Athens, 12-06-2023 Prot. No.: 1510 DECISION 25/2023 The Personal Data Protection Authority (hereinafter "the Authority") convened at the invitation of its President in a videoconference meeting on Tuesday 12-13-2022 at 10.00 , in order to examine the case referred to in the present history. The President of the Authority, Konstantinos Menudakos, the regular members Spyridon Vlachopoulos, Konstantinos Lambrinoudakis, Charalambos Anthopoulos, Christos Kalloniatis, Aikaterini Iliadou and Grigorios Tsolias were present, as rapporteur. Present, without the right to vote, were Efrosyni Siougle, specialist scientist - informatics, Stefania Plota, specialist scientist - lawyer, as rapporteur's assistants and Irini Papageorgopoulou, employee of the administrative affairs department, as secretary. The Authority took into account the following: With the complaint No. G/EIS/479/21-01-2020, A (hereinafter "complainant") informed the Authority that the complained Piraeus Bank S.A. (hereinafter "Bank"), according to the joint letter from ..., of the Bank and the Loan and Credit Receivables Management Company Alternative Financial Solutions M.A.E.D.A.D.P. (hereinafter "AFS company"), transferred his personal data to the latter (Administrator of the claim according to Law 4354/2015), without however having a legal reason and right to do so, as, according to the complainant's claims, no claim existed now at his expense. Specifically, with the above letter, the Bank informs the complainant 1-3 Kifisias Ave., 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr 1 that it has entered into an agreement with the company AFS for the assigning to it the management of the Bank's claims from the granting of loans and/or credits to debtors, whose debts or some debts have become overdue and/or have been terminated or settled and that "the Bank's claims arising from the contracts loan or credit in which you are involved in the capacity of debtor and/or co-debtor and/or guarantor and/or security provider, included in the Portfolio and from 20-09-
2019 onwards, the management of your contract(s) was undertaken by the Administrator and for this purpose your personal data was transmitted by the Bank to the Administrator for the purpose of managing its claims from your contract(s). Furthermore, the complainant complains that the Bank did not answer him satisfactorily and in detail, as he requested, with his application from ..., with which he exercised to the Bank the right of access and information in relation to the transfer of his personal data to the company AFS. Specifically, the complainant states in his application to the Bank from ... that he independently exercises the right of access and information in relation to the processing of personal data concerning him pursuant to art. 15 GDPR and art. 33 n.4624/2019 and requests that they inform him personally and in detail about a. the exact date of transmission of his data to the Administrator, b. the manner and purpose of their transmission, c. in detail all its data at the time of their transmission to the Administrator and in particular according to the Bank's letter from ... the numbers of the

loan agreements, the corresponding amounts due per loan agreement, the existing real collateral per loan agreement, and d. any other his data that may have been collected by the Bank during the management of its claims after the transmission of its claims to the Administrator. The complainant received by post on … the second letter from the Bank from …, in which the Bank states that he was mistakenly sent the letter, dated …, which had the form and content of the individual letter sent by the Bank for purposes informing the natural persons connected in any capacity with the Bank's claims, which derive from loan and credit agreements and their management has been assigned by 2 Bank to the AFS company, within the framework of the agreement on the assignment of the claims management to the AFS company from the Bank from non-performing loans and credits, in accordance with Law 4354/2015. The Bank states that the sending of the letter is solely due to systemic, technical reasons, asking him to ignore its content and that his personal data remains physically with the Bank (digital infrastructures, technical applications, etc.), without referring to the right of access exercised. Following this, the Authority, in the context of examining the above complaint, sent the Bank and the AFS company the no. prot. C/EX/479-1/20-05-2020 document, inviting them to place themselves in writing against the accused and asking additional questions. The Bank responded to this document with letter no. letter C/EIS/5039/20-07-2020, in which he stated that: i. the Bank, in accordance with the provisions of Law 4354/2015, as applicable, entered into an agreement for the delegation of the management of its claims from the granting of loans and/or credits to debtors, whose debts or some debts had become overdue and/or had been terminated or settled (hereinafter: the "Portfolio") to the company AFS and already INTRUM HELLAS ANONYMOUS COMPANY FOR MANAGEMENT OF LOANS AND CREDITS (hereinafter: "Intrum" or "company" or "Administrator") and in its context as above agreement, from ... AFS and already Intrum, in the capacity of Manager, took over the management of all the contracts included in the Portfolio. It is noted that at the time of the assignment of the above claims management, the company AFS belonged to the Bank Group and in particular was a 100% subsidiary of the Bank. ii. the Bank proceeded with the required information of all borrowers, debtors, co-debtors, guarantors, collateral providers and in general the natural persons involved in the contracts included in the Portfolio, which was provided both with a relevant press release and subsequently with sending a personalized information, in addition to the detailed information through the form: "Information on the processing of personal data" (Data Privacy Notice) at the start of the implementation of the GDPR, including the possibility of transmission to Companies 3 Management of Claims from Loans and Credits, according to the provisions of Law 4354/2015, as applicable. iii. Due to the large volume, due to a failure in the system configuration (for technical reasons) of the produced lists of recipients

