainant insisted, saying that according to the Bank the relevant procedure should be carried out by the 2nd Company, the complained Company, "in the context of goodwill, despite the fact that the specific procedure escaped its responsibilities", as it claims, contacted 'exception of the procedure with the bank cooperating with it (Alpha Bank) and through it a request for maturity of the installments was forwarded to the issuing bank of the card (National Bank) and then, in its response, it informed the complainant "that a request for maturity has been submitted installments to the issuing Bank, namely the National Bank through our partner. Our Company forwarded the said request to Alpha Bank and Alpha Bank in turn forwarded the request to the issuer since, as mentioned above, our Company does not know which is the issuing Bank of each card, from which the transaction has been carried out. » The complained Company also maintains that the complainant, invoking the right of access to his personal data, requested to be given the Company's internal correspondence with the Bank, through which it appeared that the said request had indeed been submitted. However, according to the Company's response, this claim, on the one hand, does not fall under the right of access according to article 15 of the General Data Protection Regulation (GDPR), on the other hand, corporate correspondence is protected by confidentiality according to article 19 of the Constitution. Therefore, according to the complained Company, the complainant's request did not constitute an exercise of his right of access as a subject to his personal data. In this context, the Company also initially asserted that "there was never any request made by the complainant regarding the above, but all communication was made through messages (chat) on our Company's social networking page on Facebook.". In view of the above, the basic positions and claims of the Company initially consist in the fact that a) the said request of the complainant does not constitute an exercise of the right of access to his

personal data, as the internal correspondence of the company does not constitute personal data of the customer, it is confidential and is protected by the constitutional provisions of increased formal force, and that b) even if it is considered that the request in question concerns the right of access of the subject, the Company provided the customer with all the necessary information, i.e. that his request was forwarded by the Company to the Bank . In support of its claims, the Company cited the complainant's conversations via Facebook messenger messages to its page. These conversations are dated 6/26/2020 and it appears from them that the complainant asked: "what actions have been taken?" Has the bank been informed?' and stated that "from bank 3 they told me that they do not have any request. They asked me in which bank it was made and the receipt so they could investigate it." The responses that appear to have been given by the Company's representatives were as follows: "Your request for maturity of installments has been submitted to the issuing bank", "A request has been forwarded to the bank of the card that has been charged and we have detected that you have received the receipt by email of the cancellation", and "The request to the bank has been registered. The communication that has been made with the bank is an internal communication and it is not possible to share it. The proof of cancellation you have received confirms the cancellation request you have made. On the part of our company, all the necessary actions have been taken in order to promote your request". Following this and given the Company's claim that "there was never any request made by the complainant regarding the above, but all communication was made through messages (chat) on our Company's social networking page on Facebook", the Authority with no. prot. C/EX/5208-2/27-10-2020 its letter to the Company requested to be clarified within 15 days, if this claim means that in the Company's opinion the right of access was never exercised by the complainant and it was requested to sent the written Policy and Procedure followed by the Company regarding the management of the access requests of the subjects, on the basis of which the Company refused to satisfy the relevant request. After two requests by the Company (under no. prot. C/EIS/7538/03-11-2020 and C/EIS/8087/24-11-2020) for an extension of the response deadline to the above document, of which the the second was not accepted (see the Authority's response document under no. prot. G/EX/8087-1/27-11-2020), with the under no. first C/EIS/8333/04-12-2020 its document, the Company responded that in its opinion a) the requested electronic document does not include personal data of the complainant and b) the exchanged electronic documents of the complained Company with third parties through payment systems are confidential under contractual obligations and therefore any their disclosure to third parties entails the relative responsibility of the Company. Therefore, the reasoned rejection of the complainant's request on its part must be considered correct. Despite this, however, it

stated its intention to eventually bring the relevant electronic document to the attention of the complainant, considering the Authority's document "as a legal basis for the removal of our contractual confidentiality obligations". The Company also pointed out that as a controller it provides three ways to exercise the rights of the subjects under the GDPR (physical presence, letter 4 to the Administration Offices, or e-mail to PersonalData@kotsovolos.gr), without however submitting requests in other ways (such as, in this case, via messages on a social network) affect the legality of the submission, although it may have an impact on the company's response times, for organizational reasons. The Company, responding to the relevant question of the Authority regarding whether it considered the communication in question and the complainant's request as an exercise of the right of access to his personal data, clarified that its relevant claim had the meaning that "[…] due to the instrument, which used by the complainant (through messages (chat) on our company's social networking page on Facebook) but also due to the number of messages, which were exchanged on a series of topics, the relative request of the complainant was not clear that it constituted a request for the exercise of the right access based on Article 15 of the GDPR". Finally, with the same document, the Company notified the Authority of its corporate "Instruction for the Management of Personal Data Subject Requests", which, according to the same response, has been communicated to all staff and is followed when processing personal data subject requests in accordance with articles 12-23 of the GDPR. At the same time, with the under no. prot. C/EX/5208-3/27-10-2020 its document, the Authority asked the complainant to clarify a) how exactly he exercised the right of access to his personal data, according to the complaints and b) if for the satisfaction of the right of access he has exercised requires, in his opinion, the notification of the company's correspondence with the bank in its entirety (i.e. by providing a copy of the relevant letter/e-mail) or his request could also be satisfied by the notification of the data concerning the correspondence in question (e.g. date and addresses of sending/receiving the e-mail, any protocol numbers, etc.), so that it may end up with the same result. With the nos. prot. C/EIS/7419/29-10-2020 and C/EIS/7498/2-11-2020 his response documents to the Authority, the complainant replied that his request was submitted via facebook messenger and that for his satisfaction he would it was sufficient to inform him of the details of the request (of the Company to the Bank), i.e.: Date, from which department of the Company it was made, to whom, protocol number and proof that the recipient received it, as the complainant had been informed via messenger. In continuation of the above, the complainant through his electronic communication with the Authority on 11/1/2021 and 18/1/2021 stated that he did not receive any information from the Company, despite what was mentioned in no. prot. C/EIS/8333/04-12-2020 document of the latter. 5 I.B) According to the second above complaint (prot.

