REPUBLIC OF CYPRUS OFFICE OF THE COMMISSIONER FOR PROTECTION OF PERSONAL DATA No. Fac.: 11.17.001.008.001 Tel: 22 818456 Fax: 22 304565 June 17, 2020 [SENT, BY HAND of the General Manager of Bank of Cyprus Public Company Ltd. .E. (Attn. P.O. 21238 1504 NICOSIA) I refer to the complaint submitted to my Office regarding the above matter and in continuation of the correspondence between us which ends with the letter of the External Legal Symbol of Bank of Cyprus Public Company Ltd , Chrysafinis & Polyviou D.E.P.E., dated 05.06.2020 and I inform you of the following: Cyprus Public Company Ltd (hereinafter "the Bank") and the insurance company Eftoliiv I_1a, who, as stated, requested as he has a copy of his insurance policy with number M-056482. Specifically, the complainant provided a copy of the correspondence he had with the Nicosia Regional Manager of the Bank of Cyprus, who, in a letter dated 23.09.2019, informed him that i: Iasonos 1, 2nd Floor, 1082 NICOSIA / P.O. 23378, 1682 NICOSIA-CYPRUS, Tel. +357 22818456, Fax+357 22304565 e-mail: sopiini55ioin@€i3i3rGthiosini.9on.sg, n/th^diiib: Hir^/nnnnnn.eIvivrGiosiioni.ronhg DECISION Exercise of right of access by Mr. G. 1. 1. On 01.21.2020, I received a complaint from Mr. is delayed and is objectively difficult and time-consuming, which is why the Bank is willing to cancel this limit insurance with your signed application.' 1.2. Based on the task of examining complaints provided to the Personal Data Protection Commissioner by article 57(1)(f) of Regulation (EU) 2016/679 (hereinafter "the Regulation") and article 24(b) of the Law which provides for the Protection of Natural Persons Against the Processing of Personal Data and for the Free Circulation of Such Data (Law 125(I)/2018), with the same letter from my Office, dated 02.03.2020, a letter was sent to the Data Protection Officer of the Bank and to the Data Protection Officer of Eutolith 1_ia, with which they were informed of the above complaint. In the same letter, I asked for their positions/opinions regarding the said allegations and additionally to inform me: (a) The safekeeping/storage areas of old/expired/cancelled contracts and (b) the technical and organizational measures for their safekeeping and protection. 1.3. In a letter from my Office dated 03.02.2020, I informed the complainant that I invited the Complainant Defendants to report their positions/opinions to me no later than February 23, 2020 and that he will be informed in writing of their response. 1.4. On 20.02.2020, the company Evtoliv Da sent a letter to my Office, in which it stated the following: The Bank is the owner of the group limit insurance contract and has the right to manage it. He is responsible for the inclusion and removal of members in the Perimeter Insurance contract as well as the signing, delivery and custody of the originals and copies of the contracts of the members of the Perimeter Insurance. The insurance company Evtoliv Oa has the obligation to pay the benefit it will receive based on the terms of the contract. Regarding the request of Mr. , no form is in the custody of the insurance company Evtoliv IM 1.5. With her reply letter

dated 20.02.2020, Dr. The Bank's Nicosia Regional Manager informed me that: Once a limit insurance contract is drawn up with a customer and assigned to the benefit of the Bank, it is kept in an archived safe deposit box at the relevant Bank branch. When the Bank closes a branch or the storage space available at the branch is used up, then the archived safe deposit box ends up in the Bank's central safe deposit box, which holds an ISO certification and observes all the necessary safekeeping and security measures as to the protection of the documents resulting from it. Despite the relevant research, it was not possible to locate the client's contract in the relevant archived box a? yal£io. 2 The Bank has also inspected the physical file of the client, where all the original contracts/contracts and communication with the client are included, including his identification, where again it was not possible to locate the specific contract. 1.6. Based on the above data and the data before me as well as the data and evidence of the investigation, it appears that the Complainant company Autoiiiv Iia, as a separate legal entity and therefore as a separate controller has not carried out illegal processing of personal data and therefore there is no case against her but only against the Plaintiff, the Bank. 1.7. Subsequently, by my letter dated 11.05.2020, the Complainant was informed that, prima facie, I found a violation of her obligation under Articles 5(1)(f), 5(2), 15, 32 and 33 of Regulation, as well as Article 33(1)(c) of Law 125(I)/2018 and she was asked to submit to me her positions/opinions on the above and the reasons why she believes that she should not be imposed any administrative sanction, within a period of 4 weeks from the above date. Additionally, in the same letter, she was asked to inform me of her turnover. 1.8. Stig (18.06.2020, the External Legal Advisors of the Bank, i (Chrysafinis & Polyviou D.E.P.E.), acting on behalf of the client iys, (Bank), sent me a letter and informed me, among other things, that : (a) The client's limit insurance has been concluded on January 24, 2000 for the amount of £20,000 (twenty thousand Cyprus pounds) to secure a current account in the name of the company *" ' Ltd. (b) According to the then filing procedure of the Bank (part of Policy/internal procedure attached), the original was kept by the client, one copy was to be filed in the client's file and one copy was filed in a separate file (ouch iiib). in 2000, as a result of which his file, which is in the possession of the Bank, contains the specific copy. (c) Initially, the client's account was at the Molou branch in Limassol, which has terminated his statements. The records of that store have been kept in an associated warehouse and to date it has not been possible to locate the particular document. Nevertheless, the Defendant in the complaint does not consider that there has been a violation of Articles 4 and 5(1)(f) of the Regulation, since it cannot be proven that any breach of security led to accidental or illegal destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed. On the one hand, there was no loss of the customer's personal data, and on the other hand, the form did

