No. Fax: 11.17.001.009.056 March 4, 2022 BY HAND DECISION Collection of e-mail address when connecting the data subject to the Wi-Fi service of The Mall of Cyprus (MC) Plc Referring to the complaint submitted to My office, in relation to the subject under reference and with fax no. 11.17.001.009.056, I bring to your attention the following: Incidents of the Case: 2. On April 6, 2021, a complaint was sent to my Office by XXXXXX (hereinafter "the Complainant"), who attached relevant correspondence that he had exchanged with the Responsible Data Protection Officer (DPO) of The Mall of Cyprus (MC) Plc (hereinafter "the Complainant" company). In the correspondence, the Complainant expressed various concerns, some of which were answered and/or resolved before the relevant complaint was sent to my Office. What remained to be investigated in relation to the Complainant's complaint, was the condition placed on a person using wireless networking (Wifi), such as first filling in his electronic address (email) in the corresponding field, in order to be provided this service. 2.1 The defendant filed the complaint in a letter dated March 29, 2021 to the Complainant, based this condition on Article 6(1)(f) of Regulation (EU) 2016/679 (hereinafter "the Regulation"), clarifying that by using the electronic address Ms. the complaint could identify "new users" as potential new potential visitors/customers. The e-mail address makes it possible to identify "new users" more precisely than with other methods, while the rights of the data subjects remain unaffected. He referred the Complainant to the Policy Statement which states that "The personal data collected through the connection process to our free Wi-Fi is not used for purposes also the YPD 1 of direct marketing and is only used for statistical reasons", adding that the data collection is compatible with Article 5 of the Regulation and the principle of minimization, since the data collected is limited to what is absolutely necessary for the specific purpose. 2.2 In connection with the above response, my Office on August 18, 2021 sent a letter to the Complainant, requesting clarification on various issues, as follows: (a) How did it come to the conclusion that the data collected is the absolute necessary for the specific purpose? (b) What other methods did she consider before settling on this particular method as the most appropriate, for the purposes of identifying new potential visitors/customers more accurately? (c) What is the legal interest (benefit) arising for the company by identifying the new potential visitors/customers? (d) What appropriate guarantees have been taken regarding the rights and freedoms of the data subjects, if the data collected is used for statistical purposes? (e) Has he applied the provisions of Article 89(1) of the Regulation? (f) Has an impact assessment been carried out (see Article 35 of the Regulation)? (g) For how long are the e-mail addresses of visitors/customers kept after they visit the site and connect to the free internet service and in what form? (h) Is the subject informed before using the free internet service and what information is provided? 2.3 On September 14, 2021, the

Complainant, in relation to the above questions, clarified the following: (a) They ended up choosing to request an email address, as the mildest and least intrusive measure for the purposes of locating new visitors to its facilities. There is no verification of the e-mail address and it is possible for someone to declare a fictitious address and connect again, in contrast to other cases of providing free WiFi known in Cyprus, Greece, Italy, France, Romania, Bulgaria and Germany where the subject is asked to declares an e-mail address, then a relevant link is sent to the address he has declared and he is asked to activate the link in order to be provided with the service. In the present case, information is requested which is not always personal data in the event that the subject has not declared his real address. (b) Many solutions were studied that are applied both in Cyprus and Greece, as well as at the EU level and concern the provision of free WiFi by businesses in the industry (Mall) or other types of businesses such as companies in the catering industry (cafes), stadium operating companies or airports etc. Several e-mail (which most verify), device name, online identifier, i.e. Internet Protocol (IP) address, mobile phone number and in rarer cases and businesses receive 2 residential address. In most cases the details are verified, either by sending a message to the mobile phone or email with a link to activate the WiFi download after verification. Kathy gave as an example the complaint of Eleftherios Venizelos Airport in Athens, where according to their position, the user's mobile phone number, e-mail address and IP address are collected during the connection. As a second example, the Complainant cited the case of the company Apifon in Greece, which is a service provider and offers related services in various Malls in Greece, and which asks the user for a mobile phone number and email address, the which the user then has to activate in a link he will receive in the declared email address, which means that it must be real and active, before he can access the WiFi. (c) Their legal interest is twofold. First, the Mall of Cyprus rents space within its premises. Providing free WiFi as a service is used to attract tenants. This is done on the basis of certain statistics that it presents to interested tenants such as the number of visitors on weekdays, weekends and holidays, but also the number of first-time visitors as opposed to regular visitors. The progress rate of new guests is an important consideration for tenants in deciding whether to rent. For the same reason, that is to attract tenants, the Complainant organizes events. It is an important element to recognize visitors during an event to measure its effectiveness, so that decisions can be made to repeat it or not. Secondly, the Complainant must maintain its WiFi provision at a satisfactory level in order to satisfy guests and tenants and maintain its market leadership position. That is why they must control the number of users connected, depending on the capacity of the infrastructure (bandwidth, simultaneous users, etc.). That is, what is required in ISO 27001 is called Capacity Management. This comes as a mandatory field in relation to the requirements of ISO

