Athens, 03-10-2022 Prot. No.: 2438 DECISION 55/2022 The Personal Data Protection Authority met, at the invitation of its President, in an extraordinary meeting via teleconference 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 the security issues of said processing as well as the related risks, and taking into account the international, during the disputed period, specifications regarding contactless debit and/or credit 1 Kifisias Ave. 1-3, 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr cards based on the relevant information provided by the Mastercard and Visa companies, issued Decision No. 48/2018, with which it addressed a recommendation1 to the due to 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, the Authority, 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 to have 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, ALFA Bank and Eurobank the document No. C/EX/4271/14-06-2019, with which it requested the said Banks to inform as to the actions they took in order to comply with the aforementioned recommendations of the Authority mentioned in Decision No. 48/2018. Eurobank responded with its letter No. … (Authority No. G/EIS/5324/02-08-2019), stating the following: 1) The Bank, since November 2018, supports the ability to disable contactless transactions upon customer request. The relevant request can be submitted in various ways (by visiting a physical store, via e-mail, via telephone, etc.) placed orders for new cards whose specifications do not include the feature in question. Therefore, new cards issued, whether debit or credit, do not carry this feature. The Bank enables cardholders with this feature to contact it, in any way they wish, and request the deactivation of the specific feature. In this case, the Bank proceeds to issue a new card. Further, a reliable technical solution is being explored so that the said feature is automatically disabled by using the card at an ATM/POS. 3) The specific storage (amount and date of the last 10 transactions) is of no use

to either the Bank or the holder and does not pose any risk. To read them, one needs to procure special hardware (hardware that will accept the card) equipped with appropriate software (software that will "read" the content of the chip) as the data is not transmitted during a transaction. As for the risk, it is limited to the ability of a third party to "read" them, because it presupposes, on the one hand, that the card will be removed from the owner's possession without him realizing it, and on the other hand, that the third party will have the appropriate equipment - while also the usefulness of said data to the third party who will read it is doubtful. Subsequently, the Authority, and given that there was a relevant document request by A (Authority's original no.: Γ/EIS/6348/01-10-2021) – who had submitted a relevant complaint to the Authority regarding the mandatory replacement of debit/credit notes of cards with new contactless cards - to be informed whether the Banks have complied with the provisions contained in Decision No. 48/2018 of the Authority regarding the part of informing cardholders about the maintenance of 4 transaction history on this chip, pointing out that the same did not receive such information, sent to Eurobank the document No. C/EXE/2600/15-11-2021, with which he asked the Bank to specifically clarify the actions it took regarding the issue of compliance of the history of the latest transactions on the credit/debit card chip (for those cards that had the feature in question), clarifying in particular whether it has duly informed all the holders of the above cards of the said processing, regardless of whether, in the meantime, the their cards have already been replaced due to the expiry of the older ones. Eurobank responded with document No. G/EIS/205/12-01-2022, stating the following: 1) The data registered in the memory of the "chip" of the specific cards that have this feature only relate to the amount and date of the last ten (10) transactions. Of these specific data that are put in the specific processing (observance) it is impossible to arise in any way, even indirectly, h identity of the cardholder, and therefore there is no question of personal data, nor of their processing in the sense of the GDPR. 2) Even if it is assumed that the above data are personal data, the specific processing consists only of their storage, i.e. keeping them in the memory of the "chip" of the card. They are therefore kept in an object, the card, which is in the possession of the customer (cardholder) and is used by him alone, at POS and/or ATMs of all banks and not only the bank that issued it. During this use, the POS or ATM, in which the card is used, authorizes the transaction based on the PIN, which is entered by the customer where required. For this procedure, there is no question of "reading" or any other processing of the details of the transactions (amount, date) previously carried out with the card because these are completely unrelated to the specific processing consisting in the identification of the 5 owner. After all, the above identification process of the owner is completed with the possibility of credit/debit cards that do not store transaction data in the "chir". exactly the same as in 3)

