Athens, 04-04-2022 Prot. No.: 851 DECISION 6/2022 (Department) The Personal Data Protection Authority met, at the invitation of its President, in a regular meeting in the composition of the Department at its headquarters on 08/02/ 2022, in order to examine the case referred to in the history of the present. The meeting was attended by teleconference by Georgios Batzalexis, Deputy President, in opposition to the President of the Authority, Constantinos Menoudakos, and regular members Charalambos Anthopoulos, Spyridon Vlachopoulos and Konstantinos Lambrinoudakis attended as rapporteur. At the meeting, by order of the President without the right to vote, Haris Symeonidou, special scientist - auditor, attended as assistant rapporteur and Irini Papageorgopoulou, employee of the Authority's administrative affairs department, as secretary. The Authority took into account the following: With the no. prot. C/EIS/8267/02-12-2020 complaint by A (hereinafter the complainant) against Piraeus Bank (hereinafter the complainant), of which she is a client, complaining about a repeated incident of violation and non-satisfaction of the right to rectification of her personal data. In particular, according to the complaint, the movements of the complainant's debit card are notified by the complainant Bank to the electronic addresses ... and ... which belong to a third party, with the same name and common name as the complainant and not to the complainant's address (...). This fact was disclosed by the complainant, as she claims in her complaint, to the complained Bank, initially orally on … at branch X, at which time she received the assurance that the problem 1-3 Kifisias Avenue, 11523 Athens T: 210 6475 600 E : contact@dpa.gr www.dpa.gr will be corrected, and subsequently on ..., via an electronic mail message (e-mail) to the Data Protection Officer of the complainant, who received no. first ... . Furthermore, the non-satisfaction of the right to correct the personal data of the complainant is complained of, as despite her request to receive the relevant information to her correct email address (…) submitted in the above-mentioned ways to the complainant, the notifications regarding the movements of the debit of the card continued to be sent to the above addresses that do not belong to her, as informed by their recipient, and not to her own e-mail address. The Authority, in the context of examining the above complaint, with no. prot. C/EX/740/02-03-2021 her document, invited the complainant to present her views on the complainants, explaining specifically what exactly happened in the case at hand and what is the prescribed procedure to be followed to avoid a similar incident . In her response, the complainant was asked to clarify in particular: a) whether and how she responded to the request for correction of the complainant's personal data, which was made with her e-mail from ... to the Data Protection Officer of the complainant, stating, in case of non-compliance timely response, the reasons for the delay, b) why did the complainant not notify the Authority of the said incident of violation, in accordance with article 33 GDPR, as soon as she was notified about it by

the complainant, c) if and how she informed the complainant about the alleged breach, providing her with the information required by Article 34 GDPR, and d) what measures the complainant has taken to deal with the repeated incident of data breach under consideration and to mitigate its adverse consequences, i.e. to mitigate danger caused to the complainant by it. The complainant in her response from … (with Authority no. C/EIS/1772/12-03-2021) states first of all that the complainant's account is joint / separate with B, joint beneficiary of the account in question and that both the complainant and the said co-beneficiary have activated the Alerts management service (alert packages) through which notifications of transactions carried out on the account are sent by e-mail. For this purpose, the complainant has declared in this case as the desired e-mail address ... to which the relevant notifications are sent, and correspondingly the joint beneficiary of the account in question, B has declared the e-mail address ... to which the relevant notifications are also sent. Furthermore, as the complainant states, after the complainant's request to the Bank from ..., it was found that the address declared by the co-beneficiary differs only by one dot from the e-mail of the alleged final recipient of the Alerts with details ..., but this differentiation is not recognized by Google's Gmail e-mail service, with the result that notifications sent to the declared address (with the period) are delivered to the address ... (without the period), since the system considers them identical: "the non-recognition of the dot symbol that would distinctly differentiate one e-mail address from the other, is a weakness and an error of the Google company, consequently the two e-mail addresses (in this case the one declared by B ... email for receiving alerts, ... and the email of alleged final recipient ...) to be recognized by Google as an email address. The consequence of the above error by Google is the sending of electronic material to the e-mail address other than the one declared by the co-beneficiary as the e-mail address for receiving Alerts for the movements of the above account, i.e. to the e-mail ..., instead of being sent to the correct and declared on behalf of B, which is registered in the Bank's e-mail systems with data ...". The complainant therefore points out that it is not a matter of "forwarding" the notices to a third party's address, given that she sends the notices to the address actually declared by B..., and that she proceeded with an internal investigation in cooperation with the competent Bank Units, from which it emerged that the address ... is not found as declared in the Bank's systems and does not appear to correspond to a natural person who maintains a transactional relationship with the Bank and that the sending of Alerts on the part of the Bank for the movement of the aforementioned joint account is carried out immediately to the electronic addresses that have been declared by the above two co-owners, in accordance with the defined procedure for activating the Alerts notification package, as well as in accordance with the relevant procedures of the bank that have been notified to the co-owners when

