Athens, 26-09-2022 Prot. No.: 2364 DECISION 52/2022 (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 19/07/ 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 the absence of the President of the Authority, Constantinos Menoudakou, and was attended by Grigorios Tsolias, regular member, as rapporteur, and Demosthenes Vougioukas, alternate member in place of regular member Konstantinos Lambrinoudakis, who he did not attend due to disability although he was 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: With the no. prot. C/EIS/642/25-01-2021 complaint by A (hereinafter complainant), directed against Alpha Bank A.E. (hereinafter the complainant), of which a customer is entitled, complaining about the illegal transfer of a document containing his personal data from the [region] Y branch of the complained Bank to B, the complainant's opponent in the context of a civil dispute pending before [region] F Specifically, according to the Single-Member Court of First Instance 1-3 Kifisias Ave., 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr complaint, the above opponent of the complainant submitted as relevant to the ... proposals of his lawsuit, a certified copy of the Notice of Operational Risk from ..., signed by the employees of the complainant, Mr. C and Mr. D. This document describes in detail the complainant's visit to the [area] Y branch of the complained-of Bank on ..., and the exact details of his bank accounts, the amounts of money he deposited that day and the movements he made (transferring money from his wallet to his bank account) are mentioned. The exact content of the document in question is as follows: "Today ... came to our Shop .. a.m. Mr. A sat in the Manager's office and asked to visit his locker, with the intention of taking money from the locker to count and deposit it into his account at our Bank. The Manager informed the desk manager D .. pm about the client's wish to proceed with the visit procedures. The Director and the counter manager went down to the counter area according to the regulations and then I called the customer. The customer alone, as required, made his visit to the closed box office area and left it .. pm. He then went to the cash register .. pm where, according to the Central Cashier E, he presented him with ... bundles of banknotes of ... euros and asked him to count them, as soon as the cashier has counted the first bundle, the customer asks him "... euros?" and the cashier answers "no ... euros" he counts the same bundle again and tells him "... total ... euros" then the cashier counts the second bundle and tells the customer "… total … euros". Then .. pm the treasurer called the Director to

inform him about the above. In the presence of the customer and the Manager, the ... bundles of ... euro banknotes were counted again ... times. The customer takes out other ... bundles of ... euros and gives them to the cashier to count them, the count is done and the cashier tells him "... euros and in total ... and ... ... (Presence of Manager). The customer was monologuing that someone put … euros in his safe deposit box and called on his mobile phone for a few minutes telling his interlocutor that the money is … euros more. He informed the Manager and the cashier that in his locker last time (about ... years ago) he had a total of ... euros and the reason for visiting it was to leave in the locker ... euros and deposit the remaining ... euros in his account, he expressed surprise from the event and requested .. pm to finalize the deposit of … euros in his account … as well as a copy of the transaction with the detailed analysis of the money. After the departure of the customer (.. am), the Store made an agreement and a detailed count of the cash register where at the end of .. am there was no difference...". And according to the complaint, the complainant's approval as a subject was not requested for the granting of the said document containing his personal data to his opponent, Mr. B, while the complainant maintains that "he was not even aware of the creation of an Operational Risk Incident Notification document from the Bank for what took place on the above date". Furthermore, the complainant states that on … with his written request to the [area] Y branch, he requested to be informed of the reason for granting the disputed document to the third party, B, given that a similar request of the complainant had been rejected in the past by the Bank on the grounds that documents documenting the Bank's internal procedures cannot be granted to any third party. The response received by the complainant pursuant to no. ... and ... letters of the branch [region] Y was, as stated, initially that the above document of the Announcement of an Operational Risk Event "was submitted in the context of criminal proceedings and in exercise of the right of judicial protection, to refute your lawsuit against the Bank's employees" and then, in response to a newer application-protest of the complainant, that "the invocation and production of the [disputed document] was entered legally, in defense of a superior interest". The complainant states that he is not aware of this document being presented in any criminal proceedings, while in his opinion the Bank's answer is vague, because it does not clarify in which criminal proceedings the document in question was presented. Furthermore, according to the complainant, the "superior interest" invoked by the Bank for granting the document to his aforementioned opponent is not sufficiently justified. The Authority, in the context of examining the above complaint, with no. prot. C/EX/1081/16-04-2021 its document, invited the complained Bank to present its views on the complained, providing all relevant documentation. In her response, the complainant was asked to clarify in particular: a) if she issued the document in question to the complainant's opponent, B, with

what legal basis and procedure, b) in the event that the above processing was based on Article 6 par. 1 item f GDPR, what were the legal interests pursued in this case, specifying the weighing procedure followed, in order to judge whether said legal interests prevail over the interests, fundamental rights and freedoms of the complainant, as a subject, and c) if was the complainant informed as a subject of the above processing according to articles 13 and 14 GDPR, and, in case of a negative answer, with what justification. The complainant, in her response from … (with Authority no. C/EIS/2881/28-04-2021) stated first of all that the complainant, who happens to be a client of the Bank, submitted on … the no. lawsuit against the employee of the Bank for ... years, B for misappropriating the amount of €... from the complainant's safe deposit box, while in addition on he claimed that he had suffered because of the aforesaid embezzlement. Specifically, according to the complained-about Bank, the complainant, who has entered into a safe-deposit box rental contract with the Bank, claimed that on ... he handed over the key to his safe-deposit box to Mr. B, then Manager of the branch [area] Y, in order for the latter to go to the complainant's mailbox to withdraw an amount of €... and give it to him. On .., when the complainant visited his safe, he claimed on the one hand that an amount worth … € was missing from it and on the other hand that this amount had been embezzled by Mr. B, who for his part denies having received the key to the safe of the complainant. Subsequently, as reported by the complained Bank, during a visit of the complainant to his safe deposit box on …, the allegedly embezzled amount of € … was found by the complainant inside it, who then presented it to the cashier for deposit into his bank account, where it was counted several times by the employees of the store, a fact that was confirmed in writing by them, who drew up the Operational Risk Event Announcement from ... This is the document that the complainant claims was granted to Mr. B in violation of personal data protection legislation. With regard to the use of the document in question, the complainant in her document from ... argued that Mr. B was the Manager of the branch [region] Y and represented the Bank, so that the legal interest of the Bank and himself were identical, at least in this particular case, since any acceptance of the complainant's claims by the competent Courts would have direct adverse effects for the Bank as well. For this reason, after Mr. B's request to the (then) Management of Branches X, it was granted the Notification of an Operational Risk Event from ..., in order to protect its legal interests and that of the Bank pursuant to article 6 paragraph 1 f. of the GDPR, which in this case, according to the complainant, consist in the exercise the right to judicial protection (refutation of the complainant's allegations of misappropriation of his money). As the complainant claims, this document was submitted in the context of the criminal proceedings and specifically to refute the complaint filed by ... (criminal file with A.V.M. ...) against Mr. B and other executives of the Bank, with related issues in

