Athens, 06-08-2018 Prot. No.: G/EX/4986/08-06-2018 HELLENIC REPUBLIC PERSONAL DATA PROTECTION AUTHORITY A P O F A S I NO. 48/2018 The Personal Data Protection Authority met in its headquarters on 24/04/2018 at 10:00 a.m. following the invitation of its President, in order to examine the case referred to in the present history. The President of the Authority, Konstantinos Menudakos and the regular members of the Authority, Konstantinos Christodoulou, Antonios Symvonis, as rapporteur, Spyridon Vlachopoulos, Konstantinos Lambrinoudakis, Charalambos Anthopoulos and Eleni Martsoukos were present. Constantinos Limniotis, IT auditor, as assistant rapporteur, and Irini Papageorgopoulou, employee of the Authority's Administrative Affairs Department, also attended the meeting, as secretary. The Authority took into account the following: The Consumer Protection Directorate of the Ministry of Economy, Infrastructure, Shipping and Tourism forwarded to the Authority, with the number of ... and dated ... its document (Authority's number: C /EIS/2819/18-05-2015) the complaint - with all supplementary and related documents - of A against the National Bank of Greece SA - hereinafter, National Bank - regarding the debit card that the Bank issued to ... to its complaining customer, to replace his old card. This new card supports contactless transactions – i.e. transactions that can be carried out without entering a PIN on his part, but only by showing the card, without contact or placement, at 1-3 Kifisias Avenue, 11523 Athens, Tel. : 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -1- corresponding reader device, as long as the financial transaction does not exceed twenty-five (25) Euros. The complainant claims that he did not give his consent to be issued a debit card with these features (ie contactless) and also that he does not wish to have such a card due to security risks arising from its use. Also attached to the above document is the document that National Bank sent to the complainant on ..., in response to his written objection to the Bank receiving the card, in which document it is stated, among other things, that the possibility of using DebitMasterCard contactless technology transactions for purchases worth less than 25 Euros without the use of a PIN is a mandatory feature of the card according to the guidelines of the international organization Mastercard. The National Bank also states in its above response that the new card meets all the security safeguards provided by international organizations, as well as that the replacement of the old card with the new contactless card is in accordance with the terms of the contract with the complaining customer of his debit card – specifically, he refers to clause 2 of the contract between them, in which it is stated that "the card on which the holder's name is imprinted belongs and remains the property of the Bank", as well as clause 12 where it is stated that "due to the indefinite duration of this contract, the Bank reserves the right to unilaterally supplement or modify the terms of the contract for an important reason". Furthermore, it is pointed out in said document that the complainant has the possibility to

request the change of his daily purchase limit to zero (0) Euros. The said document was forwarded by the National Bank to the Directorate of Consumer Protection, in response to a related document of the Directorate regarding the Bank's views on the complaint. The same complaint, with all the supplementary and related documents in the file, was forwarded to the Authority and by the Consumer Advocate with the no. prot. ... and from ... his document (No. prot. Authority: C/EIS/3198/05-06-2015). In a relevant document of the Consumer Advocate, National Bank responded by sending him the above-mentioned response to the complainant. The Consumer Ombudsman informed the complainant about this, who responded to the Ombudsman saying that there are inherent weaknesses in RFID technology – technology used in contactless cards – in terms of security, and also that the cost of purchasing equipment to exploit these weaknesses is not large, referring to 1-3 Kifisias St., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -2- corresponding web links1 with relevant information, while also requested that his complaint, through the Advocate, be communicated to the Authority. It is also noted that the Consumer Advocate, with no. ... and from ... his document which he communicated to the Authority (No. of Authority: C/EIS/3444/16-06-2015) also informed the Bank of Greece about the complaint in question, sending it all the documents of the case file. The Authority, in the context of examining the complaint in question, sent to National Bank the document No. C/EX/2819-1/05-06-2015, with which it requested the Bank's views on the complaint, stating in particular the following questions: a) What kind of data is kept on the chip of the card in question, as well as which of them are sent to the corresponding "reader" device during the process of charging the account of its owner through a contactless transaction, b) what kind of technical measures are in place to protect this data (both those kept on the card and those transmitted during the contactless transaction with the device-"reader"), c) if it provides its customers with the option of not granting it or completely disabling it of the characteristic of that card that allows contactless transactions to be carried out. Subsequently, given that a period of more than two (2) months had passed without a response, the Authority again sent to National Bank the letter No. C/EX/2819-2/16-09-2015 inviting it resubmit its views and the necessary clarifications within fifteen (15) days. Following this, National Bank (and, in particular, the Regulatory Compliance and Corporate Governance Department of the Bank & the Group) sent the Authority the document No. … /… (Authority No.: C/EIS /5102/06-10-2015), in which he points out, among other things, that the Bank has adopted MasterCard's contactless transaction technology, in which the MasterCard card is equipped with a chip and an antenna. For purchases up to 25 Euros, the holder is not required to enter a PIN – the payment is made automatically by touching the card to the terminal, without having to hand it over to the cashier. The limit of 25 Euros has been