opening the account. Furthermore, the complainant claims that she sent a reply to the complainant on ..., with which, however, "in compliance with the current institutional framework that imposes bank secrecy, she did not mention the email address declared by the joint beneficiary of the account, but pointed out to the client that she would the email addresses that have been declared for receiving notifications must be checked by all account holders, indicating all the possible ways to do so (winbank, visiting a store, phone banking) clarifying that these are actions that can be carried out by the each user of the service, i.e. each co-beneficiary of the above account and only himself as the subject of the data, […], which obviously did not happen. The bank cannot and should not be able to intervene in the relevant statements of its customers". According to the complainant, given that the electronic address ... has been declared by the complainant's co-beneficiary and not by her, no right of correction was exercised in accordance with Article 16 GDPR, since the complainant's allegations "did not concern her personal data, but to the personal data of a third party, since the information she mentions in her applications concerns what was declared by the joint beneficiary of the account, who has not addressed any request to the Bank to date, nor does she allegedly legally authorize A to exercise on his behalf a right arising by the GDPR". Subsequently, with its letter from ..., the complained bank clarified to the complainant "that there is no correlation from the mention of the letter (e) in your e-mail address, i.e. the ... for the delivery of the notices to B with the letter (i), but association due to the (.) dot, which is present in the email address … and is declared to the co-beneficiary of your account who also has the Winbank Alerts service activated." Therefore, the complained Bank reported to the Authority that, in its opinion, in compliance with the current legislative framework, it has taken all the actions required by applying the appropriate technical and organizational measures for the legal observance, processing and safe preservation of the personal data file. Regarding the looming incident of violation, the Bank stated that "from the most comprehensive investigation carried out (...) the Bank never carried out a promotion data to a third party email and personal information of A was never disclosed to a third party, therefore there was no incident of personal data breach – leakage. Therefore, as assessed by the Bank's Personal Data Protection Office, none of the conditions provided for in articles 33 and 34 of the GDPR were met." Despite all this, with the no. prot. C/EIS/2171/30-03-2021 her document, the complainant informed the Authority that the problem still exists, as electronic notifications about her account movements continue to be sent from the complained bank to the said third party, attaching as proof of her claims fourteen (14) notification messages (Winbank Alerts) concerning the same number of transactions of herself and her co-beneficiary husband, which had been sent within 2021 to the address of the above third party and had been forwarded to the complainant for her information .

Subsequently, the Authority, with no. prot. C/EX/2288/12-10-2021 and C/EX/2289/12-10-2021 Summons it invited the involved parties to a hearing at the meeting of the Authority's department on 19-10-2021 and, after adjournment to 10-11-2021, in order to present their views on the case. During the hearing, the parties developed their views and they were given a deadline of 15 days (until 01-12-2021) to submit briefs. During the meeting of 10-11-2021, the complainant was present, and on behalf of the complained-of Bank Mr. Ioannis Krinis and Mrs. Vassiliki-Maria Saldari from the Bank's Legal Service, Mr. C, from the Digital Banking department), D from the Operational Support department, and E, the Bank's Public Relations Officer, who did not take the floor. The parties involved were given, during this meeting, a deadline and the complainant did not submit a memorandum, apart from No. prot. C/EIS/7139/04-11-2021 of its document, which it had submitted before the hearing, and the Bank submitted the no. prot. C/EIS/7890/02-12-2021 her memorandum. The complainant, both with no. prot. C/EIS/7139/04-11-2021 her document as well as during the hearing, she supported what was mentioned in her complaint, adding that in the end and in order to resolve the issue, her husband and co-beneficiary of the account, visited her... again the bank and requested to be "exited" from the account, as well as to cease from now on any notification service sent in the past due to his specific status as a co-beneficiary. According to the complainant, the co-beneficiary was forced to take this action in order to stop the notifications being sent to the incorrect address, since despite having requested several times both by phone and by visiting the complainant that the error be corrected, the problem continued. The complained-about Bank, both with its memorandum and during the hearing, repeated the positions it had supported with the no. prot. C/EIS/1772/12-03-2021 her opinion document and in particular put forward the following allegations: a) That the submission of the relevant requests from ... and ... on behalf of the complainant, without authorization from the co-beneficiary and her husband, under of which he is entitled to exercise the right of correction on his behalf, but also the complaint in question, concerned a request for correction of the electronic address for receiving alerts declared on ... by a third party (the complainant's co-beneficiary) ... and for this reason, according to with the complained-about Bank, the provisions of Article 16 of the GDPR regarding the right to correction do not apply, given that the requested correction did not concern her personal data, i.e. the address declared on her behalf (at …) as the address for receiving alerts … b) That he legally sent the relevant notices to the e-mail address declared by the co-beneficiary of the complainant..., and the fact that the relevant or mail reached a third party with the address …, which differs by one dot from the address stated above, is solely due to the error of Google, which is unable to recognize the dot symbol in the part before the @ symbol, resulting in it becomes impossible to differentiate the above two addresses. Therefore,