question (initial hearing ..., at which point it was postponed), and the complainant's lawsuit against the Bank and against Mr. B from ... in weighing its primacy over the rights and freedoms of the complainant, it took into account Article 5 para. 1 c (principle of proportionality), as well as Article 21 para. 1 of the GDPR, according to which, if the subject data subject objects to the processing of his personal data, the controller no longer processes the personal data, unless the processing is carried out, inter alia, to establish, exercise or support legal claims of the controller. In her opinion, Mr. B, as an employee of the Bank, is not a "third party" in relation to the Bank as a data controller, but a body of it, as follows from the definition of the concept of a third party in accordance with Article 4 (10) GDPR. In particular, the Bank claimed that "Mr. B, as the Manager of the Bank's branch in [area] Y from ... to ..., by order, on behalf of the Bank's legal entity and under its direct supervision, processed personal data of of its customers, including the complainant, in which case he already knew, even before the Operational Risk Notice was issued to him by ..., the details of the account held by the complainant at the store in question and in general all aspects of his contractual and transactional relationship with it and therefore, he is not considered a third party for the Bank". Therefore, according to the complainant, in the case of the processing in question (transmission of the document to Mr. B) it is "circulation of an internal document of the Bank between services directly involved with its content, i.e., the Bank's executives who investigate operational risk events and of the Manager of the store in which, according to the complainant's claims, the event under investigation took place". Based on the above allegations, the complainant argued that the granting of the document in question to Mr. B was carried out legally, in order to defend the legal interests of herself and her above-mentioned executive, which are undoubtedly superior to the freedoms and rights of the complainant , in accordance with Union and national law. Furthermore, the complained-about Bank, with its response document, argues that, even if Mr. B were considered a third party, his legal interest in receiving the Operational Risk Declaration document from ... for the purposes of judicial protection, prevails over the rights of the complainant according to above analysis, since this supremacy occurs, according to relevant decisions of the Authority, "in particular, when the provision of personal data is necessary for the recognition, exercise or defense of a right before a court", while pointing out that the document of the Operational Risk Announcement, even though it contains personal data of the complainant, it has the character of "purely an internal document of the Bank, as it records facts and events concerning the Bank and its operation, therefore it is not disclosed to third parties". Further, with respect to the complainant's allegation that the Bank did not comply with his corresponding request for a document, which he believes he had a legitimate interest in obtaining, to prove his allegations in the lawsuit he has filed against Mr. B, the complainant states

that the document that the complainant requested from the Bank on ... (a document from which it appears that Mr. B assigned the responsibility of supervising safe deposit boxes to the employee of the branch [area] Mr. D on ...) is an "internal document, as it captures internal procedures of the bank" and as such was not granted to the complainant, while the client did not have a legal interest in its granting either, as this relates to events subsequent to the embezzlement that the complainant claimed took place on ..., and therefore this would be of no use for the defense of his legal claims. It is noted that the complained Bank did not respond to the Authority's question regarding informing the complainant in accordance with Articles 13 and 14 GDPR and did not take a position as to whether, in its opinion, it had such an obligation. Upon the relevant request of the complainant, the Authority granted him a copy of the document with the views of the complainant (G/EX/1244/18-05-
2021 transferable). Subsequently, the complainant, under no. prot. C/EIS/3269/19- 05-2021 his document, the complainant asserted the following to the Authority: a) That on his action from ... with filing number ... before the Multi-Member Court of First Instance [region] F, against the complained Bank and B, for the award of compensation due to the embezzlement of the amount of ... euros, the final decision of the aforementioned Court was issued with the number ..., which the complainant submits to the Authority, and which partially accepted his action, awarding to the complainant compensation in the amount of ... euros and monetary satisfaction due to moral damage in the amount of ... euros. b) That the history of his dispute with the complained-about Bank, as proved also in the context of his above lawsuit, differs from that set forth in the Operational Risk Announcement, thus disputing the facts described in the disputed document. c) That the complained-about Bank itself confirms that its interests are identical with those of Mr. B, even though the latter was not the Manager of Branch [area] Y as of ... but was working in another branch of the Bank, with the consequence that he was not he is only in his capacity - as the Bank maintains - in a position to know the existence of the document in question, which was drawn up on ..., i.e. after .. years, during which no bond or relationship of dependence connected him with the Branch of [region] Y. Thus, it is not clear how he was informed of the existence of the document in question, so that he could request its issuance with his request from ... to the then Department of Branches X. d) That with its above assertion, the Bank essentially asserts that the Manager of any of its stores, and/or any employee who has served for a period of time as a Deputy Manager in a particular store, is able to know at any time, even after the end of his duties at that particular store, customer account information of the store in question and all aspects of the customer's transactional relations with it, the amounts he deposits and the announcements of operational risk that may take place in the store. e) That the Bank's claim that, even if Mr. B is considered a third party, he had a superior legal

interest in being granted the document in question, contradicts its other claim that it is an internal document that is not shared with third parties, but and with the answer that the complainant gave to the complainant himself: Specifically, with his (note: he probably means ...) application, the complainant asked to be granted a copy of a document from which it emerged that Mr. B (at the time who was the Manager of the [area] Y Store), assigned the responsibility of supervising the safes to Mrs. D on …, from which, according to the complainant, it is clear which employee was responsible for supervising the safes and therefore had a legitimate interest to know of this, for the purpose of establishing, exercising and supporting the summons against Mr. B for the crime of criminal embezzlement due to his capacity as an agent (for which the latter was in fact referred before the Three-member Court of Criminal Appeals Ψ). The complainant refused to grant this document to the complainant, on the grounds that "the documents which reflect the Bank's internal procedures cannot be granted to any third party". Despite this, one year later the Bank granted his opponent the Notice of Operational Risk Event, although according to it it is an "internal document that is not granted to third parties". f) Finally, that the complainant should have informed him before the document in question was transmitted to his opponent, Mr. B, just as she should have informed him before the judicial use of the document in question even by the Bank itself, as against him, in accordance with article 13 par.3 GDPR (information before the further processing of personal data for a purpose other than that for which they were collected), also citing the Authority's decision 16/2019, and claiming that this purpose of processing is other than the original purpose of the collection. Thus, the complainant comes to the conclusion that the Bank illegally forwarded to his opponent the from ... Notice of an Operational Risk Event, which includes his personal data (i.e. data on his cash balances, the money he had in his safe deposit box, the money he extracted from his safe deposit box, the money he deposited in cash, which were large sums of money), with the result that the interest of the complainant, as the subject of the personal data contained in the document in question, should not be granted to third parties, since he did not provide his consent, he was not informed before the transmission nor was the said document communicated to him, to even be informed of its existence, while he became aware of the document in the context of his opponent's lawsuit. Given the above, the Authority, with no. prot. C/EXE/456/16-02-2022 and C/EXE/455/16-02-2022 calls invited those involved to a hearing before the Department of the Authority via video conference on 02-03-2022, in order to present their views them on the case. During the meeting of 02-03-2022, the complainant and his attorney, Christos Demeroukas (A.M. ...) and on behalf of the complained Bank, lawyers Ioannis Mourgelas with AM ..., Konstantina Spourli with AM ... and the F, Data Protection Officer of the Bank. During the hearing, the parties developed their