set by the international organization MasterCard as a specification of the terminal and not as a characteristic of the card, it cannot be modified and is valid throughout Europe. In the same document it is also mentioned that the technology of contactless transactions, which is based on the short-range wireless technology NFC (Near Field Communication) 1 Specifically, in the links https://greek1.blogspot.gr/2015/04/rfid.html#axzzEY1OR57oH and http://www.ebay.com/bhp/rfid-reader-writer-usb. 1-3 Kifisias St., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -3- is already implemented in fifty-six (56) countries around the world and in twenty-nine (29) countries in Europe, it is as secure as the MasterCard credit card, while similar technology is also available from Visa. With regard to the specific questions raised by the Authority, National Bank, in its above document, states the following: a) In addition to the technical information regarding the card's communication with the terminal, the card's chip contains the number card, its expiry date, the name of its holder and the PIN in encrypted form. b) The cryptographic keys for the protection (encryption) of the stored data are kept only by the issuer of the card, i.e. the Bank. The information sent during the contactless transaction is only the card number and its expiration date, as well as other purely technical information to complete the transaction. In cases where the cardholder enters a PIN, it is always encrypted in order to be sent to the issuer for verification. c) Since contactless transaction technology is a technical feature of the card, the Bank cannot interfere with its operation. It is up to the holder to declare to the employee of the business with which he transacts that he wishes to carry out the transaction using a PIN. Also, its owner can change the permissible limit for card transactions at any time. Finally, the Bank also provides additional information about the security of the processing, noting that the contactless transaction does not remove the card from the hands of its owner, as well as that it is not possible to carry out a contactless transaction by mistake because the card is activated exclusively if theits owner approaches it at a terminal at a distance of less than 5 cm, while the relevant procedure must also have been completed at the company's cash register, nor is there any risk of double and/or multiple billing. Also, any fraudulent transactions, which according to the statistics are nil, can be disputed by the holder using the same procedure as for credit or debit card transactions using a PIN. Furthermore, each cardholder must take every possible precaution for the safe keeping of his card, while the Bank provides a 24-hour telephone service line for any declaration of its loss or theft, while there is also a special team that monitors with 1 Kifisias St. 3, 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -4- specialized software all electronic transactions, in real time, on a twenty-four-hour basis, in the control framework , prevention and suppression of electronic fraud. Finally, it should be noted that the capabilities of the

cards for contactless transactions have been set based on the specifications of international organizations, so there is no possibility of derogation and therefore the disposal of the old debit cards no longer exists. Subsequently, the Authority sent to National Bank the document No. C/EX/2819-3/30-10-2015 - and subsequently, due to no response, the document No. C/EX/663/05-02-2016 document – in order to provide additional clarifications. In particular, taking into account that during a contactless transaction the card number and its expiry date are sent unencrypted, the Authority requested that the reasons why it is not possible to deactivate the feature of the card that allows contactless transactions to be carried out , in the event that a customer requests such a deactivation, noting that, since the specific operation relates to the technical implementation of the card and the Bank is not in a position to respond, they should contact the relevant body (MasterCard or whoever else may decide the Bank necessary) in order to have the relevant documentation. The Authority also requested that any written documentation available to the Bank be forwarded that demonstrates that personal data protection issues were taken into account already during the design of the card (e.g. Data Protection Impact Assessment - DPIA). In response to this, National Bank sent the Authority the document numbered ... and from ... (Authority number: C/EIS/1282/26-02-2016), to which the reply from ... is attached of MasterCard to the Bank. As noted in MasterCard's document, issuers have the ability to offer cardholders a choice between contactless or conventional payment methods, and the activation and deactivation of the contactless profile is possible after the card is issued - ie, the issuer may decide whether to enable the contactless interface or not for a specific card. To this end, National Bank points out in its above document that the deactivation of the profile that allows contactless transactions to be carried out on specific cards after their issuance requires the adoption of a different authorization policy for specific cards, which requires complex and L. Kifisias 1- 3, 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -5- technical changes and upgrades. Therefore, the relevant project was chosen not to be systematically supported by the Bank, given that each user retains the freedom to use or not use the specific profile as the case may be. Therefore, contactless interface is by default a feature of new debit cards, while a different product (contactless card) is not systemically supported – and therefore not provided. Finally, in the above MasterCard document it is pointed out that a thorough privacy impact assessment (Privacy Impact Assessment) has been carried out for the contactless transaction product, based on the corresponding framework for preparing privacy impact assessments and data for RFID applications2 (Privacy and Data Protection Impact Assessment Framework for RFID Applications) of the EU, dated 12-01-2011. The assessment was submitted to European regulatory authorities: the German regulatory authorities were