of the above personalized letters, a list of recipients of the above personalized letters, which included customers, as well as other persons who were involved in contracts that were not part of the Portfolio, as they showed a zero balance, like the complainant. iv. As soon as the aforementioned accidental sending of the letters in question was established, the Bank informed them that the initial letters from ... were accidentally sent to them and that this was due solely to systemic, technical reasons and, among other things, informed them that the personal their data remained with the Bank. v. The personal data of the persons in question had remained and remain with the Bank, registered in the Bank's digital infrastructure, technical applications, systems etc. and have not left the Bank's systems and applications, nor have they been transferred to the systems and applications of another legal entity, were not transmitted by the Bank to Intrum, there was no transfer of them to Intrum's systems and applications, while the company did not gain access to said data nor did it process them in any other way. vi. In the main, there was no processing of the personal data of the persons in question by AFS and already Intrum and consequently there was no incident of violation, nor of course was any risk caused to the rights and freedoms of natural persons. Taking into account and weighing the above, the Bank did not proceed with any recording of the incident or any notification of a personal data breach. 4 Accordingly, Intrum with no. prot. C/EIS/5008/17-07-2020 electronic message brought to the attention of the Authority that: i. the Bank entered into, in accordance with the provisions of Law 4354/2015 as applicable, an agreement for the delegation of the management of its receivables from loans/credits to debtors whose debts had become due in whole or in part and/or had been terminated or set up (hereinafter the "Portfolio") in the company, with effect from ..., ii. the Bank together with the company informed, through a personalized letter, all natural persons involved in the claims included in the initially defined Portfolio and the "first wave" of sending personalized information took place on ... and concerned a significant number of contracts , as they were included in the Portfolio at the start of the aforementioned partnership between the Bank and the company, iii. from what emerged from its investigation and in response to the complainant, his personal data was never passed on to the company and remain in the Bank. Based on relevant information from the Bank, with data on the production date of the aforementioned "first wave" of personalized letters, the claims linked to the complainant's loans/credits did not meet the criteria on the basis of which the Portfolio under management was defined and therefore there was no issue of transmission to the company and therefore, they have never been processed by company officials, iv. from what the Bank has explained to the company, the complainant was included in a list of recipients of personalized information, dated ..., for the Bank's assignment of management to the company, thanks to a systemic/technical

error. The Authority, following the above, sent the under no. prot. C/EX/479-2/04-12-
2020 letter to the Bank and Intrum to provide further 5 clarifications, to which the Bank responded with the no. prot. G/EIS/1106/15-02-
2021 document: i. Two agreements were presented to the Authority, which resulted in the assignment by the Bank to the company AFS (now Intrum) of the management of the Bank's receivables portfolio and the provision by the latter to Intrum of some services related to the management of receivables, among which are the provision of the required access by the Bank to authorized employees of the company, in order to fulfill the purposes of the management, following the assignment of the receivables portfolio management in question. ii. The company AFS was renamed to Intrum and the name was changed without a change of legal entity and the VAT number and number remain the same. GEMI, therefore, there was no need to enter into other contracts, as there is no change, no change of the legal entity and since no change took place other than the name of the recipient of the personal data, there was no obligation to provide any special information to the customers, as it would be without object would only cause confusion. iii. As stated in the information letters for the assignment of claims management from the Bank to Intrum and as provided for in Chapter 11 (Data Protection) of one of the above agreements, both the Bank and the Administrator, i.e. Intrum, act as two independent responsible parties processing, both in terms of the data provided to them and in terms of the data they collect themselves in any way, in the context and for the fulfillment of the purposes of the above claims management delegation agreement and therefore bear the relevant obligations of those in charge processing. The reason why the Administrator has been designated as an independent data controller is because he carries out his duties by defining the purposes, manner and means of personal data processing - during the management of the portfolio of claims assigned to him - independently of the instructions of the owner of the claim, i.e. the of the Bank, in the context of its extensive management role and its supervisory obligations and defines 6 independently of the person assigning the management, i.e. the Bank, the purposes and means of data processing in the context of the collection, recording, archiving and use of personal data for the fulfillment of its supervisory obligations and its compliance with the regulatory and institutional framework that governs its operation. In addition, all of the above results from the way of operation, as well as from the policies and procedures that the Administrator observes, in the exercise of his powers, from which it follows that he generally operates as an independent data controller and which are also referred to in relevant agreement. iv. In addition to the data that the Administrator receives from the Bank, through its access to its systems, it may also process additional data, such