27001, with which Mall of Cyprus complies. (d) The greatest guarantee is the possibility provided to the subject to provide a false e-mail address, as no cross-checking is done, nor is verification required. In addition, the appropriate technical and organizational measures mentioned in field (e) below are also applied. (e) The provisions of Article 89(1) of the Regulation have been applied by definition, since all the measures provided for by the ISO 27001 standard that is followed (secure storage, access, etc.) are included. The principles of Article 5 are also followed. (f) No impact assessment has been carried out since the processing in question does not fall under any of the cases a or b or c of Article 35 paragraph 3 of the Regulation. The impact assessment in accordance with Article 35 shall be carried out before the processing. This is not a new treatment but 3 pre-existed the Regulation. The Defendant of the complaint has carried out an impact assessment for the CCPPs, which, although they existed before the Regulation, are nevertheless included in case c of Article 35 par. 3. Nevertheless, even if an impact assessment were carried out, it would not be able to offer reduction measures risk as (a) there is no risk due to the possibility of natural persons to declare a false e-mail address and (b) all appropriate technical and organizational measures are applied for all processing. (g) E-mail addresses are kept for a period of one month andthen they are destroyed by permanent deletion (via overwrite). The information is not used for marketing purposes. (h) Natural persons are informed by both the Privacy Policy (Greek and English) and the terms and conditions Policy. There it is announced that the e-mail address is not used for marketing purposes, as well as all the other necessary points in accordance with Article 13 of the Regulation. Legal Aspect: 3. In Article 4 of GDPR 2016/679 personal data is interpreted as "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 the physical, physiological, genetic, psychological, economic, cultural or social identity of the natural person in question", the processing as "any act or series of acts carried out with or without the use of automated means, on personal data or sets of personal data, such as collection, registration, organization, structuring, storing, adapting or changing, retrieving, searching for information, using, communicating by transmission, dissemination or any other form of disposal, association or combination, restriction, erasure or destruction" and as controller "the natural or legal person, public authority, agency or other body which, alone or jointly with other , determine the purposes and manner of processing personal data; where the purposes and manner of such processing are determined by Union law or the law of a Member State, the controller or the specific criteria for his appointment may be provided by the Union law or the law of a Member State'. 3.1 The

General Principles that govern the processing of personal data are reflected in Article 5 par. 1 of the Regulation. One of them concerns the Principle of Data Minimization which establishes Article 5(1)(c) of the Regulation and obliges the data controller to ensure that the data it collects "is appropriate, relevant and limited to what is necessary for the purposes for the which are processed (``data minimization'')'. In any case, "The controller bears responsibility and is able to demonstrate compliance with paragraph 1 ("accountability"). (see Article 5 par. 2) 3.2 In Article 6, par. 1 of the Regulation, the legal bases are defined according to which a processing of personal data becomes lawful. Among them, when "the data subject has given consent to the processing of his personal data for one or more specific purposes", or when processing "is necessary for the performance of a contract to which the data subject is a party or to measures are taken at the request of the data subject prior to the conclusion of a contract", or when "the processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, unless these interests are overridden by interest or fundamental rights and the freedoms of the data subject which require the protection of personal data, in particular if the data subject is a child." (see paragraphs (a), (b) and (f) respectively and Corrigendum to the Regulation dated 4.3.2021). 3.3 The legal basis on which a processing of personal data is based, is disclosed in the context of transparency and accountability of the data controller (see Article 5), to the data subject when receiving his personal data (see Article 13 of the Regulation). The data controller must (in the event that the data subject does not already have this information) inform, among other things, about "the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing," and in the event that "the processing is based on Article 6 paragraph 1 letter f), the legitimate interests pursued by the controller or by a third party," (see par. 1 paragraphs (c) and (d). Additionally, the controller processing may inform, among other things, about "whether the provision of personal data constitutes a legal or contractual obligation or a requirement for the conclusion of a contract, as well as whether the data subject is obliged to provide the personal data and what possible consequences it would have the non-provision of such data" (see par. 2 subsection (e)). 3.4 According to the interpretation given in Article 4 par. 11, the consent of the subject of the terms is "any indication of will, free, specific, fully informed and indisputable, by which the data subject manifests that he agrees, by statement or by a clear positive action, to be the subject of processing of the personal data concerning him" (see . also Corrigendum to the Regulation dated 4.3.2021). 3.5 Recital (32) further explains that: "Consent should be provided by a clear affirmative action which constitutes an identifiable and unmistakable indication of the data subject's agreement in favor of the processing of data concerning him, for example free, specific , in full 5 by written statement, including by electronic means, or

