No. Fac.: 12.10.001.011.001 A/A 45/2019 March 4, 2020 Ms. xxxxxx xxxxxxxxxx Hellenic Bank Data Protection Officer DECISION Subject: Personal data breach notification I have instructions to refer to the breach notification you sent to the Office of the Personnel Data Protection Commissioner Character, via email on September 20, 2019 and to inform you of the following: 1. Incident a) Data entry In the data breach notification, it was stated that the incident came to the attention of the Bank when a customer (S.G.) contacted the store and made a complaint because he was seeing card and account details of another customer (M.K.) in his Web Banking. After investigation it became clear that both clients were registered in the Bank's system with the same passport number. In addition, the new card of M.K. due to the automatic joining in the system, it was automatically sent to SG's address, which SG also mentioned to you. After the above information, the card was canceled and requested by SG. to return it to the Bank. Following clarifications requested from you, by your letter dated November 4, 2019, you mentioned that the web banking of M.K. created on 06/29/2016. On 05/02/2019, the update was made, with the result that M.K. and S.G. have the same passport number in the Bank's system. The persons involved could have access to the data but could not make money transfers to the detriment of the other subject. Due to the fact that the incident was due to human error, and not to an error in the procedures or systems, the Bank reminded the involved colleagues of the proper observance of the "four eye principle" and the actions resulting from the "messages". On January 17, 2020 (after the issuance of a prima facie decision by my Office on December 16, 2019 by which I concluded that there was a prima facie violation of Articles 32 par. 1(b) and 33 par. 1), you clarified further that the examination of the incident continued even after the submission of the Notification dated 20/09/19 and from the examination of the incident, other facts have become clear. You clarified that on 29/5/19 the Bank was informed by a specific customer (S.G.) that he was viewing, through the Web Banking service, information relating to the account number and card details of another customer. After that, immediate measures were taken so that S.G. to see only his own data. You added as new data, that on 4/16/19, due to an error by a Bank employee when typing the details of M.K. (without stating the reason for the entry), was mistakenly entered as the passport number of M.K., the new passport number of S.G. This number was registered in the Bank's data for the first time and for this reason it did not show any warning. Subsequently, on 2/5/19, due to an update of the details of the S.G. his new passport number was registered, which was initially registered on 16/4/19 in the data concerning M.K.. The system then presented the employee with a warning message about the existence of another customer with the same number. The employee, relying on the fact that the details of S.G. confirmed by documents she had at her disposal, she proceeded to register the new passport number. Entry 1

was approved by a second employee. On 2/5/19, the Bank's system automatically updated MK's details, as a result of which he has the same address as S.G. You also mentioned that finally as it became clear, on 2/5/19 M.K. he did not have a personal account with the Bank, but maintained a company account to which the debit card, issued on 9/8/19 in his name, was linked. The data presented to S.G. through the Web Banking service, they concerned the company account and not the personal account of M.K. and the address that appeared to be the address of M.K. was the address of S.G. They were not presented to S.G. any movement data of the company account or transactions made with the company card and the only time SG had secured access. on Web Banking after 2/3/19, it was 28/5/19, one day before informing the Bank. Although when you were notified on 29/5/19 M.K.'s passport number was corrected so that M.K.'s details not to appear in SG's Web Banking, however, the Bank's employees did not proceed to correct M.K.'s address either. As a result, when on 9/8/19 a new card was issued in the name of M.K., it was sent to the address of S.G. S.G. informed you of the receipt of the card on 8/26/19. Then, you proceeded to cancel the card and correct the address of M.K. You asked S.G. to return the card back to you, however by October 9, 2019 when we asked for clarification on this, the card had not been returned. In your letter dated November 4, 2019 You stated that the above incident was the result of human error when updating the account, and not an error in processes or systems. You repeated the same with your letter dated January 17, 2020 stating that the Bank did not identify an immediate need to differentiate its systems and procedures, since the incident was due to human error and not to any defect in the system itself or the procedures established by the Bank. b) Warning message In clarifications requested from you regarding the operation of the four-eye principle and the warning message, which existed and functioned as security measures, in your letter dated October 9, 2019 you reported that “an authorized staff member (user 1) is changing the identification number. When submitting the change in step 1, and before the system proceeds to step 2, an automatic check is made for an existing customer with the new identification number. If there is another existing customer, a warning message "WARNING: AT LEAST ONE CUSTOMER EXISTS WITH THE NEW TRIFOLD" is displayed on the user's screen 1. A related circular from the Bank, dated 02/03/2016, provides guidelines for the correct processing of the process and requires that user 1 confirm the customer details before proceeding with the change. To proceed to step 2 of the above procedure, user 1 must enter "Y" on the system screen. Second authorized member of staff (user 2), automatically receives on his screen the existing and the new value of the elements that change. It approves the change whenever the change is applied to the system, or rejects it, in which case the change is considered non-occurring." With your letter dated January 17, 2020 You reported that on the second entry of the