completely satisfied and closed the case, while the regulatory authorities of other EU countries such as the authorities of France, Switzerland and Poland concluded that the technology in question did not raise privacy and data protection issues. A second related complaint was forwarded to the Authority by the Consumer Advocate. Specifically, with no. ... and from ... his document (authority number: C/EIS/1102/22-02-2016) forwarded a complaint, together with all the relevant documents in the file, of B against Piraeus Bank SA. -henceforth, Piraeus Bank- with which he complains about the change of his debit card to a new card with the possibility of contactless transactions (as in the previous case, purchases of up to twenty-five (25) Euros can be made without entering a PIN, in a contactless way). The above document is also attached with no. first ... and from ... document that Piraeus Bank sent to the complainant and the Consumer Advocate, in response to the complainant's written objection to the Bank. In this Piraeus Bank document it is pointed out that contactless transactions have been established as the main alternative payment method worldwide, especially for small value purchases, which can be made quickly and securely, without the card leaving the holder's hands. Therefore, as the Bank states in its document, the complainant's request regarding the mandatory entry of a PIN in every card transaction cannot be protection of persons against the processing of personal data. 1-3 Kifisias St., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -6- satisfied. Furthermore, a newer document from the complainant to the Consumer Ombudsman is attached to the above document, in which a number of online links3 are listed with information related to the security issues raised by the use of a card for contactless transactions, as well as the one with no. first ... and from ... a letter from the Consumer Advocate to the Bank of Greece, with which - by analogy with A's previous related complaint - he informed it about the complaint in question, forwarding to it all the documents in its file case. The Authority, in the context of examining the complaint in question, sent to Piraeus Bank the document No. C/EX/1102-1/18-04-2016, with which it requested its opinions on the complainants, stating new and the specific questions it had addressed, with its previous documents, to the National Bank. Subsequently, Piraeus Bank responded with the document numbered ... and from ... (authority number: C/EIS/4118/29-06-2016), in which it states that the Bank, as a member of international organizations Visa and MasterCard, but also based on the PCI/DSS (Payment Card Industry Data Security Standard) certification it has, it follows and implements protocols and procedures in order to meet modern needs and technological developments. At the same time, every new product that reaches the final stage of its commercial availability has gone through all the required control stages in order to receive the corresponding certifications from Organizations. In addition, for all card transactions, the Bank carries out continuous checks for the security of customers

on a 24-hour basis and all days of the year. These checks concern both classic and contactless transactions. Regarding the customer's request to disable the limit of twenty-five (25) Euros for contactless transactions without the use of a PIN, this is not possible since the specific limit is set by the Visa and MasterCard organizations and concerns the reception data of the cards and not the cards. The Bank also states that the goal of this technology, which is used internationally, is ease of use and the reduction of transaction processing time, as well as that, if the customer so wishes, he has the possibility to ask the store's service employee not to carry out the transaction contactless but by entering a PIN, Specifically,3 http://thesecretrealtruth.blogspot.com/2015/08/contactless.html, http://www.telegraph.co.uk/technology/internet-security/11758990/Contactless-cards-at-risk-of-fraud -warns- Which.html and http://www.theweek.co.uk/prosper/53317/contactless-cards-what-are-risks. http://makpress.blogspot.gr/2015/07/contactless.html, links are 1-3 Kifisias Ave., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -7- even for purchases worth less than 25 Euros. In the same document, Piraeus Bank also mentions the corresponding claims that National Bank had invoked regarding the fact that it is not possible to make a double charge or a charge by mistake by simply passing near the receiving machine, that in order to carry out a contactless transaction the card will must come within 8cm of the receiving machine and remain close to it long enough to hear the beep, and also that the customer, being responsible for the safekeeping and safekeeping of his card – as with any other card, for contactless transactions or not – should take all appropriate measures of proper use and protection. Regarding the type of data stored on the card's chip, Piraeus Bank states in its document that it concerns data common to all debit cards, as well as data related to the individual customer (without specifying exactly what these data are). Finally, Piraeus Bank reports that the complainant, upon receiving his new plastic card due to the expiry of the old one, also received an accompanying letter informing him of its features as well as the new contactless transaction technology. When new cards are issued, customers are informed about the contactless transaction technology supported by the cards through the contract they sign, a copy of which they receive. In continuation of the above, following a special check carried out by the Authority's employees on 20-09-2016 through the freely available software application Credit Card Reader v.4.2.2 available for the Android operating system, it was found that the data sent by a contactless MasterCard during its contactless operation is indeed the card number and the expiry date, but in addition - also unencrypted - information is sent regarding recent card transactions, i.e. the date of the transaction and the amount of money. The same check, with the same software application, of the data sent contactless from VISA cards,