views, received a deadline and filed within the deadline, while the complainant no. prot. G/EIS/4594/17-03-2022 memorandum, and the complained against no. prot. G/EIS/4741/18-03-2022 memorandum. The complainant, both during the hearing and with his memorandum, argued that the Bank illegally did not inform him before granting the document to his opponent Mr. B and that the from ... relevant general request of his opponent to the Bank ("Please grant copies of notices of operational risk, event book and video material which concern Mr. A and which are directly or indirectly related to the case in which the above involves me with the non-existent charge...") is made after the fact (after the submission of the complaint on his behalf), since it has not been recorded, which proves that Mr. B had received inside information about the existence of the document in question, while he had ceased to be the manager of store [area] Y, and that the document was granted to him without any request having been made. Furthermore, he points out that he does not know if the Bank has also provided other personal data to Mr. B, in response to the above request and that if this happened without his knowledge, this is another flagrant violation of his rights as a subject. In addition, the complainant questions whether it is common for a bank to record as an operational risk event the fact that a customer was "monologuing" about the contents of his deposit box, even mentioning specific amounts (according to the document in question, the complainant "monologued that someone put … euros in his mailbox and contacted his mobile phone for a few minutes saying that the money is … euros more"), as well as what is the risk that should be reported by the Bank in this case. The complainant emphasizes that the Bank repeatedly refuses to grant him documents that he has a legitimate interest in receiving and which do not include personal data "of this kind", such as the document from which the assignment of teller duties to Ms. D on ... (according to with the latter's affidavit) and which the Bank considers "an internal document, which reflects its internal procedures and cannot be granted to any third party". According to the complainant, this attitude of the Bank contradicts the granting of the disputed document to his opponent, because, in his view, Mr. B is just as much "any third party" for the Bank as the complainant himself . The complainant stated at the hearing that his action for damages against Mr. B was accepted at first instance and the appeal is pending, while he has also filed a petition for misappropriation which is also pending, and with his memorandum he recounts what happened at …. Finally, he emphasized that the Bank has not responded regarding the legal basis for the transmission of the document to his counterparty and, in the event that the processing was based on Article 6 para. 1 GDPR, what are the legal interests pursued in this case, so that to judge whether they prevail over his own. The complainant Bank during the hearing argued the following:

- That there are procedures according to which any event that constitutes an operational risk must be recorded in order to

avoid it in the future. In this context, the Bank was asked to submit with its memorandum the relevant Policy and operational risk management procedures, from which the concept of operational risk can be derived, the terms of the relevant records (such as, for example, if the movements are always recorded and activities of all customers in the stores) as well as the instructions given to the employees. - That the Branch Manager represents the Bank, therefore any accusation against the Bank or against its Manager is addressed to both of them and they are co-judicial, therefore they have a single legal interest, the defense of the rights of the Bank and its Manager. - That in this case, Mr. B requested that the Bank give him all the Operational Risk Notices that had been drawn up in the context of the case in question, of which there were dozens. According to the Bank, the legal basis for the transfer in question is the overriding legal interest of the controller (i.e. the Bank) in legal protection, but also of the Manager who is not a third party in this case in the sense of the definition of article 4 no. 10 GDPR, because it acts under the supervision of the Bank. In support of its claim, the Bank referred to decisions 149/2013 and 153/2013 of the Authority. - That what the complainant requested was the request of Mr. B (his opponent) to be granted all the Bank's documents related to the case, however the Bank refused after weighing the conflicting legal interests, because it considered that the complainant has already released his data in the context of the trial. Responding to the claim of the complainant, that the said "publication" had taken place in the context of Mr. B's personal action against him for defamation, the Bank argued that it is the same, single case, which consists of several different documents. - In response to the Reporter's question regarding the reason why the complainant was not informed about the drafting of the Operational Risk Event Announcement, the Bank's representative stated that the recording of incidents aimed at improving the Bank's procedures does not constitute the collection of personal data, while the complainant was present on … when the document was drawn up, therefore the Bank was not obliged to inform him. For this reason, the Bank was requested with its memorandum to provide the general Information of the Bank's customers on the processing of their data, as subjects according to article 13 GDPR. - In response to the Reporter's question regarding the reason why the complainant was not informed of the transmission of the above Notice to his counterparty, so that he may have the possibility to object to it in accordance with Article 21 of the GDPR, the Bank replied that it did not there is a right to object in the event that the legal basis is the overriding legal interests related to the support of legal claims. In this context, the Bank was asked to submit with its memorandum the Policy on access to personal data by subjects and third parties. - In addition, the Bank was requested with its memorandum to clarify what is the exact purpose and legal basis of the processing of personal data in the context of the recording of

operational risk events, as well as whether the transmission that took place falls under the same purpose or is a further purpose of processing, a copy of the Bank's record of processing activities pursuant to Article 30 GDPR, and a copy of Mr. B's application for the granting of documents or the document produced in court and the Bank's response showing what was ultimately granted. With its G/EIS/4741/18-03-2022 memorandum, the Bank first emphasized that the facts of the case have not yet been finally decided and do not concern the procedure before the Authority. As for tracking Operational Risk Events, the Bank argued that, according to the Bank of Greece, supervisory authority of credit institutions and member of the system of central banks of the euro area member states (Eurosystem), the monitoring of operational risk events is a basic principle of the organizational structure of banks and consequently an important criterion for their evaluation. In particular, the internal control system of each bank must include checks of: the consistency of the application of procedures, the quantitative and qualitative effects of violations of security rules, and the existence of immediate review mechanisms of procedures to deal with the identified weaknesses.1 In other words, the handling of the operational risks arising from the non-consistent application of the procedures, the failure to study the effects of security breaches and the absence of procedures adjustment mechanisms must be controlled, in order to prevent the recurrence of the same risks in the future. According to the Bank of Greece, every credit institution must have a political and independent, specialized management function "for all forms of risks, including operational" and procedures for systematic recording of relevant events that create operational risk and for informing the competent service units, as well as independent operational risk management unit and an adequate system for the assessment and management of these risks. The Bank stated that in response to its above regulatory obligations it has set up a specialized Market Risk and Operational Risk Department and has drawn up a specific Operational Risk Management Policy (an excerpt of which it submits as relevant 2) and a Manual of Procedures for the Management of Operational Risk Events (which it submits as relevant 3). In said Related 3 is included the definition of the concept and indicative examples of the Operational Risk Events that must be announced in accordance with the 1 Act of the Governor of the Ministry of Finance 2577/9.3.2006, for the framework of operating principles and evaluation criteria of the organization and the internal control systems of of credit and financial institutions, Chapter II par. 2.8 (Government Gazette A'59/20.3.2006), available on the website of the Bank of Greece: https://www.bankofgreece.gr/RelatedDocuments/ΠΔ.ΤΕ_2577-9.3.2006_Framework_of_operating_principles_and_criteria_of_evaluation_of_SEE.pdf Policy the bank's. In particular, an Operational Risk Event is defined as "the result, whether voluntary or involuntary, internal or external, of the manifestation of