as registrations of new data, after direct communication with the data subjects involved in loans that meet the perimeter criteria and management (e.g. new contact phone number, new ID card number, new financial information, recent settlement statement, etc.) or data related to claims (e.g. additional data related to the loan portfolio. This data is collected by the Administrator either directly from the above data subjects, or legally from other sources or Teiresias S.A. The processing in question is based on valid legal bases of processing, such as, for example, that in accordance with the provisions of Law. 4354/2015, as applicable, management of claims by the Administrator, the examination and evaluation of requests for regulation, settlement, the conclusion of the settlement agreement, the settlement of debts, the conclusion of a compromise agreement, compliance with legal obligations of the Administrator arising from the institutional and regulatory framework that governs its operation, etc. v. The following are defined as the delimited perimeter of claims management by the Administrator: i. Claims characterized as Non-Performing (according to EBA definitions), ii. Claims that are regulated, for which the monitoring period has not yet expired, also as defined in the EBA definitions, iii. Claims that were even one day late, as the said management is no longer covered by a unit of the Bank, iv. Special cases, such as customers who have filed for bankruptcy, customers who are seeking adjustment due to financial difficulties. of recipients vi. Claims with a zero balance, either at the time the transaction was initiated or at a later time do not need management, do not meet the criteria for management by the Administrator and were inadvertently included in the list of personalized letters, never having any access to their data by the Administrator , as they did not meet the criteria for management by the Administrator and consequently the Administrator did not process the data of the persons in question. The said failure related to the system configurations of the generated lists of recipients of the personalized newsletters, as a result of which he inadvertently joined and systemically produced a list of recipients of the said personalized letters, which also included customers and other persons not involved in the managed portfolio, as they were showing zero balance. Therefore, for the above reasons, the persons in question received the personalized letters by obvious mistake. It is clarified that no data transmission is carried out from the Bank to the Administrator, except for providing the Administrator with access to its systems, which is activated exclusively and only if specific management criteria are met, when the requirements for the management of claims that have been included in the perimeter are cumulatively met (existence of a debt in combination with a time criterion, i.e. days of delay). The Bank provided files (log files) according to which at points in time after the date on which management was taken over by the Administrator, i.e. after ..., access to the complainant's data was exclusively provided to employees of the Bank, as can be seen from the

