Athens, 03-10-2022 Prot. No.: 2434 DECISION 56/2022 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 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 Alphabank 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, Alphabank Bank and Eurobank Bank 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. Alphabank responded with document No. G/EIS/4901/12-07-2019, stating the following: 1) The risks from the use of contactless cards for transactions are theoretical, and a number of arguments are listed, such as that their owners are aware of this, the executives of the businesses cooperating with the Bank have been trained to ask each customer if they want a contactless transaction, if there is a customer complaint the amount will be returned, etc. In any case, the Bank gives the possibility to its customers, if they request it, to deactivate the possibility of contactless transactions from their cards. 2) With regard to keeping, on the card's chip, the history of the transactions made through it, the Bank states that this characteristic is only carried by Mastercard cards, i.e. it concerns a small part of the cards issued by the Bank and grants. It only concerns the observance of the last ten

(10) transactions and was implemented based on Mastercard instructions. Said information is of no use and poses no risks, stating in particular that any third party who finds or steals a card has no interest in reading said information, while the cardholder, in addition to knowing his transactions , it needs special equipment to "read" this information. In any event, the Bank has ordered new Mastercard-branded cards without the feature in question, which will be issued either to new customers or to existing customers in replacement of cards already issued to them. 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 complied with the provisions contained in Decision No. 48/2018 of the Authority regarding the part of informing cardholders about keeping a history of transactions on this chip, pointing out that he did not received such information, sent to Alphabank the document No. C/EXE/2603/15-11-2021, with which it requested the Bank to specifically clarify the actions it took regarding the issue of compliance with credit/debit card (for those cards that had the feature in question), clarifying in particular whether it duly informed all the latest transactions on the chip history of the 4 holders of the above cards for the said processing, regardless of whether, in the meantime, the their cards have already been replaced due to the expiry of the older ones. Alphabank responded with the document No. G/EIS/8351/23-12-2021, stating the following: 1) The amount of a transaction and the date on which it took place is, according to the Bank's claims , objectively impossible to lead, in any way and in combination, directly or indirectly, to a determination of the identity of a natural person. The owner is identified by the other information stored on the card chip (such as the PIN) and printed on it (such as its number), which are used for this purpose by all cards issued including those with the VISA marks, which do not have the possibility to store the above transaction details. Consequently, the transactional profiling of the holder could only be done if a third party obtained possession of the card with which the transactions were carried out and had the necessary expertise and infrastructure to "read" the contents of the "chip". But the third party who steals or finds another person's card with the intention of using it illegally, on the one hand learns the personal data of its legal owner, which are printed on it, and on the other hand can cause the latter much more damage by using it instead of trying to find out what the legal owner's last ten transactions were. And if the third party is a relative who "borrowed" the card, he obviously knows the financial capabilities of its legal owner and his related personal data, so he still has no reason to bother finding out where they were made. last ten transactions 2) The data recorded in the memory of the "chip" are not personal data within the meaning of the GDPR, they cannot be used to create a

profile of a specific natural person and are 5 completely useless to any third party who acquires the card , but also to the holder, the business in which the card was used and the Bank. They are useless to the owner because he knows where and how he used his card, while he receives a relevant receipt and monthly updates that include all the details of every transaction carried out during the immediately preceding month. In business they are useless because every business knows all the transactions that take place in it, as well as whether their consideration was paid "in cash" or by card. In the latter case, she also knows all the details of the card, which are the personal data of its legal owner, on the one hand because based on this, she will be paid the price of the transaction by the Bank, and on the other hand, because if there is a transaction dispute, she will have to locate it in order to act accordingly. Finally, the bank that issued the card obviously knows all the personal data of its customer - the cardholder, as well as all the transactions carried out with it because it pays the businesses in which the card was used, charges the account of the holder and periodically informs both the business, as well as the owner for the transactions carried out with it, the corresponding debits and credits of their accounts. Following all of this, the Bank concludes that the recording of the above two items (amount and date of transaction) in the memory of the "chips" of the specific cards, with MasterCard marks, in addition to the fact that these are not personal data according to the GDPR , poses no risk to the owner, because they are completely useless to any third party. 3) In addition to the above, the Bank has already proceeded to order new cards without the above feature, with which it replaces the MasterCard cards that have this feature gradually upon their expiration and the majority of the old cards have already been replaced. In particular, the ordering of MasterCard cards with the above 6 possibility was stopped already in April 2018, before the start of the application of the GDPR, and the stock of the cards that had been ordered and received until then was exhausted in July 2019. Therefore, since then the cards issued either for the first time, or to replace already issued ones, they are not able to store the above information. 4) To abolish the above possibility, it is not enough just to produce cards without it, but the machines that personalize the cards must also be adapted accordingly, i.e. they register on their chips and print the personal details of the owners on the plastic. This adjustment is not the result of a simple intervention in these machines, it is of a permanent nature, so that they must follow the rate of expansion of card production from the post-April 2018 orders. 5) In conclusion, the Bank summarizes that it did not inform the owners of the above cards because: a) the storage of the specific information, and not personal data (as the Bank claims), in the memory of the "chips" of their cards absolutely poses a risk for them, b) if, despite this, it were to proceed with relevant information, it would create unjustified concern and confusion for the owners, which would affect, practically without reason,

