

Republic of Cyprus

No. Phone: 11.17.003.012.002

OFFICE OF THE SECURITY COMMISSIONER

PERSONAL DATA

character

DECISION

Report receiving unwanted calls

Incidents of the Case

Positions of the complainant

In the complaint, as well as in a letter from the complainant dated 25

Pursuant to the duties and powers conferred on me by section 57(1)(f) thereof

Regulation (EU) 2016/679 for the protection of natural persons against

processing of personal data and for free movement

of these data (hereinafter the "Regulation"), I examined a complaint submitted to

My office on April 10, 2021 regarding spam calls received by Mr. XXX

(hereinafter the "complainant") from Epic Ltd.

Based on the investigation, I found a violation of the Regulation by the company Epic Ltd

(hereinafter the "Teacher") and, therefore, issue this Decision.

A.

2.

May 2021, the following was reported:

2.1. the complainant was receiving, on XXX's phone number, unanswered calls

phone calls from the number XXX, at inappropriate times, such as noon or

Saturday, while in case he had time to answer these calls, the calls

were interrupted

2.2. on April 10, 2021, the complainant contacted her customer line

To her, at number 136, informing about the calls she received from the person in question
phone number and stating that he is not a client of Ms. The complainant
he received the answer that this number belongs to the sales department of Kathy and that
he should not receive such calls, since he is not a client of the Defendant,

2.3. the complainant considers the specific calls to be a violation of
his personal data.

3.

she replied on June 9, 2021, the following:

In response to a letter from my Office, dated May 26, 2021, Prof.

Professor's positions

Iasonos 1, 2nd floor, 1082 NICOSIA / PO Box 23378, 1682 NICOSIA. Tel: 22818456, Fax: 22304565

E-mail: commissioner@dataprotection.gov.cy, Website: <http://www.dataprotection.gov.cy>

In response to a letter from my Office, dated September 3, 2021,

taking the incident very seriously, instructions were given to re-check it

3.1. the complainant's phone number belonged to a client of the Defendant and,

July 2020, had been transferred to another telecom provider. Hence at

in the past there was a customer relationship between the Customer and the owner of the number, and

this number was in the telephone directory of Kathy's customers,

3.2. the complainant's phone number "was in the phone book

customers" of Ms. "and incorrectly during the termination of the services o

certain number was not removed from the list and therefore they have been made

phone calls",

3.3. after the complainant's call, as referred to in point 2.2. her

present, "it had been realized by the sales team that the number did not belong to

our existing customer and immediately stopped making calls to this number

and removed from the customer list",

3.4.

specific customer list to avoid such cases,

3.5. it was not her intention to disturb or elaborate further

personal data of the complainant.

4.

She informed my Office, on September 10, 2021, about the following:

4.1. the complainant's telephone number before being transferred to another provider,

belonged to the complainant,

4.2.

the results of the review of the specific customer list showed

that "numbers of customers whose customer base had been included by mistake

"relationship" with Ms. "had ended",

the number of telephone numbers contained in the customer directory is 6845,

4.3.

while the number of telephone numbers that the directory should not contain

customers are 332 and the relevant numbers have been removed,

4.4. it was not her intention to disturb or elaborate further

personal data of persons with whom it does not maintain a customer relationship, nor purpose

of calling people who are not its customers.

5.

Madam, who informed me, on January 17, 2022, about the following:

5.1. "a call was made to all 332 numbers that

inadvertently

were listed", but no message has been sent to them

these numbers,

5.2. the portability policy (transferring the customer's number to another provider) which

follows Kathy when she is asked by customers to transfer to another provider, it is in accordance with the Decree on Number Portability of the Communications Commissioner (KDP 64/2017), and Law 112(I)/2004, article 75, as amended. This policy attached to Ms letter to my Office,

5.3. the Lady repeated that it was not her intention to disturb persons who had cease to be its customers or to further process their personal data,

5.4. the time of deletion of customer data with which it ceases to have contractual relationship with Kathy, is indicated in the data deletion policy and depends on the type of data. Kathy's data deletion policy

is being revised and the revised policy will be sent to my Office, when the review process is complete. However, Kathy sent to the On January 4, 2022, I sent a letter with clarifying questions to

2

My office the policy that was in force at the given time (Data Retention Policy, V1.2, with a release date of September 9, 2020).

5.4.1. Ms.'s data deletion policy, which was submitted to my Office,

includes the following categories of personal data ("Personal Data categories'):

invoices

"A. Customer Data - your name, surname, national identification number / passport number, email address, residence and billing address, contact number(s), payment records,

issued per service per month, details of authorized

representatives per contract, direct debit details (where needed), debit or credit

card details (where needed), any customer preferences (where needed), voice

recordings and complaints filed through epic call center or through any other

support channels of epic

B. Telecommunication / traffic and Billing data – location data, called subscriber number, date, starting time and duration of the calls made and/or the data volume transmitted, IP address, internet browsing, number of identification of subscriber devices, details of modem data, TV traffic data, Set Top Box data, TV channels and programs watched, Video on Demand (VOD) data, billing records;

C. CCTV data - Closed Circuit Surveillance System processing in epic stores and other premises where needed for security purposes.