by oral statement. This could include filling in a box when visiting a website, choosing the desired technical settings for information society services or a statement or behavior that clearly states, in the given context, that the data subject accepts the processing proposal of the relevant personal data. Therefore, silence, pre-filled boxes or inaction should not be taken as consent. Consent should cover all processing activities carried out for the same purpose or for the same purposes. Where processing has multiple purposes, consent should be given for all those purposes. If the data subject's consent is to be given upon request by electronic means, the request must be clear, comprehensive and not unreasonably disrupt the use of the service for which it is provided." (see also Corrigendum to the Regulation dated 4.3.2021). 3.6 Also according to recital (42): "... Consent should not be considered freely given if the data subject does not have a genuine or free choice or is unable to refuse or withdraw consent without prejudice ." 3.7 Additionally, Article 7 explains the conditions governing consent-based processing as follows: "1. When the processing is based on consent, the controller is able to prove that the data subject consented to the processing of the personal data. 2. If the data subject's consent is provided in the context of a written statement that also concerns other matters, the request for consent shall be submitted in a way that is clearly distinguishable from the other matters, in an understandable and easily accessible form, using clear and simple wording . Any part of this statement that constitutes a violation of this regulation is not binding. 3. The data subject has the right to withdraw his consent at any time. Withdrawal of consent does not affect the lawfulness of processing that was based on consent prior to its withdrawal. Before giving consent, the data subject is informed accordingly. Withdrawing consent is as easy as giving it. 4. When assessing whether consent is given freely, particular consideration is given to whether, among other things, for the performance of a contract, including the provision of a service, consent to the processing of personal data that is not necessary for the performance of the said contract." 6 3.8 In relation to consent and whether it is given freely, the Guidelines 5/2020 issued by the European Data Protection Board clarify the following: "13. The element "free" implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid. If consent isbundled up as a non-negotiable part of terms and conditions it is

presumed not to have been freely given. Accordingly, consent will not

be considered to be free if the data subject is unable to refuse or withdraw

his or her consent without detriment. The notion of imbalance between the

controller and the data subject is also taken into consideration by the

GDPR.

14. When assessing whether consent is freely given, one should also

take into account the specific situation of tying consent into

contracts or the provision of a service as described in Article 7(4).

Article 7(4) has been drafted in a non-exhaustive fashion by the words

"inter alia", meaning that there may be a range of other situations, which

are caught by

terms, any element of

inappropriate pressure or influence upon the data subject (which may be

manifested in many different ways) which prevents a data subject from

exercising their free will, shall render the consent invalid."

"32. Article 7(4) is only relevant where the requested data are not

necessary for the performance of the contract, (including the provision of a

service), and the performance of that contract is made conditional on the

obtaining of these data on the basis of consent. Conversely, if processing

is necessary to perform the contract (including to provide a service), then

Article 7(4) does not apply."

this provision.

In general

3.9 In the same Guidelines, the provision of services is given as an example

photo editing through a mobile app, in exchange for

collection of user data for targeted advertising purposes;

According to the example, consent obtained from the user, no

can be considered as free, since if it does not allow processing it does not

may receive said service.

"Example 1: A mobile app for photo editing asks its users to have their GPS localization activated for the use of its services. The app also tells its users it will use the collected data for behavioral advertising purposes. Neither geolocation nor online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.