the reliability of the specific trading systems and indeed the period when the state makes continuous efforts to expand transactions with cards, as a means of reducing tax evasion and security of traders from the pandemic, c) to deal with the above extremely unfavorable result, many working days and significant costs would have to be allocated, which would be added to the cost of information, d) consequently updating would be extremely dangerous and unprofitable. 7 The Bank does not mention that, even if it was a matter of processing personal data, the third case of article 14, par. 5 (b) of the GDPR, for the exemption from the obligation to inform, would apply. Finally, the Bank states that, with regard to consent, the issue of the legal basis of the comparative processing could be raised if the specific data, to which the specific storage relates, were personal data. However, according to the Bank's claims, storing only the amount and date of the transaction does not constitute processing of personal data. 6) The Bank also states that it was not a party to the case for which Decision 48/2018 was issued. However, she briefly brought the above to the attention of the Authority in her letter of 11.7.2019, to which she did not receive a response and, therefore, considered that they were accepted. Subsequently, the Authority invited Alphabank to a hearing, via video conference, at the Plenary meeting of 14-06-2022 (see call with prot. no. C/EXE/1333/02-06-2022). During the meeting of 14-06-2022, Mr. B, Mr. C Deputy Director ..., Mr. D, Director ... and Mr. E, Data Protection Officer, attended as representatives of Alphabank. After the meeting, the data controller was given a deadline to submit a memorandum, which he submitted, within the set deadline, with document number C/EIS/8620/07-07-2022. The following are mentioned in the memorandum in question: a) With reference to the issue of contactless transactions, with the above-mentioned letter of 11.07.2019 to the Authority, the Bank, after presenting for the first time the reasons why there is practically no risk of the contactless operation of the cards, informed that a very limited number of requests from cardholders had until then been submitted for the deactivation of the above feature, all of which had been satisfied (and this despite the considerable publicity received by the above Decision of the Authority), as well as that technical 8 implementation had already started at the Bank so that basic card products without the possibility of contactless transactions were made available to its customers. Following this, the Authority did not return to the specific issue until the hearing procedure described above, during which the Bank confirmed what had been reported at the time. So this particular feature is now widely known among cardholders, very few of whom have so far requested the deactivation of this feature: about 6,000 holders out of 4,000,000 customer-holders (0.15% rate). In any case, Alpha Bank supports the possibility of deactivating contactless transactions at the customer's request at any branch of the Bank and by telephone at its customer service center. In fact, this possibility has now been incorporated into the contract

for the issuance and use of the card (relevant documents have been submitted with the Bank's memorandum). b) Regarding the issue of maintaining the transaction history on the card chip, the Bank addressed the Authority for the first time with the above-mentioned letter of 11.07.2019, in which, after noting that the specific possibility was provided only by the MasterCard Card Organization for the cards that bear his marks and that in practice the storage of the relevant data on the one hand was not useful for those involved in card transactions (holder-business-bank), and on the other hand does not pose any risk for the holders, he informed that, in response to the as above Decision, had already ordered the new cards with the MasterCard brands without this possibility, so that from the following month (August 2019) the new cards that would be granted henceforth would not have this possibility. So gradually there would be no cards with the ability to store transaction data. With the latest letter from the Bank to the Authority dated 21.12.2021, the following was clarified: i) Only the cards with the MasterCard brands have the above storage facility and not the cards with the VISA brands, so that the 9th issue concerns the approximately 50% of the cards issued by the Bank, ii) The storage concerns only two items of the last ten (10) transactions: the amount of the transaction and its date, iii) Since it is impossible to identify the cardholder from the above information, this is not personal data within the meaning of the GDPR, iv) The above information is useless to the cardholder, the business in which it was also used in the Bank, issuer or recipient, because they acquire and process all personal data, and not just details, of each card transaction, in the context of the activity and operation of each of them. Finally, the Bank argued that, even if it were accepted that the above information is personal data, the relevant information to the subjects-owners, for whom the above storage poses absolutely no risk, would cause unjustified disturbance and concern in the market, which it would hurt, not just the specific cards, but the card trading system as a whole. For this reason, he did not proceed with relevant information pursuant to article 14, par. 5 (b) of the GDPR. c) This specific case concerns the two specific elements of transactions with cards bearing Mastercard's marks: the amount of the transaction and its date. Only these details are stored in the chip of the specific cards, as confirmed by MasterCard. According to the Authority's Decision, "keeping this data raises data protection issues since the card's movements can create a profile of its owner in terms of his consumption habits". From this proposal it follows on the one hand that the two above items are considered personal data and on the other hand that the consumer profile of a specific natural person can be derived from their combined processing. According to the GDPR (article 4, par. 1) personal data is any information that concerns an identified or identifiable natural person. The natural person whose identity can be ascertained indirectly through reference to another identity identification element, such as name, identity number, location data, etc., is not

