Athens, 02-02-2023 Prot. No.: 267 DECISION 4/2023 (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 18/01/ 2023, in order to examine the case referred to in the present history. The meeting was attended by teleconference by Georgios Batzalexis, Deputy President, in opposition to the President of the Authority, Konstantinos Menoudakos, and was attended by the alternate member Georgios Kontis, as rapporteur, as well as the alternate members Demosthenes Vougioukas and Maria Psalla, in place of the regular members Konstantinos Lambrinoudakis and Grigorio Tsolia who did not attend due to disability although they were legally summoned in writing. The meeting was attended, by order of the President without the right to vote, by Haris Symeonidou, specialist scientist - auditor as assistant rapporteur and Irini Papageorgopoulou, employee of the Authority's administrative affairs department, as secretary. The Authority took into account the following: is the client and beneficiary With the no. prot. C/EIS/5802/15-09-2021 his complaint, A (hereinafter the complainant), is directed against the Bank of Piraeus (hereinafter the complainant), whose bank account he complained about the illegal and without prior information provision of personal data of to his opponent, B. In particular, according to the complaint, in the context of a lawsuit pending against the complainant by the aforementioned opponent before the Single-Member Court of First Instance X, the opponent invoked and submitted with its ... motions, the detailed motions of two bank accounts (with numbers ... and ...) of the complained Bank, 1-3 Kifissias Ave., 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr in which the complainant was initially a joint beneficiary with first beneficiary his aunt, C the genus B, and from her death on ... and henceforth, sole beneficiary. According to the complaint, the presented detailed movements of the above accounts also concerned the period of time after the death of his aunt, up to and including ... . Furthermore, the complainant states that as soon as he became aware of the above, he went to Branch Ψ, where the manager D invoked bank secrecy and claimed that the Bank would never provide the information in question. Then, with his letter G/EIS/7545/18-11-2021, the complainant notified the Authority of the request he submitted to the Bank (with protocol number ...) through his attorney, Stefanos Topalis, and with the G/EIS /1103/27-01-2022 and C/EIS/6617/03-05-2022 documents he communicated to the Authority the answers he had initially received via sms regarding the progress of his request and the final written response from the Bank, according to with which the Bank has taken all the necessary measures in order to protect the banking confidentiality of its customers in accordance with the current institutional framework, as well as that it is competently taken in cases such as the case at hand brought to its attention, in accordance with its internal procedures . In the context of investigating the complaint, the Authority as

2022 document invited the complainant to present her views on the complainants. The complainant was asked to clarify, in particular, a) whether she provided the aforementioned statements of the complainant's account balance to his opponent, B, with what legal basis and procedure, b) in the event that the above processing was based on article 6 par. 1 point f GDPR, what were the legal interests pursued in this case, specifying the weighing procedure followed, in order to determine whether they prevail over the interests, fundamental rights and freedoms of the complainant, as a subject, and c) if he was informed the complainant as a subject for the above processing according to articles 13 and 14 GDPR, and, in case of a negative answer, with what justification. 2 With the under no. prot. C/EIS/7717/06-06-2022 its response, the complained Bank first of all states that the complainant kept joint bank accounts with the deceased C and that B, also a client of the Bank, citing the status of one of of the legal heirs of the above-mentioned deceased aunt of C, a status that arose from her relative legalization as an heir held at the Bank - submitted a request to grant her details and movements of the bank accounts, in which her aunt was a living beneficiary. Subsequently, "due to an obvious oversight and due to an incorrect assessment of the facts and the individual data and parameters on the part of the employee to whom B addressed" as stated by the complainant, the employee in question, after receiving the relevant request, gave the requested details and bank account movements. That is to say, the official, relying on the legalization documents of the applicant, as the legal heir of the co-beneficiary of the complainant, considered "out of an obvious oversight and from his own incorrect assessment", that the applicant had inheritance rights and inheritance claims in relation to these bank accounts as well and wrongly considered that he also had the right to obtain knowledge of the requested information concerning the specific accounts, so he granted her request "due to human error and carelessness, but without intent and malice". According to the complainant's response, the Bank was immediately notified of the matter, its competent Units were immediately mobilized for the thorough investigation of the case and the conduct of all relevant internal procedures. He also mentions that, as emerged from the employee's examination, he did not know the applicant, by mistake he did not see who the joint beneficiaries of the specific accounts were, he was misled and gave her the account movements, while relying on her status as a legal heir, he judged that he did not even need to seek the opinion of the Bank's Legal Department. With its same answer, the Bank maintains: a) that it took all appropriate actions to investigate and deal with the case at hand, b) that in general through the procedures, policies, internal regulations it has drawn up, training seminars it conducts, of the exercise of continuous 3 supervision, training and guidance of the staff, ensures the safeguarding,