3.10 According to Article 35(1) when a type of processing “may poses a high risk to the rights and freedoms of individuals

of persons, the controller carries out prior to processing, assessment of the effects of the planned processing operations'. The assessment impact is required in particular in the case where there is:

"a) systematic and extensive assessment of personal aspects in relation with natural persons, which is based on automated processing, including profiling, and on which they rely decisions that produce legal effects about the physical person or similarly significantly affect the natural person,

b) large-scale processing of special categories of data that referred to in article 9 paragraph 1 or personal data character involving criminal convictions and offenses which referred to in article 10 or

c) systematic monitoring of publicly accessible space in large scale. (see par. 3)."

3.11 In Guidelines WP 248 rev. 01, in relation to the assessment of the impact on data protection (DPA) and its determination whether the processing "may entail a high risk" for the purposes

of regulation 2016/679, it is clarified that the cases which

referred to in par. 35 paragraph 3, are indicative. "When it's not

clear as to whether it is necessary to carry out an EAPD, the Article 29 working group

recommends that an EAPD be carried out, as in any case it is a useful tool

for controllers in order to comply with

data protection legislation." “There may be acts

"high risk" processing that are not included in that list,

but they involve correspondingly high risks." “These processing operations will

they must likewise be subject to a DPA. For this reason, the criteria that

listed below sometimes fall short of a simple explanation of what will

was to be understood by the three examples of Article 35(3) thereof

GDPR."

3.11.1 Nine criteria are also defined which should be used by

controllers in order to determine whether they should

conducted a data protection impact assessment (DPA) or not. Compared with

the definition of large scale are taken into account (a) the number of

of involved subjects either as a specific or as a percentage of related

population, (b) the volume of data and/or its scope, (c) the duration or o

permanent nature of the processing and

(d) its geographical scope

activity.

3.12 According to recital (71):

“The data subject should have the right not to

subject to a decision, which may include some

measure, which assesses personal aspects that the

concern, obtained solely on an automated basis

processing and which produces legal effects against him

of that person or significantly affects it in a similar way,

8

such as automatically denying an online credit application or practices

of electronic recruitment without human intervention. Processing

this includes "profiling" consisting of

any form of automated data processing

personal to assess personal aspects

relating to a natural person, in particular analysis or prediction

aspects related to performance at work, financial

condition, health, personal preferences or interests, the

reliability or the behavior, location or movements of the subject of

data, to the extent that it produces legal effects against him

person thereof or significantly affects it in a similar manner. However,

making a decision based on it

processing,

including profiling, should be allowed

when expressly provided for by the law of the Union or a Member State, in

to which the controller is subject, including for purposes

monitoring and prevention of fraud and tax evasion

according to the regulations, standards and recommendations of the institutions

bodies of the Union or national supervisory bodies and in order

to ensure the safety and reliability of the service provided by

controller, or when it is necessary for the conclusion or the

execution of contract between data subject and controller

processing or when the data subject provided the express

his consent. In any case, this treatment should

be subject to suitable guarantees, which should

include specific information of the data subject

and the right to secure human intervention, the right

expression of his opinion, the right to receive justification thereof

decision taken in the context of said assessment and the right

challenging the decision. This measure should not concern

child."

her

Thinking:

4. In the present case what is being examined is the provision of electronics

address from a subject to the Complaint, for purposes

connection to the wireless network service (Wi-Fi).

4.1 In the policy statement, which is posted on the website of the

of the complaint

(https://mallofcyprus.com/terms-privacy/), is updated

data subject how his personal data is collected, between

other cases and when connecting to the wireless network ("When

you are connected to our Wi-Fi"). It is also informed that the collection of

given these is done after his consent and after he accepts them

terms and conditions set by the Complainant in order to

the service is provided. ("Purposes of Processing & the Legal Bases of Data

Processing ….. Consent: ….. when you agree with the terms and conditions in

order to connect to our wireless network").

9

4.2 The Defendant reported the complaint in writing to the Complainant and subsequently

in my Office, how the legal basis for the provision by the subject of

data of his electronic address in order to give him access

in the service, is based on Article 6(1)(f) of the Regulation, i.e. on the law

interest.

4.3 In fact, the Complainant benefits from this procedure,

which is the collection of the subjects' personal data, the

which he then uses for the purposes he has mentioned. THE

however, providing the data of the subjects to the Client, takes place afterwards

obtaining consent and after the subjects accept the terms and

terms and conditions set as a prerequisite.

Therefore, the legal basis of the Complaint for the collection of

personal data is not the legitimate interest (Art

6(1)(f)), but consent (Article 6(1)(a)), as is the information that

gets the subject from the policy statement.