same passport number on 2/5/19, the system presented the clerk with a warning message about the existence of the same unique number. The employee relied on the documents at her disposal and approved the entry of the number in question. The entry was also approved by a second employee, but who, as you now say, contrary to what you stated on October 9, 2019, did not receive any warning message and had no reason to question the correctness of the entry. You also added that when entering a passport or ID number in the system, the cooperation of two Bank employees is required (four eye principle), so that one can detect any mistake of the other. The first enters the data into the system and the second approves it. If a unique number that is already registered in the system occurs, the system displays a relevant 2 warning message to the employee who makes the entry, but not to the employee who approves it. The system allows entry, despite the warning, since there are cases where the unique number is linked to two or more customers/persons or accounts. If the first employee decides to proceed with the entry, the second employee who is asked to approve it does not receive a corresponding warning message from the system. c) Acknowledgment By sending the Breach Notification form on September 20, 2019 to my Office, which you marked as "Complete" (a term used when the investigation of an incident has been completed and what caused it has become clear), you indicated that the incident occurred on 2/5/19, approximately ended on 30/5/19, while the Data Protection Officer became aware on 29/5/19 and you notified the Authority on 20/9/19. You attributed this delay to the complexity of the incident, which resulted in the involvement of various departments of the Bank such as the Information Security Service, the Bank's Customer Service Branch, the Personal Data Office, the IT department, Fraud Management Operations and the Operational Risk Management Unit. You varied your position again on January 17, 2020, stating that the examination of incident continued after the Notification was submitted (even though the Notification sent on 20/9/19 was marked as "Complete"), with a view to fully understanding the relevant facts and determining any steps that could be taken to improve procedures. You reiterated that the Bank was informed on 29/5/19 but added that the incident was registered in the Bank's relevant system and the office of the Bank's Data Protection Officer (the "DPO") was informed on 28/8/19 (two days after the second time you were notified by SG and three months after SG was first informed about the double registration incident), at which time the mechanism for handling possible personal data breaches was activated. After investigating and evaluating the incident in cooperation with other relevant departments of the Bank, the Notification was submitted to my Office. You further added that the Notice to my Office contained the information which was available at the material time and which supported the filing of the notice. You also mentioned that due to the fact that the investigation of the incident continued even after the Notification, with the result that it

became clear that the incident concerned the account of a legal entity and that the only consequence for a natural person was the disclosure of the name of the holder of the relevant corporate card, it may not have been necessary the notification had not even been submitted to the Office since, under Article 33 of the GDPR, notification is not required when the breach is not likely to cause a risk to the rights of the natural persons concerned. 2. Possible consequences No sensitive personal data is included. You considered the severity of the potential consequences to be low. On September 20, 2019, you reported that the data exposed was name, mailing address, card number, iban, card type, currency, interest rate, late interest rate, last payment date, last payment total, last transaction date, current month transaction total, status by mail, points accumulated, points redeemed, points available, primary or supplementary card, card status, date of issue, expiration date, primary card limit, card balance, available primary card balance, reserved amount, overdue amount, standing order, standing account order, standing order rate and minimum payout amount. 3 On January 17, 2020, you varied your position at this point as well, stating that the disclosed information related to a company account and was the company account number, the number of the company debit card linked to the company account, the name of the company debit card holder (M. K.), date of last corporate debit card transaction and corporate debit card expiration date. From the above data, you say, personal data are only the data concerning M.K. as the owner of the corporate debit card, i.e. his full name. The rest of the information concerns the company account and the company debit card that was linked to it and therefore do not constitute personal data of M.K.. You added that S.G. did not become aware of any transactions carried out through the company account or with the debit card and the address presented in SG's Web Banking. it was his. Additionally, you mentioned that M.K. has not suffered any financial or other damage from the disclosure of his name to S.G., nor was there any risk of damage to M.K.'s rights. since it was not possible to access details of previous transactions or perform new unauthorized transactions, for which an additional security code is required - one time password. 3. The data subject M.K. has not been notified You consider that the seriousness of the consequences to the data subject is small and for this reason, even though you were asked by my Office by letter dated September 24, 2019, the affected data subject was not notified, since you mentioned in your letter d. October 9, 2019, that: "(a) The persons involved could not carry out unauthorized operations/fraud through Web Banking that would result in possible financial damage due to the measures the Bank has in the system, (b) No there were identification details that could make identification easy (c) Immediate measures were taken to deal with the incident as described in the notification (all details were corrected in the Bank's systems)." 4. Measures taken before the incident As you mentioned, there was the four-eye principle, a

