No. Fax: 11.17.001.008.141 December 3, 2020 BY HAND Subject: Complaint against Astrobank Ltd Decision Following correspondence between us, in relation to the said complaint/complaint, I am informing you of the following: The complainant's positions on to Astrobank Ltd: 2. According to the content of the complaint (as presented through a letter from the complainant XXXXX, dated August 24, 2020 sent to Astrobank Ltd and communicated to my Office by the submission of the complaint on August 31, 2020), the complainant claims that his data has: (a) been illegally shared with third parties and (b) has not been updated to be presented as corrected. 2.1 Specifically, on May 26, 2020 the complainant wanted to create a bank account with Astrobank, for the company XXXXX, (the "company"), in his capacity as a Director of the company in question. The company in question already previously had an inactive account. According to his claim, various emails were exchanged between employees of the said company and a certain employee of Astrobank on this matter, which appeared to be proceeding for approval. On or about June 8, 2020, in a telephone conversation between the company's employees and the Astrobank employee, they were informed by the latter that the opening of the new account could not proceed, as the complainant was involved in an arms purchase in Syria and the His name was on OFAC's Specially Designated Nationals (SDN) sanctions list. The company employee informed the complainant and the complainant, offended that the employee had become privy to such information, instructed the company employee to send a relevant letter to Astrobank held by the US Treasury and dated XXXXX 2020, where he indicated that his name was no longer on that list. He then spoke complainingly on the phone with the Astrobank employee, explaining the matter. On June 13, 2020, it was made clear to the complainant that the opening of the account would not be approved. 1 2.2 The complainant considers that the rejection of his request was based on incorrect and non-updated information which the Bank used, at its own risk. The non-approval brings damaging consequences in relation to the processing of the said company's work. He further considers that there was an illegal disclosure to third parties (employees of Astrobank and XXXXX) of the incorrect information. According to the position of the complainant, Astrobank had a responsibility as it holds correct and up-to-date data and under no circumstances should incorrect data be known to third parties. Astrobank Ltd's response to the complainant's allegations 3. complainant's allegations, by letter dated August 31, 2020. He denied the complainant's claims that there was a telephone notification that his name was on the sanction list and therefore the account would not be opened. In relation to opening the account, they had generally made inquiries and after evaluating the application, decided to reject it. On the contrary, they say, they themselves were informed by a letter from the company requesting the opening of a bank account. 30/6/2020, regarding the inclusion of the complainant's name in the

sanctions list and in any case after the request has been rejected by the bank. The Bank had not requested that this letter be sent to it and denies the disclosure of information to the company's employees and therefore a violation of the complainant's personal data. Astrobank Ltd first responded to 3.1 Following a letter from my Office, Astrobank Ltd, in addition to the response they gave on August 31, 2020, also stated the following: 3.2 The OFAC lists and other lists are used in an advisory capacity on matters of compliance with the instructions of the Central Bank on issues of prevention, prevention and combating money laundering and terrorist financing and are updated on a continuous basis and are always up to date. The same lists also contain historical references, such as the complainant's name being on the OFAC list at some point and then being removed. The removal of the complainant's name was known to the Bank. Therefore, there is no question of improper updating. 3.3 The Bank rejected the complainant's request to open an account, after collecting and studying all the relevant information/documents for the purposes of evaluating the application. She had given no specific reason for her refusal to grant his request. Instead, it was an employee of his own company (after the Bank's negative response), who reported that XXXXXX's name was on the OFAC list, sending a letter to that effect on June 30, 2020. 2 3.4 Astrobank Ltd, did not disclose any information regarding her research and other personal data of the complainant to third parties and his allegations are unfounded. 3.5 They also noted that OFAC lists are public and freely accessible at https://sanctionssearch.ofac.treas.gov. /. The complainant's response to Astrobank Ltd's positions in relation to the above were as follows: 4. According to the complainant, Astrobank appears to be different from the initial position it put forward, that he had been informed by a letter from his company (dated 30/ 6/202) for the removal of his name from the sanctions list, now stating that they were aware of this fact. In its letter, Astrobank Ltd (dated 31/8/2020), had made no mention that they were ultimately aware of this fact. These allegations have now emerged. It is the complainant's position that the exact facts can be deduced from the content of the letter dated 6/7/2020 to Astrobank Ltd where it appears that at the time in question they were not aware that his name was no longer on the sanction list. 4.1 In the letter submitted by the complainant in support of his above positions (Exhibit 5), he seems to explain to the Bank the reasons for his inclusion in the said list of sanctions, but also for the removal of his name in the end, arguing that the company XXXXX is a healthy company, which already cooperates with two major Banks of Cyprus, without facing any problems. The letter ends, with the complainant stating that he would feel obliged to proceed with the opening of the account, which would help the company run smoothly. 4.2 The complainant further stated that before sending the letter dated 30/6/2020 from his employee to the Bank, preceded by a telephone communication in which the Bank employee stated that