4.4 Access to the service takes place only when and if the subject of

data accept the terms and conditions. The defendant did not file the complaint

has presented to my Office the terms and conditions. But it follows

how is included and/or should the update be included, how

main reason for the collection of personal data is

their processing for statistical purposes, as stated in the declaration

policy. In other words, a contractual relationship is created, since for the provision of one

service an exchange is requested (offer and acceptance). In such a case,

according to Article 7(4) of the Regulation it is taken into account whether for the

execution of this contract and the provision of the service, is set as

consent to the processing of personal data is a condition,

which processing is not necessary for its execution. The Guidelines

Lines 5/2020 clarify that when consent is grouped as non

negotiable part of the terms and conditions, then it is presumed that she

not freely given. This also reflects the explanation given in

recital (42) of the Regulation since, as in the present case,

if the data subject does not provide consent for the

processing, will be harmed by not providing access to the service.

Accordingly, any consent obtained from

4.5

data subject in the present case, it is presumed not

it has been freely given. Nor do I consider it necessary to edit it

electronic address of a subject, in order to be able to become

able to access the service.

4.6 The purposes for which Kathi invokes the complaint against her

service of its legitimate interests, could be achieved with the

finding other, less intrusive and/or invasive means for

rights of subjects.

4.7 I also consider that the method now used by Kath

complaint, does not serve exactly the purpose it invokes, namely

10

counting the number and frequency of visits to its premises,

provided (a) the user may use a false email address;

which it can change every time it connects to the network and not

lead to the verification of his identification, (b) are not necessarily linked

all visitors with Cathy's wireless network during their visit and (c)

the categorization, according to what the Court has mentioned, is carried out internally

one month from the last registration, and the electronic

address after the expiration of this time period, is deleted.

4.8 In relation to the purpose invoked by the Defendant in relation to the network management (Capacity Management) again can be found other ways, less intrusive and/or intrusive towards their rights subjects, since for the measurement of the capacity of the infrastructure (range zone, concurrent users, etc.), personal collection is not required data, but the measurement of all connected devices and/or o volume of data used through the network.

4.9 Consequently, I consider that the reasons invoked by Ms complaint cannot be accepted, as long as there are other ways less intrusive and/or intrusive towards the rights of the subjects. In based on this conclusion, I consider that Kathleen collects the complaint more data than is necessary in relation to the purposes which it invokes, as much as to enable the service to be provided wireless network to its guests, in violation of its principle minimization (Article 5(1)(c) of the Regulation).

4.10 Now in relation to the view expressed by the Defendant in the complaint that there was no need to carry out an impact assessment and the reasons for it invoked, it should be mentioned that the cases referred to in the Article 35(3) of the Regulation, are indicative. Even if it is not clear necessity of impact assessment, its implementation is a useful tool for the controllers in order to comply with the Regulation.

In the present case, however, with what the Defendant has mentioned in the complaint I believe that a systematic evaluation of personal aspects of subjects and monitoring them in a publicly accessible space, in large scale. The processing results in the “profiling” of the subjects,

since their personal aspects are evaluated, such as the frequency of visits

at the site of the Complainant. Although the Defendant informs the Complaint

the data subjects that their data is used for

statistical purposes, does not inform about the fact that it proceeds to

this ("profiling") processing. I therefore think that Ms.

of the complaint to have carried out an impact assessment on the processing, so

so that the necessity and proportionality in relation to the purpose had been assessed, h

assessment of risks and impacts to data subjects, such as

and the prescribed measures to deal with them.

Conclusion:

11

5. On the basis of the above findings and the authority provided to me by the

Article 57(1)(a) for monitoring and enforcement of the Regulation and Article 58(2)

for imposing remedial measures where and where necessary and exercising the powers

these and in particular the powers granted to me by subsection (d) of Article 58(2)

of the Regulation, I decide and issue the following orders:

5.1 The Mall of Cyprus (MC) Plc is instructed to:

(a) Stop collecting the email addresses of its subjects

data, and

(b) Delete any e-mail addresses collected for provision purposes

access to the wireless network service.

5.2 In light of my instructions as above, it is provided to The Mall of Cyprus

(MC) Plc, exclusive deadline to comply with the above, within one

month from the date of receipt of this Decision. At the end of it

one month, the Complainant to inform my Office about the actions

in which he has undertaken.

Irini Loizidou Nikolaidou

Data Protection Commissioner

Personal Character

12