warning message in the system in case there are duplicate identification numbers. Also, the Personal Data Office has sent to everyone the personal message/Data Protection Awareness Message in order to emphasize the importance of confidentiality for the Bank and the use of personal data only for the purposes of performing their duties and within the framework of the powers it has set by the Bank. In addition, the Bank has conducted an online seminar for all staff regarding the application of the General Regulation on personal data. In the clarifications requested of you, you replied that "the training and education of the Bank's staff is carried out on a continuous basis, among other things, through various seminars, revision of the Personal Data Office. We note that the latest GDPR seminars have been held by the Bank from 15/03/2019 to 03/05/2019 online for all staff. In addition, on September 4, 2019, the Information Security Service launched a seminar on the protection of personal data and Information Security, which has been attended by 1738 employees of the Bank to date. The seminar is scheduled to end on October 14, 2019. policies, instructions and 4 Additionally, the Personal Data Office prepares "Awareness Messages" which are sent to all staff at regular intervals. The aim of sending the Awareness Messages is the vigilance of the staff regarding the Bank's obligations to comply with the GDPR. In particular, the following Awareness Messages were sent: Awareness Message regarding confidentiality was sent in December 2018. Awareness Message regarding what constitutes a breach of personal data in March 2019. Awareness Message regarding the rights of natural persons according to with the General Regulation on the Protection of Personal Data (hereinafter "GDPR") in June 2019. Awareness Message which concerned the sending of personal data via electronic messages in September 2019." 5. Measures to deal with the incident After the information you received from S.G., as you state in the Violation Notice dated September 20, 2019, you proceeded to: (a) restore and correct the data, (b) cancel the card and (c) requested by S.G. to return the card to the Bank. In addition, with your letter dated January 17, 2020 you mentioned that although the Bank did not identify an immediate need to differentiate its systems and procedures, instructions have been sent by the General Manager of the Bank's Private Sector to all staff to be particularly careful when entering personal data into the systems of the Bank, so as to avoid such incidents as much as possible. It is planned to give more intensive briefings to the Bank's staff from the General Directorate of Personal Data Management on issues related to the management of personal data during the updating of the Bank's systems, and the possibility of taking additional measures is being considered in order to strengthen the security of information in the Bank's systems, as well as the possibility, if technically feasible, that the warning message concerning a common identifier is presented twice, both to the employee who enters the information into the system and to the person who approves it, to

minimize as much as possible the possibility that it will not be detected by a by either of them any error or carelessness. 6. Admitting mistakes You admit and acknowledge with your letter dated January 17, 2020 the need for the Bank to take immediate action to investigate incidents involving data of natural persons and to submit a relevant notification to my Office within the deadline specified in Article 33 of GDPR 2016/679, from the point of time ascertained by reasonable degree of certainty that a personal data breach has occurred. You also acknowledge the fact that in the present case (and while there was still the perception that the incident involved an account of a natural person) there was a delay in submitting the Notification. You also state that the Bank will take the necessary steps to ensure that, if in the future submission is required notification to office of the Commissioner, it will be submitted within the relevant deadline, even if the Bank does not yet have all the necessary information at its disposal. For this purpose, the Bank intends to make further updates to the staff, underlining the responsibility of everyone for timely recognition and registration in the relevant system of the Bank of possible personal data breach incidents. You also admit that neither of the system's safeguards prevented the error that was made, because under the circumstances the safeguards could only operate effectively with the input of the Bank employees involved. The Bank employee, you say, should, in accordance with the instructions of the Bank's Organization and Procedures Department, have investigated the reason for the presence of the warning message in order to identify the mistake made by her colleague on 16/4/19 and so as to avoid what followed. You conclude from this that the cause of the incident was human error and carelessness when applying the Bank's procedures when entering data into the system. The system itself, you state, has no weakness or defect, while the system's safeguards failed in the present case because of the actions and decisions of the officials involved. 7. Mitigating factors presented by you There was no intention you say to ignore the role of the Supervisory Authority and instead you seek to have excellent cooperation with my Office, taking seriously any guidance and recommendations, responding as soon as possible to whatever you are asked. You cite as the cause of the incident human error during the performance by a Bank employee of a specific task within the scope of his duties (entering the customer's details in the Bank's system). You also cite unusual specific circumstances, which did not prevent the error that was made in entering the details on 16/4/19 when S.G.'s new passport number. was registered in the Bank's system as M.K.'s passport number. During the year 2019 alone, more than 15000 registrations were made in the Bank's system. This is an isolated incident, while similar entries of customer details in the Bank's system have been made on a daily basis for years. The likelihood of such an incident happening again is extremely small. The data was revealed for a limited time, on 28/5/19 when