confirmation of the Human of the Bank's staff which was also provided, without the slightest involvement of the Administrator, as the criteria for his management and access were not met. 8 vii. The Bank also provided data on behalf of Intrum regarding the total number of unique loans and the number of unique customers who received the initial information letter. A letter was received by the principal debtors/co-debtors/guarantors and collateral providers, while it was not sent to deceased/and unaddressed customers. - Number of people sent a letter due to the system configuration failure: Total number of unique customers who received the initial letter : 23,259. - Number of persons to whom a follow-up letter was sent informing the Bank of the mistaken sending of the initial letters, as well as the time at which said letter was sent: Total number of unique customers who received the referred to as "apology letter" : 23,259. The referred to as "apology letters" were delivered to ELTA on ... . viii. The Administrator is granted the possibility to access the relevant files and systems of the Bank, only with regard to data related to claims that are included in the defined perimeter and meet the management criteria and this for the fulfillment of the purposes of said management. In particular, it is noted that according to the technical specifications for the implementation of access by the Administrator, said access to the Bank's relevant systems: (a) is provided to authorized users of the Administrator, who have been determined based on role and duties and (b) is activated exclusively and only when specific management criteria are met, when the requirements for the management of the perimeter requirements are cumulatively met (existence of debt in combination with a time criterion, i.e. days of delay). Consequently only in these cases data is also processed by the Administrator. ix. Therefore, only if all the access conditions are met, i.e. the existence of all the requirements management criteria included in the perimeter, the Administrator gains access to the data of a specific requirement, through authorized users defined 9 based on role and responsibilities and in accordance with the secure user access regulations. During this process of providing access to the Administrator, the following security measures are taken and observed, among others: minimization of data processing, incorporation of the necessary guarantees in the processing for data protection, providing access only to authorized users - employees of the Administrator , based on role, responsibilities and tasks, ensuring confidentiality, integrity, availability, reliability of processing systems, access control, access techniques to authorized users, implementation of the need to know principle, log files, compliance with regulations for secure user access . x. There are files (log files), which arise from the Bank's customer-centric system (ICE) and concern the inclusion of customers in the perimeter or the production files of the letters sent for the 1st time and include information such as CRS/Date of file production/ Type of letter. When the letters are sent, a file is returned by the company Inform Lykos SA. and the information is

then exposed in the electronic filing of the documents on the intranet (internal network of the Bank). xi. In the middle of …, after the Bank became the recipient of relevant complaints from customers, it became aware of the issue and immediately, around …, the internal procedures to investigate, identify and manage the matter began with the cooperation of the Bank's competent units. Following the above processes and after the required controls were completed, at the end of ... the above failure was identified and confirmed, at which point the Bank took all the required dynamic actions to immediately and effectively deal with and restore it. In particular, the referred to as "apology letters" were drawn up and sent immediately, dated ... and the above failure in the systems was remedied by drawing up the required corrective actions and taking the appropriate technical and organizational measures. 10 xii. To the Authority's request to the Bank to provide all the log files, the latter replied that it is not possible for the Bank to provide any relevant document since it is the Bank's entire portfolio. The Bank's procedure has been submitted to the Authority under the title: "Dealing xiii. Security Incidents". Intrum responded with the no. prot. C/EIS/1076/12-02-2021 document as follows: Regarding the above points (i, ii, iii) the company has contributed the same data i. with what the Bank mentioned above. ii. With reference to the way in which the Bank's clients have been informed about the change of management companies, the company stated that "there was no change in the purpose of the Company except that its name and distinctive title were changed and there was no change in the recipient of the of personal data to which the Bank had transmitted the personal data." iii. Both the Bank and the company act as Independent Processors and this applies both to the data that the former transmits to the latter and to the data that each collects to fulfill the purposes of the agreement between them, as the increased obligations and duties of the company, as derived from the regulatory framework in force that governs the operation of the company, demonstrate that the management of claims on its part is equivalent to the management that can be carried out by a credit institution and has increased institutional obligations for the satisfaction of which it is called upon to have a specific organizational structure, to establish Policies and procedures that will define the framework for the exercise of its activities. iv. Private loans with a zero balance do not meet the criteria for inclusion in the managed perimeter and are therefore not assigned to the company for management, and the Bank informed the company, in mid-October 2019, that 11 creditors with a zero balance had, by mistake, been included in a file of clients - recipients of the personalized letters dated ... although they were not involved in the portfolio assigned to the company. The error in question was the product of a system misconfiguration when defining the initial portfolio to be assigned to the company for management and resulted in the sending of a personalized information letter to clients outside the portfolio of receivables actually taken over