not contain any information, such as results of medical examinations, evaluations of treating physicians, or any data falling under the special categories of personal data. (d) The Bank does not have the slightest reasonable suspicion that the form is located anywhere outside the Bank. The difficulty in renewing it is due to the fact that, in 2000, the filing process did not provide for electronic storage of records and, on the other hand, to the transfer of the customer's accounts from Limassol to Nicosia to a store that has also terminated its operation and its files were transferred to the central archives the bank's. Therefore, they believe that article 32 of the Regulation has not been violated, which is why the Bank did not notify any breach of personal data, as provided by the provisions of article 33 of the Regulation. 3 (e) Since 2012, the company Evtoiv Iia, has automated the sending of confirmation of insurance premium certificates and therefore the complainant received relevant information every year at least since 2012. Therefore, the Bank is in compliance with article 15 of Regulation, regarding the right of access. With the insurance premium certificates, the Bank notified him on an annual basis, since 2012, the following information: Insurance contract number Insurance contract title Renewal date Insured member's name Insured member's ID number Insurance certificate number Insured amount Date of inclusion Coverage period Life insurance premium Total insurance premium incapacity Paid premium The above is proof of compliance of data processing activities. (f) Since 2000, the filing process has improved significantly. In particular, applications are now filed both electronically and in the clients' files which are in a fire-safe area (today's recorded filing process is attached). (g) The current measures are appropriate and effective in accordance with Article 5(2) and that since 2000 the procedures have been improved, upgraded and developed with the passage of technology. (h) As of May 2018, the Bank fully complies with the Regulation. In particular, it fulfills all the requests of its clients regarding their rights and proceeds with immediate information to the Commissioner regarding issues of information leakage and acts on the basis of her instructions. Furthermore, the Bank has adopted a relevant record retention policy, which it implemented in 2020. The Bank has also recorded its processes in an activity log and carried out an impact assessment for all processes and the systems that support them. Where deemed necessary, reviewed procedures or set timelines for actions that needed to take place. (i) Regarding the filing process, since 2011 the Bank has started scanning various agreements and forms signed by the customer and today most of the forms are scanned. This helps both the easy and safer way of archiving and the immediate availability of these data in case the data subjects exercise the right of access based on the Regulation. In particular, the participation applications in question are now archived both electronically and in the clients' files which are in a fire-safe area. (j) The Complainant did not disclose the incident as there is not the slightest suspicion that

the document is outside the Bank. Considering the branch closures, the merger of the Bank with the former Laiki Bank and the changes in storage facilities, it is not certain whether the relevant document has been lost or simply misplaced based on filing procedures and therefore not access to the margin insurance contract has been made possible to date. 4 Legal Framework 2.1. Article 4 - Definitions: ""personal data": 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 an identifier such as a name, an identity number, location data, an online identifier or one or more factors that characterize the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person." . ""processing": 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 the alteration, retrieval, retrieval of information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, restriction, deletion or destruction." "filing system': any structured set of personal data that is accessible according to specific criteria, whether that set is centralized or decentralized or distributed on a functional or geographical basis.". ""controller"? the natural or legal person, public authority, agency or other entity that, alone or jointly with others, determines the purposes and manner of processing personal data" when the purposes and manner of such processing are determined by the law of Union or Member State law, the controller or the specific criteria for his appointment may be provided for by Union law or Member State law." ""health-related data": personal data relating to the physical or mental health of a natural person, including the provision of health care services, and which disclose information about his or her state of health." ""personal data breach": the breach of security leading to accidental or unlawful destruction , loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise submitted to processing". Article 9(1) of the Regulation provides that "special categories of personal data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data for the purpose of indisputable identification of a person, data concerning health or data concerning a natural person's sex life or sexual orientation. 2.2. Article 5 - Principles governing the processing of personal data: The principles governing the processing of personal data are defined in article 5(1) of the Regulation. Among them, personal data "are processed in a way that guarantees the appropriate security of personal data, including their protection against unauthorized or unlawful processing and accidental loss, destruction or deterioration, using appropriate technical or organizational measures ("integrity

and confidentiality")." (article 5(1)(f)). In addition, paragraph (2) of the same article provides that "the controller bears the responsibility and is able to demonstrate compliance with paragraph 1 ("accountability")". 2.4. Article 15 - Right of access of the data subject: 2.4.1. Based on article 15 of the Regulation: "1. The data subject has the right to receive from the controller confirmation as to whether or not the personal data concerning him is being processed and, if this is the case, the right to access the personal data and the following information: a) the purposes of the processing, b) the relevant categories of personal data, c) the recipients or categories of recipients to whom the personal data have been disclosed or are to be disclosed, in particular recipients in third countries or international organizations, d) if possible, the period for which the personal data will be stored or, when this is impossible, the criteria that determine the period in question, e) the existence of the right to submit a request to the data controller for the correction or deletion of personal data or to limit the processing of the data of a personal nature concerning the subject of d data or the right to object to said processing, f) the right to submit a complaint to a supervisory authority, g) when personal data are not collected from the data subject, any available information about their origin, h) the existence of automated decision-making , including profiling, provided for in Article 22 paragraphs 1 and 4 and, at least in these cases, significant information about the logic followed, as well as the significance and intended consequences of said processing for the data subject." . Furthermore, paragraphs 3 and 4 of the same article provide that: "3. The controller provides a copy of the personal data being processed. For additional copies that may be requested by the data subject, the controller may charge a reasonable fee for administrative costs. If the data subject submits the request by electronic means, and unless the data subject requests otherwise, the information shall be provided in a commonly used electronic format. 4. The right to receive a copy referred to in paragraph 3 does not adversely affect the rights and freedoms of others.' 6 2.4.2. Recital 63 of the Regulation states that: "A data subject must have the right to access personal data collected and concerning him and be able to exercise this right and at reasonable regular intervals, in order to is aware of and verifies the validity of the explanation. This includes the right of data subjects to access their health data, including medical record data that includes information on diagnoses, test results, evaluations by treating physicians and any treatment or procedure provided. Therefore, each data subject should have the right to know and be notified in particular of the purposes for which the personal data is being processed, if possible, for how long the personal data is being processed, which recipients receive the personal data character, what logic is followed in any automatic processing of personal data and what could be the consequences of such processing, at least when it is based on profiling. The controller should be able to provide remote