did not show the sending of the above card movement data (it appears that, when operating contactless VISA cards, the card number and date are sent expiry thereof). Based on the above finding, the Authority sent to Mastercard Greece letter No. C/EX/6148/06-10-2016, requesting its opinions on the above observation regarding the data of recent movements/transactions 1-3 Kifisias St., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -8- which are transmitted without contact. With the same document, the Authority asked whether the aforementioned characteristics of the card (i.e. the data that is kept and sent intact) are known to the Banking Institutions that cooperate with MasterCard to issue cards, as well as whether there is a difference in the implementation of the cards provided by Greek Banking Institutions in relation to other states. Finally, the Authority requested the submission of the aforementioned privacy assessment study conducted by MasterCard for the said contactless cards. In response to the above document, Mastercard (Greece facility) sent the Authority document number C/EIS/180/12-01-2017, in which it states, among other things, the following: a) Mastercard does not issue payment cards to cardholders. In Greece, as in other markets worldwide, cards are issued by banking and financial institutions, which make decisions regarding the implementation and operation of cards and other payment products in the market. b) The use of contactless transaction technology is at the discretion of the issuers. Issuers are the controllers of personal data and are charged with establishing a direct financial relationship with consumers/cardholders. The issuers in this relationship determine, among other things, the type of payment card issued for each cardholder, as well as the relevant technical characteristics of the card. c) Mastercard provides its customers, banking and financial institutions, with the basic infrastructure of contactless transaction technology, as well as all relevant information necessary to be reviewed by issuers before the implementation of each product. Each issuer has the discretion to proceed with the selection of the technical features of the contactless transaction cards it provides to its customers. Therefore, only the issuers are able to provide detailed information about the respective implementation and technical characteristics of the payment products they provide. d) The basic categories of personal data that are kept on the card chip and can be read without contact are the personal account number4 (necessary to identify the issuer and specific account of the holder 4 This is the card number, which is also called "Primary Account Number (PAN)". Kifisias St. 1-3, 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -9- of the card that is connected to the card of contactless payments) and the expiry date of the card (necessary to establish the date beyond which the card can no longer be used). Also, third-party data is kept only if supported by the publisher. This field can be used by publishers to store information related to device type or personal data such as customer loyalty program number.

Mastercard strongly advises issuers not to enter personal data in this field. Finally, transaction logs are kept only if supported by the issuer. This record may include: i) Approved transaction amount, transaction currency code and transaction date. This data can be used by the issuers in the context of resolving disputes concerning transactions, as well as to provide information to cardholders regarding their recent card movements. ii) Data provided by merchants when necessary to calculate the amount charged – for example, the location and/or time of a certain transaction to calculate the fare in the case of transit/transportation. Regarding the transaction log, issuers have the discretion to decide: 1) whether this is necessary, 2) how many transactions will be logged (with a minimum of 10 if the issuer has chosen to support said feature), 3) make the transaction log unreadable by contactless card readers. e) All information related to the processing of personal data in the context of contactless payment technology is known to the issuers. Based on this information, publishers are able to determine the implementation and operation of the technology in question that they provide to their customers. No specific technical characteristics of this technology are foreseen in Greece – it operates based on global technical requirements. f) The privacy impact assessment study carried out by Mastercard – and attached to the above Mastercard document – took into account the optional nature of the contactless payment function, including the possibility of subsequently deactivating its function. In particular, the risk study describes various alternatives offered by Mastercard to issuers to decide how they wish to allow their customers to exercise their right to refuse the use of contactless Kifisias Street 1-3, 11523 Athens, Tel. .: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -10- of operation in advance or later. Also, the Authority, with its document No. prot. C/EX/4942/27-06-2017, requested the opinions of VISA Hellas (a company with which Piraeus Bank has a contract, which concerns the second complaint), in particular as to the type of data and other characteristics of the processing carried out through contactless technology, as to whether Visa obliges issuers (banking institutions) to issue exclusively contactless cards to their customers, if any the technological possibility, in oneissued contactless card, to deactivate the feature that enables contactless transactions so that the card functions as a conventional (i.e. contactless) card and – in an affirmative case – if this deactivation can be carried out by the issuers (Banking Institutions), as well as whether an impact assessment on the protection of personal data has been carried out for the processing in question. Visa Hellas responded with document No. G/EIS/6719/19-09-2017 in which it states, among other things, that international security standards have been adopted for this technology (which it names), as well as and that, at present, Visa does not require card issuers in Greece to ensure that the cards they issue are contactless. Related requirements have been set in some European countries and Greece is going to be