by the company. v. The Bank has undertaken to provide access to the company's authorized personnel to its systems (the Bank's systems) and to a limited extent to data related to the receivables under management. vi. The company does not have at its disposal historical data dated ..., as the managed perimeter has since changed and the company cannot refer to data on that date, except with the assistance of the Bank. With the conclusion of the above-mentioned agreements from ... the Bank gave the necessary access to the company's personnel to loan/credit data in the perimeter, as it had been configured, setting as the start date for the company's management operations the ... date which it notified and to the customers-recipients of the personalized letters. Subsequently, the Authority called under no. prot. C/EXE/1621/29-06-2022, C/EXE/1620/29-06-2022 and C/EXE/1619/29-06-2022 documents the complainant, the Bank and the Intrum company, respectively, as legally represented, to appear at the Authority's Plenary meeting on Tuesday, 07-05-2022 in order to discuss the aforementioned complaint. At this meeting, the postponement requests submitted by the complainant and the Bank were examined and accepted. Subsequently, the Authority called again with the under no. prot. C/EXE/1814/13-07-2022, C/EXE/1816/13-07-2022 documents, respectively, the above involved parties, as legally represented, to be presented at the meeting of the Plenary of the Authority on C/EXE/1813/13-07-2022 and 12 Tuesday, 19-07-2022 in order to discuss the aforementioned complaint. At this meeting the complainant attended, on behalf of the Bank, B, Vasiliki Maria Tsaldari (AMDSA...) and C, Data Protection Officer and on behalf of the Intrum company, D and E, Director of Regulatory Compliance - Data Protection Officer (...). During this meeting, those present, after developing their opinions, submitted the complainant, the Bank and Intrum under no. prot. C/EIS/9037/22-07-2022, C/EI/9260/01-08-2022 and C/EIS/9222/29-07-2022 memoranda respectively. The complainant with his memorandum of 22-07-2022 submitted to the Authority detailed statements of debts and payment statements of the Bank for the year 2016 from which it appears, as he claims, that at the time of the illegal processing of his personal data, i.e. the year 2019 , not only did he not owe the defendant the complaint, but the latter had issued and delivered relevant payment receipts to him as early as 2016. The Bank with its memorandum of 01-08-2022, beyond what it had claimed with the answers he provided to the Authority before the discussion, he states that despite the fact that persons involved in zero balance loans, including the complainant, were mistakenly included in the list of recipients of the personalized letters, no access was ever made to their data by the Administrator, as they did not meet the criteria for management by the Administrator and consequently the Administrator did not process the data of the persons in question. The particular failure concerned claims with a zero balance and the reason why the above claims were inadvertently included in the said list was because in most cases, at some distant

moment in the past, the claims may have been presented or marked systemically with indication of delay, as happened in the case of the complainant. Given, however, that in the meantime and already at the time of the assignment of management by the Bank to the Administrator, the claims in question with a zero balance - as was the case of the complainant - had now been paid in full, while there were no 13 pending in relation to those that need management, they had not been marked ("did not carry a relevant flag") as claims under the management of the Administrator (they had not been included in the Visibility perimeter with the debts visible to be managed but in the Servicing perimeter with the debts of potential management) as they did not meet the criteria and conditions of any management by Administrator, and therefore the Administrator never gained any access to said data. For this reason, after all, the Administrator does not know the complainant, has not gained access and in general has not received knowledge of any of his data and in general any element that concerns him, and neither does the Bank, when submitting the complainant's right of access and in the context of his questions regarding the transmission and in general processing of his data by the Administrator, he answered in the negative. In the cases of the complainant and the other customers, in addition to sending the letters of apology, the Bank also proceeded to gradually close the accounts with zero balance, after carrying out all the necessary checks. Also, regarding the definition of the company as an independent data controller, the Bank claims that, as provided in the legislative framework governing its operation, the Administrator is allowed to undertake the legal and accounting monitoring of the claim until the full or partial payment of the debt. In particular, the Administrator has the right to act all the prescribed management operations, which may consist in particular of legal, accounting monitoring, collection, carrying out negotiations with debtors, entering into agreements of compromise or arrangement and settlement of debts, in accordance with Code of Ethics, as established and in effect. Finally, the Bank states the reasons why the conditions for notification of a personal data breach incident were not met in this particular case claiming that the "Security Incident Handling" Procedure resulting from the "Security Incident Management Policy" was applied and considering that the 14 Administrator did not access and therefore did not process in any way the data of the persons related to the zero balance contracts in question, as is the case of the complainant, as they did not fall within the defined management perimeter, did not meet the management criteria and generally did not required any management by the Administrator, it is concluded that no incident of data breach took place and therefore no risk to the rights and freedoms of natural persons was caused. Consequently, the conditions for recording an incident, according to the GDPR, were not met through the Bank's above-mentioned procedure, while the unnecessary disclosure of incidents that do not constitute data breaches or do not