no. C/EIS/6315/16-09-

2020), the complainant, in his letter dated 06/07/2020 to the Bank, requested to be notified whether a request has been submitted by the Company for the maturity of the installments and the release of the amount charged to his credit card for a product that has be returned, a request to which, as the complainant states, he received no response, despite the lapse of two months. In the context of examining this complaint, the Authority sent the complained Bank the no. prot. C/EX/6315-1/08-10-2020 its document for the provision of opinions, asking for clarification in particular whether the complainant exercised, as he states, a right of access to data concerning him, as well as if and how the Bank in its above request, including in its response every element relevant to the case. Then, with the no. prot. C/EIS/7505/02-11-2020 in its document the Bank argued that the complainant's request which was initially submitted by phone and then, following guidance from the Branch [region] X, through the Bank's form on 6/7 /2020, did not concern the exercise of a GDPR right on his part, but his information on the method of refunding money from a third company trading consumer goods, for a transaction which was carried out by charging a card issued by the Bank, but was settled through another bank with the with which the company involved cooperates. Furthermore, according to the Bank's response, during the period when the said case was under investigation, the complainant addressed the Consumer Advocate, submitting a relevant complaint against the Company, which was forwarded on 22.9.2020 to the Bank for its views. As the Bank maintains, the latter responded to the Consumer Advocate regarding the procedures related to the transaction and the manner of debiting and crediting the installments of the complainant's credit card, communicating its response to the complainant. In view of the above, the Bank claims that the relevant request, which did not concern the exercise of a GDPR right, was examined by it and the appropriate actions were taken, of which the complainant was immediately informed, based on the procedure followed by the bank for responding to requests received through supervisory authorities. 6 Subsequently, the Authority, with no. prot C/EX/508/28-01-2021, C/EX/511/28-01-2021 and C/EX/512/28-01-2021 Summons invited the involved parties to a hearing at the meeting of the department of 03 /02/2021. During the hearing, the parties developed their views and were given a 10-day deadline to submit briefs. During the hearing of 02/03/2021, the complainant, the attorneys-at-law of the complained-about company KOTSOVOLOS, Apostolos Nicolaidis (A.M. ...) and Antonios Broumas (A.M. ...) appeared, while on behalf of the National Bank, B , Head of the Directorate …, B, Executive of the Directorate …, C, Executive of the Directorate …. Also present were ..., DPO of the Bank and ..., Deputy DPO, who did not take the floor. The parties involved were given, during this meeting, a

deadline and submitted in due time, the complainant the no. first G/EIS/961/08-02-2021 and G/EIS/962/08-02-2021 memoranda, and the Company no. prot. C/EIS/1111/15-02-2021 its memorandum, while the Bank did not file a memorandum. In particular, with regard to the first complaint, the complainant argued that, despite his request for installments to mature, the installments continued to be debited and credited, while according to telephone information he had from both National Bank and Alpha Bank, no relevant request had been submitted by the Company. In his telephone communications with the various departments of the Company, all the employees declared themselves incompetent and he never managed to speak with a supervisor or manager, despite the assurances of the employees that they would call him. According to the complainant, finally, there was no issue of a "gray zone", as the Company claimed during the hearing, but of "complete indifference and contempt" towards him as a data subject. The Company, during the meeting, after stating that it withdraws, does not reinstate and does not support the legal claims it had submitted during the pre-hearing stage, supported both orally and later with its memorandum the following: - That it is mainly a consumer dispute (procedure for canceling a transaction and debiting the complainant's card) in respect of which she fulfilled all her obligations, and the complainant's complaints mainly concern the provisions of Law 2251/1994 on consumer protection and the provisions of Law 4537/2018 for payment services. - That the complainant's request for access to the installment maturity request was submitted via facebook messenger in the context of a multi-day conversation, and the employees who manage the Company's social media, although they have been notified 7 the relevant Guidelines for the management of subject requests under the GDPR, did not properly evaluate the complainant's request and did not assess it as an exercise of the right of access, which is due to a) their reduced readiness to accept such requests, due to the nature of their work (as usual manage requests concerning offers, after-sales service, damages, etc.), b) that a customer had never been asked in a similar case to forward corporate correspondence with the bank, c) that the complainant's complaint was mainly of a consumer nature, d) the number of messages exchanged (over 50). - That on 6/22/2020 the complainant received the information in writing that "As an exception to the process, a request for maturity of installments has been forwarded", therefore, according to the Company, "from the beginning the customer had at his disposal and knew from his communication with the our company, the date of submission of the request by our company to the cooperating bank Alpha Bank (22.6.2020)". - That, in this case, whether it was a right of access based on Article 15 GDPR belongs to a "grey zone", due to its conflict with commercial confidentiality, that is, with the explicit contractual obligation of the Company to maintain the confidentiality of the information it exchanges with Alpha Bank. The relative weighting, judged by the

