Athens, 03-10-2022 Prot. No.: 2433 DECISION 53/2022 The Personal Data Protection Authority met, at the invitation of its President, in an extraordinary meeting via video conference on 21-

7-2022, following the postponement of its meeting from 19-7-2022 and following its meeting from 14-06-2022, in order to examine the case referred to in the history of the present. Konstantinos Menudakos, President of the Authority, the regular members Spyridon Vlachopoulos, Konstantinos Lambrinoudakis, as rapporteur, Christos Kalloniatis, Aikaterini Iliadou and Grigorios Tsolias, as well as the alternate member Nikolaos Livos in place of regular member Charalambos Anthopoulos who, although invited, were present legally and in writing, he did not attend due to a disability. At the meeting, without the right to vote, the auditor Konstantinos Limniotis, IT specialist, as assistant rapporteur, and Irini Papageorgopoulou, an employee of the Department of Administrative Affairs, as secretary, attended the meeting, by order of the President. The Authority took into account the following: Following relevant complaints against the National Bank of Greece S.A. (hereinafter National Bank) and Piraeus Bank SA. (hereinafter Piraeus Bank), the Authority examined the issue of personal data processing through contactless debit/credit card transactions. The complaints in question concerned the mandatory replacement of debit/credit cards with new ones, which by default had the possibility of contactless transactions. The Authority, after examining issues regarding the protection of personal data raised by the said processing, also taking into account the international, during the disputed period, specifications regarding the intact 1 Kifisias Ave. 1-3, 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr debit and/or credit cards based on the relevant information provided by Mastercard and Visa companies, issued Decision No. 48/2018, with which it addressed a recommendation1 in the said Banks, if a customer declares to them that he does not wish to have a card with the possibility of carrying out contactless transactions, either to provide the possibility of deactivating the contactless operation of such a card or to grant a new card without the possibility of contactless transactions. Further, in the context of examining the above complaints, the Authority found that in some cases of credit/debit cards, a history of recent transactions carried out using the card is kept on the chip of the card, which can also be easily read without contact. In particular, the said information related to the transaction history consists of the date of the transaction and the amount of money. For the feature in question found on Mastercard cards, the company in question informed the Authority that it is not a mandatory feature and it is up to the respective issuer whether or not to incorporate it into the corresponding banking product (credit/debit card) that it provides to the his client. With regard to this issue, which the Authority examined ex officio, with the above Decision, addressed the following recommendation2 to the Banks in question: if a card issued to a customer

has the option of keeping a transaction history on its chip activated without having given his specific consent, the customer should be informed in any appropriate way (e.g. via e-mail, via a message when connecting to personalized electronic services of the data controller, via postal letter, etc.) regarding this processing, giving him the possibility to stop this processing. Furthermore, in each new edition/grant, the feature in question should be deactivated from the beginning, and only be activated if there is a special 1 According to article 19 paragraph c' of Law 2472/1997 which was in force during the disputed period 2 In accordance with article 19 par. c of Law 2472/1997 which was in force during the disputed period 2 consent of the customer, as long as he has been previously informed about this processing. Subsequently, the Authority, with document no. prot. C/EX/6257/16-07-2018, forwarded the above Decision to all Greek Banks (with notification to both mentioned above), pointing out that, although the complaints submitted to the Authority and examined in the context of the aforementioned Decision concerned two specific Banking Institutions, they should proportionately - to the extent that each Bank provides its customers with cards of the technology in question - take care to fulfill all that is perceived in said Decision. After all, the Authority had previously addressed all the Banks, with its letter No. C/Eξ/4943/27-06-2017, requesting, among other things, information as to whether they provided contactless debit/credit cards and with what characteristics (such as what information is stored on their chip). In this document, as also mentioned in Decision 48/2018, ALFA BANK SA. (hereinafter Alpha Bank) and EUROBANK ERGASIAS SA. (hereinafter Eurobank) had not responded to the Authority, while they also did not respond even after the relevant reminder documents with no. prot. C/EX/276/12-01-2018 and C/EX/275/12-01-
2018 respectively. Subsequently, the Authority sent to National Bank, Piraeus Bank, Alpha Bank and Eurobank the letter No. C/EX/4271/14-06-
2019 document, with which he requested the Banks in question to inform about the actions they took in order to comply with the aforementioned recommendations of the Authority mentioned in Decision No. 48/2018. National Bank responded with its letter No. … and from … (Authority No. C/EIS/5727/21-08-2019), stating the following: The Bank has completed all the required actions so that 1) debit and prepaid card holders who do not wish their cards to have the possibility of contactless transactions can submit a relevant request through specific procedures, while said requests are immediately satisfied. 3 2) At the same time, the procedures have been initiated so that the customer can deactivate the functionality in question, if he so wishes, also through Internet Banking. 3) For credit cards, this possibility will exist after the transition of credit cards to the new card system, which was expected to be completed in March 2020. 4) With regard to keeping track of transactions on the