protection and lawful processing of personal data as well as the guarding of banking confidentiality, c) that he had informed and trained the specific employee as well – like all employees, so that perform his duties in compliance with the legal and regulatory requirements of the Bank, including the need to seek advice from its Legal Service, however, due to human error, obvious oversight and due to hasty and reckless action, relying on the status of the applicant as a legal heir, did not comply with the above procedure and hastened to provide the requested information, d) that the Bank has initiated the relevant disciplinary procedures, e) that, in conclusion, the case under consideration does not fall within the scope of the Bank's responsibility, any violation could not be attributed to the Bank and finally, f) that according to a decision of the Belgian Data Protection Authority in a case regarding the mistaken sending of electronic mail to subjects other than the intended recipients (Beslissing ten gronde 07/2021 van 29 januari 2021) and despite the fact that accidental data processing also constitutes an objective fact and processing, the specific erroneous processing does not constitute a violation of personal data, since the unintentional processing described in the above decision was not due to insufficient technical and organizational measures from on the part of the controller, given that Article 33 GDPR should be applied in conjunction with Article 32 GDPR, and therefore the personal data breach of Article 33 presupposes a breach of the provisions of Article 32 GDPR. Therefore, since human error cannot in any case be excluded, the Belgian Authority came to the opinion that there was no violation of the provisions of Articles 32 and 33 GDPR. In conclusion, although the complained Bank acknowledges that in this case the complainant's data was illegally processed and improperly transmitted, because this is due to human error, misjudgment and misdirection by the employee and not to failure to take the appropriate technical and organizational measures of Article 32 GDPR, considers that she has complied with the relevant 4 its obligations by investigating the incident and initiating relevant disciplinary proceedings, without notifying the incident to the Authority in accordance with article 33 GDPR, applying the above interpretation of this article by the corresponding Belgian Authority. Given the above, the Authority, with relevant calls, invited those involved to the board of the Authority's Department on 09-11-2022, in order to present their views on the case. During the meeting, the complainant was present together with his attorney, Stefanos Topali (…) and on behalf of the complained Bank, attorney Vasiliki – Maria Saldari (…), E, F, Regional Director, responsible for the involved branch and Z, DPO of the Bank, who did not take the floor. Subsequently, the parties were given a deadline and submitted in a timely manner, G/EIS/12002/23-11-2022 his complainant's memorandum, while the complained-of G/EIS/12098/28-11-2022 her memorandum. During the meeting and with his memorandum, the complainant repeated what was mentioned in his complaint