included in them soon. Visa specifications also allow issuers to configure card parameters, which can enable or disable contactless transaction functionality during the card's lifecycle. Visa has also prepared an impact assessment on the protection of personal data, which it submitted to the Authority with its above document. Finally, the Authority, with its document No. G/EX/4943/27-06-2017, requested relevant information on contactless cards from all Credit Institutions operating in Greece with headquarters in Greece5 and, specifically from: i) NATIONAL BANK OF GREECE S.A., ii) ALFA BANK S.A., iii) ATTICA BANK, ANONIME BANKING COMPANY, iv) PIRAEUS BANK S.A., v) EUROBANK ERGASIAS S.A. . with the relevant list, dated April 2017, from the website of the Bank of Greece. 1-3 Kifisias St., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -11- EPIRO COOPERATIVE BANK, xi) PAGRETIA COOPERATIVE BANK CO-OPERATIVE BANK OF N. EVROS CO-OPERATIVE BANK, xiii) CO-OPERATIVE BANK OF KARDITSAS CO-OPERATIVE BANK, xiv) CO-OPERATIVE BANK OF THESSALIA CO-OPERATIVE BANK, xv) CO-OPERATIVE BANK OF PIERIA - OLYMPIC PISTI SYNP.E., xvi) DRAMA COOPERATIVE BANK SYNP.E., xvii) SERRON COOPERATIVE BANK SYNP.E. From the above Institutions, the under iii, viii, ix, x, xii, xiii, xiv, xv and xvi replied that they do not provide their customers with products of this technology6. THE INVESTMENT BANK OF GREECE S.A. (item vi), with its document no. prot. standards set by this organization. It does not provide the option of retroactively disabling contactless functionality, nor does it allow its customers to receive a card without this technology. The Bank also states that the limit for making contactless transactions is a total of 25 Euros in three (3) consecutive contactless transactions, beyond which the use of a PIN is mandatory. AEGEAN BALTIC BANK A.T.E. (item vii), with its document no. prot. the international organization Visa. The Bank states that the data stored on the card's chip are data related to the customer's details that he/she provides when applying for a card as well as data related to the operation of the card, while some of them can be read without contact (e.g. name, card number, expiry date) through a suitable device - "reader". The personalization of the data on the card is carried out in accordance with the standards and guidelines of the Visa organization. If a customer of the Bank expresses a specific objection, the possibility to receive a card of this technology is not provided, while there is the possibility, always following a written instruction of the customer, to parameterize the functionality of this card afterwards, resulting in 6 With the nos. C/EIS/5479/18-07-2017, C/EIS/5348/13-07-2017, C/EIS/5254/10-07-2017, C/EIS/5329/12-07-2017 , C/EIS/5376/14-07-2017, C/EIS/5363/13-07-2017 and C/EIS/6768/21-09-2017 documents respectively C/EIS/5357/13-07-2017, C/EIS/5289/11-07-2017, 1-3 Kifisias St., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -12- months enables