transaction chip, in Debit M/C and Business M/C debit cards that are issued do not comply with this requirement, while for the other card products, the removal of this feature has been initiated by the end of 2019. Also, the relevant Departments of the Bank are working on solutions to remove the history on old cards as well, without the need for their owner to make a request. According to the schedule, the procedures in question were expected to be completed at the end of 2019. Subsequently, the Authority, and since there was a relevant written request by A (Authority's prot. no.: Γ/EIS/6348/01-10-2021) - who had submitted a relevant complaint to the Authority regarding the mandatory replacement of debit/credit cards with new contactless cards - to be informed whether the Banks complied with the provisions contained in Decision No. 48/2018 of the Authority regarding the part of informing the cardholders for keeping a history of transactions on this chip, pointing out that he himself did not receive such information, sent to National Bank the letter No. C/EXE/2601/15-11-
2021 document, with which he requested the Bank to specifically clarify the actions it took regarding the issue of keeping the history of the latest transactions on the credit/debit card chip (for those cards that had this feature), clarifying in particular if he duly informed all the holders of the above cards about the said processing, regardless of whether, in the meantime, their cards have already been replaced due to the expiration of the old ones. National Bank responded with the document No. G/EIS/3650/09-03-2022, stating the following: 4 1) National Bank has in recent years adopted the technology of contactless transactions through debit, credit and of prepaid cards it issues, in the context of the continuous upgrading and improvement of the products and services it has. This feature was based on NFC (Near Field Communication) wireless technology, a ground-breaking and innovative technological solution, which - in addition to facilitating and speeding up transactions - has proven extremely important in the current situation and has contributed significantly to preventive measures received by all agencies in the context of dealing with the pandemic. 2) Furthermore, the Bank had informed the Authority regarding the schedule of its actions in the context of its compliance with the no. 48/2018 of Decision. In particular, the Bank had launched the required actions to deactivate the possibility of conducting contactless transactions for those customers who requested it from the beginning of 2019, while it is noted that the relevant possibility is now available for all NBG cardholders. It is now possible for customers to remove the functionality of contactless transactions on all card products through the Internet & Mobile Banking service on their own initiative. Those customers who are not users of the said service, can request the cancellation at their cooperation Store and this will be implemented through the Card System. The implementation of the above was done gradually and was combined with the transition of the products to the new System, which was completed in