operational risk, i.e. the risk of economic or quality impacts due to the inadequacy or failure of internal processes and information systems, the human factor, voluntarily or involuntarily, as well as the advent of external events". Some indicative operational risk events are: Supervisory and regulatory fines, third-party lawsuits against the bank, external or internal fraud cases (e.g. embezzlement of amounts from customer accounts), cyber security incidents, management and execution errors transactions, incidents of personal data breach, theft and vandalism of fixed assets, shop burglaries, etc. In the Operational Risk Management Policy (related 2) it is stated that "Lawsuits against the Bank and Group Companies are a specific sub-case of operational risk events with special characteristics, for the which are subject to additional requirements…" (p. 11 under iv), and that "Operational risk events are monitored at all stages, from their initial recognition to their accounting". Parenthetically, it should be pointed out that the Bank did not explain how the facts described in the disputed by ... Announcement and in particular those that the complainant "monologued" and the content of his mobile phone conversation with a third party fall under the concept of "operational risk event" according to with the above. In addition, the Bank provided the relevant extract of its Processing Activities File pursuant to Article 30 of the GDPR in relation to the processing carried out for the purpose of the Management of Operational Risk Event Notifications and the entry of data into the operational risk event database (Related 10). In this file, among other things, the "financial and transactional profile and the "evidence of legal disputes and complaints" are mentioned as data subjects and customers, as data categories, as processing operations the collection, registration, storage and use of the data and as a legal basis the "legal obligation of the Processor" (without reference to a specific provision from which the obligation derives). With its memorandum, the Bank invokes as a legal basis for drawing up such Announcements, not only its legal obligation to manage and deal with operational risks, but also its legal interest to improve its procedures, even though the latter legal basis is not mentioned in the activity record. It is also noted that the Bank does not cite specific evidence for the weighting from which it (should) result that its legitimate interest in improving its procedures is superior to the fundamental rights and freedoms of the affected data subjects, as they are affected from said processing. Furthermore, with its memorandum, the Bank also provided the Article 13 GDPR Information to the subjects regarding the processing of their personal data by the Bank as Processor (Related 11). As he argued, the subjects are sufficiently informed about the processing that takes place in the context of the management of operational risk events because in Chapter III of the information it is stated that "the Bank may also process the necessary cases from the aforementioned data: - for their compliance with obligations deriving from the respective legislative regulatory and supervisory framework, as applicable from

time to time and the decisions of the authorities or courts, - for the exercise of its rights and the defense of its legitimate interests". From this, according to the Bank, it follows that the processing of this specific case "is fully covered by the notification, since the announcement of an operational risk event was drawn up within the framework of the Bank's regulatory obligation and was made available to its Director - and not to a third party - in the same context, since he was the Manager of the Branch in which the reported event took place, but also for the defense of the common legal interests of the Bank and the Manager", while in Chapter V it is stated that the recipients of the data include "the relevant employees of the Bank" (under a), "lawyers" (under b) and "judicial, prosecutorial and other authorities" (under g). Therefore, the Bank claimed that its customers, including the complainant, are informed "completely and accurately" about any processing of their personal data, including this particular one. In relation to the transmission of the document to Mr. B, the Bank argued that the said opponent of the complainant "was not a third party" in relation to the Bank, because during the long period of time during which this particular case unfolded, they were drawn up and sent to within the Bank's competent departments, several announcements of operational risk events and by him, as head of the competent Unit (of Branch [area] Y), while "the fact that he was at some point transferred to another branch does not cut him off from the ongoing case , as the relevant trials continue", in which the complainant has been made a joint litigant (of the Bank). Mr. B's request to receive copies of the notices of operational risk events related to the specific case, which include the Notice in question (...), according to the Bank, was based on the legal basis of Article 6, paragraph 1 f), GDPR i.e. the legitimate interest of the Bank as data controller and its "Branch Manager", which consists in their judicial protection (according to Article 20 of the Constitution) but also in the right to personality and the protection of the honor and reputation of the individual (article 5 par. 1 and 2 of the Constitution). The Bank argued that the GDPR "recognizes this as a superior right when the second paragraph of Article 21 par. 1 stipulates that the right to object is not opposed when the processing concerns the establishment, exercise or support of legal claims", and "therefore the legitimate interest in judicial protection is self-evidently superior to any other right". Thus, it comes to the conclusion that, on the one hand, the grant to Mr. B is not a grant to a third party, and on the other hand, it is not based on the legal interest of both, which in this case consists of the right to judicial protection. Regarding informing the complainant about the transmission in question, according to the Bank, "there was no question of informing him, according to the Regulation", since "the personal data of Mr. A included in this document had already been made public by himself to the above persons", therefore, according to the Bank, the complainant already had the relevant information within the meaning of articles 13 par. 4 and 14 par. 5 a)

GDPR. It is noted that the Bank did not provide the Policy on access to personal data from subjects and third parties requested in the context of the hearing. CONSIDERED ACCORDING TO 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 (Official Gazette A´ 137) it follows that the Authority has the authority to supervise the implementation of the provisions of the GDPR, this law and other regulations that concern 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 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. In particular, paragraph 1 states that: "Personal data: a) are processed lawfully and legitimately in a transparent manner in relation to the data subject ("legality, objectivity and transparency"), b) are collected for specified, explicit and legitimate purposes and are not further processed in a manner incompatible with those purposes; further processing for archiving purposes in the public interest or for the purposes of scientific or historical research or statistical purposes is not considered incompatible with the original purposes in accordance with Article 89(1) ("purpose limitation"), [...]'. According to the principle of accountability introduced by the second paragraph of the aforementioned article, the controller "bears the responsibility and is able to demonstrate compliance with paragraph 1 ("accountability")". This principle, which is a cornerstone of the GDPR, entails the obligation of the data controller to be able to prove his compliance to the supervisory authority. According to established Jurisprudence of the Authority2, the existence of a legal basis (art. 6 GDPR) does not exempt the responsible 2 See indicative Decision 26/2019 APD, sc. 5. processing from the obligation to observe the principles (art. 5 par. 1 GDPR) regarding the legitimate character, necessity and proportionality as well as the principle of minimization. In the event that any of the principles provided for in article 5 paragraph 1 of the GDPR is violated, the processing in question is considered illegal (subject to the provisions of the GDPR) and the examination of the conditions for applying the legal bases of article 6 of the GDPR is omitted. Thus, the illegal collection and processing of personal data in violation of Article 5 GDPR is not cured by the existence of a legitimate purpose and legal basis. 3. Further, according to the definitions provided by Article 4 of the GDPR: personal data means "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one whose identity can be ascertained, directly or indirectly, in particular by reference to an