contactless transactions. The reason why the Bank does not offer the possibility of issuing cards for contactless transactions from the beginning is on the one hand the cost and on the other the harmonization with the wider domestic and international competition in the field of cards. The other institutions did not respond to the Authority's above document, apart from Piraeus Bank (item iv), which with its document No. C/EIS/5949/07-08-2017 basically repeated briefly what she had said about her previous paper. The Authority sent a special reminder to ALFA BANK SA. (item. ii) and EUROBANK ERGASIAS S.A. (item v) with her documents No. G/EX/276/12-01-2018 and G/EX/275/12-01-2018, to which she also did not receive a response. The Authority, after examining the above-mentioned facts, after hearing the rapporteur and the clarifications of the assistant rapporteur, who then withdrew before the conference and decision-making, and after a thorough discussion, CONSIDERED ACCORDING TO THE LAW 1. Article 2 of Law 2472/1997, defines that "personal data" is "any information that refers to the subject of the data". "Data subject" is "the natural person to whom the data refer, and whose identity is known or can be ascertained, i.e. can be determined immediately or indirectly, in particular based on an identity number or on the basis of one or more specific elements that characterize the his physical, biological, mental, economic, cultural, political or social status". Therefore, it is noted that debit and/or credit card data, such as the card number and its expiry date, are personal data. In the same article it is also defined as processing of personal data "any task or series of tasks carried out, by the State or by a legal entity of public or private law or an association of persons or a natural person with or without the aid of automated methods and applied to personal data , such as collection, registration, organization, 1-3 Kifisias Ave., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -13- preservation or storage, modification, export, use, transmission, dissemination or any other form of disposal, association or combination, interconnection, blocking (locking), deletion, destruction'. Also, a controller is defined as anyone who determines the purpose and manner of processing personal data, such as a natural or legal person, public authority or agency or any other organization, while a processor is defined as anyone who processes personal data on behalf of the controller (natural or legal person, public authority or agency or any other body). In these cases, both the National Bank of Greece (for the first case) and Piraeus Bank A.E. (for the second case) are the controller, since they provide their customers with a banking product (debit card for contactless transactions), through which they process their personal data - in the context of making charges to each customer's bank account based on the transactions they carry out using the card - and for which product each Bank has chosen the purpose and method of processing. 2. According to no. 4 par. 1 item a) of Law 2472/1997, in order for personal data to be lawfully processed, it must

be collected in a lawful and lawful manner, for specified, clear and lawful purposes and be lawfully and lawfully processed for these purposes (principle of purpose) . In addition, according to no. 4 par. 1 item b) of Law 2472/1997, personal data must be relevant, relevant, and no more than is required each time in view of the purposes of the processing (principle of proportionality). Furthermore, the processing of personal data is only permitted when the subject has given his consent, as mandated by no. 5 par. 1 of Law 2472/1997. It is noted that, according to article 2 par. k' of Law 2472/1997, consent means "any free, expressand a special declaration of intent that is expressed in a clear way, and in full knowledge, and by which the data subject, after being informed beforehand, accepts that the personal data concerning him/her be the subject of the processing". As an exception, the processing of personal data is permitted, and without the consent of the data subject, if any of the following cases apply. gr, www.dpa.gr -14- which are provided for, in a restrictive manner, in par. 2 of this article. In particular, processing is permitted without consent when: "a) it is necessary for the execution of a contract, in which the contracting party is the subject of the data (…)". 3. Article 10, paragraph 3 of Law 2472/1997 stipulates that the data controller must take the appropriate organizational and technical measures for data security and their protection against accidental or unlawful destruction, accidental loss, alteration, prohibited dissemination or access and any other form of unlawful processing. These measures must ensure a level of security commensurate with the risks involved in the processing and the nature of the data being processed7. Taking into account the risks involved in the processing of credit card data, in particular in the case of accidental or illegal access or dissemination, it follows that, in this case, the controller should take measures that ensure a high level of security. 4. According to no. 11 par. 1 of Law 2472/1997 the data controller must inform the data subjects in a convenient and clear manner at least about their identity, the purpose of the processing, the recipients or categories of recipients of the data, as well as about the existence of the right of access (as provided for in article 12 of Law 2472/1997). 5. In this particular case, both National Bank and Piraeus Bank replaced the debit cards of their complaining customers with new ones, 7 Moreover, and in article 32 of Regulation (EU) 2016/679 on the protection of natural persons against the processing of personal data, which will be implemented in the Member States on 25 May 2018, it is stated that the controller and the processor, taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and freedoms of natural persons, apply appropriate technical and organizational measures in order to ensure the appropriate level of security against the risks, including, among others, as appropriate: "a) the pseudonymization and encryption of personal data, b) the