circumstances, is not self-evidently in favor of satisfying the complainant's request. However, according to the Company's claims, although the complainant did not initially receive the document he requested, "[…] but as early as 22.6.2020 he received information about the time of its submission, about the recipient which was Alpha Bank, etc. so with suitable alternative measures, our company [...] provided the complainant with sufficient data and information for the processing of his data and for the manner and time of submitting the maturation request in order to serve his request". - That the Company brought the question of weighting to the attention of the Authority, in order to immediately grant the document "if deemed relevant", not for the purposes of attraction but "for the purpose of legal certainty and harmonization based on the interpretation of the law by the supervisory authority itself authority" and that after receiving from the Authority its summons to a hearing, it then finally proceeded to satisfy the right of access. - That, finally, on 3/2/2021 the Company sent the body of the request (the requested document) by e-mail to the complainant, who replied on 8/2/2021 that "[…] after so many months, he has not no importance. I told you again and again that the bank does not know anything about maturity and you did not care", an answer from which it follows, according to the Company, that the complainant himself treats the dispute as consumer in nature. 8 - In the alternative and for the case where it is judged that there is a violation of the provisions of the GDPR, the Company invoked the special circumstances that must be taken into account in the context of the application of article 83 par. 2 of the GDPR (an individual incident concerning a subject is due to negligence', full satisfaction of the right in the end, lack of previous violations by the data controller, lack of financial benefit from the violation). Finally, the Company provided the form of Instructions for the Management of Requests of Personal Data Subjects, stating that it is committed to re-evaluate it regarding the referral of cases within the Company, in view of the questions submitted by the Authority in the context of the hearing. It is noted that, although in the context of the hearing, the Company was asked if it has appointed a Data Protection Officer (DPO), and in case of an affirmative answer, if his opinion was sought on the case in question, the relevant question was not answered either during the meeting or through of the memorandum. The Authority has not been notified of the appointment of the Company's DPO. Regarding the second complaint, the complainant repeated what was stated in his complaint and complained that the Bank did not provide him with the information he requested (confirmation if there is a request for maturity of installments for his card). The Bank, during the meeting of 3/2/2021, argued that the complainant's case in question did not concern the exercise of the right of access based on Article 15 of the GDPR, but his information on how to refund money from a transaction made with bank card, and did not file a statement after the hearing. The Authority, from the hearing procedure,

from the elements of the case file, as well as from the memoranda submitted to the Authority and after hearing the rapporteur and the assistant rapporteur, who left after the discussion of the case and before the conference and the taking a decision and after thorough discussion, IT WAS CONSIDERED IN ACCORDANCE WITH THE LAW 1. 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 (Official Gazette A΄ 9 137) 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 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”) (…) ». 3. According to the provisions, from the provision of article 5 paragraph 2 of the GDPR it follows that the controller bears the responsibility and must be able to prove his compliance with the principles of processing established in paragraph 1 of article 5 As the Authority1 has already judged, 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 data controller is obliged to design, implement and generally take the necessary measures and policies, in order for the data processing to be in accordance with the relevant legislative provisions. 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 an obligation of the controller on the one hand to take the necessary measures on his own in order to comply with the requirements of the GDPR, on the other hand, 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. 10 to prove its above compliance at any time, without even requiring the Authority, in the context of exercising its investigative and auditing powers, to submit individual - specialized questions and requests to ascertain compliance. 4. According to the definitions of article 4 no. 1 and 2 GDPR "means "personal data": any information concerning an identified or identifiable natural person ("data subject"); an identifiable natural person is one whose identity can be ascertained, directly or indirectly, in particular through reference to an identifier such as a name, an identity number, location data, an online identifier or one or more factors that characterize the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person' . 5. According to recital 26 of the Preamble of the Regulation, "The principles of data protection should be applied to any information that concerns an identified or identifiable natural person". According to Opinion 4/2007 of OE 29, the term "personal data" includes information that touches the private and family life of individuals in a narrow sense, but also information that concerns any activity of the individual, such as employment relationships or the financial or social behavior of the individual. It therefore includes information about individuals, regardless of the position or status of the persons in question (consumer, patient, employee, customer, etc.). The term includes information that is available in any form. Information can be considered to "relate" to an individual when it relates to that individual, i.e. when by reason of its content, purpose or effect it is linked to a specific person, and its use is capable of impacting on the rights and his interests4. In some cases, the information contained in the data primarily concerns objects, which usually belong to someone or affect someone, so indirectly it can be considered that the information refers to the persons in question.5 6. According to the provisions of article 15 par. 1, 3 and 4 GDPR: "1. The data subject has the right to receive from the data controller confirmation as to whether or not the personal data concerning him/her exist 4 Cf. CJEU C-434/2016 Nowak decision of 20/12/2017 par. 34-39.5 Opinion 4/2007 of OE 29 on the meaning of the term 'personal data' p. 7-10. 11 processing and, if this happens, 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 shall be provided in a commonly used electronic format. 4. The right to receive a copy referred to in paragraph 3 does not adversely affect the rights and freedoms of others.' According to the reason GDPR Recital 63 “This right should not adversely affect the rights or freedoms of others, such as professional secrecy or intellectual property rights and, in particular, copyright protecting software. However, these factors