identifiable. 10 In this particular case, the above specific elements cannot, at the discretion of the Bank , to be combined with any other identification data of the owner, unless someone acquires the card, on the chip of which they are stored. The card is in the possession of its owner, who, according to the contract for its issuance and issuance, is the only person who must possess and use it. In fact, the card must be in the holder's possession at the time of the transaction since he must use it at the POS and he must enter the PIN. Furthermore, as far as the business in which the card was used is concerned, it does not come into its possession, while the POS does not have the possibility to "read" the above information registered on it. But even beyond these, the merchant who accepts cards to pay the price of the products and/or services he sells, obtains all the details of each transaction carried out by the owner and then receives them aggregated with each periodic clearing of his account from the Bank, which credits his account with the amount of transactions carried out. Therefore, on the one hand, the merchant cannot read the specific field of the card's memory and on the other hand, he has all the data of the transactions carried out with him, including the amount and date of each transaction. cards in the store The third pillar of card transactions is the Bank, which contains all the data from every transaction of the holder with his card, because it clears these transactions, crediting the accounts of the merchants where the transactions took place with the consideration them and correspondingly debiting the accounts of the owners who made them. Therefore, the Bank has at its disposal every personal data of the holder concerning the transaction, including of course the amount and the date of each transaction, so that there is no need to "read" the specific field of the card, which is not in its possession. 11 There is practically no risk for the owner from the above two specific elements of the last ten transactions he carried out, even in the case that his card would be illegally in the possession of a third party, in which case it could theoretically be argued that these in combination with the personal data identification of the holder are imprinted on the card, they become personal data. And this is because the person who obtains the card illegally will also try to use it illegally at the owner's expense, either in a commercial store or at an ATM, if of course he also obtains the owner's PIN, and then throw it away. Therefore, as the Bank states, the thief will not be interested in learning the consumer habits of the owner and much more in having procured the special device or the special software (reader) for reading the field of the chip, in which the above two are registered data. Following the aforementioned, there is no question of identifying the owner with the specific two elements, so that these are not personal data in the sense of the GDPR, nor is there a question of third party access to them. But even if it is assumed that these two items are personal data, it would not be possible to establish the consumer profile of the holder only from the amount and date of the last ten transactions of the cardholder, without knowing