possibility of ensuring the confidentiality, integrity, availability and reliability of processing systems and services on a continuous basis (…)". In the same article it is stated that when assessing the appropriate level of security, the risks deriving from the processing are taken into account, in particular from accidental or illegal destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or submitted by otherwise processed. Furthermore, in article 35 of the Regulation it is stated that when a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, may entail a high risk for the rights and freedoms of natural persons , the controller carries out, before processing, an assessment of the effects of the planned processing operations on the protection of personal data. 1-3 Kifisias St., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -15- which differ from the previous ones in that they have technology for contactless transactions (as described above). The replacement of the cards, in both cases, was mandatory – that is, their complaining customers were not given the opportunity to obtain a new card with the same technology as their old card (ie without the possibility of contactless transactions). In both cases, it seems that upon receipt of the new card, there was clear information from each Bank to its customer that it is a card with technology that supports contactless transactions - but without detailed information on the individual characteristics of said processing, such as which data is transmitted contactlessly or which data is held on the card chip. The new technology, as pointed out by both Banks in their memos to the Authority, provides the advantage that, with its use, transactions worth up to 25 Euros are carried out more easily and quickly (since the holder does not need to enter the PIN , nor should it be placed in the slot of any terminal device-reader). 6. In terms of processing security, the use of the new card primarily raises the following risks, which risks did not exist with the older debit card technology: a) If the card falls into the hands of a malicious third party (e.g. loss by its owner), then he will be able, without knowing its PIN, to make a series of purchases, worth up to 25 Euros each. b) Given that such a card can emit, through high frequency radio waves8, personal data such as its number and its expiry date, it is possible for someone with a device to read these signals and be in their range, to record them. In order to assess the risks in question, in relation to the relevant security measures taken, the following are noted: a) Both Banks state that any fraudulent transactions can be disputed by the cardholder with the same procedure followed in transactions with credit or debit cards using a PIN, as well as that the cardholder has in any case the 8 Information on NFC technology, but also on RFID technology in general, can be found at the link http://nfc-forum.org /. 1-3 Kifisias St., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -16- responsibility for its safe keeping.

Furthermore, both Banks monitor on a twenty-four-hour basis all card movements in the context of fraud prevention and avoidance. It should also be taken into account, when assessing this risk, that any theft or misappropriation of the card, regardless of whether the card has contactless transaction technology or not, may in any case bring about extremely unfavorable consequences for its owner: for for example, any malicious person, who has the card in his possession, will be able to make purchases of products or services via the Internet with a financial value not limited to 25 Euros but up to the maximum allowable monetary limit set for the specific card. Therefore, with regard to the risk in question, it must be accepted that it is not primarily a risk of greater intensity than the general risk of loss or theft of any other card. However, it must be taken into account that its malicious use as a contactless card, for purchases worth up to 25 Euros, is easier to carry out compared to its malicious use for online purchases. b) The Banks do not mention, for the risk in question, specific measures they have taken to deal with it. National Bank states that the only data transmitted by radio waves, in an unencrypted form, is the card number and its expiry date (i.e. not the name of the holder, nor the three-digit CCV/CVV security number), while Piraeus Bank does not provide detailed information. However, taking into account the relevant response from Visa Hellas, the same technology is used and the cases are the same – therefore, the same data (ie the card number and its expiry date) are transmitted in all cases by radio waves and no more. The above risk cannot be considered as having an extremely low probability of occurrence: and this is because, despite the fact that in order to record the radio waves emitted by the card one would have to be at a very close distance (of the order of 5 to 8 cm), in however, this recording can be done with appropriate equipment that is not expensive or also with low cost. dpa.gr-17- software that can be installed on "smart" mobile devices9 - moreover, with corresponding software it became possible to control the transmitted data by the Authority's controllers. The non-encryption of transmitted data potentially allows such recording to take place. The aforementioned risk may result, in the event of the relevant threat being implemented, in the following consequence: Having malicious knowledge of the card number and its expiry date, he may attempt to purchase a product via the Internet by debiting/crediting the bank account with to which the card is connected, and this purchase may be completed successfully if the relevant online store does not apply the appropriate security measures (such as requiring the user to enter the three-digit security code CCV/CVV10). Therefore, it becomes clear that for the risk in question it cannot be considered that the consequences it may bring to the rights and freedoms of natural persons are of low severity. It is noted that in the relevant privacy impact study prepared by Mastercard for contactless transaction technology and submitted to the Authority, the above risk is indeed recognized as existing. As