cause a risk to the rights and obligations of the subjects is achieved, among other things, as this practice is in line with the principle of accountability and GDPR principles. notification of an incident of violation, or The Authority, after examining the elements from the entire file, after hearing the rapporteur and the clarifications from the assistant rapporteurs, who were present without the right to vote, after a thorough discussion, THINKS IN ACCORDANCE WITH THE LAW 1. Because , from the provisions of Articles 51 and 55 of the General Data Protection Regulation (Regulation 2016/679) and Article 9 of Law 4624/2019 (Official Gazette A´ 137) it follows that the Authority has the authority to supervise the implementation of the provisions of the GDPR, of this law and other regulations concerning the protection of the individual from the processing of personal data. In particular, from the provisions of articles 57 par.1 item. f GDPR and 13 para. 1 item g' Law 4624/2019 it follows that the Authority has the authority to deal with the complainant's complaint against the Bank, for illegal processing of personal data concerning him and violation of the right to access data and the Authority's authority is established according to 15 articles 2 par. 1 and 2 of Law 4624/2019 to exercise the above competence, as well as to examine ex officio the participation of the Intrum company in the above processing of the data of the complainant and the Bank's customers. 2. Because Article 5 of the GDPR defines the processing principles that govern the processing of personal data. Specifically, it is defined in paragraph 1 that personal data, among others: "a) are processed lawfully and legitimately in a transparent manner in relation to the subject of the data ("legality, objectivity, transparency"). 3. Because, according to article 5 par. 2 of the GDPR "the data controller bears the responsibility and must be able to demonstrate his compliance with the processing principles established in paragraph 1 ("accountability")". As the Authority1 has judged, with the GDPR a new model of compliance was adopted, the central point of which is the principle of accountability in the context of which the controller is obliged to design, implement and generally take the necessary measures and policies, in order for the processing of data to be in accordance with the relevant legislative provisions. In addition, the controller is burdened with the further duty to prove himself and at all times his compliance with the principles of article 5 par. 1 GDPR. 4. access of the data subject. 5. Because Article 25 para. 1 of the GDPR provides that the controller effectively implements, both at the time of determining the means of processing and at the time of processing, appropriate technical and organizational measures, designed to implement data protection principles and the incorporation of the necessary guarantees in the processing to ensure that, by definition, only the personal data necessary for the respective purpose of processing are processed in a way that fulfills the requirements of the GDPR and protects the rights of the subjects. Because, with the provisions of article 15 GDPR, the right is regulated 1 See Authority

decision 26/2019, paragraph 8, available on its website. 16 Because in the complaint under consideration, based on what the Bank claims, 6. Intrum as Administrator does not know the complainant, has not gained access to and has not been aware of any of his data and in general any element concerning him. Also, according to the data in the file, the selection of the recipients of the initial letter and all the actions to send them were done by the Bank, which has a unit responsible for the strategy it draws in the context of loans in arrears. 7. Because according to the principles of data processing according to Article 5 GDPR, personal data is processed lawfully and legitimately in a transparent manner in relation to the subject. According to the principle of accountability, the controller "bears responsibility and is able to demonstrate compliance". This principle, which is a cornerstone of the GDPR, entails the obligation of the controller to be able to demonstrate compliance, including the legal documentation of each processing operation it carries out in accordance with the legal bases provided by the GDPR and national data protection law. Any processing of personal data is lawful, only if at least one of the conditions set out in article 6 paragraph 1 of the GDPR applies. If one of the aforementioned conditions is met, then this also constitutes the legal basis for the processing. In the complaint under consideration, it appears from the data in the file that the Bank, as the data controller, automatically processed the personal data of a large number (23,259) of natural persons without a legal reason, as due to the lists of recipients of the personalized letters mentioned in the generated lists, it was included in diversion and a list of recipients was systematically produced, which included clients and other persons who, although not involved in the managed portfolio, as they had a zero balance, received the letter in question. Therefore, the data in question did not need any processing and there was no legal basis for the processing to which they were subjected, namely the production of the list and the sending of the letter to the data subjects. Consequently, the Authority finds that the 17th violation of the principle of legality (articles 5 par. 1 a' and 6 GDPR) has occurred by the Bank as the controller of the personal data of the above-mentioned natural persons, among of which and the complainant so that there is a reason to exercise the right according to article 58 par. 2 item. i' corrective power of imposing a fine, as will be listed below. 8. Because with the information currently available, there has been no transmission of the data of the above persons to the Administrator. However, given that the general audit is ongoing and has not yet been completed, the Authority expressly reserves the right to exercise its powers regarding this specific issue in the future. 9. Because, moreover, in this particular case, it appears from the information in the file that, during the selection process of the natural persons, in which the Bank would send an information letter, the appropriate measures were not taken to ensure that this choice was made with the necessary guarantees for the application of the principle of the legal processing