identifier such as a name, an identity number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, financial, cultural or social identity of the natural person in question" (item 1). processing means "any operation or series of operations carried out with or without the use of automated means, on personal data or sets of personal data, such as collection, registration, organization, structuring, storage, adaptation or alteration, retrieval, retrieval of information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, restriction, deletion or destruction" (item 2) as a recipient is defined as "the natural or legal person, the public authority, agency or other body, to which the personal data is disclosed, whether it is a third party or not [...]" (paragraph 9) and a third party is defined as "any natural or legal person, public authority, agency or body, with the exception of the data subject, the controller, the processor and the persons who, under the direct supervision of the controller or the processor, are authorized to process the personal data" (item 10). 4. According to article 6 par. 1 sec. in the GDPR "1. The processing is lawful only if and as long as at least one of the following conditions applies: […] f) the processing is necessary for the purposes of the legal interests pursued by the controller or a third party, unless the interest or the fundamental rights and freedoms of the data subject which require the protection of personal data, in particular if the data subject is a child". Paragraph 1 of Article 21 of the GDPR on the right to object provides that: "The data subject has the right to object, at any time and for reasons related to his particular situation, to the processing of personal data concerning him, which is based on Article 6(1)(e) or (f), including profiling under those provisions. The controller no longer processes the personal data, unless the controller demonstrates compelling and legitimate reasons for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or support of legal claims claims". In addition, paragraph 4 of the same article states that "when the processing for a purpose other than that for which the personal data have been collected is not based on the consent of the data subject or on the law of the Union or the law of a Member State which is necessary and proportionate measure in a democratic society to ensure the purposes referred to in Article 23 paragraph 1, the controller, in order to ascertain whether the processing for another purpose is compatible with the purpose for which the personal data are initially collected, takes taking into account, among others: a) any relationship between the purposes for which the data of the intended further personal character have been collected and the purposes of processing, b) the context in which the personal data were collected, in particular with regard to the relationship between the subjects of the data and the controller, c) the nature of the personal data, in particular for the special categories of personal data processed, in accordance with Article 9, or whether personal data

related to criminal convictions and offenses are subject to processing, in accordance with article 10, d) the possible consequences of the intended further processing for the data subjects, e) the existence of appropriate guarantees, which may include encryption or pseudonymization". Furthermore, according to Recitals 47 and 50 of the GDPR “The legitimate interests of the controller, including those of a controller to whom the personal data may be disclosed or of third parties, may provide the legal basis for the processing, provided that they do not override the interests or fundamental rights and freedoms of the data subject, taking into account the legitimate expectations of the data subjects based on their relationship with the controller. Such a legitimate interest could for example exist where there is a relevant and appropriate relationship between the data subject and the controller, such as if the data subject is a client of the controller or is in its service. In any case, the existence of a legitimate interest would need a careful assessment, including whether the data subject, at the time and in the context of the collection of the personal data, can reasonably expect that for this purpose it can be carried out processing. In particular, the interests and fundamental rights of the data subject could prevail over the interests of the controller, when personal data are processed in cases where the data subject does not reasonably expect further processing of his data" (App. . 47) and "The processing of personal data for purposes other than those for which the personal data were originally collected should only be allowed if the processing is compatible with the purposes for which the personal data were originally collected. In this case, a legal basis separate from that which allowed the collection of the personal data is not required. […] In order to ascertain whether the purpose of the further processing is compatible with the purpose of the initial collection of the personal data, the controller, if it meets all the requirements for the lawfulness of the initial processing, should take into account, among others: any links between of these purposes and purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of the data subject based on his relationship with the controller regarding their further use; the nature of the personal data; the consequences of the intended further processing for the data subjects; and the existence of appropriate guarantees both for the initial and intended acts of further processing" (Ref. 50). 5. Regarding compliance with the principle of transparency, Articles 13 and 14 GDPR specifically define the information to be provided to the data subject by the data controller, both in the event that the data is collected from the data subject (Article 13) and in the event that the data has not been collected from the subject (Article 14). Mandatory information includes at least "a) the identity and contact details of the controller and, where applicable, his representative, b) the contact details of the data protection officer, where applicable, c) the purposes of the processing for which they are intended the personal data, as well as

the legal basis for the processing, d) the relevant categories of personal data, e) the recipients or categories of recipients of the personal data, f) as the case may be, that the controller intends to transmit personal data character to a recipient in a third country or international organization and related information, g) the period for which the data will be stored, or, if this is impossible, the criteria that determine said period, h) information about the rights of the subject in accordance with articles 15-22 GDPR", while, according to article 13 par. 3 GDPR, "When the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject, before such further processing, with information for this purpose and any other necessary information, as referred to in paragraph 2". And according to the Article 29 Working Party's Transparency Guidelines under Regulation 2016/679 (WP260), Article 13 of the GDPR applies if personal data is collected "[…] from a data subject through observation (e.g. using data recording devices or data recording software such as cameras [...]" (§ 26). In order to ensure the principle of transparency of processing, Article 12 para. 1 GDPR states that: "The controller takes appropriate measures to provide the data subject with any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and Article 34 regarding the processing in a concise, transparent, comprehensible and easily accessible form, using clear and simple wording, in particular when it concerns information specifically addressed to children. The information is provided in writing or by other means, including, where appropriate, electronically. When requested by the data subject, the information may be given orally, provided that the identity of the data subject is proven by other means". The information, according to the same article, is provided during the collection of the data. Furthermore, according to the aforementioned Transparency Guidelines (WP260 rev.01), when informing subjects in accordance with Articles 13-14 GDPR, the information provided should be specific and definitive: "The use of linguistic designations such as "may", "certain", "often" and "likely" should also be avoided. Where data controllers choose to use vague wording, they should be able, in accordance with the principle of accountability, to demonstrate why the use of such wording could not be avoided and why it does not undermine the lawfulness of the processing." (§ 13). Finally, it is noted that in paragraph 5 of Article 14 of the GDPR there are exceptions to the obligation to inform the subject, including in cases where "...b) the provision of such information proves to be impossible or would entail a disproportionate effort [...] or if the obligation referred to in paragraph 1 of this article is likely to make it impossible or to greatly damage the achievement of the purposes of said processing. In these cases, the data controller shall take appropriate measures to protect the rights and freedoms and legitimate interests of the data subject [...]'. There is no corresponding provision for the obligation to inform based on article 13,