access to a secure system through which the data subject obtains direct access to the data concerning him. This right should not adversely affect the rights or freedoms of others, such as professional secrecy or intellectual property right and, in particular, the copyright protecting the software. However, these factors should not have the effect of refusing to provide any information to the data subject. Where the controller processes large amounts of information about the data subject, the controller should be able to ask the data subject, before the information is provided, to specify the information or processing activities related to the request." 2.5. Article 32 - Processing security: 2.5.1. According to the provisions of article 32 of the Regulation, which concern 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 seriousness for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures in order to ensure an appropriate level of security against the risks, including, among others, as appropriate:" "b) the ability to ensure the confidentiality, integrity, availability and reliability of processing systems and services on an ongoing basis, c) the possibility of restoring the availability and access to personal data in a timely manner in the event of a physical or technical event, d) a procedure for the regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure the security of the processing .». 2.5.2. In paragraph 2 of the same article, it is stated that: "When assessing the appropriate level of security, the risks deriving from the processing are taken into account, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted , stored or otherwise processed'. 7 2.5.3. According to the last paragraph of recital 39 of the Regulation: "Personal data should be processed in a way that ensures the appropriate protection and confidentiality of personal data, including to prevent any unauthorized access to this data personal data and the equipment used to process them or the use of such personal data and said equipment." 2.5.4. Recital 74 of the Regulation states that: "Responsibility and obligation to indemnify the data controller should be established for any processing of personal data carried out by the data controller or on behalf of the data controller. In particular, the controller should be required to implement appropriate and effective measures and be able to demonstrate the compliance of the processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, context, scope and purposes of the processing and the risk to the rights and freedoms of natural persons." 2.5.5. With reference to Article 32 of the Regulation, recital 83 of the Regulation adds that: "To maintain security and avoid processing in violation of this

Regulation, the controller or processor should assess the risks involved the processing and implement measures to mitigate such risks, such as through encryption. These measures should ensure an appropriate level of security, which includes confidentiality... When assessing the risk to data security, attention should be paid to the risks arising from the processing of personal data...” . 2.6. Article 33 - Notification of a personal data breach to the supervisory authority: 2.6.1. Article 33 of the Regulation defines specific obligations for data controllers regarding personal data breach incidents. Specifically, in the event of a personal data breach, the data controller shall notify the competent supervisory authority without delay and, if possible, within 72 hours of becoming aware of the personal data breach, unless the personal data breach is unlikely to cause 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. 2.6.2. With regard to the notification of a personal data breach, recital 85 states the following: "The breach of personal data shall be followed". if not dealt with properly and fairly. to result in physical, material or non-material damage to Natural Persons, such as loss of control over their personal property data or the limitation of their rights, discrimination, abuse or identity theft, financial loss, illegal removal of pseudonyms, damage to reputation , loss of confidentiality of personal data protected by professional secrecy or other significant economic or social disadvantage for the natural person concerned. Consequently, if the data controller becomes aware of a breach of personal data, 8 he/she should, as soon as possible and, if possible, within 72 hours of becoming aware of the fact, notify the personal data breach to the competent supervisory authority. except: if the data controller can demonstrate, according to the law of accountability, that the breach of personal data is not likely to endanger the rights and freedoms of natural persons. If such notification cannot be obtained within 72 hours, the notification should be accompanied by a justification stating the reasons for the delay and the information may be provided gradually without undue delay.' 2.6.3. Regarding article 33 of the Regulation, recital 87 of the Regulation adds that: "It should be verified whether all appropriate technological protection measures and organizational measures have been put in place for the immediate detection of any breach of personal data and the immediate notification of the supervisory authority and the data subject", as detailed in the 06-02-2018 Guidelines of OE 29 (Working Group of Article 29) for the notification of a data breach (vP 250 ton. 1). 2.6.4. According to the Guidelines of the Working Group of article 29 of Directive 95/46/EC (currently European Data Protection Board - EDPB) on the Notification of Personal Data Breach ("Regulation of Personal Data Protection Act 2016/679 IA/P 250 1), dated 06.02.2018, two types of personal data breach are those categorized as "loss" and "availability breach". Specifically, according to the above Guidelines: "Regarding the 'loss' of