Furthermore, if the possession of the card falls to a third party, the above specific details are practically inaccessible and completely useless, since the personal data printed on it (name, surname, card number, expiration date, CVC code) and much more he is given the opportunity to use it causing damage (e.g. financial) to its rightful owner. To this end, the third party has no reason to be informed of the last ten transactions (amount, date) carried out by the legal cardholder, nor to profile him. 4) The process of replacing the cards with new ones that do not have this feature began in July 2019 for debit cards and in October of the same year for credit cards, is ongoing and the majority of cards have already been replaced. 5) The Bank, despite the relatively extensive publicity of Decision 48/2018, has accepted and satisfied a very small number of requests for card replacement for this reason. The Bank also examined the possibility of automatically deactivating the above storage by using it in an ATM / POS, however, for the above reasons and the zero relative demand, combined with the disproportionate cost, it did not proceed with any relevant mass implementation. 6) Since, according to the Bank's claims, it is not about personal data and their processing, there is no question of informing the owners of these cards and their relative consent. Subsequently, the Authority invited Eurobank to a hearing, via teleconference, at the Plenary meeting of 14-06-2022 (see call with prot. no. 6 C/EXE/1334/02-06-2022). During the meeting of 14-06-2022, Mr. B, Head of ..., Mr. C, Data Protection Officer and D, attended as representatives of Eurobank. 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/8666/08-07-2022. The said memorandum states the following: At the Bank, as soon as the content of the Authority's Decision 48/2018 became known, a series of meetings were immediately held with all its competent services and with the participation of the Bank's Data Protection Officer, during which decisions were taken for its compliance with the Decision and a specific timetable for their execution was approved. For the issue concerning the conduct of contactless transactions using cards for an amount less than 25 euros, the Bank has fully complied with the content of the Decision. In particular, the Bank implemented the necessary technical infrastructure and developed a special procedure for its customers to have the possibility of deactivating the contactless operation of their cards. Out of a total of approximately 3.2 million cards, the Bank has received only 1,358 related requests, (percentage 0.043%), all of which it has satisfied. In fact, the fact that there have been cases of customers who changed their minds and requested the reactivation of contactless transactions, which the Bank also carried out, is characteristic. For the second issue concerning the history of transactions kept on the card chip, the Bank, as it has already informed the Authority, in full compliance with the Decision as early as July 2019 for debit cards and from October 2019 for

credit cards, configured the new cards as a whole in such a way that they do not store on their chip the transaction history (amount and date of the last 10 transactions) carried out using these cards. It is noted that: (a) this configuration concerns Mastercard cards, as VISA 7 cards do not store transaction history data on the chip, (b) the 10 transactions stored on the card's chip are transactions carried out only with the "presence » of the card itself (and not in any other way (e.g. through online shopping) and (c) at the date of the memorandum, more than 2/3 of the Bank's issuing cards do not store the said information on their chip transaction history data In relation to the remaining cards on which said transaction history data is still kept, the Bank points out that: a) These cards will be replaced on the basis of their expiry date or at any earlier time in the event of their loss or theft with the Bank's new cards, in which transaction history data will not be kept. The largest percentage of these cards, based on their expiry date, is expected to be replaced by 31.12.2023. b) With regard to informing the owners of these cards regarding the observance of the above two historical data on the chip of the card, the Bank considers that this information should not be provided because: i) The relative risk for the owners of the cards in question is very limited, since as far as the Bank is concerned, it can neither have access to these details through the card itself, nor does it have any benefit from maintaining the historicity of the two details on the card's chip. He cannot have access to these details through the card itself as these two historical details are not required by the POS (and therefore by the Bank) when carrying out the transactions. But the Bank does not have the same benefit from keeping these details on the card's chip, given that both the two details of these last 10 transactions and other relevant details are kept by the Bank in its systems anyway. If the Bank wanted to further process the data of the cardholders (e.g. to compile their profile), it would obviously do so, under the conditions of the law, relying on the data it holds in its 8 systems and not on the restricted (and not accessible by her) information inside the card chip. As for any third party attempting to gain illegal access to these details (e.g. by stealing the card), practically the only risk to the cardholder is that person carrying out transactions with the card and not using some historical data that would they were useless to him. Even if a card thief had the necessary technical infrastructure to "read" the card's chip, his intention would be to make immediate use of it and not to profile the person from whom he removed the card. Informing the owners of the specific cards about the fact that the history is kept on their chip would create an unjustified panic in the banking ecosystem (since the issue does not only concern the Bank in question) but also in the economy and society in general. This information, possibly magnified by people who develop conspiracy theories through social networks, could create such confusion in the banking market that the call centers of the banks and their branches would be flooded with customers

who would request an immediate replacement of their cards, which would be practically impossible, given the great difficulties banks as a whole are facing in supplying cards as a result of the pandemic and the global chip shortage. It is possible that many avoided using their cards, with whatever consequences this fact would have had on the economy. The above would have the consequence, among other things, that the banks would have to use large resources for the communication management of an essentially non-existent and without any substantial risk for the holders of these cards issue, in order to restore consumer confidence in the cards and 9 ii) iii) to be reassured of any concerns they may have. The Bank's opinion is that applicable in this case would be par. 5(b) of article 14 of the GDPR, which makes it unnecessary to provide the relevant information to the said data subjects. Furthermore, the memorandum states that, in any case, the Bank continues, based on its relevant planning, to replace the cards in question with new ones, so that by the end of the next year, the largest percentage of these cards will have been replaced. 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 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, this law 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 GDPR 10 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 person responsible processing either 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 cost 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". 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 11 following conditions (legal bases of the processing) applies: "a) the data subject has consented to the processing of 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 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 the fundamental rights and freedoms of the data subject that require 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 par. 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 information provided to the data subjects or the data is collected from the subjects themselves or not) and any communication under Articles 15 to 22 (which concern the rights of data subjects to object3 to data processing, including Article 21 processing) regarding 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 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