and pointed out that the violation of the right of access in the form of leaking - providing information to a third, unauthorized person, as well as the violation of his banking confidentiality and the omission of any official notification of him, as the subject of the data, even later, agreed by the complained Bank. The complainant emphasized that his personal data provided to a third party formed the basis and was used against him in the context of a lawsuit before the Single-Member Court of First Instance X and pointed out that the Bank did not provide information about the branch, the employee involved and the special circumstances (how to submit of the application, accompanying documents, information about the "legitimization of heirs" invoked by the Bank) nor about the findings of the disciplinary process that resulted in a reprimand, in order to determine whether the leak of his data, which concerned two accounts over a period of several years , is indeed due to human error on the part of the employee in question. In conclusion, he argued that the breach of his data was done with intent, probably in the context of getting to know the specific employee, without any weighing taking place and that ultimately it was not an isolated incident due to an oversight, but a systemic failure of the Bank, which , ignoring the dynamics of small societies such as that of Ψ allows corresponding behaviors. However, the complainant did not provide any evidence to prove this claim. The complained-about Bank, both during the meeting and with its memorandum, argued the following: - That according to the employee's testimony, on ... came to the store B, who was completely unknown to him, and invoking the status of her heir deceased C, requested to be informed of the movement of her accounts, and the employee provided the requested information, without requesting the opinion of the Legal Service, based on the Legalization of Heirs document from … (provided as Related 1), which had been legally issued in accordance with the Bank's relevant procedures after all the necessary legalizing documents had been taken into account and which included the applicant as the legal heir of the above death, inadvertently overlooking the fact that there were co-beneficiaries in the accounts and despite the fact that in the observations of the said document explicitly states the following: "The heirs can be given information about any individual accounts as well as any other products and legal relationships that they had with our Bank. No information should be given about any joint accounts.' The Bank stated that this was a hasty, reckless action that was due to human error and not fraud on the part of the employee, which occurred through no fault of its own. - With regard to the manner in which the incident was handled after becoming aware of it, the Bank asserted that the competent Units were immediately mobilized and thoroughly investigated the incident, subsequently disciplinary proceedings were initiated against the employee in question who was asked to provide explanations and after weighing all the parameters of case, he was given the disciplinary penalty of a strong

verbal reprimand and was placed under constant supervision and monitoring by the Bank's competent bodies. 6 - Regarding its general compliance with the GDPR, the Bank emphasized that it has taken all the appropriate technical and organizational measures for the security of the processing, and as proof of the relevant claim, it provides an indicative description of these measures, providing and referring to the relevant procedure documents and its policies, as well as information and training documents for its employees for the protection of banking confidentiality and for compliance with GDPR processing principles. In addition, the Bank refers to the relevant memos that it issues from time to time, addressed to all of its staff, such as on the matter in question, the memo from ... of the Regulatory Compliance Group, regarding the observance of banking secrecy (Related 4), where it is mentioned expressly that banking secrecy applies even in the case of heirs of a deceased co-beneficiary, who are not entitled to receive knowledge of the movements and the balance of the joint joint account, but also other Policies and Procedures concerning the management of the details of a deceased customer. Therefore, the Bank claims that it has taken all the necessary measures and established all the necessary procedures, but it cannot prevent the immeasurable factor of human error. - In relation to the measures taken after the occurrence of the incident in question for the future, the Bank stated that it issued the official memo 2022/1252 dated 06/23/2022 to all its staff (provided as Related 10) and to which reiterates the instructions on strict observance of banking secrecy even in the case of the heirs of a deceased beneficiary, who are not entitled to receive knowledge of the movements and the balance of the joint separate account. - Finally, regarding the non-disclosure of the incident to the Authority pursuant to Article 33 of the GDPR and to the subject, pursuant to Article 34 of the GDPR, the Bank reiterated its initial claim, that in order for a data breach to occur in accordance with the definition of Article 4 . 12 GDPR, there must have been a breach of security, which is related to the lack of adoption and implementation of appropriate technical and organizational measures of Article 32 GDPR, which is not the case in this case, while he considers that the specific incident does not fall within the scope of the Bank's responsibility nor can it be imputed to her, as it is solely due to human error, which she could not have prevented. Therefore, in its opinion, there has been no violation of the provisions of articles 32 and 33 GDPR. 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. In particular, from the provisions of articles 57 par. 1 item f of the GDPR and 13 par. 1 item g´ of Law 4624/2019 it follows that the Authority has the authority to deal with A's complaint against Piraeus Bank and to exercise, respectively, the powers granted to it by the provisions of Articles 58 of the GDPR and 15 of Law 4624/2019. 2. Article 5 par. 1 of the General Regulation (EU) 2016/679 for the protection of natural persons against the processing of personal data (hereinafter GDPR) sets out the principles that must govern a processing. According to article 5 par. 1 a) and f) GDPR "1. Personal data: a) are processed lawfully and legitimately in a transparent manner in relation to the data subject ("legality, objectivity and transparency"), [...] f) are processed in a way that guarantees appropriate data security of a personal nature, including their protection from unauthorized or illegal processing and accidental loss, destruction or damage, by using appropriate technical or 8 organizational measures ("integrity and confidentiality")", while as pointed out in the Preamble of the Regulation, "The personal data should be processed in a way that ensures the appropriate protection and confidentiality of personal data, including to prevent any unauthorized access to such personal data and the equipment used to process it or the use of these personal data and the equipment in question" (Ref. Sk. 39 in fine). Furthermore, according to the principle of accountability which is expressly defined in the second paragraph of the same article and constitutes a cornerstone of the GDPR, the data controller "bears the responsibility and is able to demonstrate compliance with paragraph 1 ("accountability")". This principle entails the obligation of the controller to be able to demonstrate compliance with the principles of art. 5 para. 1. 3. According to the provision of article 24 para. 1 GDPR: "1. Taking into account 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 applies 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. 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 the 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 the case may be: a) the pseudonymization and encryption of personal data, b) the ability to ensure privacy, 9 integrity, the availability and reliability of processing systems and