of the data of the persons in question and it was not ensured that only the data necessary for the purpose of informing persons about the transmission of their data. More specifically, according to the Bank's answers, a) the first perimeter (1A - servicing) includes the debts potentially managed by the Administrator and the second perimeter (1B - visibility) the visible debts to be managed by the Administrator, b) the company Intrum can manage through the Bank's systems the cases in which both of the above conditions (1A and 1B) are cumulatively met and c) claims with a zero balance, such as the complainant's (which had now been paid in full, while there were no pending in relation to those that need management), were not managed by the Administrator because they were included in the first perimeter but not in the second. However, these claims should not be included in the first perimeter either, since they do not constitute a potential debt to be managed by the Administrator. 18 Therefore, in practice the Bank did not have the appropriate procedures and measures to apply the same criteria to the same persons in both cases since it excluded the persons in question (with zero paid debt) from the second perimeter but not from the first, which is also seen as unnecessary since the second perimeter was sufficient for the creation of the list of information letters and for the Administrator's corresponding access to the Bank's systems. From the fact that, after the failure was discovered, the Bank proceeded, as it claims, to immediately restore it in the systems by drawing up the required corrective actions and taking the appropriate technical and organizational measures, i.e. the gradual closing of the accounts that carry a zero balance, after carrying out all the necessary checks, it turns out that the Bank could, without further burden at any level, have taken the appropriate measures from the beginning. The Authority's finding of incomplete planning, in violation of the GDPR, is also reinforced by the fact that the Bank did not identify on its own what it constantly refers to as a "systemic failure" that led to the sending of 23,259 letters but only after complaints of its customers. Therefore, based on what is set out above in paragraph 5, the Authority considers that the Bank as a data controller has violated articles 25 par. 1 of the GDPR and there is reason to exercise the right under article 58 par. 2 item. i' corrective power of imposing a fine, as will be listed below. 10. Because regarding the right of access exercised by the complainant on …, based on the initial information letter, according to which his personal data was transmitted to the Administrator, the complainant received as a response from the Bank the letter of apology from …, the content of which was general and addressed to all customers who had received, as he claimed, due to the systemic error, the original letter, with the statement that their personal data remains physically with the Bank and the request that the recipients ignore the content of the original letter. The Bank, with the above response, did not actively respond negatively to the question of whether the data of the complainant was transmitted to the Administrator 19 of the subjects, but

limited itself to recalling the initial letter and its content, indicating that the processing that was inadvertently mentioned has not taken place and has not the data has been transmitted to the Administrator. However, according to Article 15 of the GDPR, the subject has the right to receive from the controller active confirmation as to whether or not the data concerning him is being processed and, if so, the right to access further information. The fact that the data "remains physical" at the Bank, as stated in the reply letter to the complainant, does not provide the necessary and requested information to the subject as to whether the data concerning him has undergone further processing, as the copies of the data that " "remain physical" in the Bank, they could at the same time have been transferred to another legal entity or have been subjected to other forms of processing. Therefore, the Bank, which as the controller has the obligation to adequately satisfy the right of access, should have answered the applicant/complainant specifically that his data were not processed for the purpose mentioned in the first letter sent by mistake and were not forwarded to the Administrator . Also, he should have clearly and fully answered all four questions of the complainant (see history of the present), which also refer to all of his personal data held by the Bank at the time of sending the letter and any other data collected after sending it (see questions under items c and d). Although the complainant refers to his requests for access to his data at the time or after their transmission to the Administrator, the Bank should have accepted his request as access at the time of sending the letter or after it, given that the complainant , as the recipient of said general letter was informed that his data had already been transmitted to the Administrator. In view of the above, the Authority considers that the Bank has not adequately satisfied the complainant's right of access pursuant to Article 15 para. 1 GDPR and there is reason to exercise the right of access pursuant to Article 58 para. 2 item. i' corrective power of imposing a fine, as will be listed below. 20 11. Because from the entire file and based on the hearing process, it appears that the Bank, as the controller of the personal data of the complainant as well as a large number of other debtors, has violated articles 5 par. 1(a), 6, 25 para. 1 and 15 para. 1 GDPR. 12. Because from the entire file and based on the hearing process, the Authority did not establish, based on the facts concerning the Bank, a violation of the GDPR by Intrum respectively. The Authority expressly reserves the right to exercise its powers against Intrum in the event that evidence emerges in the context of the ongoing general audit of the case. 13. According to the GDPR (Ref. Sk. 148) "in order to strengthen the enforcement of the rules of this Regulation, sanctions, including administrative fines, should be imposed for each violation of this Regulation, in addition to or instead of the appropriate measures that are imposed by the supervisory authority in accordance with this Regulation". 14. Based on the above, and after the Authority established that the violation of the provisions of the GDPR in this case was due to a systemic

