No. Fax: 11.17.001.008.015 April 19, 2021 BY HAND Subject: Complaint for personal data breach DECISION Following the correspondence between us, in relation to the said complaint, I am informing you of the following: Facts: 2. The January 21, 2020 a complaint was registered in my Office by XXXXXX (hereinafter the "Complainant") in relation to a telephone call received on January 15, 2020 by an employee of Trust Insurance Ltd (hereinafter the "Ms") at telephone no. of XXXXX. He was told the call was to update customer profile information. When asked by the Complainant where they had found the phone number, the employee replied that she would research it and get back to you. Despite this, the employee did not come back, nor did she proceed with the issue of updating information. 2.1 Various letters were exchanged between my Office and the Complainant on the one hand, and my Office and the Defendant on the other. Various topics were mentioned within the correspondence exchanged. I will focus on the issue of the complaint though, which is how Trust Insurance Ltd came to know of the Complainant's Greek phone number. 2.2 The Complainant's position in relation to this matter is that the person who informed Trust Insurance Ltd of his Greek telephone number did so without his consent. He never consented and/or gave his approval to any person or employee of the company to share the relevant number. Nor was he informed by any employee so as to consent, either before or after this fact. He had a personal relationship with the company employee, which was terminated, prior to sharing his phone number. 2.3 After clarifications were requested, the Defendant's final position on how to obtain knowledge of the Complainant's Greek number, was that as the insurance profile employee assured them, she renewed the Complainant's 1 herself "in 2019, adding the Greek number his phone number, as an alternative contact phone number, at his request and/or after mutual agreement, as in the previous phone numbers that existed – one was not valid (that of the employee) and the other, which was his Cypriot number, was not answered and she was no longer to undertake to manage his contracts, since he himself was informed by her that she had given the said number.' This had been done “after the termination of their personal relationship. And he himself with their breakup, as she reports, told her to give it to whatever issues she still had pending ….. This was when their personal relationship was terminated so that the company would communicate directly with him. When in 2020 the relevant department failed to contact him about his contracts (one expired and the other was about to expire) he contacted our employee who provided them with the specific phone number (the one he had already registered and in the system)." It is the position of the Defendant that everything that followed constitutes vindictive actions against their employee, on the part of the Complainant. 2.4 Regarding the matter of updating the Complainant's information, the Defendant stated that it was not completed as the Complainant did not contribute and did not consent to its completion. Initially, the

Professor stated that they did not inform the Complainant about how to obtain knowledge of his new number after the employee called on January 15, 2020 and his related question, because speaking with the employee who had a personal relationship with him in the past and informing her about it, she had mentioned to them that she would undertake to inform him herself. Then followed the letter from my Office dated January 31, 2020, informing them of the registered complaint on behalf of the Complainant. They have no other number to reach him at. The employee then informed them that the Complainant was aware of the addition of his new phone number to the contact numbers. Finally, the Prosecutor clarified that her position is that the Complainant himself had reported to their employee after the termination of their relationship, "to give it to whatever issues he still had pending". 2.5 The Complainant, on the other hand, stated that he never refused to update information, since the employee who called him on January 15, 2020 did not return to inform him of the source of the knowledge of his new phone number, nor did the employee with whom he maintained a personal relationship, regarding her action to add his phone number to contact information. That is why he addressed my Office. 2.6 During the exchange of correspondence, the Complainant also put forward the position that the contracts were made without his knowledge and that he has learned about their payment, after the termination of his relationship with the employee in question. In any case, the Defendant presented the relevant insurance policies and/or proposals, which appear to have the signature of the Complainant. This position was denied by the Defendant, further arguing that for one of the two insurance policies, there were two compensation claims within the year 2019, with one being satisfied and the other pending. 2 2.7 I make it clear that whether or not the insurance contracts were legally binding is not something that will be examined by my Office. If the Complainant believes that there is forgery of contracts and or falsification of documents and or any other offense, he should report to the Police Authorities and follow the prescribed legal procedure. What I will examine is the legality of obtaining knowledge of the Complainant's Greek telephone number, in combination with the obligations of a data controller. 2.8 Bearing in mind the above facts, on February 5, 2021 I issued a prima facie decision against the Defendant for violation of Article 6(1)(a) GDPR 2016/679, i.e. the processing of personal data without the consent of the subject of the data. The Complainant was called upon to state the reasons why she believes that no remedial measure or administrative sanction should be imposed 2.9 On March 12, 2021 the Complainant replied essentially repeating the positions she advanced before the issue of the prima facie decision, as to how they came to know the Complainant's new telephone number. He also reiterated that the complaint was registered maliciously. In support of this position he sent a mobile phone screen print of messages, which were allegedly sent by the Complainant to the Defendant's