the complainant was on the sanctions list. The complainant attached the employee's e-mail. 30/6/2020 with the Bank, to demonstrate, as he stated, that there was never an update of his personal data and that he never informed his employee that he was on the sanctions list in the past (Exhibit 6). 4.3 I note here that Exhibit 6 is a series of correspondence sent between an employee of the complainant and an employee of Astrobank on the subject of "OPENING OF A BANK ACCOUNT" and with the first letter starting on 26/5/2020 and the last letter being date 27/7/2020. In this correspondence, the employee acting on behalf of the complainant appears to provide Astrobank Ltd with the requested documents needed to open an account. 4.4 At this point I consider it important that I quote part of the content of Exhibit 6, consisting of five messages sent by 3 the complainant's employee to Astrobank Ltd, starting on 5/6/2020, 19/6/2020, 23/ 6/2020 and two on 6/30/2020. The first message of 6/30/2020 was sent at 10:42AM and the second a few hours later, at 1:49PM: "Dear Mr. XXXX, Please find attached the additional requested documents and please do not hesitate to contact me."

…… "Dear Mr. XXXX, Please find attached the following as requested: 1) Copies of ID Cards for XXXX. 2) Utility Bill of XXXXX. 3) Utility Bill of the company. 4) Financial Statements of the company. Thank you in advance Should you need any further clarifications or assistance, please do not hesitate to contact me." ……. "Dear Mr. XXXX, As per today's communication please find attached the Application for opening the account amended as requested and please proceed with the new Company account. Thank you in advance Should you need any further clarifications or assistance, please do nothesitate to contact me." …….. "Dear Mr. XXXX, After sending our last documents as you requested, please proceed with the opening of bank account. Thank you in advance. Should you need any further clarifications or assistance, please do not hesitate to contact me."

……. Dear Mr. XXXX, For the upgrade of your internal systems please find attached the Letter from U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). (Underlining mine) 4 Considering the attached please let us know for the reason of your refusal to open the company's account. (Emphasis mine) Thank you in advance" 4.5 Finally, the complainant stated that he never questioned whether the OFAC lists are public or not. What he raises is that his name from XXXXX 2020 until today is not in the result of the investigation. If someone does a search on XXXXX they will get the phrase "Your search has not returned any results." as a result. Therefore, if the Bank had relied on correct up-to-date information, on or about June 2020, this misinformation would not

have arisen. Finally, he considers that the Bank, as the controller of this data, relied on non-updated facts which it disseminated to third parties. Legal Aspect 5. 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, an identity number, location data, an online identifier or one or more factors specific to 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 ». 5.1 In the "Guidelines" issued by the European Data Protection Board on personal data breach notification on October 3, 2017 and revised on February 6, 2018, it is explained that personal data breaches can be categorized according to the following principles information security: "Breach of privacy" – when there is unauthorized or accidental disclosure of personal data or unauthorized or accidental access to personal data. 5 “Breach of integrity” – when there is unauthorized or accidental alteration of personal data. "Breach of availability" – when there is an accidental or unauthorized loss of access to personal data or accidental or unauthorized destruction of personal data." 5.2 Also according to the same Guidelines, it is clarified that "... a breach is a type of security incident" which can result either from an attack on the organization from an external source, or from internal processing that violates security principles. 5.3 Article 5 of GDPR 2016/679 states the Principles governing the processing of personal data, such as e.g. that the data must: "d) be accurate and, where necessary, updated; all reasonable steps must be taken to promptly delete or correct personal data that is inaccurate, in relation to the purposes of the processing ("accuracy "), 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")." 5.4 Articles 24 and 32 of the Regulation are also related to the issue of data security, where Article 24 states the responsibility of the controller to "implement 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 apply 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) of ability to ensure the privacy, integrity, availability and reliability of processing systems and services on an ongoing basis". 5.5 In Article 6 of the Regulation, in addition to the data subject having consented to a processing, other cases are mentioned where a processing of personal data is lawful, such as e.g. when: "b) the processing is necessary for the performance of a contract to which the data subject is a party or to take measures at the request of the data subject prior to the conclusion of a contract, c) the processing is necessary to comply with legal obligation of the controller,