while the only exception to the relevant obligation of the data controller exists "when and if the data subject already has the information" (article 13 par. 4 GDPR). As pointed out in the OE 29 Guidelines on transparency (WP 260 §56): “According to the principle of accountability, data controllers must demonstrate (and record) the information already held by the data subject, how and when you received it, and that no changes have occurred since then to that information that would make it out of date. In addition, the use of the wording "provided" in Article 13(4) makes it clear that, even if the data subject has been provided with certain categories of information under Article 13 in the past, the data controller still has the obligation to provides this information in order to ensure that the data subject now has the full set of information listed in Article 13(1) and (2)'. 6. Finally, with the provision of article 21 paragraph 1 GDPR it is defined that: "1. The data subject has the right to object, at any time and for reasons related to his particular situation, to the processing of personal data concerning him, which is based on Article 6 paragraph 1 letter e) or f), including profiling under the provisions in question. The controller no longer processes the personal data, unless the controller demonstrates compelling and legitimate reasons for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or support of legal claims claims". 7. In accordance with Act Governor TtE 2577/9.3.2006, on the framework of operating principles and evaluation criteria of the organization and internal control systems of credit and financial institutions (Government Gazette A'59/20.3.2006, Ch. II par. 17)3: "For the planning, development and monitoring of the risk policy, each credit institution has a specialized and independent risk management function, which covers the whole range of activities for all forms of risks, including operational". In Appendix 5 of the Act of the Governor of the Ministry of Finance 2595/20.08.2007 on the Specification of Risk Management Principles and Criteria by Risk Category (Government Gazette B' 1748/31.08.2007)4 the following provisions are provided: "7. OPERATIONAL RISK 7.1. Policies and procedures are in place to assess and manage operational risk, including that arising from low-frequency, high-impact events. 7.2. Without prejudice to the definition referred to PD/TE 2590/20.8.2007, credit institutions clearly articulate what constitutes operational risk for the purposes of these policies and procedures. [...]". Finally, from the Act of the Governor of the Ministry of Finance 2590/20.8.2007 on the Minimum Capital Requirements of Credit Institutions for Operational Risk (Government Gazette B' 1747/31.8.2007, Chapter B, par. 5 a) and chapter C. par. 1 a) and b)5 provides that credit institutions must have procedures for systematic recording of the relevant events that create operational risk and for informing the competent 3 https://www.bankofgreece.gr/RelatedDocuments ΠD.TE_2577-9.3.2006_Framework_of_operating_principles_and_criteria_of_evaluation_of_SEE.pdf 4. gr/RelatedDocuments/ TE.TE_2590-

20.8.2007_Minimum_Capital_Requirements_of_Credit_Institutions_for_Operational_Risk.pdf service units, as well as an independent operational risk management unit and an adequate system for the assessment and management of these risks. The Act in question refers to article 2 par. 12 of Law 3601/2007 which defined Operational Risk as "the risk of damage occurring due either to the inadequacy or failure of internal processes, natural persons and systems or to external events, which includes and the legal risk". Law 3601/2007 has been repealed by the newer Law 4261/2014, which in article 3 no. 48 includes the following definition: "48) "operational risk": operational risk, as defined in point 52 of par. 1 of article 4 of Regulation (EU) No. 575/2013", where operational risk is defined in the same way : "operational risk" means the risk of losses due to the inadequacy or failure of internal processes, people and systems or to external events and includes legal risk. 8. In the case under consideration, the following emerged from the information in the file: The complainant maintains a safe deposit box at the store of the complained Bank in [region] Y since …. The manager of the store in question was from … to … Mr. B. On the day he opened the safe deposit box in question, the complainant states that he withdrew an amount of € … from the bank account he maintains at the same Bank and deposited this amount in his mailbox. Subsequently, on … he cashed a check for the amount of € … at the same shop and also placed the money in his safety deposit box, which thus contained a total of € …. According to the complainant, after the imposition of the restrictions on cash withdrawals (capital controls) on ..., on ..., he himself handed over the key to his safe deposit box to the Manager of the store Y of the complainant, Mrs. B, because as she had informed him, she was expecting a remittance and he would turn off the store's cameras for a while, in order to take this opportunity to take … € from the complainant's safe and hand it over to him, as the complainant needed cash to cover medical expenses …, which happened on the same day, as claims the complainant, therefore there should be … € left in his box. Subsequently, after the restrictions were lifted and when access to the lockers was allowed, the complainant visited his locker on …, at which time he found that there were only … €, i.e. missing … bundles of …€ totaling … €. Following this, on ... the complainant filed a petition for embezzlement against Mr. B. At the same time, based on the above facts, the complainant filed on ... a lawsuit against the complained Bank and against Mr. B, for compensation and restoration of his moral damage due to tort. On the said action, the under no. ... final decision of the Multi-Member Court of First Instance [region] F, which partially accepted the lawsuit at first instance and awarded the complainant compensation in the amount of ... and amount ... as monetary satisfaction for his moral damage (...) while other lawsuits followed against the witnesses of the accused for perjury and slanderous defamation. Furthermore, on ... the complainant states that he visited his box again at the

store of the complainant in [area] Y and immediately afterwards he went to the cashier and deposited an amount of ...€ euros into his account, and in particular: ... bundle (...€) of ... € and … wads (...€) of …€, which he claims he took from his locker, as well as another wad (…€) held with a simple rubber band, which he claims he took out of his pocket. It follows that the Operational Risk Incident Announcement was drawn up by the managers of the Alpha Bank Branch [area] Y, Mr. C and D, according to which the complainant allegedly stated that he "found again" in his safe deposit box the lost amount of ... €. In particular, the document in question contains, among other things, the following: "... The customer was monologuing that someone put ... euros in his safe deposit box and called on his mobile phone for a few minutes telling his interlocutor that the money is ... euros more. He informed the Manager and the cashier that in his locker last time (about ... years ago) he had a total of ... euros and the reason for visiting it was to leave in the locker ... euros and deposit the remaining ... euros in his account, he expressed surprise from the event and requested .. pm to finalize the deposit of … euros to his account … as well as a copy of the transaction with the detailed analysis of the money. The Store, after the departure of the customer (.. am) made an agreement and a detailed counting of the cash where upon completion, .. am there was no difference". The complainant disputes the events as recorded in the document in question and claims that in his locker he found only …€ (as he had left it during his previous visit on …), from which he received the amount of …€ (in … bundle of € … caught with Bank of Greece tape and … bundles of € …, caught with Alpha Bank tapes), while the second bundle of € … that he showed at the till was caught with a simple rubber band and he already had it in his pocket when he entered in the store, he never declared to the cashier, as he states, that he "found" this amount again in his safe. The above from ... document of the Announcement of an Operational Risk Event was granted by the complained Bank to Mr. B after the latter's request from ... to the (then) Department of Branches X... (according to the response under prot. no. C/EIS/ 2881/28-04-2021 of the Bank) and was used as an evidentiary document in the context of the aforementioned lawsuit of the complainant. With the present complaint, the complainant complains about the fact that the document in question, which includes his personal data, was forwarded, without his prior information and consent, to his opponent, Mr. B, who already from the end of year ... he was not working as a Manager of Branch [region] Y and was therefore a third party in relation to the Bank. 9. It should first be pointed out that the disputed document includes in any case personal data of the complainant, regardless of the fact that the complainant disputes the facts recorded in it, since it contains information that "concerns" him as a subject . And according to Opinion 4/2007 of OE 29 regarding the meaning of the term "personal data", the information does not need to be true or proven to be classified as