October 2021. The Bank reports that the vast majority of its customers 3) use the possibility of contactless transactions every day, especially after the event of the pandemic, when it was also decided interbanking that the limit of transactions that can be completed intact should rise to 50 euros (from 25 euros that used to apply), in the context of the measures against the spread of the coronavirus. During the last three years, a minimum of 5 requests to disable contactless transactions were submitted, all of which were granted. 4) With reference to the observance of the historicity of transactions, the Bank states that, on the one hand, it has never actually used the functionality in question and, on the other hand, in all the cards now issued by the Bank, the functionality in question is completely disabled. However, given that the cost of an emergency reissuance of all cards would be extremely high, as well as the fact that such an action would cause great disruption to the market and make it significantly more difficult for its customers to transact, the Bank preferred the gradual replacement of the cards that had the historical record activated, on the anniversary of their renewal. Therefore, the cards in question after their expiration date are replaced in their entirety with cards that will not respect history. As regards the cards that were issued with this functionality and are still in circulation, the Bank initiated the necessary actions already in 2019 so that it is possible to abolish the observance of historicity, without the holders making requests to reissue the cards their. 5) Furthermore, it was assessed that informing all holders regarding the keeping of the history would also be very costly and in addition would create confusion among the clientele and possibly concern regarding the security of the transactions through the cards in question, without actually there is – as stated by the Bank – an actual and substantial risk for the customers in question, as the data kept in the history were elements of the last 10 transactions carried out with the card, which could not be attributed or associated with a specific person and their reading required the use of special equipment and the physical presence and proximity of the card. 6) Finally, the Bank points out that any adjustment to the way the products and/or services provided by the Bank operate, 6 requires careful planning, involves large operating costs and requires a reasonable period of time for implementation. In this context, the Bank takes into account all the relevant risks (risks regarding the security of transactions, the protection of customers and their personal data, reputation, etc.) and ends up prioritizing and prioritizing its actions with a view to optimal customer service and the smooth functioning of the market. Subsequently, the Authority invited the National Bank to a hearing, via video conference, at the Plenary meeting of 14-06-2022 (see call with No. Prot. C/EXE/1335/02-06-2022). During the meeting of 06-14-2022, Mrs. B, Director ..., Ms. C, Head of ..., D..., Head of ... of the Bank and the Group, Mr. E, Head of ... of the Bank and the Group, Ms. F, Head ... of the Bank and the Group, Ms. G, Supervisor..., Ms. The Supervisor... and Mrs. Th,

Data Protection Officer, as representatives of the National Bank. After the meeting, the data controller was given a deadline to submit a memorandum, which he submitted, within the set deadline, with document No. C/EIS/8654/08-07-2022. The following is mentioned in the said memorandum: In recent years, the Bank has adopted the technology of contactless transactions through the debit, credit and prepaid cards it issues, in the context of the continuous upgrading and improvement of the products and services it has available. This feature was based on the short-range NFC (Near Field Communication) wireless technology, which is now well-established as it has been widely adopted internationally and, in addition to facilitating and speeding up transactions, proved extremely important during the pandemic and contributed significantly to the preventive measures taken by all agencies in the context of limiting the spread of the coronavirus. 7 After the issuance of Decision 48/2018, the competent units of the Bank investigated the available alternative options with the aim of both the Bank's compliance with the provisions contained therein and the smooth operation of the market, and planned the implementation schedule of the measures selected . In view of both the Bank's compliance with the provisions of the above Decision of the Authority, as well as the better quality of service to its customers, the Bank proceeded with the following compliance actions: a) Regarding the possibility of deactivating contactless operation, the possibility of granting of a new contactless card for operational reasons, as the Bank would then have to maintain, maintain and from time to time upgrade two systems to support contactless and contactless cards, which would jeopardize the smooth execution of transactions. Therefore, the Bank proceeded to implement the first alternative provided for in the Decision, i.e. to provide the possibility of deactivating contactless transactions without a PIN, by setting the relevant limit to zero. In particular, customers can request the zeroing of the limit of contactless transactions without a PIN through their partner branches, through the Bank's contact center and through the Internet and Mobile Banking applications. Customers - cardholders are informed of the above possibility when they are served by their cooperation Branch, when submitting the request for the issuance of the card and/or when receiving it, as well as from the Bank's Contact Center. In addition, relevant information has been included in the pre-contractual information form for the cards, as well as on the Bank's website (related attached documents were submitted by the Bank to the Authority, together with the aforementioned memorandum). The related requests that the Bank has received from 2018 until today are minimal and have been satisfied in their entirety. At the same time, the Bank points out that the vast majority of its customers make use of the possibility of conducting contactless transactions every day, especially after the outbreak of the pandemic, when it was decided interbank through the Hellenic Banks Association that the limit of transactions that can be completed