employee, with whom he had a personal relationship in the past. In these messages, insults and threats are expressed towards the person of their employee, such as e.g. "HHHHHH." Also attached was a Written Statement by the Defendant's employee, in which she described the relationship she had with the Complainant and the position that after their separation in August 2019, they agreed and had authorized her, that in the event that someone contacted her about any financial obligations of his, would inform him of the new telephone number. He also noted that the Complainant was constantly changing phone numbers. On the basis of their above agreement, the Complainant's contact information was updated in the Customer's systems, recording the new phone number. The previous number registered in the systems was already out of service. She has also given the new phone number to the school where her children attended, to the Police, to a Claimant's lawyer for the Complainant's debt in Athens and to other people who bothered her about his debts. 2.10 The Court also referred to the provisions of Article 7 of GDPR 2016/679 as well as recital (32), which explain the conditions for obtaining consent, the controller's burden of proof, the data subject's right to revoke per at any time his consent and that this does not affect the legality of the processing based on the consent, before the withdrawal, as well as the possibility that the consent was given orally. The Defendant considers that the Complainant's consent has been documented by the Written Statement of her employee, which describes the circumstances under which verbal consent was given. He also argued that the processing based on the prior verbal consent and 3 carried out with the telephone call to the Complainant on January 15, 2020, was lawful. With his refusal to proceed with an update and with his substantial objection regarding the manner in which the Defendant became aware of the phone number, the Defendant deleted his phone number and informed her employee about it. It is the position of the Defendant that despite the refusal, the processing at the time it was carried out was legal. 2.11 Despite the above, the Defendant stated that in the event that it is judged that the collectionof the oral consent of the Complainant, it was not under the circumstances n

best method that could be followed, to avoid the like

incidents, intends to take new corrective action. This will be either download

updating/changing information in writing, or by recording it

order, in case it is done by phone.

2.12 Finally, Kathy set out the mitigating factors that could

be taken into account, such as the double status of their employee (insurance company and

former partner of the Complainant), the deletion of his new number

Complaining immediately after his refusal for further use, the non

causing harm to the Complainant, the individual incident and the

ulterior motives behind the complaint.

Legal aspect

3. The General Principles governing the processing of personnel data

character, are reflected in Article 5 par. 1 of the GDPR

2016/679. "The controller bears the responsibility and is able to

demonstrate compliance with paragraph 1 ("accountability"). (see Article 5 par. 2)

3.1 In Article 6, par.1 of GDPR 2016/679, the legal bases are defined

according to which a processing of personal data

becomes legal. Among them, the fact that a processing may "be

necessary for the performance of a contract of which the data subject is

contracting party or to take measures at the request of the subject of

of data prior to the conclusion of a contract", or when "the data subject

has consented to the processing of his personal data for

one or more specific purposes'.

3.2 The legal basis on which a processing of personal data is based

character, is disclosed in the context of transparency and accountability of the person in charge

processing (see Article 5), to the data subject upon receipt

of his personal data (Article 13 of GDPR 2016/679). In case

this, the data controller must inform the data subject

data, among others, for "the purposes of the processing for which

intended for the personal data, as well as the legal basis for it

processing," in the event that "the processing is based on Article 6

paragraph 1 point f), the legal interests pursued by

data controller or by a third party," or "whether the provision of data

of a personal nature constitutes a legal or contractual obligation or requirement for the

conclusion of a contract, as well as whether the data subject is obliged

4

to provide the personal data and what possible consequences will

had the failure to provide these data".

3.3 According to the interpretation given in Article 4 par. 11, the consent

of the data subject is "any indication of will, free,

specific, express and full knowledge, with which the subject of

of data manifests that it agrees, by statement or by clear positive action, to

are the subject of processing the personal data that the

concern".

3.4 Recital (32) further explains that:

“Consent should be given by clear affirmative action which

to constitute a free, specific, explicit and fully informed indication

of the agreement of the data subject in favor of the processing of

of data concerning it, for example by written statement, between

others by electronic means, or by oral statement. This could

to include filling in a box when visiting

website, the selection of the desired technical settings

for information society services or a statement or

behavior that clearly states, in the specific context, that the

data subject accepts the processing proposal

intimate personal data. Therefore, the silence, the

pre-filled boxes or inactivity should not

taken as consent. Consent should cover the

set of processing activities carried out for him

purpose or for the same purposes. When processing has multiple

purposes, consent should be given for all of these

aims. If the consent of the data subject is to

given upon request by electronic means, the request must be

clear, comprehensive and not unreasonably disrupt its use

service for which it is provided."