personal data: "Indeed, the data protection rules provide already that some information may be incorrect and give the data subject the right to have access to that information and challenge it through appropriate means of legal protection". These personal data of the complainant were collected by the Bank, as the controller, through observation by the subject and were processed for the drafting of the contested Operational Risk Event Announcement document, which has been included in the Bank's filing system. Therefore the relevant processing falls within the scope of the GDPR (Article 2 para. 1 GDPR). With reference to the processing in question (recording of the behavior of the complainant at Branch [area] Y of the complained Bank on ...), the opponent of the complainant Mr. B is a third party, because his status as Manager of the Branch in question had ceased from ... , while the Bank did not claim that his duties in the year ... were related in any way to the processing in question. 10. With reference to the legality of the initial processing, i.e. the collection and recording of information concerning the complainant and the drafting of the Operational Risk Event Announcement by the Bank's employees, the following is noted: As emerged from the file's information, purposes of said processing in general (compilation and keeping of Notices of Operational Risk Events) is the management of operational risks and the improvement of the Bank's procedures. As legal bases for the relevant acts of personal data processing, the Bank invokes, on the one hand, its compliance as a data controller with its legal obligation to manage operational risks (Article 6 para. 1 c GDPR in conjunction with the provisions referred to in Sec. 6 Acts of the Governor of TtE) (for the first purpose of processing), on the other hand its legitimate interest to improve its procedures (Article 6 par. 1 GDPR) (for the second purpose of processing). However, this second legal basis is not mentioned in the Bank's record of processing activities pursuant to Article 30 of the GDPR, nor was it documented based on the principle of accountability before the Authority, the weighting on the basis of which the controller found that this legal interest outweighs the rights and freedoms of subjects. In this case, even if it is considered that the expression of the complainant "someone put ... euros in my mailbox" falls under the concept of "operational risk event", the recording of his behavior as it took place with the document in question (that, i.e. " he was monologuing' and 'talking on his mobile phone' referring to her specific information) does not appear to fall under the necessary data processing provided by the Bank's Policies and Procedures for the purposes of managing Operational Risk Events. Furthermore, since this recording is a collection of personal data from the subject (collection through observation according to WP 260 § 26 , see above s. 3), the observance of the principle of transparency on the part of the Bank, as data controller, presupposes the prior information of the subject according to article 13 GDPR. From the overview of the subject information text provided by the Bank, it appears that the recording of operational

risk events as an act of collecting and processing personal data is not referred to with "clarity and completeness", as the Bank unfoundedly claims, nor can it be considered that the relevant information is covered by the general phrase "the Bank may also process the necessary case-by-case data from the aforementioned data: - for its compliance with obligations deriving from the respective legislative, regulatory and supervisory framework, as applicable from time to time and the decisions of the authorities or courts , - for the exercise of its rights and the defense of its legitimate interests". Therefore, it was impossible for the complainant to know, at the time he was monologuing or talking on his mobile phone inside the Store, that his behavior was being recorded: as he states in his complaint "I was not even aware of the creation of the said document". In addition, the Bank's argument that the complainant "already knew the information" so that his notification under Article 13 was unnecessary, because he was present and "published his personal data himself", is also unfounded. The "monologue" and conversation on the phone does not constitute "disclosure of personal data", while in no case can it be considered unnecessary to inform the subject of the fact that his behavior is being recorded as well as of the other elements of the processing (purpose, legal basis, time of observance, etc.), for the sole reason that the subject is present when this behavior is manifested. Moreover, in this case the facts are disputed by the parties involved, so it is up to the controller under the principle of accountability to substantiate the claim that the complainant "already knew the information" he should have provided to him according to Article 13 GDPR. It is also noted that from the content of the Operational Risk Event Announcement from ... it is not clear what the risk is in this case or in which category the event falls according to the Bank's Manual, given that at the end it is expressly stated that no cash difference was found. Therefore, a violation of the principle of legality and transparency of the processing regarding the initial collection and registration of the complainant's data in the by ... Announcement of the Event of Operational Risk (articles 5 par. 1 a' and 13 GDPR) is established. (operational risk event management, improvement 11. Furthermore, regarding the transmission of the document in question to the complainant's counterparty, it is first noted that the Bank did not explain whether the purpose of the transmission was the same as the original purpose of collecting and maintaining the data of procedures and avoiding incidents of risk in the future) or a further purpose (as appears to be derived from the invoked legal basis, i.e. her superior legal interest in judicial protection), the legality of which would have to be judged in accordance with Article 6 para. 4 GDPR . After all, according to article 13 par. 3 GDPR, if the specific processing act (transmission of the document) served a purpose other than the purpose of the initial collection of the data, the Bank had to inform the complainant about this purpose as well as about the other information of article 13 par. 2 GDPR. The basic position of the Bank is that Mr.