contactless should rise to 50 euros (from 25 euros which used to be 8), as part of the measures against the spread of the coronavirus. In any case, the relative number of customers using this feature is dynamic, as cardholders may at any time request the deactivation and/or reactivation of PIN-free contactless transactions according to their preferences. Although, as mentioned above, the number who requested the deactivation of contactless transactions without a PIN is small. B) In terms of maintaining the history of transactions, in the past, for Mastercard cards issued by the Bank, the functionality of storing on the card chip details of the last 10 transactions carried out with the physical presence of the card was activated (therefore transactions carried out remotely, such as payments in online stores, are not stored). The details of the transactions in question that are stored are the date of the transaction, the amount of the transaction and the currency of the transaction, which alone cannot identify the cardholder. This functionality was described as an innovative feature of the cards in Mastercard's specifications, which under conditions could be used as an adjunct in the dispute resolution process, and which was simultaneously adopted by many other Banks pan-European and international. Furthermore, in the context of servicing transactions and in accordance with the provisions of the relevant legislative framework, the Bank keeps information in its systems regarding the movement of the card. This information, includes both the transactions carried out with the physical presence of the card, as well as the transactions carried out remotely (e.g. E-commerce). Therefore, the Bank has no reason to use - as it has never used - the information stored on the card's chip, since on the one hand the information in question is fragmentary since it does not include all transactions, concerns the result of the transaction and does not constitute a condition of this, on the other hand, its utilization would require the use of special equipment and the physical proximity of the card, which is in the customer's possession. 9 Therefore, taking into account what is mentioned in no. 48/2018 Decision of the Authority, as well as the zero usefulness of the specific functionality, the Bank initiated the required actions and reconfigured the characteristics of the Mastercard cards it issues, so that in all the Mastercard cards now issued by the Bank, the due functionality to be completely disabled. The Bank emphasizes in its memorandum that the possible emergency and simultaneous mass reissuance of all of our Mastercard cards, the vast majority of which are debit cards, i.e. cards with much greater use than credit cards, would present significant practical difficulties (especially if they proceeded and the rest of the Banks in corresponding actions) and would cause great disruption in the market, with a visible risk that a significant portion of its customers will not immediately receive the new card, which would significantly hinder their ability to transact. In this context, the gradual replacement of the cards that had the historical preservation activated, on the anniversary of their renewal, was

advanced. Furthermore, according to the information provided by the competent Unit of the Bank, the Mastercard cards issued by the National Bank are currently active in total 3,963,414 (3,772,101 debit cards and 192,313 credit cards), of which 3,121,821 cards represent a percentage 78.8% of the total have already been replaced by cards that no longer keep transaction history. In addition, the remaining cards will also be replaced on their renewal anniversary with cards that will no longer have transaction storage functionality. In terms of informing its customers about the processing that consists in maintaining the history of transactions, the Bank initially proceeded to investigate the most suitable solutions for its compliance with the above Decision of the Authority, on the one hand, on the other hand, to weigh the risks for the cardholders due to historical records. Although the Bank reserves reservations as to whether the data stored on the card's chip (date, amount and transaction currency) constitute personal data of the holders, only in the sense that the aforementioned 10 of the Authority decided to deactivate data cannot to lead to their identification, the Bank respecting the Decision the specific functionality in the cards issued from now on (whether it is new issues, or reissues of existing cards). The said action required some reasonable planning time, reconfiguration of the card features and supply of new cards, during which time any information to the customers could not in practice be accompanied by the provision of the possibility of withdrawal on the part of the customer and the choice of another product without observing the functionality, as the Bank did not yet have such products. Further, it was assessed that informing all holders of the history record would create confusion among customers and possibly concern regarding the security of transactions through the cards in question, without actually presenting a real and substantial risk to those customers. , as the data kept in the history were elements of the last ten (10) transactions carried out with the card, which could not be attributed or associated with a specific person and for their reading required the use of special equipment and physical presence and card proximity. In addition, from the assessment of the risks for the cardholders, the following considerations emerged: A) There are no substantial security risks for the cardholders due to the storage of the transaction history, since in order to read the data, the malicious person would have to have the suitable reader and to have physical proximity to the card, and the data it would collect would relate to transactions already carried out. B) Simultaneously with the compliance actions contained in Decision 48/2018, the Bank had launched actions for the implementation of the process (Strong Customer Authentication), in accordance with the provisions of Delegated Regulation (EU) 2018/389 of the Commission of of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication Strong Customer Identification 11 and