S.G. connected to the Web Banking system. He informed the Bank and the following day the Bank took the necessary measures to terminate said access. It concerns two data subjects/natural persons. S.G. (for which we have no information as to whether M.K. had access to his data), M.K. (name and debit card details), and M.K.'s corporate account. M.K. you say he has not suffered any financial or other damage from the disclosure of his name to S.G. nor has there been a risk of damage to his rights (e.g. he has been a victim of fraud or identity theft or suffered any damage to his reputation or adverse discrimination). The Bank or any of its employees did not secure any financial or other benefit. It was not possible to access details of previous transactions or perform new unauthorized transactions, since an additional security code - one time password - was required. No unauthorized transactions were carried out and there were no, or may be, financial consequences for the company - customer who maintains the Company Account with the Bank as a result of the specific error. Nor were there, or could there be, any consequences for M.K. as the holder of the relevant corporate card. They were not presented to S.G. any movement data or other transactions made with the card. 6 Finally, you mentioned that the client, most of whose details were eventually revealed, was a legal entity and not a natural person. The only consequence for the individual was the disclosure of the name of the holder of the relevant corporate card, where a notification to my Office under Article 33 may not even have been required. 8. Summary of events up to and including January 17, 2020 Accepting the facts as they have been reported by you up to and including January 17, 2020, the incidents surrounding the reported incident are as follows: The web banking of M.K. created on 06/29/2016. On 16/4/19, due to an error by a Bank employee when typing in M.K.'s details, the new passport number of S.G. was mistakenly entered as his passport number. The new passport number of S.G. until that moment it did not exist in the Bank's data. This number was registered for the first time and therefore did not display any warning. On 2/5/19, the details of S.G. were updated. During the said update, the new passport number of S.G. was registered in the Bank's data, for the second time, since it already existed in the Bank's data, when it was registered on 16/4/19 as the distinguishing number of the M.K.. The system then presented the employee with a warning message about the existence of another customer with the same number. The employee, relying on the fact that the details of S.G. confirmed by documents available to her, she proceeded to confirm the entry of the new passport number, without further investigating the warning message that had appeared on the computer screen. The entry was also approved by a second employee, who, however, did not receive any warning message and had no reason to question the correctness of the entry. According to the four eye principle, when entering a passport or ID number in the system, the cooperation of two Bank employees is required,

so that one can spot any mistake by the other. The first enters the data into the system and the second approves it. If a unique number that is already registered in the system occurs, the system displays a relevant warning message to the employee who makes the entry, but not to the employee who approves it. The system allows registration, despite the warning. If the first employee decides to proceed with the entry, the second employee who is asked to approve it does not receive a corresponding warning message from the system. On 29/5/19 you were notified by S.G. that he saw card and account details of M.K. in its Web Banking. An investigation was carried out and it was found that the passport number of S.G. had been entered twice. M.K. he did not have a personal account with the Bank, but maintained a company account with a debit card linked to it, which was issued on 9/8/19 in his name. The data presented to S.G. through the Web Banking service, they concerned the company account and not the personal account of M.K. They were not presented to S.G. any movement data of the company account or the company card and the only time that S.G. had secured access. on Web Banking after 2/3/19, it was 28/5/19, one day before informing the Bank. Although when you were notified on 29/5/19 and M.K.'s passport number was corrected. so that the data of M.K. not to appear in the SG's Web Banking, however the Bank's employees did not proceed to correct M.K.'s address. As a result, when on 9/8/19 a new card was issued in the name of M.K. , it was sent to the address of S.G. S.G. informed you once again on 26/8/19, about the receipt of M.K.'s card. Then, you proceeded to cancel the card and correct M.K.'s address. You asked S.G. to return the card back to you, however as of October 9, 2019, the card had not been returned. As mentioned above, the Bank was informed by S.G. for the first time on 29/5/19 and for the second time on 26/8/19. The incident was registered in the Bank's relevant system and the office of the Bank's Data Protection Officer was informed on 8/28/197, at which time the mechanism for handling possible personal data breaches was activated. Following investigation and evaluation of the incident in collaboration with other relevant departments of the Bank, the Notification was submitted to the Commissioner's office on 20/9/19 which you characterized as "Complete". Further clarifications were requested from my Office by letters dated 24/9/19 and 15/10/19 which were answered with your respective letters dated 9/10/19 and 4/11/19. On 12/16/19 I issued a prima facie decision, according to which I concluded that, based on the data up to 12/16/19, there appears to have been a violation by the Bank of Articles 32 par. 1(b) and 33 par. 1 of GDPR 2016/679 and you have been invited to present the reasons why you believe that any corrective measure or administrative sanction, as well as as you informed me about Hellenic Bank's turnover for the previous financial year. On 1/17/20 you set forth the mitigating factors, as well as new nuanced facts, which were incorporated into the original facts as stated by you. 9. Legal Aspect Article 4 of GDPR 2016/679

defines that "personal data" is "any information concerning an identified or identifiable natural person (data subject)". The same article also defines as processing "any act or series of acts carried out with or without the use of automated means, on personal data or sets of personal data, such as collection, registration, organization, structuring, storage, adaptation or alteration, retrieval, retrieval of information, use, communication by transmission, dissemination or any other form of disposal, association or combination, limitation, deletion or destruction". Further, a controller is defined as anyone (the natural or legal person, public authority, agency or other entity) who, "alone or jointly with another, determine the purposes and manner of processing personal data". The same article defines a personal data breach as "the breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed". The principles governing the processing of personal data are defined in Article 5 par. 1 of GDPR 2016/679. In paragraph f) of Article 5, it is specifically stated that personal data must be "processed in a manner that guarantees the appropriate security of personal data, including their protection against unauthorized or unlawful processing and accidental loss, destruction or deterioration, using appropriate technical or organizational measures ("integrity and confidentiality"). Furthermore, in paragraph 2 of the same article, it is stated that the controller bears responsibility and is able to demonstrate compliance with paragraph 1 ("accountability"). Article 24 of GDPR 2016/679 refers to the controller's responsibility to implement appropriate technical and organizational measures in order to ensure and be able to demonstrate that the processing is carried out in accordance with this regulation and, where necessary, that these measures are reviewed and updated . When justified in relation to the processing activities, the applicable measures include the implementation of appropriate policies. The observance of approved codes of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 of GDPR 2016/679, may be used as evidence of compliance with the obligations of the controller. Article 29 also states that "every person acting under the supervision of the data controller or processor, who has access to personal data, processes said data only on the instructions of the data controller, unless he is obliged to do so by the law of the Union or the State 8 the appropriate level of security against a member.", while similarly in Article 32 par. 4 it is stated that "The data controller and the processor shall take measures to ensure that any natural person acting under the supervision of the controller or processor who has access to personal data processes them only on the instructions of the controller, unless obliged to do so by Union or Member State law." According to Article 32 par. 1(b) of GDPR 2016/679, the data controller and the processor should "apply appropriate technical and organizational measures in order to ensure the risks,