……. f) the processing is necessary for the purposes of the legal interests pursued by the controller or a third party, unless these interests are overridden by the interest or the fundamental rights and freedoms of the data subject that require the protection of 6 personal data, in particular if the data subject is a child." 5.6 I should also add that according to recital 14 of GDPR 2016/679: "(14) The protection provided by this regulation should apply to natural persons, regardless of nationality or place of residence, in relation to the processing of data their personal nature. This regulation does not cover the processing of personal data concerning legal entities and in particular businesses incorporated as legal entities, including the name, type and contact details of the legal entity. 5.7 Furthermore, with regard to the Prevention and Combating of Money Laundering Law of 2007 (188(I)/2007), some passages related to this case are listed as follows: "58. An obliged entity shall implement sufficient and appropriate policies, controls and procedures, which are commensurate with its nature and size, to effectively mitigate and manage money laundering and terrorist financing risks in relation to the following: (a) The determination of identity and the exercise of due diligence regarding the customer, in accordance with the provisions of articles 60-66 of this Law ……

…….. (d) internal control, assessment and risk management for the purpose of preventing money laundering and terrorist financing;" "58A. (1) For the purposes of paragraph (d) of article 58, an obliged entity shall take appropriate measures in order to identify and assess the money laundering and terrorist financing risks it faces, taking into account risk factors, including those related to its customers, countries or geographical areas, products, services, transactions or banking service delivery channels: Provided that, these measures are proportionate to the nature and size of the obliged entity. (2) Those referred to in the subsection are updated and made available to the competent Supervisory Authority." 1 (1) risk assessments are documented, 5.8 According to Article 62 of the same Law: "(4) When an obligated entity cannot comply

with the due diligence requirements regarding its customer, as defined in paragraphs (a), (b) and (c) of subsection (1) of article 61, does not carry out a transaction through a bank account, does not enter into a business relationship or does not carry out the transaction, as the case may be, terminates said business1 The Law refers to the Central Bank of Cyprus as the competent Credit Supervisory Authority

Institutions (see Article 59).

relationship and is considering reporting a suspicious transaction to

relationship with the customer in the Unit, in accordance with the provisions of article 69.

Thinking:

6. In the present case, according to the facts that have been presented

in my Office, the complainant requested to create a new bank account

account with Astrobank Ltd, for the company XXXXX, (the "company"), under

his capacity as a Director of the company in question.

6.1 According to the position of the complainant, on or about June 8,

2020, an employee of Astrobank Ltd, in a telephone conversation he had with

employee of the complainant, informed that the opening of the account did not

could proceed as the complainant was involved in

arms purchase in Syria and his name was on the sanctions list

OFAC's Specially Designated Nationals (SDN). The complainant felt

offended and instructed the company employee to send her

relevant letter held by the US Treasury dated YYYY 2020, for removal

of his name from said list. He considers that the Bank, as responsible

processing of this data, was based on non-updated facts

which he disseminated to third parties (employees of Astrobank and XXXXX),

6.2 Astrobank Ltd, denies the complainant's allegations, stating

that he himself had informed them about this event on 6/30/2020. The bank

she had not requested that this particular letter be sent to her and refuses disclosure

information to company employees. The Bank rejected his request

complaining about opening an account, after collecting and studying them all

the relevant information/documents for application evaluation purposes. He did not have

state a specific reason for its refusal to grant his request.

The removal of the name of the complainant was known to the Bank and

therefore, there is no question of improper updating. In any case, the

OFAC lists as well as other lists are used

consulting on matters of compliance with the instructions of the Central Bank

on matters of prevention, prevention and combating legalization

proceeds from illegal activities and terrorist financing.