common and secure open communication standards, further removing the possibility of transaction on behalf of the malicious person. C) In any case, cardholders retain the possibility of disputing transactions they do not recognize, in accordance with existing procedures. D) Meanwhile, due to the pandemic, there were many announcements by the relevant government agencies about measures that could be taken to limit the spread of the coronavirus, among which was avoiding the use of cash, as well as conducting contactless transactions. In this context, there were many requests for the issuance of new cards from customers who, until that time, chose to transact mainly with cash. Given these developments, the Bank decided that it would not be possible to seamlessly serve the requests to issue new cards at the same time as the requests to reissue cards due to the observance of history, with the risk that a portion of the clientele will be left without a card in the middle of quarantine, and without access to electronic markets. E) Cards have a certain lifespan anyway, and all cards that are reissued no longer retain history. Therefore, the number of cards with history in circulation is decreasing every day. The Bank concludes that, weighing the above based on the principle of proportionality, it considered that the intended result – namely the granting of cards with the functionality of history disabled – could be achieved through the actions it had already initiated. The Authority, after examining all the elements of the file and after hearing the rapporteur and the assistant rapporteur, who (assistant) was present without the right to vote, after a thorough discussion DECIDED IN ACCORDANCE WITH THE LAW 12 1. In accordance with the provisions of articles 51 and 55 of the General Data Protection Regulation (EE) 2016/679 (hereinafter, GDPR) and article 9 of Law 4624/2019 (Government Gazette A

137), the Authority has the authority to supervise the implementation of the provisions of the GDPR, the law this and other regulations concerning the protection of the individual from the processing of personal data. 2. According to article 4 par. 1 of the GDPR, personal data means "any information concerning an identified or identifiable natural person ("data subject")", while "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' . And in the introductory paragraph 26 of the GDPR it is stated that "in order to judge whether a natural person is identifiable, all the means that are reasonably likely to be used, such as his separation, should be taken into account, either by the data controller or by a third party for the direct or indirect verification of the identity of the natural person. In order to determine whether any means is