including, among others, as the case may be: (…) b) the ability to ensure the confidentiality, integrity, availability and reliability of processing systems and services on a continuous basis" taking into account the risks "arising from the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed." (Article 32 par. 2). Furthermore, according to Article 33 par. 1 of GDPR 2016/679, in the event of a personal data breach, the data controller must "immediately notify and, if possible, within 72 hours of becoming aware of the breach of personal data to the supervisory authority competent in accordance with Article 55, unless the breach of personal data is not likely to cause a risk to the rights and freedoms of natural persons. Where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a justification for the delay.' According to recital (85) "… If such notification cannot be obtained within 72 hours, the notification should be accompanied by a justification stating the reasons for the delay and the information may be provided gradually without undue delay." Article 33 par. 4 of the Regulation is also relevant, which states that "In the event that it is not possible to provide the information at the same time, it can be provided gradually without undue delay." According to Article 34 par. 3 of GDPR 2016/679 "When the breach of personal data may put the rights and freedoms of natural persons at high risk, the data controller shall immediately notify the data subject of the breach of personal data ." An exception exists in the event that the controller (a) has implemented appropriate technical and organizational protection measures of such a nature as to render the personal data unintelligible to those not authorized to access it, (b) has subsequently taken measures to ensure that it is not more likely to result in the high risk referred to in paragraph 1 to the rights and freedoms of the data subjects and (c) the communication requires disproportionate efforts. In such a case, the announcement may be made publicly or in such a way that the data subjects are informed in an equally effective manner. In Article 38 of GDPR 2016/679, among other things, it is stated that "The data controller and the processor shall ensure that the data protection officer participates, properly and in a timely manner, in all matters related to the protection of personal data." but also "support the data protection officer in the exercise of the tasks referred to in article 39 by providing necessary resources for the exercise of said tasks and access to personal data and processing operations, as well as resources necessary to maintain his expertise." 9.1. Guidelines - Obtaining Knowledge 9 Regarding the issue of "knowledge" and whether or not the DPO has acquired knowledge of the breach, relevant direction is given through the "Guidelines" issued by the European Data Protection Board regarding the notification of a breach of personal data, on October 3, 2017 and revised on February 6, 2018, stating that: "The precise point in time at which a controller may be

deemed to acquire 'knowledge' of a particular breach will depend on the circumstances of that particular breach. In some cases, it will be relatively clear from the outset that a breach has occurred, while in others it may take some time to determine whether personal data has been compromised. However, the emphasis should be on taking timely action to investigate an incident to determine whether personal data has been breached and, if so, to take corrective action and make disclosures, if required. … After first being informed of a possible breach by a person, a media organization or other source, or when it has itself identified a security incident, the controller may conduct a short-term investigation to determine whether a breach has actually occurred. During this period of investigation, the controller cannot be considered to have acquired "knowledge". However, it is expected that the initial investigation should commence as soon as possible and ascertain with a reasonable degree of certainty whether it has a violation is noted; a more thorough investigation may then follow. Once the controller becomes aware of a notifiable breach, it must be notified without delay and, if possible, within 72 hours at the latest. During this period, the controller should assess the potential risk to persons in order to determine whether the requirement for notification has been triggered, as well as the actions required to address the breach." "Although the GDPR allows for late notifications to some extent, this should not lead to the conclusion that this is a regular occurrence." 9.2 Guidelines - Risk and High Risk Assessment According to the "Guidelines" breach notification is not required to be made in all circumstances. As mentioned: Notification to the relevant supervisory authority is required, unless the breach is likely to endanger the rights and freedoms of individuals. The notification of a violation to the person should only be made if the violation is likely to cause a high risk to his rights and freedoms. Regarding the issue of not notifying the data subject of the breach based on the exceptions of Article 34 par.3, the Guidelines clarify that in such a case "controllers should be able to demonstrate to the supervisory authority that they comply one or more of these conditions. It should also be noted that while notification may not initially be required if there is no risk to the rights and freedoms of natural persons, this may change over time and the risk should be reassessed. . If a controller decides not to communicate a breach to the person, Article 34(4) explains that the supervisory authority can ask it to do so if it considers that the breach is likely to cause a high risk to the persons. Alternatively, it may consider that the conditions of Article 34(3) have been met, in which case notice to the persons is not required. If the supervisory authority decides that the decision not to communicate to data subjects is not properly justified, it may consider exercising its powers and imposing sanctions.' It is the controller's responsibility to assess the risk that could arise from the incident so that it can take effective action to contain and address the breach, but also to help determine whether notification to