the Bank maintains that the reported incident "could not in any way fall within its scope of responsibility or be prevented or avoided by the Bank by taking any measures, as it falls solely within Google's sphere of responsibility , without the possibility of any intervention on behalf of the Bank and at the initiative of the Bank". c) That any voluntary attempt on the part of the Bank to settle the issue concerning the co-beneficiary of the complainant would be illegal: In particular, according to the complainant, the possible change of the recipient's e-mail address without a previous relevant request from the same and without his own consent would constituted "arbitrary and illegal processing of his data", stopping the sending of alerts would contribute "to the non-transactional and unjustified cancellation of the alerts service provided free of charge by the Bank to him", while even any telephone updates from the Bank, would constitute "by definition processing of the data of said co-beneficiary, i.e. of B, outside the legal purposes of processing the personal data of this subject". Finally, the complainant Bank states that on ... the co-beneficiary of the complainant went to a branch of the Bank and gave an order to cancel the alerts service and to change his e-mail address which had been declared until then, changes which the Bank proceeded with in accordance with its procedures, considering that that "every aspect of the approach to the case has been completed, that no incident of leakage of the complainant's personal data was detected in any way that requires further involvement, taking measures and other actions and that the complaint in question proves to be unfounded". The Authority, after examining all the elements of the file and after hearing the rapporteur and the assistant rapporteur, who left after the discussion of the case and before the conference, after a thorough discussion, THINKS IN ACCORDANCE WITH THE LAW 1. From the provisions of Articles 51 and 55 of the General Data Protection Regulation (Regulation (EU) 2016/679 – hereinafter, GDPR) and Article 9 of Law 4624/2019 (Government Gazette A´ 137) it follows that the Authority has the authority to supervise the implementation of the provisions of GDPR, this law and other regulations concerning the protection of the individual from the processing of personal data. 2. According to article 5 par. 1 f) GDPR "1. The personal data: f) are processed in a way that guarantees the appropriate security of the personal data, including their protection against unauthorized or illegal processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality")", while as pointed out in the Preamble of the Regulation, "Personal data should be processed in a way that ensures the appropriate protection and confidentiality of personal data, including to prevent any unauthorized access in this personal data and the equipment used to process it or the use of this personal data and said equipment" (App. Sk. 39 in fine). 3. According to the provision of article 24 par. 1 GDPR: "1. Taking into account the nature, scope, context and purposes of the processing, as well as the risks of varying probability of