reasonably likely to be used to verify the identity of the natural person, all objective factors, such as the costs and time required for identification, should be taken into account, taking into account the technology that is available at the time of processing and technological developments". 3. According to article 4 par. 7 of the GDPR, a data controller is defined as "the natural or legal person, public authority, agency or other entity that, alone or jointly with others, determines the purposes and manner of personal data processing; when the purposes and manner of such processing are determined by Union law or the law of a Member State, the controller or the specific criteria for his appointment may be provided for by Union law or the law of a Member State". 13 4. According to article 5 paragraph 3 of the GDPR the data controller bears the responsibility and must be able to prove his compliance with the processing principles established in paragraph 1 of the same article, which include legality, objectivity and transparency of processing in accordance with article 5 par. 1 item a' - i.e. the data must be processed lawfully and legitimately in a transparent manner in relation to the data subject. In other words, with the GDPR, a compliance model was adopted with the central pillar being the principle of accountability in question, i.e. the 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 and, in addition, he must prove himself and at all times his compliance with the principles of article 5 par. 1 of the GDPR. 5. Furthermore, Article 6 para. 1 of the GDPR provides, among other things, that the processing is lawful only if and as long as at least one of the following conditions applies (legal bases of the processing): "a) the data subject has consented to the processing his personal data for one or more specific purposes, b) the processing is necessary for the performance of a contract to which the data subject is a contracting party or to take measures at the request of the data subject prior to the conclusion of a contract, (...) f) the processing is necessary for the purposes of the legal interests pursued by the controller or a third party, unless these interests are overridden by the interest or fundamental rights and freedoms of the data subject that require the protection of personal data (...)". 6. With reference to the principle of processing transparency, the GDPR imposes specific obligations on data controllers regarding the information they must provide to data subjects. In particular, in accordance with Article 12 para. 1 of the GDPR, the data controller takes the appropriate measures to provide the data subject with any information referred to in Articles 13 and 14 (which concern the 14 information provided to the data subjects either the data is collected from the subjects themselves or not) and any communication in the context of articles 15 to 22 (which concern the rights of the subjects of objections3 to data processing, including article 21 processing) about the processing in a concise, transparent, comprehensible and easily accessible format. Furthermore, paragraph 2 of Article 12 of

the GDPR provides that "the data controller shall facilitate the exercise of the rights of the data subjects (…)". of the right 7. In particular, in article 13 of the GDPR it is defined that "when personal data concerning a data subject is collected from the data subject, the controller, upon receiving the personal data, provides the data subject with all the following information: a) the identity and contact details of the controller and, where applicable, the representative of the controller, (…) c) the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing, (…)" (see par. 1 of article 13 of the GDPR). 8. In this particular case, for the processing which consists in storing, on the chip of the debit/credit card of the National Bank, the history of the last ten (10) transactions carried out through it, which can be read intact, the said The Bank is the controller, in the sense of article 4 par. 7 of the GDPR. In fact, as emerged from the initial examination of the case with Decision No. 48/2018 of the Authority, the technological feature in question is provided as an optional option on cards by the Mastercard company - i.e. it is up to each issuer ("Bank") if will enable it or not. Moreover, National Bank 3 According to Article 21 of the GDPR, "The data subject has the right to object, at any time and for reasons related to his particular situation, to the processing of personal data concerning him, which is based on Article 6(1)(e) or (f), including profiling based on those provisions. The controller no longer processes the personal data, unless the controller demonstrates compelling and legitimate reasons for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or support of legal claims claims". 15 actually started, as described in the present history, the issuance of cards without this technological feature – which, moreover, as he notes, he never used. 9. For the processing in question, National Bank did not provide relevant information to the data subjects (i.e. to the holders of the cards in question). It should be pointed out that the Authority, already with Decision No. 48/2018 (which was based on the legal framework in force before the GDPR), identified the said deficiency and sent a recommendation to the data controller in order to remedy it – that is, it adopted the milder possible choice. 10. In the absence of the relevant information, which in any case is an obligation of the controller according to the above, the legal basis of said processing is not clear. Such processing could in principle have as a legal basis consent4 (Article 6 para. 1 letter a' of the GDPR), as long as the data subjects declare freely, in full knowledge and clearly (with a statement or a clear positive action) that they specifically and explicitly consent to the processing in question, but these conditions do not apply in this case. Also, the processing in question cannot be considered as necessary for the performance of a contract - and, therefore, the legal basis cannot be that of article 6 par. 1 item. b' of the GDPR - since, after all, there are a number of corresponding debit/credit/prepaid cards without the feature in question, which, moreover, as