should not have the effect of refusing to provide any information to the data subject." Furthermore, according to paragraphs 1-4 of article 33 of Law 4624/2019, "1. Apart from the exceptions provided for in paragraph 2 of article 29 and paragraph 2 of article 30, the right of access of the data subject, in accordance with article 15 of the GDPR, does not apply when: a) the data subject is not informed in accordance with item bb' of cases a' and b' of paragraph 1 of the previous article; or b) the data, aa) were recorded only because they cannot be deleted due to legal or regulatory provisions of the obligation to preserve them, or bb) serve exclusively protection or control purposes of the data, and the provision of information would require a disproportionate effort and the necessary technical and organizational measures make processing for other purposes impossible. 2. The reasons for refusing to provide information to the data subject must be documented. The refusal to provide information must be justified to the data subject, unless the disclosure of the factual and legal reasons on which the refusal is based would jeopardize the purpose pursued by the refusal to provide the information. Data stored for the purpose of providing information to the data subject and for the preparation of this provision may only be processed for this purpose and for the purposes of personal data protection, processing for other purposes is limited in accordance with Art. 18 of the GDPR." and according to article 32 of Law 4624/2019: "1. The obligation to inform the data subject in accordance with article 14 12 paragraphs 1, 2 and 4 of the GDPR does not exist, when the provision of the information: [...], b) in the case of private entities: aa) would damage the establishment, exercise or support of legal claims or the processing involves personal data from contracts drawn up under private law and aims to prevent damage from the commission of criminal offences, unless the data subject has an overriding legitimate interest in providing information; or bb) the competent public body has determined to the controller, that disclosure of the data would endanger national defense, national security and public safety, in the case of data processing for law enforcement purposes, no determination is required in accordance with the first paragraph. 2. If no information is provided to the data subject in accordance with paragraph 1, the controller shall take appropriate measures to protect the legitimate interests of the data subject, including providing the public with the information referred to in Article 14 paragraphs 1 and 2 of the GDPR in an accurate, transparent, understandable and easily accessible form, in clear and simple language. The data controller shall state in writing the reasons for refraining from providing information. 3. The obligation to inform the subject of personal data in accordance with Article 14 paragraphs 1 to 4 of the GDPR, except for the exceptions mentioned in Article 14 paragraph 5 of the GDPR, does not apply to the extent that through its fulfillment information would be disclosed, the which due to their nature, in particular due to the superior legal interests of a third party, must remain

confidential". Finally, according to Article 12 para. 3 and 4 GDPR "The data 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. 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. 4. If the data controller does not act on the request of the data subject, within one month of receiving the request, he informs the data subject of the reasons why he did not act and of the possibility of filing a complaint with a supervisory authority and taking legal action appeal". 7. In this case, from the information in the file and from the hearing, the following emerged: With his requests of 22/6/2020 and 26/6/2020 to the representatives of the Company via the facebook messenger service, the complainant requested to be notified of information regarding the debiting process of his credit card and specifically to be notified of the Company's request to the Bank for the total release of the installments due to product return. The complainant addressed a similar request to the Bank on 7/6/2020. The content of the Company's request to the Bank includes information regarding the progress of a specific transaction of the complainant, as the subject of the data, with a certain store and in relation to the purchase of a certain product. The said information concerns the complainant, who is specifically identified as a natural person. The mere mention of his name in the relevant correspondence makes the complainant immediately identifiable as a natural person. From this additional information, various conclusions can be further drawn regarding the transactional behavior of the subject, his consumer preferences in view of and the fact of returning the product as well as his financial options based on the fact of crediting the amount in one time or in installments , the value of the product, etc. The use of this information is capable of having an additional impact on his rights and interests, as it directly affects the ability to use his credit card for the amount of money that has been pledged. Therefore, in view of the above, the said request of the Company to the Bank, includes information "directly concerning" a certain known natural person who is identified. Therefore, the complainant as a data subject had, according to article 15 par. 1 GDPR, the right to receive from the complained companies, in their capacity as data controllers, confirmation of the processing of his personal data and access to the relevant information concerning the entire process of paying off the installments. It is also possible for the subject to exercise further rights, e.g. correction, in the event that some information concerning his transaction and its cancellation, has not been correctly transferred in the present