B is not a third party, but an organ of the Bank, as a Processor. The Bank specifically asserted that "Mr. B, as the Manager of the Bank's branch in [area] Y from ... to ... and ..., by order, on behalf of the Bank's legal entity and under its direct supervision processed personal data of its customers, including the complainant, in which case it already knew, before the Operational Risk Notice was issued to him by ..., the details of the account held by the complainant at the store in question and in general all aspects of his contractual and transactional relationship with it and therefore is not considered as a third party for the Bank". For this reason, the Bank argued that it is not essentially a transfer of personal data, but rather a "circulation of an internal document of the Bank between services directly involved with its content, i.e., the Bank's executives who investigate operational risk events and its Director store in which, according to the complainant's claims, the event under investigation took place", which transaction was carried out "to defend the legal interests of herself and the aforementioned executive, which are undoubtedly superior to the freedoms and rights of the complainant". However, the complained-about Bank did not sufficiently document the weighting from which it follows that its legal interests are superior to the complainant's right not to have his behavior recorded - and even without his knowledge - as well as information, including those concerning the content of his mailbox, or not to share this recording with other persons. In relation to informing the complainant as a subject, the Bank argued that it is done through the general information text where it is stated that the recipients of the data are the "competent employees" of the Bank. However, even if the position were accepted that the employee in question, who was no longer the Manager of the Branch, is not a third party in relation to the Bank, in no case can it be considered that he was "competent" in this case to receive the specific document , as follows from the fact that he had to submit a relevant request to be notified and he did not become aware of this in the context of the performance of his duties. It should also be noted that in the Bank's activity file it is stated that "for official reasons, the Announcements are communicated when and if required to the supporting Departments of the Bank (indicative: Internal Audit, Human Resources, Branch Network, Legal Services)", and the Bank did not claim that the recipient of the document in this case falls into any of the above categories. In addition, the complained Bank claimed that, even if Mr. B is considered a third party to the Bank, his legitimate interest in receiving the Operational Risk Notification document from … for the purposes of his judicial protection prevails over the interests, fundamental rights and freedoms of the complainant , since its use was necessary for his defense as an accused, before a court. According to the Bank, in this case, the pre-transmission information "is not mandatory because the data was already known to the subject and had already been made public by him" and "even if information had to be provided, it would be practically irrelevant, since the

subject cannot object when the processing takes place in the context of judicial protection (article 21 par. 1 of the Regulation)". But from article 21 par. 1 b GDPR in no case does an exception arise from the observance of the principle of transparency and in particular from the obligation of the data controller to inform the data subject beforehand: even if the Bank found and demonstrated "imperative and legitimate grounds for the establishment, exercise or support of its legal claims', this would not relieve it of its basic obligation of transparency, arguing that transparency in this case is 'irrelevant'. Transparency is a fundamental principle of personal data protection and is necessary in every case of processing, except for the expressly provided exceptions of the GDPR, and the purpose of this principle cannot be considered to be limited to the possibility of exercising the right to object on behalf of the subject. If there were an exceptional case of exempting the controller from the obligation to inform, the relevant exception would be expressly provided for in the Regulation, as is the case for example in article 14 par. 5 b'. On the contrary, from the wording of article 21 par. 1 b' it follows that the subject has the opportunity to exercise his right to object, so that the Processor, if the conditions mentioned there are met, has the possibility to refuse to satisfy it. In other words, the exercise of the right is a temporal and logical condition of the documented refusal of the controller to satisfy it. Consequently, the Bank's additional claim that there is not even an obligation to inform in case the conditions of article 21 par. 1 b GDPR are met is unfounded. It is therefore established that, regardless of whether the said processing act (transmission of the document to Mr. B) was intended in this case, to implement the Guidelines of the Bank of Greece for the management of operational risks or to protect the legal interests of the Bank, the latter carried out acts of processing the data of the complainant without having previously informed him as a subject, both in terms of initial processing (recording of his behavior for the drafting of the Notice of Operational Risk Event) as well as regarding the transmission of this document to his counterpart, Mr. B, as a result of which the principle of transparency and by extension the principle of legality is violatedprocessing according to art. 5 par. 1 sec. 1 GDPR in conjunction with Article 13 GDPR. With
in this way, the complained Bank deprived the complainant of it
possibility to exercise his rights from Articles 15-22 GDPR, in particular the
right of objection according to art. 21 GDPR regarding the transmission of data as well
and the right to limit the processing according to art. 18 GDPR, citing
any inaccuracy in the processing of personal data,
in order to correct them by no. 16 GDPR.

12. Following the above, from the data in the file and following her
hearing, the Authority finds on behalf of the complainant
Bank violation of the principle of legality, objectivity and transparency
of the processing (article 5 par. 1 a' GDPR) due to the absence of a legal basis against
the above as well as the absence of informing the complainant according to
Article 13 GDPR for the data processing operations carried out. With
based on the above, the Authority considers that there is a case to exercise the following
article 58 par. 2 of the GDPR its corrective powers in relation to the established
violations and that it should, based on the circumstances established, to
be imposed, pursuant to the provision of article 58 par. 2 sec. i of the GDPR,
effective, proportionate and dissuasive administrative fine according to
article 83 of the GDPR, both to restore compliance, and for
punishment of illegal behavior. Furthermore, the Authority took into account the criteria
measurement of the fine defined in article 83 par. 2 of the GDPR, the
paragraph 5 sec. b' of the same article that applies to this case,
the Guidelines for the implementation and determination of administrative
of fines for the purposes of Regulation 2016/679 issued on 03-10-
2017 by the Article 29 Working Party (WP 253) and the Guidelines
lines 04/2022 of the European Data Protection Board for
calculation of administrative fines in the context of the General Regulation which
are in public consultation, as well as its actual data
case under consideration and in particular:
a) the fact that the complained Bank violated the provision of
the article 5 par. 1 sec. a' GDPR fundamental principle of legality, objectivity
and transparency of processing, a violation that falls under, according to the provision
of article 83 par. 5 sec. 1 GDPR, in its highest prescribed category

grading system of administrative fines.

b) The fact that the processing concerned by the infringement is related to the basic one

activity of the complained Bank.

c) The fact that a natural person was affected by the violation,

however, the identified vague and incomplete information of the subjects

regarding the processing of their personal data in its context

of the Bank's Operational Risk Management Policy is systemic

problem that potentially affects all of their customers or visitors

of its stores.

d) The fact that a mismatch was found between the purpose and the legal

basis invoked by the Bank for the alleged processing operations

(legal defense before a court - overriding legal interest) and at

purpose and the legal basis respectively recorded in Article 30 GDPR

record of the Bank's processing activities (Advertisement management

Operational Risk Events and data entry into the event database

operational risk - compliance with a legal obligation).

e) The fact that the complained Bank completely contradictingly, while

characterized the nature of the document at issue as “internal, not shared

to third parties', however, granted it for external use before a court and

contrary to the purpose of its creation. It is also noted that from the Bank

did not provide Policy of access to personal data, from subjects and

third parties, even though she was asked.

f) The fact that staff data was affected by the breach

simple character, but of a special personal nature, like her event

mailbox maintenance and the contents of the complainant's mailbox (which falls

to bank secrecy).

Based on the above, the Authority unanimously decides that it should be imposed on

denounced ALPHA BANK S.A. as controller, the mentioned

in the administrative sanction, which is judged to be proportional to the severity of the

violations.

FOR THOSE REASONS

THE BEGINNING

It imposes on ALFA BANK S.A. administrative fine of forty thousand

(€40,000) euros for the violation of the provisions of article 5 par. 1 a' and

13 GDPR processing of the complainant's personal data.

The president

George Batzalexis

The Secretary

Irini Papageorgopoulou