mentioned above, is implemented optionally. Therefore, the only possible legal basis seems to be that of article 6 par. 1 item. at. And in this case, however, beyond the fact that the Bank has not documented what is the legal interest it seeks by storing this data on its customers' cards, but only states that, under conditions, the said history could used as an auxiliary during the dispute resolution process, it is required on the one hand that the processing is transparent, but this condition does not 4 See the definition of consent in article 4 para. 11 of the GDPR, as "any indication of will, free, specific, explicit and in full knowledge, by which the data subject expresses that he agrees, by statement or by a clear positive action, to be the subject of processing of the personal data concerning him ». 16 was met for this specific case, and on the other hand the data subjects should know in particular about the existence of the right to object to the processing in question (Article 21 of the GDPR), while this condition is not met in this case either. Regarding this issue, the Authority, with the recommendation it addressed with Decision No. 48/2018, asked the Bank, in addition to informing the data subjects, to give the possibility to those who wish to , to express their opposition to the processing in question and, subsequently, to take care of the satisfaction of the right (either by deactivating the specific technological feature or by issuing a new card). 11. The National Bank, although it initiated procedures on the basis of which every new card it issues does not carry the feature in question and therefore, gradually, stops the processing in question, it did not inform the cardholders of this processing, therefore not complying with the above Decision of the Authority. Therefore, there is a violation of article 13 of the GDPR which entails a violation of the article 5 par. 1 item. a' of the GDPR principle of transparency of processing. The arguments put forward by the Bank for the reasons for the lack of information lie in particular in the fact that, according to its claims, such an information would entail high costs while also there is no substantial risk for its customers in question, as the data kept regarding the Last 10 transactions carried out with the card could not be attributed or associated with a specific person and to read them required the use of special equipment and the physical presence and proximity of the card. However, these claims are unfounded for the following reasons: a) The obligation to inform about the processing and, in general, thefundamental principle of transparency of the processing exists regardless of whether or not there is a risk from the processing for the data subjects5. 5 Restrictions on rights may be imposed by EU law or Member State law under specific conditions and provided appropriate safeguards are provided, but this particular case clearly does not fall within them (see Article 23 GDPR). 17 b) Even if there is no high risk from the processing in question for the affected persons, the claim that there is essentially no risk is not sufficiently substantiated for the following reasons i) The equipment required to read the data is readily available to anyone. Specifically, as already described in the Authority's

Decision No. 48/2018, any "smart" device (e.g. "smart" mobile phone) with appropriate software (which relevant software is freely available) is sufficient in order to to read the data if the owner of the device is near the card – without even having it in his possession. ii) There is clearly a possibility - and even an easy one - to associate the data in question with the subject thereof. In fact, this does not necessarily mean that the card has been stolen/lost. For example, a third party in the close family/friend/professional environment of the data subject may, if he is in the vicinity of the said card of the data subject, read the said data intact. In any case, the card itself mentions the name of its owner on its front side. c) The claim about the high cost required for the update is not substantiated. Already the Authority, with Decision No. 48/2018, had mentioned as indicative ways of information the sending of an email message or the posting of a message when connecting users to personalized electronic services of the Bank. Furthermore, the claim that such an update would entail a large number of requests for replacement cards cannot lead the controller to the conclusion that he is exempt from the obligation to update because the management of the requests, if they are indeed excessive in number, could lead to appropriate procedures to their satisfaction. For example, it could possibly be judged that this replacement would not take place immediately, also taking into account the not particularly high risks from said 18 processing. In any case, the obligation to inform which falls on the data controller is not removed in principle from its cost, since in this particular case, in terms of the obligation to inform, article 13 of GDPR6 applies, which does not provide for any exception for the controller from the obligation to inform the data subjects. 12. The Bank additionally states that such an update would cause concern to its customers. And with regard to this claim, however, the provisions contained in the above Opinion 11 regarding the non-exemption from the obligation to inform apply in principle. Furthermore, the said claim is not sufficiently substantiated: this is because due to the fact that the risks from the processing are not high, it does not follow that a properly worded information about the said processing would cause concern. However, it does not appear that the Bank thoroughly examined appropriate information texts in order to reach the above conclusion. 13. 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. 14. The Authority further considers that, based on the circumstances established, it should be imposed, pursuant to the provision of article 58 par. 2 sub. 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 behavior. 6 Even if, however, Article 14 of the GDPR had been applied, as referred to in Article 14 para. 5 of the GDPR with regard to the information provided to the data subjects if the personal data has not been collected from the data subject,