request to the bank (see also CJEU case C-434/16, Nowak s. 57). 14 In conclusion, the complainant, through his requests, exercised the right provided by the GDPR to access his personal data against both complainants, without being required to be surrounded by a specific formula or to be exercised in a solemn manner, nor to include the reasons for the which the data subject exercises the right of access (GD 16/2017 sc. 3). Regarding the second complained Bank, a more detailed report will be made below. 8. The obligation of the complainants to satisfy the complainant's right specifically by providing a copy of their relevant correspondence, which the Company characterizes as professional, depends on whether the circumstances of par. 4 of article 15 GDPR are met in this case, i.e. if the satisfaction of the right adversely affects the rights and freedoms of others. The first complained Company initially rejected the complainant's request to receive a copy of the correspondence citing the confidentiality of communications no. 19 para. 1 S., a claim that he withdrew and did not resubmit at the hearing. Further rights of third parties that could be affected in this case are mainly personal data (e-mail addresses and any names) of the employees of the complainants who are the parties to the communication (sender and recipient or intermediate transmissions-promotions). In addition, the e-mail could also include information protected by professional-commercial confidentiality, such as indicatively related to charge cancellation procedures, which may be included in confidentiality agreements. However, these factors should not have the effect of refusing to provide any information to the data subject (see request s. 63 GDPR) and the data controller must according to article 12 par. 1 in conjunction with article 24 para. 1 GDPR to take appropriate measures to provide the data subject with any information referred to in Articles 13 and 14 GDPR and any communication within the framework of Articles 15 to 22 and Article 34 GDPR. In addition, and regardless of the application or not of the provision of article 15 par. 4 GDPR which concerns exclusively the provision of a copy and satisfaction of the subject's right of access, the complainant's right of access could in principle be satisfied by the notification of a copy of the electronic mail with the addresses of the parties and their names deleted (masked) and with visible only the part of what concerns the transmission of the complainant's data. 15 Alternatively, as he stated with no. prot. C/EIS/7498/2-11-2020 his response document to the Authority the complainant, only the information corresponding to his right of access could be communicated by the Company, i.e. the date of shipment, the sender (as a department of the first complained-about Company), the recipient (bank/department), as well as the protocol number and proof of receipt, if any, without having to be given a copy of the electronic correspondence, even with deleted information. Under the above two (2) versions, on the one hand, the right of access of the data subject would have been satisfied without raising the issue of endangering any

commercial or other related privacy, on the other hand, the principle of data minimization would have been applied in an appropriate way. In any case, the right of access can be satisfied without granting copies, while whenever the data subject requests the satisfaction of the right of access by granting copies, the data controller can satisfy it by providing the relevant information without granting and a copy of them, as long as such a choice is based on the provisions of the GDPR and the current national legislation and the relevant reasons are present. 9. In addition, the Company's refusal to satisfy the complainant's right of access was not sufficiently documented and justified, but the Company contented itself with reporting that "the communication that has been carried out with the bank constitutes internal communication and there is no possibility of sharing it". The said claim was withdrawn by the Company during the hearing as mentioned above. In any case and regardless of the validity of the above claim, the Company should, refusing to satisfy the right of access, respond by rejecting it by quoting in detail and substantiated the relevant reasons. From the submitted documents (see related communication via facebook messenger: "As an exception to the process a request for maturity of installments has been forwarded" on 22/6/2020, "Your request for maturity of installments has been submitted to the issuing bank", "It has been forwarded request to the bank of the card that has been charged and we have detected that you have received the proof of cancellation via email", and "The request to the bank has been registered. […] On the part of our company, all necessary actions have been taken to promote the your request" on 6/26/2020) it appears that the Company, despite its claims to the contrary, did not follow any of the above options (either the granting of the document, possibly with the data of third parties covered, or the 16 justified refusal to grant it document while simultaneously providing the information that interested the applicant - complainant) and in particular, it did not provide, as it claims, as an alternative way of satisfying the right "all necessary information" to the complainant. From the above information which is shown to have been given to the complainant, it was not clear either the date of the request for the maturity of the installments or to which bank it was addressed (i.e. the Alpha Bank with which she cooperates or the National Bank which is the issuer of the card of the complainant), so that based on this information, the data subject is given the opportunity to know, on the one hand, to which recipient his personal data was shared, and on the other hand, where he will exercise his rights. After all, from the same document it appears that the complainant on 26/6/2020 made an explicit reference to "his personal data", which negates the validity of the Company's claims regarding the alleged ambiguity of the request and the unpreparedness of its employees who manage the Social Media to accept requests to exercise GDPR rights. In particular, the e-mail of the complainant from 26/6/2020 had the following content: "The request to the bank has been