paragraph 1 point 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". 12 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 data controller, upon receiving the personal data, provides the data subject with all of 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 Eurobank debit/credit card, 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. Besides, Eurobank actually started, as described in its history, issuing cards without this technological feature – which, moreover, as it notes, it never used. 9. For the processing in question, Eurobank did not provide relevant information to the data subjects (ie the holders of the cards in question), as it appears from its documents to the Authority. It should be noted that the Authority, already with Decision No. 48/2018 (which was based on the legal framework in force before the GDPR), identified the deficiency in question in two other Banks and addressed a recommendation to them in order to remedy it, while subsequently notified the aforementioned Decision to Eurobank, requesting that it take care to ensure that everything contained in it is fulfilled - that is, it adopted the mildest possible option. 10. In the absence of the relevant information, which in any case is an obligation of the data controller according to the above, the legal basis of said 13 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 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 there are, after all, a number of corresponding debit/credit/prepaid cards without the feature in question, which, moreover, as mentioned above, is implemented on an optional basis. Therefore, the only possible legal basis seems to be that of article 6

par. 1 item. at. And in this case, however, apart from the fact that the Bank has not documented what is the legitimate interest it seeks by storing this data on its customers' cards, but on the contrary, it states that there is no need for such processing and did not make use of it, it is required on the one hand that the processing be transparent but this condition was not met for this particular case, and on the other hand that the data subjects know in particular about the existence of the right to object to the processing in question (Article 21 of the GDPR), while nor does this condition apply in this case. Regarding this issue, the Authority, with Decision No. 48/2018, determined that the Banks, in addition to informing the data subjects, should provide the possibility, to those of them who wish, to express the 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. Eurobank, although it initiated procedures on the basis of which every new card it issues does not carry the feature in question and therefore, gradually, discontinues the 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 ». 14 said processing, did not inform the cardholders about this processing, therefore not complying with Decision No. 48/2018 of the Authority, which was notified to it in order to be informed and take the appropriate actions. 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 main argument invoked by the Bank for the reasons of non-information lies in the fact that it considers that the data in question is not personal data and, therefore, there is no processing of personal data - so there is no obligation processing information. Furthermore, the Bank also develops reasoning to demonstrate that, even if the data is considered personal, there is essentially no risk for the affected persons. However, the claims in question are unfounded for the following reasons: a) There is clearly a possibility - and indeed an ease - of associating the data in question with the subject thereof. First of all, the card itself states on its front the name of its holder. Therefore, if a third party - who may in any case also belong to the owner's intimate social environment - manages to gain access to it and read the data in question (which, as described below, is not difficult), he can clearly to draw the conclusion about which person they concern. Therefore, and taking into account Article 26 of the GDPR, the data in question is clearly personal data and is not anonymous information, as the Bank incorrectly claims. b) The obligation to inform about the processing and in general the fundamental principle of the transparency of the processing exists regardless of whether or not there is a risk from the processing for the data subjects5. In fact, even if there is no high risk from the

processing in question for the affected persons, the claim that in essence no , but the specific case clearly does not fall under them (see article 23 GDPR). 15 there is no risk is not sufficiently documented for the following reasons: i) The data in question can be read and intact. The equipment required to read the data is readily available to anyone. Specifically, as already described in Decision No. 48/2018 of the Authority, any "smart" device (e.g. "smart" mobile phone) with appropriate software (which is freely available) is sufficient in order to read the data. ii) For contactless reading of the data, the card should be near the "reader". However, this does not necessarily mean that the card has been stolen/lost. For example, a third party close to the data subject may, if in the vicinity of said card of the data subject, read said data intact. family/friendly/professional environment 12. The Bank further states that such an update would cause concern to its customers and disruption to the banking system and the economy in general, stating that the banks' call centers and branches would be flooded with customers requesting immediate replacement of their cards, which would be practically impossible given the great difficulties banks as a whole are facing in supplying cards as a result of the pandemic and the global chip shortage. However, with regard to this claim, the provisions contained in the above Opinion 11 regarding the non-exemption of the data controller from the obligation to inform apply in principle. It should be noted that in this particular case, the data is collected directly from the data subject, in which case Article 13 and not Article 14 of the GDPR as invoked by the data controller applies, in terms of the obligation to inform - even if the article 14, it states, for the cases for which there may be an exception from the obligation to inform, that 16 "the data controller takes the appropriate measures to protect the rights and freedoms and the legal interests of the data subject, among others making the information available to the public'6. Therefore, even in such a case, a general information should be provided. Furthermore, the claim that such information would cause concern is not sufficiently substantiated: precisely because the risks from the processing are not high, it does not follow that a properly worded information about this processing would cause concern. However, it does not appear that the Bank thoroughly examined appropriate information texts in order to reach the above conclusion. Moreover, 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 and their monitoring, if they are indeed excessive in number, could lead to in appropriate procedures for 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 of said processing. And the claim about the extraordinary conditions of the pandemic is also not true, given that the Bank had been informed by the Authority of