"paragraphs 1 to 4 do not apply if and as long as: a) the data subject already has the information, b) the provision of such information proves impossible or would entail a disproportionate effort, in particular with regard to processing for archiving purposes in the public interest, for the purposes of scientific or historical research or statistical purposes, under the conditions and guarantees referred to in article 89 paragraph 1 or if the obligation referred to in paragraph 1 of this article is likely to make it impossible or to greatly harm the achievement of the purposes of said processing . In these cases, the data controller shall take appropriate measures to protect the rights and freedoms and legitimate interests of the data subject, including by making the information publicly available." 19 Furthermore, the Authority took into account the criteria for measuring the fine defined in article 83 par. 2 of the GDPR and Guidelines 4/20227 of the European Data Protection Board (which are in public consultation) and in particular that: a. the established violation of article 13 of the GDPR is subject, in accordance with the provisions of article 83 par. 5 sec. b GDPR, in the highest prescribed category of the classification system of administrative fines8, b. the violation in question constitutes non-compliance by the data controller with Decision No. 48/2018 of the Authority, c. the violation concerns a large number of data subjects - specifically, all customers of the National Bank who had debited the old version Mastercard credit card, d. the violation is continuous, since it was already established by the Authority's Decision No. 48/2018 and continues to this day, e. the activity was wide-ranging, as it concerns every "movement" of a Mastercard debit/credit card (issued by the Bank) in a physical store, regardless of the geographical location of this type of transaction, as long as it is an old-issue card that does not have replaced, f. the activity is related to the main activities of the controller, regardless of the fact that the data in question stored on the card chip, and which are already being processed legally in a different context, by the Bank (since information is stored in its systems regarding the 7 https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022- calculation-administrative_en 8 The "most important" violations are characterized as those that can result in the maximum a possible amount of a fine of 20,000,000 euros or, in the case of businesses, up to 4% of the total global annual turnover of the previous financial year, in contrast to the other violations included in article 83 paragraph 4 of the same article 20 movement of the card) , were never utilized by the Bank. g. the processing concerns data of an economic nature, for which there is a risk, in accordance with what is mentioned in the rationale of this present, of coming to the knowledge of third parties, h. the violation was intentional, since the Authority had already addressed with letter no. 48/2018 Decision related recommendation to the Bank and the latter took a strategic decision not to comply with the recommendation in question but, instead, to gradually begin to stop the processing in

question, i. the data available on the internet9 about financial income of the Bank for 2021, as well as that: a. This processing does not result in financial loss for the data subjects, b. the Bank would not obtain any financial benefit from said processing, c. the Bank took actions to gradually stop said processing. 15. Based on the above, the Authority unanimously decides that the administrative sanctions referred to in the ordinance should be imposed on the complained controller, which are considered proportional to the gravity of the violations. FOR THESE REASONS, the Authority imposes on the National Bank of Greece S.A., as data controller, the effective, proportionate and dissuasive administrative fine that 9 See https://www.nbg.gr/el/omilos/enimerwsi-ependutwn/reports/etisia-xrimatooikonomiki-ekthesi-omilou-kai-trapezas-31-12-2021 (last access: 19/8/2022) 21 corresponds to specific case in accordance with its special circumstances, in the amount of twenty thousand euros (20,000.00) euros, for the above established violation of article 13 of Regulation (EU) 2016/679, in accordance with article 58 par. 2 i' of the GDPR in conjunction with article 83 par. 5 of the GDPR. The President Konstantinos Menudakos The Secretary Irini Papageorgopoulou 2223