registered. The communication that has been carried out with the bank is an internal communication and it is not possible to share it. The proof of cancellation you have received confirms the cancellation request you have made. On the part of our company, all the necessary actions have been taken to forward your request." In response to the latter, the complainant retorted that ""internal communication that cannot be shared" I do not accept. It concerns MY personal data concerning the management of MY money and MY card that you have improperly blocked since April while I have informed you of your mistake. In order not to get involved with further procedures, please email me your relevant request to the bank" to receive the Company's negative response. 10. Furthermore, although the initial position of the Company (see under no. prot. C/EIS/6044/08-09-
2020 opinion document) was that the complainant's request did not constitute an exercise of the right of access according to Article 15 of the GDPR, then, after clarifications were requested from the Authority, the Company revised its position, until finally fully satisfying the right with provision of the entire document to the complainant on 3/2/2021, immediately after the hearing before the Authority, negating its very argumentation based on Article 15 para. 4 GDPR and the invocation of Article 17 commercial secrecy. It should be noted at this point that the audited Company finally provided the complainant with a copy of the electronic correspondence in question, considering itself that the Authority's document with which explanations were requested constitutes "a legal basis for the removal of our confidentiality agreements commitments". It is evident that such "legal basis" does not constitute the Authority's document requesting explanations for an alleged violation of the GDPR, nor does it include a provision for exercising the powers granted to it by Article 58 GDPR. In addition, with its hearing memorandum, the Company claims that it allegedly awaited the interpretation of the relevant provisions and the weighing of conflicting interests by the Authority, in order to proceed with the satisfaction of the complainant's right of access, a practice that is in complete contradiction to the compliance model introduced with the GDPR and also contradicts the principle of accountability according to article 5 para. 2 GDPR, as explained in the consideration no. 3. 11. In any case, regardless of the allegations of the first complainant which appear to be contradictory and mutually exclusive according to the foregoing, it finally emerges from her interlocutory memorandum that she accepts that she violated the GDPR by claiming that: "Although they have been trained for the inclusion of requests of articles 12-23 of the GDPR in the relevant corporate management process, our representatives in this particular case made a mistake and did not make the relevant inclusion, which would have resulted in the assessment of the relevant request as an access request of article 15 of the GDPR and its corresponding evaluation" (p.

9) as well as that "Consequently, the failure of our representatives to manage the request as it developed in the course of this conversation, as a request to exercise the right of access based on the GDPR for all the above reasons must be considered forgivable and this should be considered an isolated error in the handling of an access request" (p. 10). 12. The Authority, in the context of the exercise of its audit powers and in order to examine the claim of the audited company submitted before the hearing in which the right of access had not been exercised by the complainant, had requested on 27/10/2020 to be sent the written Policy or Procedure followed with regard to the management of access requests of the subjects in order to examine whether the denial in question was in accordance with what is provided at the level of internal compliance, on the other hand, in order to examine whether said policies and procedures comply with GDPR requirements. 18 As stated above, in order to answer the question in question and to send the relevant Policy or Procedure, after receiving a deadline of 15 days, it requested an extension and received a further deadline until 23/11/2020, while subsequently, on 23/11 /2020 again requested a second extension of 10 days, but this was not accepted by the Authority. Therefore, the company should have responded to the Authority's requests on the day of rejection of the second request to extend the deadline, i.e. on 27/11/2020, while it finally responded late on 4/12/2020 by sending the relevant response accompanied by the document "Instructions for the Management of Personal Data Subject Requests". The Company for the successive deadlines it received cites as a reason for the delay the fact that due to the situation "we have not been able to gather enough material, which we need to respond to you as most colleagues are working remotely with limited access to the Company's files". due to the COVID-19 pandemic. However, the data controller, in the context of his obligations to the requirements of the GDPR and the current legislation, must, before starting the processing of personal data (and therefore in time before the COVID-19 pandemic), have taken all the necessary compliance actions, including the design and implementation of the necessary internal policies and procedures, which must have been made known to the organization's employees, who, after the necessary training or the advice of the Data Protection Officer (DPO), if appointed, should be in position to apply them. In fact, as the Authority has judged with no. 44/2019 its decision, referring to Opinion no. 3/2010 of the Article 296 Working Group among the appropriate accountability tools include: "establishment of internal procedures before the creation of new processing operations, establishment of written and binding data protection policies available to the persons to whom the data refer, mapping of the procedures, maintaining a list of all of data processing operations, appointing a data protection officer and other persons with responsibility for data protection, providing appropriate education and training to employees in data protection, establishing procedures for managing

access, correction and deletion requests, which must be transparent for the persons to whom the data refer, establishment of an internal mechanism 6 Opinion no. 3/2010 regarding the principle of accountability of 13-7-2010 (WP 173) p. 13 et seq. and p. 14 footnote. 7 for the international standards approved in Madrid by the competent authorities for the protection of personal data. 19 handling complaints, establishing internal procedures to effectively manage and report security breaches, conducting privacy impact assessments in specific cases, implementing and overseeing verification procedures to ensure that all measures are not just on paper, but implemented and working in practice (internal or external audits, etc.)" (see par. 16 of the Authority's decision 44/2019). From the above it follows that the audited Company as the controller should have drawn up and implemented the necessary policies or procedures for its compliance with the requirements of the GDPR and the relevant legislation before starting the processing of personal data, moreover, it should have on the basis of the principle of accountability no. 5 par. 2 GDPR to have the possibility to make them available and to the knowledge of the Authority at any time, especially when they are requested in the context of the exercise of its investigative-audit powers, as in this case. Nevertheless, after 31 days had passed and the extension of the deadline had been granted, the Company failed to respond to the Authority's question, but in particular to send the requested Policy or Procedure on time, and the invocation of the excuse of delays due to telecommuting of its employees and limited access to records of the Company is judged to be unfounded and especially useless in view of the fact that the Company should have already established and put into operation the requested Policy or Procedure regardless of any problems and delays due to the special conditions of its operation due to the COVID-19 pandemic, which does not implies the retreat of the protection of personal data (cf. 05/2020 APD sc. 3). In the event that the Authority requests the submission of a policy or procedure within a certain period of time and the data controller does not respond to the relevant request, the belief is reasonably created that the Company had not drawn up and put into operation the requested Policy or Procedure or at least in form that actually applied during the critical period of time and which he should have sent to the Authority, as is the case in this case. The Authority bases this finding on two (2) elements: Firstly, since a Company has drawn up and implemented a relevant Policy or Procedure, it has no reason to delay its transmission to the Authority and in fact could have transmitted it before the of the expiry of the 15 days received as the initial deadline cumulatively both for the response to the Authority's question and for 20 the relevant transmission. By analogy, if the Authority were to carry out an on-site inspection of the Company's premises and request the delivery of the Policy or Procedure in question, any failure to deliver it promptly would also mean its non-existence, in accordance with what is extrapolated within