the obligation to inform the subjects of the data, regarding the processing in question, already in 2018 (two years before the start of the pandemic) . In any case, the 6 In particular, as stated in article 14 paragraph 4 of the GDPR regarding the information provided to the data subjects if the personal data have 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 involve a disproportionate effort, in particular with regard to processing for archiving purposes in the public interest, for scientific or historical research or statistical purposes 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." 17 obligation to inform which falls on the data controller noit is removed in principle from the costs that it will bring.

13. Based on the above, the Authority considers that there is a case to exercise the v
the article 58 par. 2 of the GDPR corrective powers in relation to
found violations.

14. The Authority further considers that it should, based on the circumstances established,
to be imposed, pursuant to the provision of article 58 par. 2 sec. i of the GDPR,
effective, proportionate and dissuasive administrative fine according to
article 83 of the GDPR both to restore compliance, and for
punishment of illegal behavior.

Furthermore, the Authority took into account the criteria for measuring the fine which
are 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 falls under,
in accordance with the provisions of article 83 par. 5 sec. II GDPR, in
higher intended class of the grading system
administrative fines8,

b. said violation constitutes non-compliance by the person in charge

processing with the instructions of the Authority formulated through it

No. 48/2018 of the Authority's Decision,

c. the breach concerns a large number of data subjects –

specifically, all Eurobank customers who

debited the old version Mastercard credit card,

d. the violation is continuous, since according to Eurobank's documents

it appears that the processing has been taking place since at least 2018 and

7 https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-

calculation-administrative_en

8 "More important" violations are defined as those that may result in

maximum possible fine of 20,000,000 euros or, in the case of businesses, up to 4% of

of total worldwide annual turnover of the previous financial year, in

contrary to the other violations included in article 83 par. 4 of the same article

continues until today,

e. the activity had a wide scope, as it concerns every "movement"

Mastercard debit/credit card (issued by

Bank) in a physical store, regardless of geography

location of this or type of transaction, if it is a card

old version that has not been replaced

f. the activity is related to its main activities

controller, regardless of whether the data in question

which are held on the card chip, and which already exist

legally processed, in a different context, by the Bank

(since information regarding it is kept in its systems

movement of the card), it does not appear that they were used by the

Bank.

g. the processing concerns data of an economic nature, for which

there is a risk, according to what is mentioned in its rationale

present, to come to the knowledge of third parties,

h. the violation was intentional, since the Authority already had

inform the Bank about Decision No. 48/2018 and

Bank made a strategic decision not to comply with the

included in it (as requested by the Authority) but, instead, to

gradually begin to stop said processing,

i. the information available on the internet9 about its financial income

Bank for 2021,

and also that:

a. This processing does not result in financial loss for the

data subjects,

b. the Bank would not obtain any financial benefit from the

9 See https://www.eurobank.gr/-/media/eurobank/omilos/enimerosi-

ependuton/navigational/oikonomika-apotelesmata/oikonomikes-katastaseis-2021/etisia-oikonomiki-

ekthesi-dec-2021.pdf (last access: 19/8/2022)

due processing,

c. the Bank took actions for the gradual discontinuation of the aforementioned

processing.

15. Based on the above, the Authority unanimously decides that it should be imposed on

reported controller referred to in the ordinance

administrative sanctions, which are judged to be proportional to the severity of the

violations.

FOR THOSE REASONS

The beginning,

It imposes on EUROBANK ERGASIAS S.A. , as controller, the

effective, proportionate and dissuasive administrative fine which

appropriate in the specific case according to the special circumstances

thereof, in the amount of twenty thousand euros (20,000.00) euros, for the above established

violation of article 13 of Regulation (EU) 2016/679, according to article 58

para. 2 i' of the GDPR in combination with article 83 para. 5 of the GDPR.

The president

Konstantinos Menudakos

The Secretary

Irini Papageorgopoulou