6.3 Having regard to the correspondence provided by the complainant,

the positions of the parties as such were advanced before me, in conjunction with the

provisions of GDPR 2016/679 and on Prevention and Combat

of the Legalization of Income from Illegal Activities Law, I conclude at

following findings:

(1) Any processing of personal data was carried out in

within the framework of a contractual relationship between the involved company XXXXX

and Astrobank Ltd (see Article 6(1)(b) of GDPR 2016/679).

(2) The information provided to the Bank for purposes

opening an account, which may contain personal data,

they did not only concern data of persons under their personal

capacity (e.g. home address), but also under their legal capacity, as

Directors, Secretaries

which do not

and Shareholders

companies,

8

are protected by GDPR 2016/679 as long as they are covered by

mantle of "legal entity".

(3) Astrobank Ltd acted in compliance with legal

obligation and especially for compliance with the Obstruction Act and

Fighting

from Illegals

Activities Law (see Article 6(1)(c) of the Regulation).

of Income Legalization

(4) In case it did not comply with the Law in question, it existed

case of being found liable for omissions and suffering administrative charges

sanctions (see article 59 of Law 188(I)/2007). So there was

possibly also the legal interest of the Bank, beyond the obligation

compliance with the relevant Law, to be protected from enforcement

sanctions (see Article 6(1)(f) of the Regulation).

(5) The correspondence produced by the complainant, to none

case does not show that it had preceded it in any form

information from Astrobank Ltd, to reject his request, v

or about 8/06/2020 as he claims, since up to 30/06/2020

the complainant's employee continued to send related documents

to the Bank, for the purpose of approving the opening request

account. In the second letter dated 30/06/2020,

employee of the complainant states that he is sending to

upgrading the Bank's internal systems, his letter

US Department of the Treasury's Office of Foreign Assets Control, and requests

at that point (well after June 8, 2020) to know

the reasons for refusing to open the account. Not in the first one

time letter, nothing more seems to be happening again,

indicating that there was some prior update from Astrobank Ltd.

(6) The Bank maintains that it had not stated a specific reason for the

her refusal to satisfy the complainant's request and no

is there anything in writing that proves otherwise.

Therefore,

correct

update or not, as long as there is no data around

from this issue.

any

examination

issue

is set

not

(7) In any case, the Bank in the context of exercising due diligence

custody, had the right not to enter into and/or terminate any

business relationship, in the event that he could not

comply with the requirements of the Law (see section 62(4)), which

it certainly does not concern GDPR 2016/679.

(8) Whether or not Astrobank Ltd now correctly assessed the risk;

on the basis of the evidence he collected, it is something which

is specialized in the Law (lex specialis), and refers to the Central

Bank of Cyprus, as the Supervisory Authority, for examination of this matter

(see Article 58(A)(2)). In any case, the Bank stated that the list

OFAC is advisory in nature and the assessment is not based

only to her.

(9) In the event that there was a question and there was any doubt cf

part of the Bank in relation to the inclusion of his name

complainant on a sanction list, the complainant could

to clarify it, as he did at some point between them

of correspondence exchanged (6/7/2020).

9

(10) Correspondence has not been shared with "third parties" and they have not

the complainant's data is breached, in the sense that

GDPR 2016/679 applies, since none had arisen

security breach that resulted in personal disclosure

data of the complainant to third parties.

(11) Furthermore, any exchange of information had taken place

under a legal basis, with employees of the responsible parties

processing (XXXXX and Astrobank Ltd). According to the GDPR

2016/679 the persons who are "under his direct supervision

controller or processor, is

authorized to process the personal data",

and do not fall within the definition of a "third" person.

from

third parties or failure to update personal data

Conclusion

Having in mind the above findings and according to the powers that I

provides Article 57(1)(f) of GDPR 2016/679 for investigation of complaints,

my conclusion is that the present complaint/complaint of the complainant

against Astrobank Ltd cannot be proceeded further since it does not

there has been a breach of the complainant's personal data and notification

in

of

complainant

due to

complaint/complaint, is rejected as unfounded.

Irini Loizidou Nikolaidou

Data Protection Commissioner

Personal Character

Ltd. Therefore,

Astrobank

the

in

10