the framework of the principle of accountability. After all, this is a document that by its nature (GDPR request management instructions addressed to the controller's staff), must be available at all times to every employee who comes into contact with customers-data subjects, in order to be able to consult them if it receives such a request. For the most part, the relevant document should be at the disposal of the Company's management and communicated to the Authority, should it request it (see art. 31 and 58 par. 1 f GDPR). Secondly, the same document "Instructions for the management of requests" which had been submitted before the hearing and late according to the above, was submitted by the company again as under no. 8 related to the hearing of her memorandum with the distinction that in the last case a pdf file was sent electronically from a file conversion to word format under processing, in which the corrections with the track changes method had inadvertently remained where the addition is found of the phrase "or through any other form of electronic submission" and the comment: "The addition is deemed appropriate before submission to the APDPH". Indeed, from the overview of the relevant document, it appears that in chapter 3 entitled "Request Management Process" and in particular in section 3.1. under the title "Ways of Submitting a Request" three (3) ways are included: by physical presence, by letter and by e-mail. In this last case, the phrase "or through any other form of electronic submission" was added, in time following the Authority's request for the submission, in order to cover the considered case of submitting an access request through the social networking application Facebook, which was not foreseen at the critical time of the incidents under consideration of the complaint. From the above it follows that the Company, while according to its declaration and in practice it used the social networking application Facebook to manage requests regarding the rights of data subjects, including the right of access, it had not included it in the relevant Policy or Procedure and therefore the latter was incomplete and did not correspond to reality. 21 Therefore, the arguments supported by her in her hearing statement according to which her employees, while they were aware of the Policy, ultimately did not perceive the request in question as a request for access because they were not familiar, cannot be accepted . The employees of the Company, who of course report to and are part of the data controller, did not respond to the request for access through the Facebook social networking application because they had never been informed of such a possibility as the relevant "Instruction" of the Company did not include such a case, nor had they be trained to recognize and distinguish the requests of the subjects in relation to the GDPR and the applicable legislation, their rights in this case. 13. Therefore, it is established that the first complained Company violated the right of access of the complainant under no. 15 par. 1 in combination with no. 12 par. 1, 2 and 3 GDPR. 14. complainant to satisfy or not his right. The bank did not provide any answer to The second

complainant With reference no. prot.G/EIS/7505/02-11-2020 in its letter to the Authority, the Bank clarified that it does not consider the complainant's request to be an exercise of his right of access to his personal data, a claim he repeated during his hearing before the Department. From the same document, only indirectly and by interpretation of its content, it could emerge that the Bank has not received a request for maturing installments from the Company, as it stated that "the transaction has not been cleared through the National Bank and the Bank proceeds with the charges and refunds based on the orders it receives from the Bank collaborating with the company." In particular, the Bank claimed in its pre-hearing memorandum, but also during the hearing, that the complainant's written request from 06/07/2020 to the National Bank of Greece S.A. through the store [area] X does not constitute an exercise of the right of access, as it appears from its content that it concerned the method of refunding money from a third party consumer goods trading company for a transaction which was carried out by charging a card issued by the National Bank but cleared by another bank . From the content of the said application it appears that the complainant requested "to be informed about whether there is a request from the company Kotsovolos/Dixons regarding the maturity of the installments and the release of the amount from my credit card for product 22 that has been returned to the company . The company claims that the request was submitted to the National Bank on 22/6 and that it received confirmation of receipt of the request from the bank on 23/6". From the above content, it appears that the applicant requested information regarding the existence or non-existence of a request from the Company regarding his issue and additionally requested confirmation or not if the relevant request has been submitted to the Bank on a specific date and if a confirmation of receipt has been sent . The complainant's request to the Bank to confirm or not the existence of the said requests that were circulated via electronic mail and included his personal data, in accordance with what has been detailed in relation to both the Company and the Bank, constitutes a request for access in his personal data under no. 15 para. 1 GDPR, without requiring, as was similarly stated, to be surrounded by a specific formula or to be exercised in a solemn manner, nor to include the reasons why the data subject exercises the right of access (AD 16/2017 sc. 3). In addition, with article 15 par. 1 GDPR, the audited Bank, as the controller of the personal data of the complainant in the context of receiving the electronic correspondence sent by the Company as stated above, in order to settle the issue related to the credit card charge of the complainant, the maturing of the installments and their repayment, carried out automated processing of personal data and therefore had the obligation to respond in any case, even if negatively to the complainant's request (regarding see STE 2627/2017, APDPX 15/2021). Therefore, while the Bank had the status of data controller and automatically processed personal data of the complainant in