occurrence and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures in order to ensure and can demonstrate that the processing is carried out in accordance with this regulation. The measures in question are reviewed and updated when deemed necessary", while in accordance with the provisions of paragraphs 1 and 2 of article 32 GDPR for the security of processing, "1. 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, the controller and the executor the processing implement appropriate technical and organizational measures in order to ensure the appropriate level of security against risks, including, among others, as appropriate: a) the pseudonymization and encryption of personal data, b) the ability to ensure confidentiality, integrity, availability and reliability of processing systems and services on an ongoing basis, c) the possibility of restoring the availability and access to personal data in a timely manner in the event of a physical or technical event, d) a procedure for the regular testing, assessment and evaluation of efficiency being of the techniques and of organizational measures to ensure the security of processing. 2. When assessing the appropriate level of security, particular consideration shall be given to the risks deriving from processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise submitted to processing". 4. Furthermore, according to article 4 no. 12 GDPR as a personal data breach means "a 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". According to the Working Group Guidelines of Article 29 of Directive 95/46/EC (currently European Data Protection Board – EDPB) dated 06-02-2018 on Personal data breach notification (“Guidelines on Personal data breach notification under Regulation 2016 /679" WP 250 rev. 1) one of the types of personal data breach is the one categorized based on the security principle of "confidentiality", when unauthorized access to personal data is found ("confidentiality breach"). A breach can potentially have various significant adverse consequences for persons, which can lead to physical, material or moral harm. The GDPR explains that this harm can include loss of control over their personal data, limitation of their rights, discrimination, misuse or identity theft, financial loss, unlawful de-pseudonymisation, damage to reputation and loss of confidentiality of personal data of a nature protected by professional secrecy, etc. (see also paragraphs 85 and 75). Incidents of data breach must be notified to the Authority within 72 hours from the moment the data controller becomes aware of them, in accordance with article 33 paragraph 1 GDPR: "1. In the event of a personal data breach, the controller shall notify the

supervisory authority competent in accordance with Article 55 without delay and, if possible, within 72 hours of becoming aware of the personal data breach, unless the breach of personal data may not 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.' The notification must have the minimum content referred to in paragraph 3 of article 33 of the GDPR, while according to paragraph 5 of the same article "The data controller shall document any personal data breach, consisting of the facts concerning the data breach of a personal nature, the consequences and the corrective measures taken. Such documentation shall enable the supervisory authority to verify compliance with this Article.' In addition, the violation must also be notified to the data subject, as the case may be and in accordance with the provisions of article 34 par. 1 and 2 GDPR: "1. When the personal data breach may put the rights and freedoms of natural persons at high risk, the data controller shall immediately notify the data subject of the personal data breach. 2. The notification to the data subject referred to in paragraph 1 of this article clearly describes the nature of the personal data breach and contains at least the information and measures referred to in article 33 paragraph 3 items b), c) and d)". 5. In the case under consideration, the following emerged from the information in the file: she receives confidentiality, which indeed The complainant accidentally discovered that her personal data was being communicated by the complained bank to a third party bearing her name, without her knowledge and without her will. It was therefore a repeated and continuous violation of the country. The complainant immediately informed the complainant in writing on … the complainant (through her DPO), who, after carrying out checks, found that the problem was due to the incorrect e-mail address that the husband and co-beneficiary of the complainant had declared for sending notifications Winbank alerts, namely at the address ..., which Google's Gmail service recognizes as identical to ... . This address had apparently been declared instead of the correct address of the complainant and the wife of the customer in question (…) which the co-beneficiary probably wanted to declare, by mistake putting the letter i instead of the (correct) e. Despite all this, the complained bank did not take any action to stop sending the notices to the third party with the complainant's first and last name, but in its letter dated ... told the complainant that each joint account holder should check through his settings the addresses for sending notifications declared by him. In this way, the complained bank continued to violate the complainant, through the unfair communication to a third party, of the confidentiality of her data while waiting for the exercise of the right to correct the incorrect address, on behalf of the subject - co-beneficiary of the complainant. Despite the complainant's renewed protest to the bank on ..., the complainant continued to be inactive, as a result of which the complainant

proceeded to submit the present complaint to the Authority, on ... . On ... the complained bank informed the complainant in a letter of the following: "We would like to clarify that there is no correlation from the mention of the letter (e) in your e-mail address, i.e. the ... for the delivery of notifications to ... with the letter (i), but correlation due to the (.) dot, which is present in the email address … and is declared to the co-beneficiary of your account who also has the Winbank Alerts service activated". 6. It should be noted that, contrary to what the complainant bank claims, the problem with the non-recognition of the dot symbol (.) by the Gmail service is known and is not relevant in this case, since this is not the critical error by the which resulted from the leak of the complainant's data. On the contrary, since the presence or absence of a period does not in practice differentiate one gmail address from another, the only significant difference between the two addresses, on which the complainant should focus, is the (jointee's) accidental i instead of of the letter e in the name ... . Furthermore, the complainant is indeed not entitled to exercise the right to correct personal data on behalf of her husband and co-beneficiary of the account, who had declared the incorrect e-mail address for receiving the alerts. In addition, no documents were provided from which the exercise of the right of correction by the co-beneficiary of the complainant and subject of the data (of the e-mail address in question) can be deduced. However, since the complainant addressed the complained Bank in the capacity of the subject of the data (information on banking transactions that she herself carried out through her account) reporting the ascertained leakage of this data to a third party, which constitutes an incident of violation of her personal data according to article 4 par. 12 GDPR and violation of the principle of confidentiality, it is now up to the Bank, as data controller, to assess the incident in accordance with Articles 33 and 34 GDPR and to take the necessary actions to address the violation, taking measures to mitigate the adverse consequences of (article 32 par. 1 item d) GDPR). In addition, the Bank should have taken additional corrective measures to ensure data security, in accordance with Articles 24 and 32 GDPR, taking into account the above incident and re-evaluating the process of declaring an electronic address by a customer and user of its services, adding, if deemed necessary, additional steps to confirm that the declared address belongs to the person who declared it. 7. In any case and regardless of the actions that the complainant and/or her spouse and co-beneficiary could take to correct their personal data by exercising their rights as subjects, the principle of data integrity and confidentiality requires measures to be taken by the complained bank as data controller, as soon as it became aware of the ongoing leakage of the details of their banking transactions to a third party, by stopping the sending of notifications until the issue is resolved. 8. Following the above, from the information in the file and following the hearing, the Authority finds on behalf of the complained Bank: a) violation of the