services on an ongoing basis, c) the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical event, d) the process for regular testing, assessment and assessment of the effectiveness of technical and organizational measures to ensure the security of processing. 2. When assessing the appropriate level of security, particular account shall be taken of the risks deriving from the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access transmitted, stored or otherwise processed." personal data 4. 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). 10 5. Incidents of data breach must be notified to the Authority within 72 hours from the moment the data controller became aware of them, in accordance with article 33 par. 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 breach of personal data, 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.' And according to recital 85, as soon as the data controller becomes aware of a personal data breach, "he should immediately notify the competent supervisory authority, unless he can demonstrate, in accordance with the principle of accountability, that the data breach of a personal nature may

not endanger the rights and freedoms of natural persons". Therefore, a "presumption" of the obligation to notify incidents of infringement to the Authority is established, with the sole exception of the absence of risk to the rights and freedoms of the affected subjects, for which the data controller bears the burden of proof, if he chooses not to make such a notification. The obligation of Article 33 is self-contained and independent from the obligation of the data controller to apply appropriate technical and organizational security measures, established by Article 32 GDPR. In addition, the violation must also be notified to the data subject, on a case-by-case basis 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)". 6. In the case under consideration, the following emerged from the information in the file: On ..., B went to a store of the complained Bank, who, invoking her status as the heir of the deceased C, requested to be informed of the movement of the latter's accounts. The employee to whom he addressed, based on the document of Legalization of Heirs from ..., which had been issued in accordance with the relevant procedures of the Bank and which included the applicant as the legal heir of the above-mentioned deceased, without requesting the opinion of the Legal Service, granted the requested detailed account statements, ignoring the fact that in two bank accounts (with numbers ... and ...) the complainant was initially a joint beneficiary with his aunt, C, as the first beneficiary, and from her death on ... and from then on, he was the sole beneficiary. Subsequently, B filed a lawsuit before the Single-Member Court of First Instance X against the complainant with the object of inheritance claims, in the context of which she invoked and presented with her proposals from ... the said detailed account movements of the complainant, which also related to the period after the death of the first beneficiary and until ... As soon as he became aware of the above, the complainant went to Branch Ψ, where manager D invoked bank secrecy and claimed that the Bank would never provide the information in question. In the month of ... of ... the complainant complained in writing about the incident in question to the Bank, submitting through his attorney-at-law the no. first ... request and subsequently received the written response from ..., according to which the Bank has taken all the necessary measures in order to protect the banking confidentiality of its customers in accordance with the current institutional framework, as well as 12 and that it is competently taken in cases such as the case in question brought to its attention, pursuant to its internal procedures. Although the Bank appears to have taken appropriate technical and organizational data security measures,