3.5 Additionally, Article 7 explains the conditions governing the

consent-based processing as follows:

"1. When the processing is based on consent, the controller

processing is able to prove that the data subject

consented to the processing of personnel data

character.

2. If the consent of the data subject is provided to

context of a written statement which also concerns other matters, the request for

consent is submitted in such a way as to be clearly distinguishable from the

other matters, in

easily accessible format,

using clear and simple wording. Each section of the statement

which constitutes a violation of this regulation is not

binding.

3. The data subject has the right to revoke the

consent at any time. Withdrawal of consent does not affect

understandable

and

the lawfulness of processing based on prior consent

of its revocation. Before giving consent, the subject of

data is updated accordingly. Withdrawal of consent is

as easy as providing it.

4. When assessing whether consent is given freely,

particular consideration is given to whether, among other things, for execution

contract, including the provision of a service, is set as

consent to the processing of personal data is a condition

of a nature that is not necessary for the execution of the contract in question."

3.6 In relation to consent provided by express affirmative action, the

Guidelines 5/2020 issued by the European Protection Council

With regard to "Consent", they clarify the following:

"76. Article 2(h) of Directive 95/46/EC described consent as an “indication of wishes by which the data subject signifies his agreement to personal data relating to him being processed”. Article 4(11) GDPR builds on this definition, by clarifying that valid consent requires an unambiguous indication by means of a statement or by a clear affirmative action, in line with previous guidance issued by the WP29.

77. A "clear affirmative act" means that the data subject must have taken a deliberate action to consent to the particular processing. Recital 32 sets out additional guidance on this. Consent can be collected through a written or (a recorded) oral statement, including by electronic means.

78. Perhaps the most literal way to fulfill the criterion of a "written statement" is to make make sure a data subject writes in a letter or types an email to the controller explaining what exactly he/she agrees to. However, this is often not realistic. Written statements can come in many shapes and sizes that could be compliant with the GDPR.

79. Without prejudice to existing (national) contract law, consent can be obtained

through a recorded oral statement, although due note must be taken of the information available to the data subject, prior to the indication of consent. The use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice.

…… ..

94. …… . In theory, the use of oral statements can also be sufficiently expressed to obtain valid explicit consent, however, it may be difficult to prove for the controller that all conditions for valid explicit consent were met when the statement was recorded."

3.7 In the same Guidelines, the issue of how the controller to prove that consent has actually been obtained, stating the following regarding:

"104. In Article 7(1), the GDPR clearly outlines the explicit obligation of the controller to demonstrate a data subject's consent. The burden of proof will be on the controller, according to Article 7(1).

105. Recital 42 states: “Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation.”

106. Controllers are free to develop methods to comply with this provision in a way that is fitting in their daily operations. At the same time, the duty to demonstrate that valid

consent has been obtained by a controller, should not in itself lead to excessive amounts of additional data processing. This means that controllers should have enough data to show a link to the processing (to show consent was obtained) but they shouldn't be collecting any more information than necessary.

107. It is up to the controller to prove that valid consent was obtained from the data

subject. The GDPR does not prescribe exactly how this must be done. However, the controller must be able to prove that a data subject in a given case has consented. As as long as a data processing activity in question lasts, the obligation to demonstrate consent exists. After the processing activity ends, proof of consent should be kept no longer then strictly necessary for compliance with a legal obligation or for the establishment, exercise or defense of legal claims, in accordance with Article 17(3)(b) and (e). 108. For instance, the controller may keep a record of consent statements received, so he can show how consent was obtained, when consent was obtained and the information provided to the data subject at the time shall be demonstrable. The controller shall also be able to show that the data subject was informed and the controller's workflow met all relevant criteria for a valid consent. The rationale behind this obligation in the GDPR is that controllers must be accountable with regard to obtaining valid consent from data subjects and the consent mechanisms they have put in place in place. For example, in an online context, a controller could retain information on the session in which consent was expressed, together with documentation of the consent workflow at the time of the session, and a copy of the information that was presented to the data subject at that time. It would not be sufficient to merely refer to a correct configuration of the respective website."

contracts/proposals

Thinking

4. In the present case, from the facts before me, it is a given that they were used on January 15, 2020, by Kathy, data personal data of the Complainant, i.e. the Greek telephone number of, without it having been received directly by the Complainant himself at conclusion of the insurance agreement between them. He had neither therefore be informed within the framework of Article 13, that this number would match

processing. This number is not found in their copies

insurance policies

were presented

registered. There is also the admission of Ms. that this number

later registered in their system, the employee who had a personal

relationship with the Complainant in the past.