principle of data confidentiality (art. 5 par. 1 f) GDPR), because the complained Bank, though, through the from … and …

lettersof the complainant and, in any case, of the under no. prot. G/EX/740/02-03-2021

document of the Authority, became aware of the fact that the personal information

of the complainant's bank transactions were leaked to a third party, namely to

owner of the e-mail address ..., continued to send the relevant ones

notices to the same address until ..., as well as violation of the

of articles 33 and 34 GDPR obligations of the complainant, given that no

reported the incident to the Authority or the subject, nor did he take any measures for it

mitigating the consequences of the breach (stopping sending notifications) and for

avoiding similar incidents in the future.

b) Insufficient technical and organizational security measures, in accordance with articles 24 and 32

GDPR, which led to the above incident. In particular, it is established that

absence of measures and procedures to confirm the correctness of

e-mail addresses declared to the Bank for receiving notifications, since

take into account the possible consequences of any incorrect declaration.

9. Based on the above, the Authority considers that there is a case to exercise the v

articles 58 par. 2 i) and 83 GDPR corrective powers (imposition of a fine)

regarding the violations established above under item a, as well as the

according to article 58 par. 2 a) GDPR corrective powers regarding the

finding the violation under item b. To determine the sanction, the Authority

takes into account the criteria for measuring the fine defined in the article

83 par. 2 of the GDPR that apply to this case.

In particular, particular consideration is given to:

a) The nature, gravity and duration of the violation, which began with

statement of the incorrect e-mail address on behalf of the spouse –

co-beneficiary of the complainant on ..., continued, despite his marking

problem to the Bank at the beginning of … orally and on … in writing,

and it ceased on ..., when the said co-beneficiary went to a branch of the Bank

to solve it

b) The small number of subjects affected (2) and the fact that no

it emerged that they suffered a financial loss

c) The fact that the violation on the part of the Bank is not attributable to fraud

d) The contributory negligence of the subject (co-beneficiary) regarding both the

incorrect declaration of an electronic address, as well as the procedure for correcting it

after the Bank's relevant instructions to the complainant.

In particular, no documents were presented to the Authority from which the

exercise of the right of correction, by the co-beneficiary of the complainant,

according to the instructions of the complained Bank

e) The fact that the Bank, despite being aware of the problem, did not take action

any action to eliminate the consequences of the ongoing

violation incident

f) The degree of responsibility of the Bank due to insufficient technical and organizational measures

security

g) The lack of previous violations of the Bank as responsible

processing, and

h) The fact that special categories were not affected by the violation

personal data.

FOR THOSE REASONS

THE BEGINNING

A. It imposes on Piraeus Bank S.A. as controller based on

article 58 paragraph 2 paragraph i of the GDPR a total fine of ten thousand (10,000

€) euros for the violation of the principle of data confidentiality (art. 5

par. 1 f) GDPR) and its obligations under articles 33 and 34 GDPR.

B. Addresses Piraeus Bank SA. as controller

warning in accordance with GDPR article 58 par. 2 a) in order to implement

appropriate technical and organizational measures to confirm their correctness

e-mail addresses declared to the Bank to receive notifications

Winbank Alerts.

The president

George Batzalexis

The Secretary

Irini Papageorgopoulou