the supervisory authority is required and , if necessary, notification to the persons concerned 10 High risk, exists when the breach may lead to physical, material or moral harm to the persons whose data has been breached and depends on factors such as (a) the type of breach, (b) the nature, sensitivity and volume of the data, (c) the ease of identification of the persons, (d) the seriousness of the consequences for the persons, (e) the special characteristics of the person, (f) the special characteristics of the controller and (g) the number of affected persons. The above factors should be considered in combination. For example, breaches involving health data, identity documents, or financial data such as credit card information can cause harm on their own, but, if used in combination, could be used for identity theft. A combination of personal data is usually more sensitive than a single piece of personal data. The more serious and likely the consequences to the rights and freedoms of individuals are, the higher the resulting risk. Further guidance for the purpose of assessing the seriousness of a breach is provided by the European Union Agency for Network and Information Security (ENISA)1. 9.3 Guidelines - Notification of a Personal Data Breach Regarding the sending of a Data Breach Notification to the Supervisory Authorities, in accordance with the provisions of Article 33 par.1, the Guidelines state the following: "... the GDPR recognizes that the data controllers do not will always have all necessary information about a breach within 72 hours of becoming aware of it, as full and complete details of the incident may not always be available during this initial period. Hence, it allows for phased disclosure. This is more likely to be the case in the case of breaches of a more complex nature, such as certain cyber security incidents where, for example, a thorough forensic investigation may be required to fully establish the nature of the breach and the extent to which personal data has been compromised . Therefore, in many cases, the controller will have to conduct further research and follow up with additional information obtained at a later stage. This is allowed as long as the controller justifies the delay in accordance with Article 33(1). OE29 considers that when the controller first informs the supervisory authority, it should also inform the supervisory authority if it does not yet have all the required information and that he will provide more details at a later stage. The supervisory authority should agree on how and when the additional information should be provided. This fact does not prevent the controller from providing further information at any other stage if it becomes aware of additional relevant details of the breach which need to be provided to the supervisory authority. The notification requirement should focus on encouraging controllers to act promptly in the event of a breach, to contain it and, if possible, recover the compromised personal data, as well as seek relevant advice from the supervisory authority . Notifying the supervisory authority within the first 72 hours may enable the controller to make sure that decisions about whether or not to inform individuals are correct." “It

should also be clear that, after the initial notification, a controller could inform the supervisory authority if, as part of a follow-up investigation, evidence emerges that the security incident was limited and no breach actually occurred. This information could then be added to the information already provided to the supervisory authority and the incident is therefore recorded as a non-violation. No penalty is provided for reporting an incident that ultimately turns out not to be a violation." “Article 33(1) makes it clear that where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a justification for the delay. This fact, combined with the phased notification approach, implies the recognition that a controller may not always be able to notify a breach within the given time frame and that a late notification may be acceptable. This may be the case when, for example, a controller is faced with multiple, similar breaches of confidentiality within a short period of time, which affect a large number of data subjects in the same way. A controller could become aware of a breach and, while investigating it, and prior to notification, identify other similar breaches, due to different causes. Depending on the circumstances, the controller may need some time to determine the extent of the breaches and, rather than notifying each breach separately, forms a substantial notification which covers several very similar breaches, with possibly different causes. This could result in notification to the supervisory authority with a delay of more than 72 hours after the controller first became aware of these breaches." 9.4 Guidelines - The role of the Data Protection Officer According to the "Guidelines" again the Data Protection Officer (DPO), among other things, it has a duty to provide data protection advice and information to the controller, cooperate with the supervisory authority and act as a point of contact for the supervisory authority and data subjects. It also plays an important role in preventing a breach or preparing to deal with a breach by providing advice and monitoring compliance during a breach (i.e. upon notification to the supervisory authority) and during any subsequent investigation by the supervisory authority . The data protection officer must be immediately informed about the existence of a breach and participate in the process of managing and reporting the breach. 10. Rationale/Comments (a) According to the Guidelines, the GDPR allows for the gradual notification of a breach, in the event that the data controller does not have all the necessary information about the breach and within the time frame set by Article 33 par .1, of 72 hours from the moment he became aware of it, especially when it comes to complex cases (e.g. a cyber security incident) and/or when he is faced with multiple, similar breaches of confidentiality in a short period of time, the which affect a large number of data subjects in the same way. In the present case, the Breach Incident was reported to my Office on 20/9/19, one month after the Bank's Data Protection Officer's Office became aware of the incident, and almost four months after the Bank was first notified time by SG, that is on 28/5/19.