error on the one hand, as the Bank, as the controller, constantly admits and repeats and on the other hand affected the rights of a large number of subjects of the data (23,259) considers that there is a case to exercise its corrective powers in accordance with article 58 para. 2 c) GDPR (order to satisfy a right) and 58 para. 2 i) and 83 GDPR (imposition of a fine) with regard to the violations identified above . 15. Furthermore, the Authority, in determining the sanction, took into account the criteria for measuring the fines defined in article 83 par. 2 of the GDPR and applicable in this case, the Guidelines "for the application and determination of administrative fines for the purposes of the Regulation 2016/679"2 of the Article 29 Working Party and the Guidelines 2 WP 253 from 03.10.2017 available at the link https://ec.europa.eu/newsroom/article29/items/611237 21 04/2022 of the European Data Protection Council3, as well as the actual data of the case under consideration and in particular: i. The fact that the Bank had not taken the appropriate technical and organizational measures and did not have the appropriate procedures in place, so that the creation of the list of its customers in question results from correct systemic parameters, while following the finding of the failure in question, from the complaints of its customers, took corrective action. The fact that the violation affected, in addition to the complainant, a large number of customers (23,259) of the Bank, whose personal data were processed without a legal reason. The fact that the Bank was negligent in breaching its duty of care and not fraud. The high degree of responsibility of the Bank in relation to the absence of technical and organizational measures in accordance with the above. The fact that it was a systemic error in the specific case under consideration is also admitted by the Bank. The fact that the Authority has not established in the past a corresponding violation of the GDPR by the Bank. The fact that the GDPR violation does not concern a special category of data according to Articles 9 and 10 GDPR. The fact that the Authority was informed of the violation by the complainant and not by the Bank.The fact that the Bank did not obtain any financial benefit from it

said processing based on the information available to the Authority.

The fact that no economic benefit was derived from said processing

(material) damage based on the information available to the Authority.

The turnover of the Bank for the year 2021, which, according to

stated in its post-hearing memorandum, amounts to €2,390m.

ii.

iii.

iv.

v.

vi.

vii.

viii.

ix.

x.

xi.

3 Guidelines 04/2022 on the calculation of administrative fines under the GDPR from 12.05.2022 under public consultation, available at https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf

Based on the above, the Authority unanimously decides that they should be imposed on Bank, as controller, the administrative ones referred to in the ordinance sanctions, which are considered proportional to the gravity of the violations.

The beginning:

FOR THOSE REASONS

A. Finds that the complained Piraeus Bank SA, as responsible processing, violated articles 5 par. 1(a) and 6 GDPR and imposes on Piraeus Bank SA according to article 58 par. 2 item i GDPR the administrative money a fine of one hundred thousand (100,000.00) euros.

B. Finds that the complained Piraeus Bank SA, as responsible processing, violated article 25 par. 1 GDPR and imposes on the Bank Piraeus SA, according to article 58 par. 2 item i GDPR, the administrative fine in the amount of one hundred thousand (100,000.00) euros.

C. Finds that the complained Piraeus Bank SA, as responsible

processing, violated article 15 par. 1 GDPR and imposes on the Bank

Piraeus SA, according to article 58 par. 2 item i GDPR, the administrative fine

in the amount of ten thousand (10,000.00) euros.

D. Gives an order, according to article 58 par. 2 item. 3 GDPR, to the complained Bank

Piraeus S.A., as data controller, to satisfy accordingly

right of access of the complainant, as mentioned in paragraph 10 thereof

present.

The president

Konstantinos Menudakos

The Secretary

Irini Papageorgopoulou