the type of transaction, i.e. if it is to buy a book or clothes or to use it in a restaurant or to buy a coffee etc. With all the above mentioned in mind, the Bank states that the question is reasonably raised why Mastercard included this feature in the features of its cards. The answer, as reported by the Bank, was given by MasterCard and reflected in the Authority's Decision: this data can be used by the issuers (of the cards) in the context of resolving disputes concerning transactions. In practice, this is an additional piece of evidence for the execution of a transaction, the execution of which the holder disputes. 12 D) As argued by the Bank, the two specific items stored on the chip of the specific cards are not personal data within the meaning of the GDPR, so that there is no question of its application and by extension the obligation to inform the holders. Even if, as a working case, it were accepted that it is personal data, any information to the specific owners, for whom, as mentioned above, there was no risk, would have extremely adverse consequences. It would create serious concern for the holders of MasterCard cards, who would automatically be in a much more unfavorable position compared to other cards, mainly VISA, which is a direct competitor of MasterCard, but also other cards, such as American Express, or of Diners. This concern would then inevitably extend to the card payment system as a whole, for the integrity of which serious doubts and concerns would be created, with the usual help of social media, about alleged monitoring of the holders. In order to deal with the above results of the update in the future, a lot of work would have to be spent and serious funds allocated, from all the publishers, probably not only the Greek ones. It therefore follows directly, according to the Bank's claims, from the aforementioned that, even if it was a matter of processing personal data, any update by providing relevant information would greatly damage the rest of the processing of cardholders' personal data for the operation of their cards and the unhindered carrying out of transactions with them and it would end up taking a huge effort and cost to reverse the unfavorable consequences of the update. Therefore, as the Bank mentioned above, it would be a matter of applying subsection b, paragraph 5 of article 14 of the GDPR, which introduces an exception to information, but also subsection a' of the same paragraph, as long as the owner is undoubtedly already aware of the above information. 13 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 (EU) 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 name, identity number, location data, 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 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". 14 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 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 15 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 form. 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). 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 item e) or f), including profiling under 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". 16 8. In this particular case, for the processing which consists in storing, on the chip of the Alphabank 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 data 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, Alphabank 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, Alphabank Bank did not provide relevant information to the subjects of the data (i.e. to the holders of the cards in question), as can be seen 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 Alphabank Bank, requesting that it take care to fulfill all that is included in it - i.e. it adopted the mildest possible option. 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 the conditions in question are not met 4 See the definition of consent in article 4 par. 11 of the GDPR, as "any indication of will, free, specific, explicit and fully informed, 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 ». 17 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 - after all, there are a number of corresponding debit/credit/prepaid cards without this feature, 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 legal interest that it seeks by storing this data on its customers' cards, it simply mentions the purpose of keeping this data that it itself invokes Mastercard, while the Bank itself states that it did not make any use of the processing in question, it is required on the one hand that the processing is transparent but this condition was not met in this particular case, and on the other hand that the data subjects know in particular and for the existence of the right to object to the processing in question (Article 21 of the GDPR), while this condition does not apply in this case either. 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. Alphabank, although it initiated procedures based on 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 Decision No. 48/2018 of the Authority which was communicated to it in order to be informed and to 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 for not informing lies in the fact that it considers that the data in question is not personal data and, therefore, 18 there is no processing of personal data - therefore it is not processed and there is no obligation to inform about the processing . Furthermore, the Bank develops reasoning to demonstrate that, even if the data is considered personal, there is essentially no risk for the affected persons, as well as that the third case of article 14, par. 5 (b) of GDPR, for the exemption from the obligation to inform, due to the fact that the information would be unprofitable and dangerous. 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 owner. 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 there is essentially no risk is not sufficiently substantiated for the following reasons: i) The data in question can be read intact. The equipment required to read the data is readily available to anyone. Specifically, as it already had 5 Restrictions on rights can be imposed by EU law or the law of a Member State under specific conditions and if appropriate safeguards are provided, but the specific case clearly does not fall under them (see article 23 GDPR). 19 is also 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 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 c) 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 claimed by the data controller applies, in terms of the obligation to inform. However, even if article 14 applied, it states, for the cases for which there may be an exception from the obligation to inform, that "the data controller takes the appropriate measures to protect the rights and freedoms and the legal interests of the subject of the data, including by making the information publicly available"6. Therefore, even in such a case, a general

information should be provided. 12. The Bank additionally states that such an update would cause concern to its customers and would affect, not only the 6 In particular, as stated in article 14 par. 4 of the GDPR regarding the information provided to the data subjects if the personal data nature have not been collected from the data subject, "paragraphs 1 to 4 shall not apply if and as long as: a) the data subject already possesses the information, b) the provision of such information proves impossible or would entail a disproportionate effort, in particular as regards 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 impair 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." 20 specific cards, but the card trading system as a whole. Furthermore, in order to deal with the results of the above information, a lot of work would have to be spent and serious funds allocated, while the Bank also raises the issue of competition between Mastercard and Visa companies. However, with regard to these claims, the provisions contained in the above Opinion 11 regarding the non-exemption of the data controller from the obligation to inform apply in principle. 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, even if the Bank considered that such an update would entail a large number of requests to replace cards, this judgment cannot lead the controller to the conclusion that it is exempt from the obligation to update because the management of the requests and their monitoring, if indeed they are excessive in number, it could lead to appropriate procedures to satisfy them: for example, it could possibly be judged that this replacement would not take place immediately, taking into account the not particularly high risks of said processing. Also, the arguments invoked by the Bank regarding the competitive environment between credit card companies cannot be accepted as reasons why the obligation to inform data subjects may be waived. In any case, this obligation, which falls on the data controller, is not removed even by the costs that it will entail, while the information, as a key aspect for the fundamental principle of the transparency of the processing, as long as it does not fall under the cases that can to be excluded from the obligations of the controller, it cannot be characterized as "dangerous" as the Bank characterizes it in this particular case. 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. 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 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 Alphabank customers who

debited the old version Mastercard credit card,

d. the violation is continuous, since according to Alphabank'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,

9 See https://www.hba.gr/4Statistika/UplPDFs/2021/2021AlphaBank(EL).pdf (last access:

8/19/2022)

23

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

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 ALFA BANK SA, 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

24