You attributed this delay to the complexity of the incident, which resulted in the involvement of various departments of the Bank such as the Information Security Service, the Bank's Customer Service Branch, the Personal Data Office, the IT department, Fraud Management Operations and the Operational Risk Management Unit, even though the incident involved two natural persons and a legal entity connected to one of them. 12 The Notification was characterized as "Complete", i.e. one whose investigation had been completed, and the controller had all the necessary information about the breach. This fact (that the investigation had been completed) is also reinforced by the way in which the data protection officer responded to the relevant clarifications requested by my Office with the two letters dated 24/9/19 and 15/10/19. In neither of the Bank's two responses was the new, differentiated evidence presented on 1/17/20 presented to me, nor was it mentioned to my Office that the investigation of the incident is ongoing, with the possibility that new data may emerge regarding the circumstances under which the breach occurred. In accordance with the Guidelines, additional/staged data could be provided if an Initial Notification was registered, any delay in the completion of the investigation was justified and the Supervisory Authority was informed of the fact of the absence of a complete picture in relation to the incident. The Supervisory Authority should have agreed on the manner and time in which the additional information would be provided. In the present case, this had not been done. The Bank, not only far exceeded the 72-hour time frame provided for in Article 33 par. 1, but also did not follow the proper procedures, as mentioned above, ignoring the role of the Supervisory Authority. Acting in the way that Hellenic Bank did, it granted itself an extension of time. It also disregarded the role of the Data Protection Officer, since it was late to activate its reporting mechanism for the incident in question. There is also your admission, since you stated that you recognize the need for the Bank to take immediate action to investigate incidents involving the data of natural persons and to submit a relevant notification to my Office within the deadline specified in Article 33 of GDPR 2016/679, from point in time when it is ascertained with a reasonable degree of certainty that a breach of personal data has occurred. Furthermore, even if, as stated on 17/1/20, the financial data presented to S.G. concerned corporate accounts connected to M.K., it is admissible on your part, that at least until 20/9/19 when you made the Notification, but even until 17/1/20 when you varied the facts, you had the impression that the data to which S.G. mostly had access concerned the natural person of M.K. It should also be said that the possibility that M.K. to have access to S.G.'s data On the contrary, in the Notice of Infringement dated 20/9/19 it is stated that two natural persons have been affected, (i.e. both S.G. and M.K.), but also in the Bank's letter dated 4/11/19 it states that "The persons involved as we have informed you through the notification could access the data, [therefore could access each other's data]

but could not, for example, make money transfers" . (b) Regarding the technical and organizational measures taken by the Bank so that it complies with the provisions of Article 32 of GDPR 2016/679, I should note the following: On 16/4/19, due to an error employee of the Bank, the number of the new passport of S.G.. was registered for the first time in the details of the customer M.K.. Due to the fact that it was the first time that this number was registered in the Bank's data, the system did not display any warning. On 2/5/19, during the updating of S.G.'s information, the new passport number of S.G. was registered for the second time. in the Bank's data. This time the system displayed a warning message. The Bank employee relied on the correctness of the documents in her possession and proceeded to confirm the registration. The confirmation was also carried out by a second person of the Bank, in accordance with the four eye principle, but this person, according to the new data you presented to us on 1/17/20, does not receive a corresponding warning message in his system as the one the first employee receives. 13 If this is the case, then what is the purpose of the approval or not by a second employee of the actions of the first, since he cannot have knowledge of the warning message that appears on the screen of the first employee? How then is the data double-checked? The expression four eye principle in itself refers to a visual control of actions, by two persons. If the second person simply confirms the actions of the first, without knowing what came before, then the said confirmation is meaningless. Let me further remind you that you have admitted that neither of the two security safeguards of the system prevented the mistake that was made, since the Bank employee, you say, should have, in accordance with the instructions of the Bank's Organization and Procedures Department, investigated the reason for his presence warning message, in order to detect the mistake made by her colleague on 16/4/19 and to avoid what followed. You reasoned that the breach was the result of human error and carelessness, under unusual specific circumstances, in applying the Bank's procedures when entering information into the system. However, this did not prevent the recurrence of a similar incident, which was notified to the Supervisory Authority on 15/11/19, with Notification Number 57/19, according to which again a customer who had access to the commercial brand Web Banking, had seen another customer's card details , due to mistakenly registering the trade name number as a personal identification number corresponding to the other customer. In accordance further with Articles 29 and 32 par. 4 of GDPR 2016/679, the data controller is responsible for the actions of persons acting under his supervision and must take measures to ensure that any natural person acting under his supervision , processes any personal data only at his command. Therefore, you cannot invoke human error to absolve you of your responsibilities, also bearing in mind that internal risks can be worse than external ones. It should also be noted that although you were notified by S.G. on 28/5/19 for the fact

that in the Web Banking system, all the account details of M.K. (even if in the end it appeared that it was a corporate account), and you took steps to remove this incident, however, a new incident that occurred on 9/8/19, when M.K.'s debit card was issued, was not prevented. and was sent to the address of SG, due to the fact that the commonaddress had remained uncorrected. Therefore, even the immediate measures that were taken, did not were sufficient to prevent the second incident of security breach data.