personal data, the term should be interpreted as a case where the data may still exist, but the data controller has lost control or access to it in them or he no longer has them in his possession. "Breach of availability" - when there is accidental or unauthorized loss of access 1 to personal data or accidental or unauthorized destruction of personal data. “While whether a breach of confidentiality or integrity has been committed is relatively clear, whether a breach of availability has been committed may be less obvious. A breach will always be considered a breach of availability where there is permanent loss or destruction of personal data.' "Consequently, a security incident that results in the unavailability of personal data for a period of time is also a type of breach, since the lack of access to data can have a significant impact on the rights and freedoms of Natural Persons." 1 1 It is commonly accepted that 'access' is a fundamental part of 'availability'. See, for example, the NI5T 5P800-53tvn4 standard, which defines "availability" as follows: "Ensuring timely and reliable access to and use of information", available at http://www.info.org/info/ International Standard 851-4009 also refers to: "Timely, reliable access to data and information services for authorized users." See || P0T The I50/IE0 27000:2016 standard also defines "availability" as the "Property of being accessible and ready for use at the request of an authorized body": :l5th-ibs27000.blM:v1:Bi 9 % The following excerpts from the same Guidelines are also listed in relation to the case: “Any breach response plan should focus on protecting individuals and their personal data. Breach notification should therefore be seen as a tool that improves data protection compliance. At the same time, it should be noted that failure to report a breach to either a person or a supervisory authority may mean that, under Article 83, a sanction is likely to be imposed on the controller. Controllers and processors are therefore encouraged to plan in advance and implement procedures aimed at detecting and promptly limiting a breach, assessing the risk to persons2 and then deciding on whether it is necessary to inform the competent supervisory authority and to communicate the violation to the persons concerned, when necessary. Notification to the supervisory authority should be part of this incident response plan.' "...a key feature of any data security policy is to provide the ability, when feasible, to prevent a breach and, should it hopefully occur, to respond promptly." "It is also important to consider that, in some cases, non-disclosure of a breach could indicate either the absence of existing security measures or the inadequacy of existing security measures." "EO 29 considers that a controller should be considered to acquire 'knowledge' when that controller has a reasonable degree of certainty that a security incident has occurred which has the effect of compromising personal data". “Article 26 deals with joint controllers and clarifies that joint controllers determine their respective responsibilities for compliance with the GDPR3. This will include determining which party will have responsibility for compliance with the obligations under Articles 33 and 34. OE29 recommends that

contractual arrangements between joint controllers include provisions specifying which controller shall responsibility for compliance with GDPR breach notification obligations.” "Article 33(1) makes it clear that, in the case of a breach which is 'not likely to cause a risk to the rights and freedoms of natural persons', notification to the supervisory authority is not required. An example may be the case where personal data is already publicly available and its disclosure does not pose a potential risk to the individual. “A breach may affect just one person or a small number of people, or a few thousand, if not more. In general, the higher the number of people affected, the more impact a breach can have. However, a breach can have a serious impact even on an individual, depending on the nature of the personal data and the context in which it has been compromised." 2 This can be ensured in the context of the obligation to monitor and review a data protection impact assessment (DPA), which concerns processing operations that may pose a high risk to the rights and freedoms of natural persons (Article 35(1) and 11). 3 See also recital 79 (of the Regulation). 10 2.6.5. The following excerpts from the book by L. Kotsali - K. Menoudakos, entitled General Data Protection Regulation - Legal dimension and practical application, chapter VI., concerning the disclosure of personal data breaches: "In the new Regulation the "principles of processing" include "integrity" and "confidentiality" (article 5 par. 1 f). The obligation of confidentiality and the adoption of technical and organizational security measures was included in the obligations of the data controller already introduced by Directive 95/46/EC: In particular, the data controller had to ensure a level of security commensurate with the risks involved in the processing and the nature of the data, so as to protect the data from accidental or unlawful destruction, accidental loss, prohibited dissemination or access and any other form of unlawful processing." "The General Data Protection Regulation adds to the corresponding regulation (Article 32) an indicative list of security measures, such as pseudonymization and encryption, but also procedures that ultimately consist in the adoption of a holistic security policy. At the same time, the adoption of technical and organizational measures seems to be emphatically adopted as an additional obligation or guarantee that balances forms or procedures of data processing that pose risks to the rights of persons. "The EU legislator defines what it perceives as a personal data breach: according to Article 4(12) it is the breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted; stored or otherwise processed. As the Article 29 Group clarifies, it may be a breach of the confidentiality, availability or integrity of the data or a combination thereof, the Regulation obliges the notification of the breach of personal data to the competent supervisory authority". “The Article 29 Panel clarifies however that for a breach to be treated as a breach of availability there must be a permanent loss or destruction of data. He notes, however, that a non-permanent

breach leading to unavailability may also require notification, taking into account possible risks to the rights of individuals. See Part 29 of the Ministry of Defense of the Republic of Croatia Rotig, Thiyothijbd or PbGdohl a3\3 oteaoit kholihioioni hnabt PTH9uil3ilon 2016/679, 03/10/2017 (\L/P 250), p. 6". 2.7. Decisions A useful reference can also be made to the following excerpts from the Greek Personal Data Protection Authority: Decision No. 98/2013 "Kataonao security is specialized in the basic objectives, namely the confidentiality, integrity and availability of the data. while complementary goals, especially from the point of view of personal data protection. they are in particular the disclaimer of responsibility (or liability) as well as the separation of data according to the purpose of the processing. According to the internationally accepted information system security standards (e.g. see series I50/IEO 27000) the appropriate measures according to article 10 par. 3 of Law 2472/1997 are part of an Information Systems Security System (I3M3). This System requires the preparation of a risk study based on the risks and the nature of the data, and among other things includes the preparation of security policy and plans, where specific technical and organizational measures are identified. These standards, in addition to being applied, are also monitored and evaluated in order to continuously adapt them to the operational needs of the data controller and to technological developments, which the data controller must take into account (see article 17 para 1 Directive 95/46/EC).' Decision No. 44/2019 "In view of the above, the Authority considers that the audited company AMRNI as a data controller: On the one hand, it did not apply all the principles of article 5 para. 1 GDPR and 6 para. 1 GDPR regarding the legality of the processing of personnel data character...that took place in the used computing infrastructure ..... but also in the context of any subsequent or further processing of the same personal data, nor did he prove by no. 5 para. 2 GDPR the observance thereof. On the other hand, he violated the provisions of articles 5 par. 1 sec. a' and f' and par. 2 in conjunction with articles 24 par. 1 and 2 and 32 par. 1 and 2 GDPR regarding the principle of secure processing (in particular "confidentiality") of personal data that took place in used computing infrastructure ..... from the failure to take appropriate technical and organizational measures, but also in the context of any subsequent or further processing of the same personal data, so as to attract the examination of compliance with the processing principles of the territories b', n', d' and e' of par. 1 of article 5 as well as of article 6 par. 1 GDPR.... 3. Rationale 3.1. Data included in an insurance policy and relating to a living person constitute "personal data". The data relating to the health and/or medical history of a living natural person, to the extent that his identity is revealed immediately or indirectly, constitute "special categories of personal data", according to the definition given in article 9(1) of the Regulation. The insurance contracts maintained by the Company and concerning its customers-insured constitute a

"filing system" based on the definition in article 4(6) of the Regulation. The collection, registration, use, search, association/combination and storage of personal data constitute processing of personal data, in the sense of article 4(2) of the Regulation. The controller is Bank of Cyprus Public Company Ltd (Article 4(7) of the Regulation). Data subjects are the customers of Bank of Cyprus Public Company Ltd (Article 4(1) of the Regulation). 3.2. In order for personal data to be lawfully processed, the conditions of compliance with the principles governing the processing of personal data (Article 5 of the Regulation) must be cumulatively met, as also follows from the decision of the Court of Justice of the European Union (CJEU) dated 16.01.2019 in the case 0-496/2017 DvyIdoHv Rodi A<3 v. IthirizoIIopi Ko! h4. According to this Decision, the existence of a legal 4 4 "57. However, any processing of personal data must be in accordance, on the one hand, with the principles to be observed in terms of data quality, which are set by Article 6 of Directive 95/46 or Article 5 of Regulation 2016/679 and, on the other hand, to the basic principles of legal data processing listed in article 7 of this directive or article 6 of this regulation (cf. decisions of 20 May 2003, Ordinance 12 of the foundation (article 6(1) of the Regulation) does not exempt the person in charge processing from the obligation to comply with the principles (article 5 of the Regulation). 3.3. As mentioned by Grigoris Tsolias, Lawyer, Member of the Personal Data Protection Authority and Member of the European Commission for Regulation 2016/679 and the Directive 2016/680: "Cumulative fulfillment of conditions for application and observance of principles no. 5 par. 1 and d GDPR (General Data Protection Regulation) The existence of a legal basis (no. 6 par. 1 GDPR () does not exempt the (processor) from the obligation to comply with the principles of art. 5 par. 1 GDPR. Unlawful collection and processing in violation of the principles of no. 5 GDPR is not cured by the existence of a legitimate purpose If one of the principles of article 5 par.1 GDPR is violated (e.g. legitimate and legal processing, security) the examination of the other principles or article 6 par.1 GDPR is omitted." 3.4. In addition, the controller is burdened with the further duty to prove at all times its compliance with the principles governing the processing of personal data, as set out in article 5 of the Regulation. Specifically, accountability is part of the principles governing the processing of personal data and implies the ability of the data controller to demonstrate compliance with the Regulation. In addition, it enables the data controller to be able to control and document the processing carried out in accordance with the technical bases provided by the Regulation. The processing of personal data in a transparent manner is a manifestation of slow and effective processing and is linked to the slow accountability*:, giving the data subjects the right to exercise control over their data by holding the controllers accountable (see Guidelines OE 29, European Parliament and of the Council 2016/679, \L/P260). The principle of accountability, in essence,

shifts to the controller "the burden of proof" of the legality of the processing. 3.5.1. In addition, the controller is burdened with the obligation to take, according to article 32 of the Regulation, the appropriate technical and organizational measures to ensure the appropriate level of security and protection of personal data according to the risks involved in the processing and the nature of the data which is the subject of the processing. In particular, the data controller must take appropriate technical and organizational measures in order to ensure the appropriate level of security against the risks that may lead to a breach of personal data. within the meaning of article 4(12) of the Regulation. 3.5.2. From the letter and the purpose of the provisions of recital 83 of the Regulation, it is clear that the obligation to observe the security of the processing by the controller has both a preventive and repressive nature. Preventive, so that applicable measures can prevent incidents of personal data breach and repressive, so that any incident can be detected and investigated. Even though, as stated in the letter dated 20.02.2020, the limit insurance contracts are kept in an archived safe deposit box at the competent branch of the National Insurance Company, etc., 0-465/00, 0-138/01 and 0-139/ 01, EII:O:2003:294, paragraph 65. as well as of 13th May 2014, Oxliv drei and Oothie, 0-131/12, Eu:0:2014:317, paragraph 71). 13 of the Bank, which end up in the Bank's central safekeeping file (custodial portfolio), which, as the Defendant claims, holds a 180 certification and observes all the appropriate safekeeping and security measures, however the result was that the insurance policy of the complainant cannot be found. Therefore, it is established that the organizational and/or technical security measures did not work in the correct and appropriate manner, as measures of a preventive nature, with the consequent inability to find the insurance policy. 3.6.1. The loss / violation of the availability (inability to locate) of the complainant's insurance policy constitutes a violation of personal data and proves the lack of sufficient and appropriate technical and organizational measures according to article 32 of the Regulation. 3.6.2. As soon as she became aware of the personal data breach, she should immediately and, if possible, within 72 hours from the moment she became aware of the fact, notify the personal data breach to my Office, as provided by the provisions of article 33 of the Regulation. Notification to my Office was not necessary if the Defendant could demonstrate that the breach of personal data would not cause a risk to the rights and freedoms of the complainant, which the Defendant did not do. If such notification could not be obtained within 72 hours, the notification should have been accompanied by a justification stating the reasons for the delay and the information could have been provided gradually without undue delay, which the Defendant did not do. I note that the fact that I was informed of the specific personal data breach through the complainant's submission of a complaint to my Office is irrelevant and irrelevant, since the obligation to notify of a personal data breach rests with the data controller. 3.6.3.

Therefore, data subjects should have the right to access the personal data concerning them and be able to exercise this right easily and at reasonable regular intervals, so that they are aware of and verify the legality of the processing. In the present case, the discovery of the complainant's insurance policy caused a risk to the rights of the company, the complainant was deprived of the right of access to his insurance policy, as a result of which, on the one hand, he cannot check the correctness/accuracy/validity of the data are contained in it and on the other hand cannot verify" the legality of the processing. 3.6.4. It means what was mentioned in paragraphs 3.6.1. - 3.6.3. above, the Defendant in the complaint had an obligation to disclose the incident of personal data breach (loss/impairment of the availability - inability to locate - the insurance contract of the tchoattonouen). 14 4. Conclusions In the case under consideration, from the data of the case file and the defendant's admission of the complaint that the insurance policy in question cannot be found, from a technical point of view, I conclude that the Bank did not comply with the following obligations deriving from the Regulation, given that: 4.1. Principles governing the processing of personal data Pursuant to Article 5(1) of the Regulation: Did not take the necessary organizational and/or technical measures to guarantee the appropriate security of personal data, including their protection from unauthorized or illegal processing and accidental loss, destruction or damage ("integrity and confidentiality"). Therefore, from the lack of appropriate technical and/or organizational measures, the risk to the confidentiality and/or integrity of personal data occurred through the loss5 6 * and/or violation of the availability8 (untraceability) of the insurance policy of the complainant . Based on Article 5(2) and recital 74 of the Regulation: It did not implement appropriate and effective measures and was not able to demonstrate the compliance of its processing activities with the Regulation including the effectiveness of these measures. 4.2. Processing security Based on Article 32 and Reason 83 of the Regulation: (a) Breached its obligation to take appropriate organizational and/or technical measures for the security of the insurance policy that contained personal data and its protection from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access stored or otherwise processed. These measures must ensure a level of security commensurate with the risks involved in the processing and the nature of the data being processed. (b) Did not assess the risks involved in the processing and did not take/implement measures to mitigate said risks, such as accidental or unlawful destruction and loss. 5 Guidelines of the Working Group of Article 29 of Directive 95/46/EC (currently European Data Protection Board - EDPB) for Personal Data Breach Notification: "With regard to the "loss" of personal data, the term should be interpreted as a case where the data may still exist, but the controller has lost control or access to it, or is no longer in possession of it.' 6 Guidelines of the Working Group of Article 29 of Directive 95/46/EC (now the

European Data Protection Board - EDPB) for the Notification of a Personal Data Breach: "Availability Breach" - when there is an accidental or unauthorized loss of access to personal data or accidental or unauthorized destruction of personal data." “While whether a breach of confidentiality or integrity has been committed is relatively clear, whether a breach of availability has been committed may be less obvious. A breach shall always be deemed to constitute a breach of availability where there is permanent loss or destruction of personal data." 15 4.3. Notification of a personal data breach to the supervisory authority Pursuant to Article 33 of the Regulation, he did not submit the relevant notification to my Office within seventy-two (72) hours of becoming aware of the incident. According to the Guidelines of the Working Group of article 29 of Directive 95/46/EC (currently European Data Protection Board - EDPB) on the Notification of Personal Data Breach ("The Notification of Personal Data Breach") 2016/679 v/P 250 Gvn. 1), dated 06.02.2018, notification of a breach would imply either the absence of existing security measures or the inadequacy of existing security measures. 4.4. Right of access of the data subject Based on Article 15 of the Regulation: Failure to take the appropriate organizational and/or technical security measures, in accordance with the provisions of Article 32 of the Regulation, contributed to an incident of personal data breach, in accordance with the provisions of Article 4 (12) of the Regulation and in non-satisfaction of the complainant's right of access to his insurance policy (article 15 of the Regulation). It should be noted that, as defined by the Guidelines of the Working Group of Article 29 of the Directive 95/46/EC on Personal Data Breach Notification, a breach can potentially have various significant adverse consequences for persons, which can lead to physical, material or moral damage. This harm can include loss of control over their personal data, restriction of their rights, discrimination, misuse or identity theft, and financial loss. It may also include any other significant economic or social disadvantage for these persons7. 4.5. The claims of the Foreign Legal Representative of the Complainant, as petitioner" in his letter dated 05.06.2020 are answered as follows: Paragraph 1 of the Complainant - limit insurance contract (a) The claim of the complaint that there was no breach of security (Articles 4(12), 5(1)(f) and 32 of the Regulation), is unfounded since, according to the European Commission7 8, a data breach occurs when a security incident occurs in relation to data for which a subsidiary or an organization is responsible, which results in a breach of confidentiality, availability or integrity. If this happens, and the breach is likely to endanger the rights and freedoms of a natural person, the company or organization must notify the supervisor without undue delay and no later than 72 hours after becoming aware of the breach. As

7 See also recitals 85 and 75 (of Regulation 679/2016). 8

Hir$://6th.6ytor3.6y/inio/13vn/13vn-Thorio/co313-Pg1:b€1on/t6thGGIi/Gy65-6y$yth55-3n-OGB3nh53Hyth5/h6Iy53hth1<:3-6Hh

3yth It is vital to have the appropriate technical and organizational to prevent possible data breaches. In addition, the Greek Personal Data Protection Authority states that9: "Traditionally, the term information/data security (information/data security) is used to describe the methodology, as well as the methods and techniques followed in order to achieve the following objectives: Confidentiality: Data must not be disclosed to unauthorized persons Integrity: Data must be accurate, complete and genuine - not incorrect, corrupted or out of date Availability:): Data must be available to users when their use is required in any of the above - from an accidental or deliberate action - constitutes, in general, a security incident. In this case, a security incident occurred in relation to the Contract concerning the employee. for which the Bank is responsible, if the person in charge of the explanation of its filing system, which is the result of the violation of the availability of the contract and, by extension, the impossibility of satisfying the right of access of the employee to personal data related to him (contract) . (b) The claim of the Complainant that there was no loss of Mr.'s personal data is unfounded and probably lies in the fact that he mistakenly believes that the contract must contain/renew personal data that pertains exclusively to his etc. so that this constitutes "personal data". Based on recital 26 of the Regulation which complements article 4(1) of the Regulation, which refers to the definition of "personal data": "The principles of data protection should be applied to any information that concerns an identified or identifiable natural person . Pseudonymized personal data that could be attributed to a natural person using supplementary information should be considered information about an identifiable natural person. In order to determine whether a natural person is identifiable, account should be taken of all means which are reasonably likely to be used, such as for example their separation, either by the controller or by a third party to directly or indirectly ascertain the identity of the natural person. In order to determine whether any means is reasonably likely to be used to verify the identity of the natural person, all objective factors, such as the cost and time required for identification, should be taken into account, taking into account the technology that is available at the time of processing and technological developments." ? P38vi€1=33·211421& 03a=PthG1:31& 5<:H6G3=ROKTAI 17 From the above it follows that ANY INFORMATION referring to a living natural person constitutes "data of a personal nature". Therefore, the personal data contained in the complainant's insurance policy constitutes "personal data". (c) Therefore, the claim of the Complainant that the disputed limit insurance contract does not contain data related to the health of the complainant, does not negate the obligation that the appropriate technical and organizational security measures must be observed every time, given that the said contract concerns the complainant and is therefore his personal data. (d) The claim of the Complainant that the Bank is in compliance with article 15 of the Regulation, which concerns the right of access,

due to the fact that, with the insurance premium certificates, the Bank notified him on an annual basis, from 2012, data relating to his insurance contract, is rejected as unfounded and untrue. For this purpose, a sample copy of the "Certificate of Payment of Group Life Insurance Contract" form has been attached, as Appendix 3, in which it is stated that: "This Certificate is issued for the sole purpose of filing it with the Department of Internal Revenue, if requested, and it has no other value or purpose, nor is it a guarantee that the premium will be tax-free.": The complainant received an annual INFORMATION/UPDATE for his insurance policy number M-056482. notwithstanding the RIGHT OF ACCESS EXERCISED IN THE INSURANCE POLICY ITSELF. IT HAS NOT BEEN SATISFIED UNTIL TODAY, despite the fact that, as Kathik admitted to the complaint, it cannot be found. From the above, it can be concluded that the Bank was NOT in a position to satisfy the complainant's right of access, depriving him of the possibility to check the validity of the investigation and consequently violated, prima facie. the provisions of article 15 of the Regulation. The Bank admitted not finding the Contract in question in its following letters: Letter dated February 20, 2020 from Dr. Nicosia Regional Manager of the Bank; "Despite the relevant investigation, it was not possible to locate the client's contract _____7 the relevant archived Safe deposit box.". "The Bank has also inspected the client's Physical File where there are all the original contracts/contracts and communication with the client including Vanouenou and his identification documents where again it was not possible to locate the contract in question". Letter dated June 05, 2020 (paragraph 1 - Limit Insurance Contract): "Delivery. It seems that a copy was filed in the client's File in 2000, with the result that his File, which is in the possession of the Bank, does not contain the specific copy." "The records of that store have been kept in attached warehouses and to this day it has not been possible to locate the document in question." 18 "The difficulty in finding him is due to the fact that.....". Letter dated June 05, 2020 {paragraph 5 - Mitigating-Final Comments): “In consideration of the closing of the branches, the merger of tg Bank with the former Laiki Bank and the closing of the storage areas. it is not the case whether the relevant meaning has been lost or simply placed in the wrong place based on the filing procedures and therefore it has not been possible to access today the limit insurance contract > Item 1 of the Defendant - limit insurance contract and Par. 5 of the Defendant - Mitigating-Final Comments The Defendant in the complaint did not manage to prove to me that the contract in question is indeed inside the Bank's premises, since to date it has not been found, an element that proves the non-existence of proper filing of documents, consequence of taking insufficient security measures, an obligation it bears as the controller of its filing system (Article 32 of the Regulation). The Bank should, based on the provisions of Articles 5(1)(f) and 32 of the Regulation, have adopted/implemented specific procedures for the proper organization/filing/classification

of both its electronic and physical filing systems. In addition, it should have procedures for the preparation of scheduled audits (internal and/or external, on an annual basis), where compliance with security measures and their effectiveness are recorded and checked. As a result of the audits, it could be the modification of the existing security policy, some security measures or the addition of new ones. Par. 3 of the Defendant - relationship with customers The relationship the Bank has with its customers, as recorded in paragraph 3 of the Defendant's letter of complaint dated June 5, 2020 and the Bank's proposal to the complainant for a refund of all insurance premiums, they are not within my jurisdiction and are therefore not reviewed and evaluated. In addition, it is information that is not related to the essence of the examination of this case, which is the receipt of a copy of the insurance policy of the complainant menu with number M-056482 during the exercise of his right of access to the personal data concerning him (Article 15 of the Regulation) . In any case, it is self-evident that the Bank's proposal to refund all insurance premiums to Mr. leads to the cancellation of the exercise of the right to privacy on the part of the data subject and the impossibility of checking the legality of the processing carried out by the Bank. The impossibility of satisfying the right of access*:, is due to a shortcoming in the way the Bank's file is operated and constitutes a shortcoming of the standards of care which he had to observe as a data controller in order to avoid the error. Par. 5 of the Defendant - Mitigating-Final Comments The claim of the Defendant in the complaint that, "to date no fine has been imposed on the Bank by the Commissioner in relation to matters of compliance of the Bank with the Regulation" is not true since, until today four administrative sanctions have been imposed (File No.: A/P 19 % 8/2006, A/P 48/2010, A/P 61/2014, A/P 67/2017 and A/P 56/2017), the which, however, will not be counted when calculating the penalty, since they do not relate to a violation of a similar nature. 5. Penalties 5.1.1. As defined in the provisions of article 83(5) of the Regulation. violation of the provisions of articles 5 and 15, incurs, "in accordance with paragraph 2, administrative fines of up to 20 000 000 EDI or, in the case of enterprises, up to 4% of the total global annual turnover of the previous financial year, depending on which is higher."5.1.2. If it is defined in the provisions of article 83/4) of the Regulation, violation of the provisions of articles 32 and 33, "in accordance with paragraph 2, administrative fines up to 10 000 000 Euros or, in the case of businesses, up to 2% of the total of worldwide annual turnover of the previous financial year, whichever is higher'.

5.1.3. Paragraph 2 of article 83 of the Regulation is quoted in its entirety:

"2. Administrative fines, depending on the circumstances of each individual case, are imposed in addition to or instead of the measures referred to in Article 58(2)(a) to (h) and Article 58(2)(j). When deciding on the imposition of an administrative fine, as

well as on the amount of the administrative fine for each individual case, the following shall be duly taken into account:

a) the nature, gravity and duration of the breach, taking into account the nature, extent or purpose of the relevant processing, as well as the number of data subjects affected by the breach and the degree of damage they suffered,

b) the fraud or negligence that caused the breach,

c) any actions taken by the controller or the processor to mitigate the damage suffered by the data subjects;

d) the degree of responsibility of the data controller or processor, taking into account the technical and organizational measures they apply pursuant to articles 25 and 32,

e) any relevant previous violations of the controller or processor, f) the degree of cooperation with the control authority to remedy the violation and limit its possible adverse effects,

g) the categories of personal data affected by the breach,

h) the way in which the supervisory authority was informed of the breach, in particular if and to what extent the data controller or processor notified the breach,

i) in the event that the measures referred to in Article 58 paragraph 2 were previously ordered to be taken against the data controller involved or the processor in relation to the same object, the compliance with said measures,

j) adherence to approved codes of conduct in accordance with Article 40 or approved certification mechanisms in accordance with Article 42 and

k) any other aggravating or mitigating factor resulting from the circumstances of the specific case, such as the financial benefits obtained or damages avoided, directly or indirectly, from the violation.

20

*

6. Actual measurement

Taking into account the provisions of article 83 of the Regulation, which concerns the General Organizations for the imposition of administrative quotas. when measuring the administrative fine, I took into account the following mitigating (a - g) and aggravating (n -1) factors:

(a) The nature of the breach: The breach concerns the Bank's contractual relationship with the data subject,

(b) The number of data subjects affected by the breach:

a person is affected.

(c) The categories of personal data affected by the violation: Given that, to date, the limit insurance contract has not been found, I believe that the personal data included in it are, at a minimum, the name, policy number and identity number, as the most common means of identification

(d) The fact that the Complaining Defendant took action to mitigate the damage

suffered by the data subject:

Kat'is made the complaint to Mr. for a refund of all insurance premiums

including interest on the signed insurance cancellation order,

(e) The fact that the Complainant cooperated sufficiently with my Office in remedying the violation.

(f) The fact that the Complaining Defendant has informed me that, at least in retrospect, she has taken additional measures that would contribute to strengthening/improving the security and protection of the insurance policies of her client-insured.

(g) The controller did not obtain a financial benefit, nor did it cause material damage to the data subject.

(h) The duration of the violation: It cannot be precisely determined, since the information that was taken into account by me, arose in the context of the investigation.

(i) The fact that I was informed of the illegal processing following a complaint to my Office and not directly from the Complainant.

(«) The fact that these are violations due to the processing of personal data (Articles 5(1)(f), 5(2), 32 and 33), which are judged to be of greater gravity and duration but also of non-satisfaction of the right of access of a subject.

7. Conclusion

In light of the above and based on the powers granted to me by the provisions of article 58(2)(i) of the Regulation, I am of the opinion that, prima facie, the non-finding, until today, of the disputed limit insurance policy of Mr. violates the provisions of the articles

5(1)(f), 5(2), 15, 32 and 33 of the Regulation.

21

Oh therefore. I DECIDED as follows

Therefore, I have decided to impose on the Complainant, Bank of Cyprus Public Company Ltd, in its capacity as the controller

of the filing system, a fine of €15,000 (fifteen thousand euros) for committing a breach of its obligation of articles 5(1)(f), 5(2), 15, 32 and 33 of the Regulation.

Irini Oivou Nikolaidou Commissioner for the Protection of Personal Data