including adequate training of its employees on procedures for granting account details to heirs, it did not appear to have taken any action after being notified by the complainant of the due incident. After the Bank's views were requested on behalf of the Authority (on 20/5/2022), the Bank replied (on 6/6/2022) that it had initiated disciplinary proceedings against the employee. The said procedure resulted in the imposition of the disciplinary penalty of a strong verbal reprimand and the supervision of the employee, according to what the Bank argued in the context of the hearing. In addition, following the incident, the Bank issued an official memo (on 23/06/2022) to all its staff reminding them of the strict observance of bank secrecy in the case of heirs of a deceased beneficiary of a joint account. However, although the Bank acknowledged that the transfer of the complainant's data in this case was unlawful and due to fault of its employee, it did not notify the Authority of the incident in accordance with Article 33 of the GDPR nor in notifying the complainant in accordance with Article 34 of the GDPR, considering that it did not have the relevant obligation, given that it had taken sufficient technical and organizational security measures during article 32 GDPR. Given the facts presented above, it is established that the provision of the personal data of the complainant to his opponent by the complained Bank was done without a legal basis, in violation of the principle of the legality of the processing (Article 5 para. 1 a' GDPR) and in violation of the principle of data confidentiality (Article 5 para. 1 GDPR). The processing in question took place despite the contrary instructions of the complainant, as Processing Manager to her staff. This is therefore a data breach incident (a security breach that led to an unauthorized disclosure), which is attributed to the misdirection of 13 a specific employee. The error of the Bank's employee does not constitute a reason for exonerating the Bank from the responsibility of properly following the procedures it has established to prevent incidents of personal data of its customers being compromised, because the employee was acting as an employee, in the context of performing the duties that the Bank had assigned him assign, consequently, the objective responsibility of the Bank according to article 922 of the Civil Code. For the same reason and given that the employee acts under the supervision and orders of the Bank (see article 29 GDPR and in contrast to the definition of "third party" in article 4 paragraph 10 GDPR), the respective employee is not considered a third party in the exercise of the tasks assigned to him and his actions are attributed directly to the Bank, as data controller. 7. Furthermore, although the Bank acknowledges that the aforementioned information falling under the complainant's bank secrecy was illegally provided, and although it claims to have investigated the incident, to have initiated the relevant disciplinary procedure and to have issued a relevant official memo reminding to the employees their obligations regarding the management of the data of the deceased, did not notify the incident to the Authority as a data breach incident according to

article 33 GDPR nor did it notify the subject according to article 34 GDPR, claiming that this does not fall within the scope of responsibility of and citing a relevant decision of the Belgian Authority, according to which, as long as appropriate technical and organizational measures have been taken in accordance with Article 32 GDPR and if the incident is due to human error that cannot be prevented and prevented, there is no notification obligation. With its memorandum, the Bank provided sufficient evidence to substantiate the claim that it has taken the appropriate technical and organizational security measures for the processing, therefore it follows that there was no violation of Article 32 GDPR. However, it should be noted that despite the adoption and implementation of appropriate security measures, it is always possible that an incident will occur which will harm the security objectives, as in this case the confidentiality of the data. The technical and organizational measures described in Article 32 GDPR are necessary for the purpose of 14 prevention, but they are not capable of preventing every possible security incident. For this reason, in addition to and independently of the obligation established by article 32 of the GDPR, in cases of violations, articles 33 and 34 of the GDPR apply and are applied, in order to deal with any violations in practice, in a "repressive" manner. In other words, it is possible for a breach of security to occur without it being due to a breach of Article 32 GDPR, contrary to what the complainant claims, as such an interpretation cannot be deduced from the letter of the relevant provisions. Furthermore, from paragraph 3 (item d) of Article 33 of the GDPR, the obligation of the controller to "take or propose to take measures to deal with the breach of personal data, as well as, where appropriate, measures to mitigation of its possible adverse consequences". In this case, the Bank did not plead that it took any measure to mitigate the consequences of the specific violation, which it recognized as such and attributed to the human error of its employee. Such a measure could be, for example, a document to the recipient of the data, stating that the provision took place illegally, by mistake of the employee and requesting their destruction. In addition, the complainant as a data subject pursuant to Article 34 GDPR was not informed of the relevant measures, in a way that could possibly contribute to mitigating the consequences of the infringement incident (if, for example, the complainant provided the Court with a document with which the Bank recognizes as illegal the transmission of data to its counterparty). In this case, in order for the subject to be informed of the Bank's position regarding the incident, he had to make a complaint to the Authority. Therefore, despite the fact that the Bank appears to have established sufficient security measures, which it updates whenever this appears to be necessary, and therefore no violation of Article 32 of the GDPR is found, a violation of Articles 33 and 34 of the GDPR on its part is found, for the above mentioned reasons. 8. Following the above, from the information in the file and following the hearing, the Authority finds on behalf of the