(c) The data subject has not been notified of the event in question. The one in charge data protection, justified this decision on the fact that (1) the involved persons could not perform unauthorized acts that would have as result in possible financial loss, (2) the subject's identity was not present of the data and (3) immediate measures were taken to address the incident, by correcting the elements. He also judged that any impact on his rights and freedoms subject of the data, is small. There is no doubt, however, that S.G. had taken cognizance of pile of financial data of a company owned by M.K. as well as the name of M.K. and/or M.K. had taken cognizance of the financial data of S.G.. Nevertheless, due to the fact that he did not could the parties engage in unauthorized acts that would result in financial harm to each other, we will accept with reservation your decision not to inform M.K.

11. Conclusion

Considering all the above facts as stated, and based on the powers which provided to me by Articles 58 and 83 of Regulation (EU) 2016/679, Article 24(b) of Law 125(I)/2018, as well as the provisions of article 43 on its General Principles Administrative Law Law of 1999, I conclude that there was a violation on the part of Hellenic Bank of one of the main Authorities governing the processing of personnel data nature and especially of Article 5, par. 1 f) of GDPR 2016/679, since he failed to guarantee

the appropriate security of personal data of data subjects

with the use of appropriate technical and organizational measures so as to ensure the
integrity and confidentiality thereof, of Article 32 par. 1(b) of GDPR 2016/679 as long as
did not apply the appropriate technical and organizational measures that it should have applied
to
the appropriate level of security against risks is ensured,
including, among others, the ability to ensure privacy, of
integrity, availability and reliability of processing systems and services in
continuous basis, as well as a violation of Article 33 par. 1, since he did not notify the Supervisory Authority
Authority within 72 hours from the moment it became aware of the fact of the violation, as
he had to.
According to recital 148 of GDPR 2016/679, in order to strengthen the enforcement
of the rules of the Regulation, penalties, including administrative fines will
must be imposed for each violation, in addition to or instead of the appropriate measures that
are imposed by the Supervisory Authority. In the event of a minor offense or if the
fine that might be imposed would be a disproportionate burden on physical
person, a reprimand could be imposed instead of a fine. You should however
due regard being had to the nature, seriousness and duration of the offence, the willfulness
nature of the breach, the actions taken to mitigate the damage, the degree
of liability or any other relevant previous violations, the manner in which the supervisory
authority informed of the violation, compliance with the measures against the person responsible
processing or of the processor, compliance with the code of ethics and any other
aggravating or mitigating factor.
Finding a violation of Articles 5 para. 1(f), 32 para. 1(b) and 33 para. 1 of
GDPR 2016/679 as explained above, based on the provisions of Article 83 of the GDPR, in
measure applied in this particular case, I take them into account below
mitigating (1-10) and aggravating (11-16) factors:

(1) The limited number of data subjects whose data they have

exposed (two in total).

(2) The absence of malice on the part of the data controller, since the violation was

result of human error.

(3) The fact that the controller was taking actions to correct his mistakes,

immediately after notification of them by the data subject.

(4) That there is cooperation between the controller and the Supervisory Authority.

(5) The fact that the controller applies policies and codes on the site

work such as e.g. Data Protection Policy, Data Protection Framework,

Information Security Policy, Disciplinary Code, and Professional Code

Behavior and Ethics, which employees must know and

apply.

(6) The fact that there was an admission of mistakes both on the subject of the system's security valves,

as well as the need for the Bank to take immediate action for investigation

incidents and submitting relevant notification to my Office within the deadline.

(7) The fact that most of the data of M.K. which were exposed to SG, as seen

after all, they belong to a legal entity that was connected to a natural person.

(8) That no unauthorized transactions took place, since it was required

additional security code – one time password and there were no financial ones

consequences for data subjects.

(9) The large number of entries. For the year 2019 alone, over 15,000 were made

entries in the Bank's system.

(10) That a banking institution has an increased degree of liability over any other

controller, to observe such security measures to preserve the

financial data of its customers.

(11) That within the year 2019, 7 more violations were notified to the Supervisory Authority

data confidentiality of Hellenic Bank customers, but not always

concerns the same incidents as in the present case.

(12) That financial data has been disclosed and its confidentiality breached;

(13) Non-observance of due process and long delay in submission

Breach Notification based on Article 33 par. 1 of GDPR 2016/679.

(14) The fact that although there were safety valves, they were not capable of

prevent infringement.

(15) The fact that human-caused violations occur frequently

error of Bank employees.

(16) Finally, the fact that the Bank became aware of the violations and realized the mistakes

which were done, after being notified both times by one of the two affected parties

persons.

Bearing in mind the above, as well as the fact that the mitigating factors are far

more than the aggravating factors, I decide not to impose an administrative fine

the time.

Nevertheless, Hellenic Bank is instructed to adopt such security measures

and practices, so that processing operations are made in accordance with its provisions

GDPR 2016/679, as they have been explained by this Decision.

Hellenic Bank is also mandated, as within three months from today, with

inform about the actions taken to comply with this Decision.

Irini Loizidou Nikolaidou

Data Protection Commissioner

Personal Character