the context of his above request, it failed to correctly evaluate it as an access request no. 15 GDPR and consequently, on the one hand, he did not provide an answer, even a negative one, and on the other hand, he did not satisfy the legal request of the complainant as he should have. 15. Therefore, it is established that the second complained Bank violated the complainant's right of access under no. 15 par. 1 cond. 12 par. 1, 2 and 3 GDPR. 16. In accordance with the GDPR (Rep. Sk. 148) in order to strengthen the enforcement of the rules of this Regulation, sanctions, including administrative fines, should be imposed for each violation of this Regulation, in addition to or instead of the appropriate measures imposed by the supervisory authority 23 in accordance with this Regulation. In cases of a minor violation or if the fine that may be imposed would constitute a disproportionate burden on a natural person, a reprimand could be imposed instead of a fine. 17. Based on the above, the Authority considers that there is a case to exercise its corrective powers according to article 58 par. 2 of the GDPR in relation to the violations found and that it should, based on the circumstances found, be imposed, according to application 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. 18. Furthermore, the Authority took into account the criteria for measuring the fine defined in article 83 par. 2 of the GDPR, paragraph 5 sub. b' of the same article that is applicable in this case and 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) , as well as the actual data of the case under consideration and in particular: A) Regarding the first complained-about company KOTSOVOLOS i. ii. iii. iv. The fact that the complainant did not satisfy the right of access exercised by the complainant according to article 15 par. 1 GDPR, only with a delay of several months and only after the intervention of the Authority. The fact that the violation in this case affected one (1) natural person as a subject of personal data in relation to the satisfaction of the right of access. 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 attributable to the negligence of the company being complained about. . 7 See OE 29, Guidelines and the application and determination of administrative fines for the purposes of Regulation 2016/679 WP253, p. 6 24 v. vi. vii. viii. ix. x. The fact of the existence of deficiencies in the Data Subjects Request Management Policy which resulted in the insufficient training of its staff in the recognition and management of these requests. The fact that the violation of the provisions regarding the rights of the subjects is subject, 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. The

lack of cooperation of the complained Company with the Authority, given that: firstly, it delayed to provide explanations and submit the requested Policy or Procedure for managing access requests, secondly, that it violated the extended deadline and despite the rejection of the second request to extend the deadline, it did not provided the explanations and did not produce the Policy or Procedure by the deadline but acted at a time of its choosing and thirdly, produced a Policy or Procedure which did not actually meet the deadline but amended it to meet the request of the Authority and to GDPR compliance requirements in view of the exercise of the Authority's audit-investigative powers. 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 1/5/2019 to 30/4/2020 its turnover amounted to 546,868,455 euros, increased by 3% compared to the previous use. B) Regarding the second complained-about National Bank i. The fact that the complainant did not evaluate the complainant's request as an exercise of the right of access, with the result that on the one hand it did not provide any answer, nor a negative one, and on the other hand, it did not satisfy the right 25 of access exercised by the complainant pursuant to Article 15 para. 1 GDPR even after the submission of the complaint. The fact that the violation in this case affected one (1) natural person as a subject of personal data in relation to the satisfaction of the right of access. 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 the negligence of the complained Bank. The fact that the violation of the provisions regarding the rights of the subjects is subject, 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. The existence of previous established violations of the complainant as a relevant audit shows that she has been imposed administrative sanctions in the past by the Authority (see decisions 194/2012 and 55/2018 APD). The fact that from the elements brought to the attention of the Authority and with based on which it found 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 Bank for the year from 1/1/2020 to 31/12/2020 the cycle

of its operations in Greece amounted to 2,363,000,000 euros.

ii.

iii.

iv.

v.

vi.

vii.

viii.

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

denounced as data controllers, those referred to in the ordinance

administrative sanctions, which are considered proportional to the gravity of the violations.

FOR THOSE REASONS

THE BEGINNING

1. Enforces on the respondent company the name Dixons South East Europe

A.E.V.E. - KOTSOVOLOS the effective, proportional and deterrent administrative

fine that is appropriate in the specific case, according to

more special circumstances thereof, amounting to twenty thousand (20,000) euros for the above

established violations of articles 15 par. 1 cond. 12 par. 1, 2 and 3 GDPR,

according to articles 58 par. 2 item i' and 83 par. 5 item II GDPR.

2. Enforces the complained company with its name National Bank

Greece S.A. the efficient, proportionate and dissuasive administrative money

fine appropriate to the specific case, according to the special ones

circumstances thereof, amounting to twenty thousand (20,000) euros for the above

established violations of articles 15 par. 1 cond. 12 par. 1, 2 and 3. GDPR,

according to articles 58 par. 2 item i' and 83 par. 5 item II GDPR.

The Deputy President

George Batzalexis

The Secretary

Irini Papageorgopoulou

27