measures to deal with this risk, the following are mentioned: i) the name of the cardholder and the three-digit security code CCV/CVV are not sent, ii) for the contactless reading of the data, the reader device must be in very close proximity to the card, iii) it is possible to deactivate contactless transactions, if the issuer (Banking Institution) chooses to do so, iv) there is the possibility of placing the card in a special case (“data protection sleeve”) which does not allow any device -reader to "read" contactless card data. From the above, and based on the data in the case file, it follows that the Banking Institutions - in this case, the National Bank and the Piraeus Bank to which the complaints under consideration concern - as issuers, do not data 9 See indicative description of such an attack at http://securityaffairs.co/wordpress/37667/hacking/nfc-attack-credit-card.html, as well as indicative reference to Android software that can read such http://www.androidauthority .com/android-app-steal-credit-card-info-nfc-96823/ (last accessed: 4/23/2018). 10 An example of such a case – see https://www.independent.co.uk/news-14-1/contactless-payment-card-theft-how-is-the-data-stolen-and-what-can-i-do-to-protect-myself-10409319.html and https://www.theguardian.com/money/2015/jul/23/contactless-card-is-too-easy-says-which (last accessed: 23/4/2018). as at 1-3 Kifisias St., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -18- have chosen the following iii) and iv) measures to address said risk. The impact assessment study prepared by Visa regarding the protection of personal data and which it submitted to the Authority, regarding this risk, characterizes the data sent intact (ie the card number and its expiry date) as pseudonymous data11, in the sense that they alone are not sufficient to identify the person without the use of additional information, which information is in the Bank's systems. Visa also states that in order to collect this data, the collection-"reader" must be very close, within a few centimeters, to the card, as well as that with this data, a malicious person cannot make electronic payments because online shops also have other security measures (such as, for example, asking for the CVV number of the card). In any case, Visa also states that issuers (i.e. credit institutions) can disable a card's contactless functionality at any time. It should also be noted that already at least one of the Banks, namely AEGEAN BALTIC BANK S.A.T.E., as stated in its document mentioned in the history of this present, provides its customers with the possibility of subsequent deactivation by a contactless card of the possibility of contactless transactions. 7. Finally, in the case of Mastercard cards, there is the possibility of storing the recent transaction history on the card, as well as the possibility of reading them contactlessly. The specific data is clearly not absolutely necessary for the basic functionality for which a debit card is intended and, therefore, should not be kept by default12 – much less without an explicit notification to that effect, as it appears that 11 With special reference to definition of pseudonymization of Regulation (EU) 679/2016. 12 It is

also noted that according to art. 25 par. 2 of Regulation (EU) 2016/679, which comes into force from 25 May 2018, the controller applies appropriate technical and organizational measures to ensure that, by default, only personal data that is necessary for the respective purpose of processing. This obligation applies to the scope of personal data collected, the extent of their processing, their storage period and their accessibility. In particular, the said measures ensure that, by definition, personal data is not made accessible without the intervention of the natural person to an indefinite number of natural persons. 1-3 Kifisias St., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -19- applies in the case of National Bank. It is also noted that the observance of this data – which is not mandatory based on the specifications set by Mastercard – raises issues of personal data protection since the card's movements can create a profile of its owner in terms of his consumption habits. Therefore, in view of the risks, the possibilities of their occurrence and their seriousness for the rights and freedoms of natural persons, this particular processing (maintenance of transaction history on the card) does not fall under any of the exceptions of article 5 par. 2 of the law. 2472/1997 and, therefore, the only legal basis for carrying out this processing through the cards in question is the consent of the data subjects (customers of each Bank who own the cards). 8. Also, with regard to the risk of malicious contactless reading of the "card number - expiry date" data, as described in Opinion 6 hereof, Banks must - as a means of dealing with this risk - provide either the possibility of deactivating the contactless function or, alternatively, the granting of a new card without contactless functionality, if the customer does not wish to have a card with the possibility of contactless transactions. 9. In view of the above, and taking into account the international standards followed regarding contactless debit and/or credit cards, credit card issuers must take appropriate measures to ensure the following: a) If the customer declares that does not wish to have a card with the possibility of carrying out contactless transactions, to be provided with the possibility of deactivating the contactless operation of the card or to be given a new, non-contactless card. b) If on a card that has been issued to a customer the ability to keep transaction history is activated on its chip without having given his special consent, the customer should be informed in any appropriate way (e.g. via email mail, through a message when connecting to personalized electronic services of the data controller, through a postal letter, etc.) regarding this processing, giving him the possibility to stop this processing. Furthermore, in each new issuance/issuance of a card, the feature in question will 1-3 Kifisias St., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -20- it must be deactivated from the beginning, and be activated only if there is a specific consent of the customer, as long as he has been previously informed about this processing. FOR THESE REASONS, the Data Protection Authority addresses, in

accordance with art. 19 par. c of Law 2472/1997, recommendation to the National Bank of Greece SA, as well as to Piraeus Bank SA, to proceed, as data controllers within the meaning of art. 2 pc. g' of Law 2472/1997, in the appropriate actions in accordance with what is described in Thought 9 hereof. The President The Secretary Konstantinos Menudakos Irini Papageorgopoulou 1-3 Kifisias St., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr