No. Phone: 11.17.001.007.009

July 12, 2021

WITH THE HAND

DECISION

Complaint/complaint about exercise of right of access and eventuality

leakage of personal data of the Complainant

(in the

Facts:

following "o

In this case, Complainant XXXXX

Complainant") sent a complaint to my Office, when specific

information was given through an affidavit to the Court. The sworn

stated, testified on 3/9/2018, among other things, that he had been informed by positive

sources and to the best of his knowledge, information and belief, the Complainant

maintained a credit account and/or deposits with the Hellenic Public Company

Ltd and/or the former Cyprus Cooperative Bank Ltd, which contained an amount

in addition to the amount claimed, in the Action in which the affidavit had been filed,

such as the bill and/or promissory note with account number XXXXX to

other credit accounts. Such accounts and/or deposits and/or

promissory notes, according to the affidavit, were deposited in

accounts of the Complainant at the Cypriot Cooperative store

Bank Ltd in Nicosia, formerly XXXXX Cooperative Savings Bank.

2. Owing to the filing of the above affidavit, the District Court

Nicosia, on XXXXX (it must be a typographical error and

decision to be XXXXX, i.e. after the entry of the affidavit

declaration1) issued a decision ordering the confiscation of the amount of

XXXXX from the Complainant's account at Hellenic Public Bank

Company Ltd. As I have only recently been informed about the above decision

an appeal is pending before the Supreme Court. This information, no

contained in the complaint sent by the Complainant to my Office on the 14th

January, 2019. Of course, the Court's Decision was issued after the shipment

of the complaint to my Office, however, if my Office knew directly as

the appeal was registered, that it was pending, probably not involved in the

1 On the Cylaw website, the corresponding published decision is dated XXXXX.

examination of the Complaint, so that there is no possibility of direct or indirect

of my intervention in the work of the Court (see Article 55(3) of GDPR 2016/679 and

article 5(a) of Law 125(I)/2018).

3. The Complainant also supplied my Office, with correspondence (but also

notes relating to telephone communications) he had with official staff

both Hellenic Bank and KEDIPES. The Complainant was asking me

letters of the day 6/12/2018 and 27/12/2018, to KEDIPES and with notification

to Hellenic Bank, as informed in what way and why the

his account number XXXXX and was asking for the files to be given to him

activity logs of the disputed account, from

date of its creation to the date of its request.

4. On 12/12/2018 Hellenic Bank, based on the Transfer Agreement

of Works (with effect from 1/9/2018) that he had signed with the former Cooperative

Bank of Cyprus, and due to the fact that the incident referred to by

Complaining it had been done before the start of the deal, he referred him

Complaining to KEDIPES, while in another letter KEDIPES dated

28/12/2018, due to the fact that the Complainant's account no longer belonged to

KEDIPES, refer the Complainant for any information or

allegations, to Hellenic Bank. On 1/14/2019, I owe her above

confusion, the Complainant went to my Office, reporting her

leak of his personal data, stating that he estimates the leak to

took place between July and August 2018. On August 5, 2019, KEDIPES

had replied that from an audit he had carried out, it was established that the former SKT

had acted legally and the Complainant's account information did not

were leaked by KEDIPES.

5. My Office, after repeated telephone communications that had both

with the Complainant as well as with KEDIPES Officers, sent a letter to

19/6/2020 to KEDIPES, due to the fact that KEDIPES did not have

satisfy the Complainant's request as he is given a Report/Audit

Trail/Activity Logs of the disputed account, from which the

information. My Office considered that the Complainant, in the context of

of his rights based on Article 15 of GDPR 2016/679, he was entitled to the

due Report. As mentioned in the letter from my Office to

KEDIPES, the purpose of the Complainant was to study the Report and to

try to trace the leak, which he estimated to have taken place between

July – August 2018.

6. KEDIPES, after the intervention of my Office, on 7/20/2020 sent me

email the audit trail to the Complainant's account. He carried out

also research, through an independent company, which he communicated to

Complaining on 26/10/2020. The investigation was carried out in such a way as to make it possible

Unauthorized Access to Complainant's Account. Part of the

for

including

the O&M department,

of the content of the Report (date 7/10/2020) drawn up after the investigation, has

as follows:

"The objective of this examination was to identify any form of unauthorized

access to the account information of a specific client during the period. For the

purpose of the assessment, the organization's systems which were included in the

examination were the (ex) core banking system (not currently in production use), the

document management system (where scanned or extracted documents from the

banking system are stored) and the email system. Within scope are also the actual

physical documents of the client's account information which are stored by an external

party, Iron Mountain Incorporated (previously Fileminders). The main period under

examination is July-August 2018."

"The main system that contains the information in scope is a banking system that has

been customized and updated over the years to meet regulatory requirements,

however still having the limitations of essentially being a “legacy” system. Logs and

reporting are only accessible through extractions in text format and mostly processed

via Microsoft Excel. It is important to note that, regarding the period under scope,

legitimate access to these reports was only possible for pre-authorised

employees (as dictated by

the roles of

“Operator/Treasurer, Central Treasurer, General User, Office Clerk

District Support, District Officer/Customer Manager, Officer

Department of Transactions”) who could download reports on their PCs with all customers

information

requirements.

Consequently, the account under investigation was included in most, if not in all, of these downloaded reports. We also cannot examine nor eliminate the possibility of employees using a personal device (e.g. smartphone) to record the contents of reports, in electronic or paper format. Furthermore, the physical documents of the account are stored at an external facility (Iron Mountain Incorporated). Finally, the account in scope had been transferred to Hellenic Bank as part of the acquisition merger that started in September 2018 and finalized in September 2019. Thus, this assessment has been limited within the KEDIPES environment only."

7. The Report in question, which was also communicated to the Complainant, it also included the activity logs. According to the Report, there was none unauthorized access to the Complainant's account. "...A review of the audit log report from the system that shows access to the account in scope did not show any unauthorized access. It is important to mention here that access to the following "programs" does not necessarily mean access to the specific account, as these programs produce downloadable reports containing multiple accounts, including the one under investigation". As further explained verbally at my Office, the inquiry mentioning the name of the Complainant, produces results for all accounts (deposit, loan, etc.) that fall under the name of the Complainant as a whole and not only to specific account from which the information may have been leaked.

The systems were such at that time, so that the result in their daily or monthly regulatory reporting

search, cannot be specialized. In any case, there wasn't

unauthorized access to the Complainant's accounts.

8. Studying the Report in question, the Complainant returned on 21/12/2020

with a new request to my Office, since according to his position, he had identified

unauthorized access to his account on 10/5/2018 at 10:44am. from

the employee number XXXXX. With the new request, the Complainant was asking

as my Office examines the reason for said employee's access.

His bill, he said, was for a promissory note which

automatically renewed. Therefore, according to his position, it was not justified

accessed 10/5/2018, date not renewed. On this, the

The complainant attached statements of the disputed promissory note account,

from 21/12/2017 to 21/12/2018 where there did not appear to be any deposit or withdrawal of money to warrant access to his account. For the above question, my Office referred the Complainant to KEDIPES, as competent to answer it. On 1/15/2021, the Complainant addressed his question to KEDIPES. 9. KEDIPES replied on 19/1/2021 that the said employee number XXXXX, as was also the answer they had given on 20/7/2020, was authorized to have access for the purpose of performing his duties. KEDIPES reiterated that it additionally proceeded to carry out an independent investigation, in order to establish whether any of the Complainant's data was illegally processed. The investigation, which had already been communicated to the Complainant, did not reveal any findings that point to illegal processing of the Complainant's data by KEDIPES. 10. The Complainant did not find this explanation satisfactory and verbally informed my Office about it. He considered that KEDIPES had not answered his questions about the specific employee number XXXXX. My Office informed by phone the YPDS of KEDIPES, which then provided clarifications to the Complainant, with a letter dated 5/2/2021. The Complainant again did not find the answer he received satisfactory. KEDIPES had stated that the employee XXXXX at the material time was an authorized user and had the role of "treasurer". The employee in question is no longer an employee of KEDIPES and has also left the former SKT in 2018. An attempt was made on behalf of KEDIPES to contact him by phone, but it was not possible. Based on additional research carried out by the KEDIPES Technology Service, on 10/5/2018 it does not appear that any act of deposit or withdrawal was made to his account. However, as part of the cashier's duties, it is to be able to access a customer

account for various reasons and not only in the case of withdrawal/deposit, as for example in the context of the process of updating customer information, or in the event that a customer requests his account information by phone . On 11/5/2018, a certain amount had been transferred to Complainant 4's current account in order to pay his own check and possibly the previous day he had contacted the store by phone asking for information about his account balances. 11. The Complainant came back on 8/2/2021, rejecting the positions put forward by KEDIPES regarding a possible telephone communication between him and an employee of the former SKT, which would justify the access to his account on 10/5/2018, stating that if he wanted to know his balance, he could know through i-banking, which he handles. The fact that on 11/5/2018 he transferred an amount from one current account (Cooperative Savings Bank XXXXX) to another current account (Regional Bank of Nicosia), it has nothing to do with the disputed account XXXXX, which was not a current account, but a promissory note. He also ruled out the possibility that it had been accessed for the purposes of updating, since this takes place by written communication with the customer. He continued to ask and demand to be informed why the employee number XXXXX interfered with his account, without any official reason at all. 12. KEDIPES did not send any response to the Complainant's demands. The Complainant contacted my Office and my Office with KEDIPES by phone for this purpose, requesting information on whether they intend to respond to the Complainant. KEDIPES finally responded on 14/6/2021, essentially repeating its earlier positions and further clarifying that on 10/5/2018 where the employee had access to the Complainant's account, there is an access description written "Customer Account Information (Bulletin)'. According to the said description, the employee number XXXXX did not make any conversion and/or change and/or correction and/or deletion of any information in his account. On July 7, 2021, the Complainant communicated to my Office, a letter he sent in response to the letter from the YPDS of KEDIPES, according to which he still did not find the answer given to him satisfactory. According to the Complainant, the above employee interfered with his account without any reason. Further, it was his position that the independent investigation that had been carried out was not sufficient since it examined only two months of 2018 and not the entire year of 2018, as he had requested in his letters dated 27/12/18 and 7/1/20. The month of May 2018 was removed from the investigation. Therefore, he again requested to be informed of the reason why employee XXXXX interfered with his account, without any official reason at all. Legal Aspect 13. Article 4 of GDPR 2016/679 defines that "personal data" is "any information concerning 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, a 5 ID number, location data, an online identifier or one or more factors specific to

the physical, physiological, genetic, psychological, economic, cultural or social identity of the natural person in question...". Data controller is defined as anyone (the natural or legal person, public authority, agency or other body) who, "alone or jointly with another, determine the purposes and manner of processing personal data", the breach of personal data as "the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed", while ""third party": 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 ». 13.1 Related to the issue of data security are Articles 24 and 32 of the Regulation, where Article 24 states the controller's responsibility to "apply appropriate technical and organizational measures in order to ensure and be able to prove that the processing is carried out in accordance with this regulation.", and in Article 32 the controller's responsibility to implement the appropriate technical and organizational measures "in order to ensure the appropriate level of security against risks, including, among others, as the case may be: (…) b) the possibility ensuring the confidentiality, integrity, availability and reliability of processing systems and services on an ongoing basis". 13.2 "In the event of a personal data breach, the data controller shall notify the supervisory authority competent in accordance with article 55 without delay and, if possible, within 72 hours of becoming aware of the personal data breach if the breach of personal data is not likely to cause a risk to the rights and freedoms of natural persons. Where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a justification for the delay" (see Article 33(1) GDPR 2016/679). The controller also documents "each personal data breach, consisting of the facts concerning the personal data breach, the consequences and the corrective measures taken." This documentation allows the supervisory authority to verify the controller's compliance with Article 33 (see Article 33(5) GDPR 2016/679). 13.3 According to the Guidelines issued by the European Data Protection Board on personal data breach notification on October 3, 2017 and revised on February 6, 2018, “…a breach is a type of security incident” 6 which may arise either from an attack on the organization from an external source, or from internal processing, which violates security principles. 13.4 In Article 5 of GDPR 2016/679, the Principles governing the processing of personal data are mentioned, such as that the data must "a) be processed lawfully and legitimately in a transparent manner in relation to the subject of the data ("legality, objectivity and transparency"), b) are collected for specified, explicit and legitimate purposes and are not further processed in a manner incompatible with these purposes; ...("purpose limitation"), c) are appropriate, relevant and limited to what is necessary for the purposes for which they

are processed ("data minimization"), d) are accurate and, where necessary, updated; must be obtained all reasonable measures for the immediate deletion or correction of personal data that are inaccurate, in relation to the purposes of the processing ("accuracy"), e) are kept in a form that allows the identification of the data subjects only for the period necessary for the purposes of processing personal data; … ("limitation of the storage period"), f) are processed in a way that guarantees the appropriate security of personal data, including their protection against unauthorized or illegal processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality") . According to paragraph 2 of the same Article "The data controller bears the responsibility and is able to demonstrate compliance with paragraph 1 ("accountability")." 13.5 Article 15 par. 1 of GDPR 2016/679 provides that: "The data subject has the right to receive from the data 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...", while in par. 3 of the same Article it is stated that "The data controller shall provide a copy of the personal data being processed...". Rationale: 14. In the present case, the issues to be examined that arose and concern the provisions of GDPR 2016/679, are two. That of the satisfaction of the right of access to the activity logs of the Complainant's account (see Article 15 of GDPR 2016/679) and the possible leakage of information regarding the ability of the Complainant to repay what is required by the affidavit, amount, due to the sufficiency of account number XXXXX and/or other credit accounts (see Article 32 of GDPR 2016/679). 14.1 With reference to the first issue to be considered, although the former Cyprus Cooperative Bank was responsible for the processing, nevertheless during the disputed time when the activity logs of account 7 were requested the internal investigation of the Complainant, on 6/12/2018 the responsible for processing was KEDIPES, where it undertook to serve the Complainant, finally giving the files to the Complainant, after the mediation of my Office, on 20/7/2020. 14.2 With reference to the second matter to be examined, that of the possible leakage of information from employees of the Bank to the affidavit in Court, initially KEDIPES carried out an internal audit, which did not bear fruit, since it did not show that information had been leaked by KEDIPES. Subsequently, and since the Complainant was not satisfied with this result, KEDIPES commissioned an independent investigation by a third company. The result of the investigation, as reflected in the Report of this company, confirmed KEDIPES, since it did not detect unauthorized access to the Complainant's account. It was pointed out both by the Report, and verbally by KEDIPES, that the way in which the data was registered in the system of KEDIPES during the time in question, did not allow for an individual investigation into the disputed term account of the Complainant ("...access to the following

"programs" does not necessarily mean access to the specific account, as these programs produce downloadable reports containing multiple accounts, including the one under investigation"). Authorized users could view and obtain knowledge and/or even print results not only from the accounts of the Complainant, but also from the accounts of all customers in the context of their duties ("...who could download reports on their PCs with all customer information for their daily or monthly regulatory reporting requirements. Consequently, the account under investigation was included in most, if not in all, of these downloaded reports."). Although the main review period of the independent investigation was July-August 2018 (as the Complainant had identified his suspicions), however, in said investigation there is an Access Status to the customer's account, from all users, with print criteria the date from 01/01/2015 until 31/12/2019. The possibility was not ruled out that an employee of the Bank had recorded the results of the Complainant's account with other means (e.g. smart phone), but this could not be proven. For the sake of clarification, it was further stated in the Report that the account data is also stored in external facilities of the Bank's partner (Iron Mountain Incorporated). Finally, the investigation was carried out within the context of KEDIPES, due to the transfer of the Complainant's account from the former SKT to Hellenic Bank, which was completed in September 2019. 14.3 According to the definition given in Article 4 of GDPR 2016 /679, for there to be a breach of personal data, it should be proven, among other things, unauthorized disclosure or access to personal data. Furthermore, according to Article 5(1)(f) the controller has responsibility, among other things, for the appropriate security of personal data and its protection against unauthorized or 8 illegal processing. As can be seen from the wording of the Regulation, in the present case there was no unauthorized access to the Complainant's personal data, since the persons who had access to his accounts were authorized. There was also no illegal processing, since access to the Complainant's account was not found, by third parties who did not belong to the controller or by people who belonged to the controller and were not authorized to have access. 14.4 What may have been, is the unauthorized disclosure of knowledge, that the balances of the Complainant's account, and in particular the account number XXXXX, had a sufficient balance, so that he could satisfy the amount required by the Lawsuit. At this point it should be mentioned that the Complainant's suspicions should not be focused only on the employee number XXXXX, since any authorized employee who could have access to his accounts over time, could record either in the form of a note, or with the use of other means and/or even to keep a copy when printing an account statement (provided that anyway the Complainant's promissory notes were deposited before the specific event and were simply renewed upon expiry). Also within the scope of the duties of the authorized users of the Bank, there was also the possibility to print daily or monthly statements

with the data of all customers, including the data of the Complainant, from where any authorized employee of the Bank could obtain knowledge of the balances and the Complainant's account numbers. 14.5 In any case, the above are possibilities and suspicions, which cannot and/or have not been documented/proved at this stage. Although the affidavit submitted to the Court refers to a specific account number, knowledge of which the affidavit could in all probability have received from an employee of the Bank and with less probability from a relative of the Complainant who could have such information, however, the transfer of knowledge to the affiant has not been documented with tangible evidence and/or sufficiently, so that I can come to a finding that indeed, an employee of the Bank (SKT), before 3/9/2018 (date of affidavit), had transferred the information to the affidavit. Conclusion: 15. Bearing in mind the above, my conclusion is that the transfer of knowledge about the existence of sufficient balances in the Complainant's bank accounts, and in particular in account number XXXXX, by employees of the Bank (formerly SKT) has not been sufficiently documented I declared under oath. 9 16. When and as long as there are such elements that can document such a thing, the Complainant can either come back, or proceed with a complaint to the Police, which has the authority to examine beyond the possibility of leakage of the Complainant's personal data, on the basis of the Protection of Natural Persons Against the Processing of Personal Data and the Free Circulation of such Data Law of 2018 (L.125(I)/2018) and the possible commission of other criminal offenses by a former employee of the Cyprus Cooperative Bank .

Irini Loizidou Nikolaidou

Commissioner of Protection

Personal Data