4.1 The position put forward by the Defendant to support this action is that the completion of the Greek telephone number was made after a request and/or in consultation with the Complainant. But it was Kathy's responsibility to present evidence to support this position (see Articles 5(2) and 7(1)). The Written Statement submitted by Kathy, her employee, after the issuance of the prima facie decision, the content of which essentially repeats them positions put forward by the Defendant cannot be considered satisfactory documentation of the information provided under the Regulation (Article 13) and receiving consent, even verbal (Articles 6 and 7) from the subject of data, even at the moment when the subject himself denies that he had given one such consent (see also Guidelines). Therefore, the claim

he has remained undocumented.

where

4.2 The Defendant further argued that the Complainant was not located at

phones which were initially registered in its systems, that the

Complaining that he kept changing phone numbers and that “When 2020

relevant department failed to contact him about his contracts (one

that expired and the other that was about to expire) contacted our employee n

which he supplied them with the particular phone number…”, adding

thus one more reason why communication had to be made with him

Complaining that his insurance policy would expire. Could

but alternatively, either it was a data update or an update

of the Complainant that his insurance policy would expire, to be sent

postal letter to one of the two addresses or to both, which he already had in

knowledge of the Defendant and had been added to the insurance contracts for purposes

of communication, which he did not do.

4.3 The fact that in the copies of

Insurance Proposals, which were submitted by the Defendant, incorrectly

the legal basis for the processing of personal data is referred to as consent

data of the Complainant, for purposes of insurance of his property. THE

correct legal basis is that of Article 6(1)(b), that is to say the processing (of

provided at the given time of personal data of the subject

of the data), "is necessary for the performance of a contract whose

data subject is a contracting party or to take measures under

request of the data subject prior to the conclusion of a contract'.

4.4 Incorrectly there is also a special provision, that in the event that the

contracting party does not provide his consent for the processing of

of his personal data, the Insurance Company will be entitled not to accept

the Proposal of the data subject, since it will not be able to process

otherwise his personal data. This denial definitely affects

adversely the interested party to be insured and in such a case, h

consent is not considered free (see Article 7(4)). This note, will

could be avoided if there was a clear legal basis for it from the start

whose personal data were collected, i.e. that of contract execution.

4.5 The same applies to the acceptance of any advertising shipment

messages, the recording of any telephone conversation possible

has a client with staff

her

monitoring and/or filming in and around Ms.

her Anything not directly related to the purposes of the contract between

Insurer - Insured and the insured product cannot be "put as

consent to the processing of personal data is a condition

which is not necessary for the performance of the contract in question" (see Article 7(4)).

Conclusion

5. Bearing in mind the above facts as listed, and based on them

powers conferred on me by Articles 58 and 83 of Regulation (EU)

2016/679, article 24(b) of Law 125(I)/2018, I find that there is a violation of

of the Insurance Company and

8

of Trust International Insurance Company (Cyprus) Ltd of Article 6(1)(a)

of GDPR 2016/679. The infringement lies in the processing of data

of a personal nature without the consent of the data subject,

since he collected and used his Greek phone number, without o

this number must have been received by him at the time of the start of the contract

your relationship. The Claimant's claim that it was given to her has also not been proven

subsequent oral consent, as had the burden of proof.

5.1 Applying the powers granted to me by Article 58(2) of the Regulation

and after taking into account all the mitigating factors he raised

my Kathy, as:

-

-

-

-

-

-

the dual status of their employee (insurer and person with whom

the Complainant had a personal relationship),

the deletion of the new number of the Complainant immediately after the refusal

of for further use,

not causing harm to the Complainant,

the individual incident,

Kathy's cooperation, as well as

its intention to take general corrective action in the manner of handling

of similar incidents, I consider it right that none be imposed

administrative sanction measure in the present case.

5.2 However, it is emphasized that this complaint will be a precedent, in

case of submitting a new complaint. In such a case any

new complaint in which a violation of GDPR 2016/679 may be found,

will be dealt with more severely.

Irini Loizidou Nikolaidou

Data Protection Commissioner

Personal Character