complained Bank: 15 a) Violation of the principle of the legality of the processing (articles 5 par. 1 a), 6 and 13 GDPR) , given that the movement data of two bank accounts of the complainant for a period of 4 years were provided illegally, that is, without a legal basis and opaquely, without informing the subject. b) Violation of the principle of data confidentiality (article 5 par. 1 f) GDPR), because the above processing led to an illegal leak of the complainant's personal information to his opponent. c) Violation of the complainant's obligations under Articles 33 and 34 of the GDPR, given that she did not notify the Authority or the subject, nor did she take measures to mitigate the consequences of the violation, such as, for example, contacting the recipient of the data in order to return or destroy the unlawfully provided personal data. 9. Based on the above, the Authority considers that there is a case to exercise its corrective powers (imposition of a fine) in accordance with articles 58 par. 2 i) and 83 GDPR with regard to the violations established above. To determine the sanction, the Authority takes into account the criteria for measuring the fine defined in article 83 par. 2 of the GDPR that are applicable in this case. In particular, the following are taken into account: a) The nature, gravity and duration of the breach: the breach concerned information on the balance and movements of two bank accounts of the complainant for 4 years, i.e. it concerned information of a sensitive nature protected by bank secrecy. It is taken into account that possibly the opponent of the complainant and recipient of the data could gain access to the information in question following a court order (production of documents). b) The fact that the violation is due to the negligence of an employee of the Bank. However, this is gross negligence, given that the document on which the employee relied to provide the requested information to his opponent 16 etc). Complainant's response (Legitimation of Heirs) included the express observation that information on joint accounts of death may not be given to heirs. c) The fact that the action of the Bank's employee establishes its responsibility as a data controller. d) The fact that only one subject was affected by the violation. e) The fact that the complained Bank, as a data controller, did not take any action to mitigate the consequences of the breach towards the subject. It is noted that the complainant would not have been informed of the Bank's position on the incident, if he had not appealed to the Authority, since the Bank's ("we comply with all measures, his initial notification from ... was formal, we are responsible" of the Bank after being informed of the incident by the complainant was not immediate, on the contrary, it took several months before he investigated it, when his opinions were requested by the Authority.f) The degree of responsibility of the Bank based on the technical and organizational security measures taken: From the data presented to the Authority that the Bank has taken appropriate technical and organizational measures in accordance with Article 32 GDPR, however, it does not appear that they are applied in every case, nor that the Bank supervises their

implementation by carrying out periodic checks on its staff. g) The way in which the Authority was informed of the violation (through a complaint). h) The large size of the complained-about Bank. i) The fact that the Bank has been fined again in the past for violating the principle of confidentiality and its obligations based on articles 33 and 34 GDPR (see decision 6/2022).

FOR THESE REASONS

THE BEGINNING

17

It imposes on Piraeus Bank S.A. as a controller based on the article

58 paragraph 2 paragraph i of the GDPR total fine of thirty thousand (€30,000)

euros for violations of the principle of legality of processing (art. 5 par. 1

a) GDPR), the principle of data confidentiality (art. 5 par. 1 f) GDPR) and

of its obligations under Articles 33 and 34 GDPR.

The president

George Batzalexis

The Secretary

Irini Papageorgopoulou

18