D. Voice Recordings»

5.4.2. The retention period of data belonging to category A. Customer

Data, are:

"1. Throughout the validity of the contract for active customers.

2. Upon contract expiration or termination the following data are not erased:

(a) Data maintained for law enforcement purposes when lawfully requested to do so by a Court of law (Law 183(I)/2007) (minimum 6 months).

(b) Data maintained for the purposes of taxation legislation (Law 95(I)/2000 and Law 4/1978), which are maintained for a period of six (6) years and up until a tax clearance is provided.

(c) Data processed for the purposes of legitimate interest (e.g. an action against a customer), which are maintained until the legitimate purpose is completed.

(d) Payment information referring to SEPA Direct Debit payments and information referring to the corresponding invoices settled which shall be maintained for a period of thirteen (13) months as per the SEPA rules."

On October 10, 2022, I sent you a prima facie Decision,

6.

having found that there is a prima facie violation of Articles 6(1), 24(1) and

(2) of the Regulation.

3

6.1. Also, before making a Decision on possible enforcement

administrative fine, the Defendant was called to submit the reasons and circumstances

which should be taken into account in the context and for the purposes of administrative enforcement

sanction, pursuant to article 58(2) of the Regulation and article 32(1) and (3) of

Law 125(I)/2018.

7.

In the context of the right to be heard provided for the reasons and the

circumstances that should be taken into account for the purposes of administrative enforcement

sanction, pursuant to article 58(2) of the Regulation and article 32(1) and (3) of

Law 125(I)/2018, the Defendant, in a letter dated November 7, 2022, quoted

The following:

7.1.1. The telephone number of the complainant belonged to a customer of the Ms

July 2020, it had been transferred to another telecom provider. Therefore, in

in the past there was a customer relationship between the Customer and the owner of the number.

7.1.2. In April 2021, Kathy called the complainant's number "to

inform about the upgrade of its services". The same applies to the other 331

telephone numbers, which received a call from Kat'is, in the same period and

had in the recent past a customer relationship with Kathy.

7.1.3. The data of the 332 data subjects who were called,

"inadvertently (...) they were included in a specific list of existing customers for

phone calls ("List")", where and "a single successful call was made" and

after this call they were removed from the list. These data were o

telephone number, name and address.

7.1.4 "The purpose of the calls was to inform existing customers about a possibility

upgrading their services".

7.1.5. The calls, to the 332 data subjects, "had no substance content or no promotional action was carried out during the calls, as the purpose of the calls concerned only existing customers" and h She "did not take advantage of the accidental call for promotional action" in them.

Also, as mentioned, no message was sent to the 332 subjects.

7.2. Regarding the violation of Article 6(1) of the Regulation, the Defendant stated that admitted, from the first moment, the inclusion of the 332 subjects in the list, as well as making the calls to them. Inevitably, their inclusion in the list, it also meant making the relevant calls. As mentioned, it is important to take into account that practically, the violation of article 6(1) of the Regulation is due to the fact that, in this particular single instance, the technicalities failed and organizational measures taken by the Defendant, while if they had not failed, the data of the 332 subjects would not have been listed and therefore would not have the calls are made. That is, there was no decision to include them, at list, former customers and actively and/or willfully violate the provisions of the article 6(1) of the Regulation, i.e. to carry out data processing ex customers for phone calls. Also, "the purpose of the phone calls it concerned existing subscribers so it could not be done nor was one done promotional action' to the 332 data subjects on whom it was conducted call.

4

7.3. Regarding the violation of articles 24(1) and 24(2) of the Regulation, and as concerns the data deletion policy, Ms. disagrees with it prima facie conclusion that the data deletion policy has been violated, as:

7.3.1. When a customer terminates their relationship with Kathy, their data

they continue to be retained in accordance with the database's data retention policy of the Plaintiff, which is uniform and in which it is clearly seen whether the contract of one client has been terminated.

7.3.2. In accordance with the data retention policy, Kathy retains all data of category A. Customer Data (including preferences of each subject), because there are reasons for preservation, for the purposes and periods referred to in the policy. Therefore, the Lady considers it correct implemented the data retention policy in its database and disagrees with the conclusion in paragraph 28b of my prima facie Decision, dated 10 October 2022, as well as in paragraphs 17, 18, 19, 24 and 25 thereof, that Ms. did not correctly implement the policy regarding the retention of data in the database her.

She refers to the following paragraphs of my prima facie Decision, dated 10 October 2022:

"17. Taking into account the above, the Defendant should proceed to termination of processing, which no longer had a legal basis, such as telephone call to complainant's number for promotional purposes. THE She also had to take all those actions to delete them personal data of the complainant, for which there was none now, due to the termination of the customer relationship, a legal basis.

Therefore, the actions that the Defendant had to take include:

18.
the removal of the complainant and his personal data from him list of people who received marketing communication from and its customer list. That is, the Lady had to remove the complainant from the above lists.

19. As a result, however, the Defendant did not remove, as she should have, the complainants from the list of people receiving commercial communication promotion. Nor, by the Court's admission, did it remove the complainant from its customer list. Of these, was telephone communication of the Defendant with the complainant to promote her services, without however there is a legal basis, in violation of Article 6(1) of the Regulation.

24.

In said data deletion policy, it does not appear to belong clearly the consent or non-opposition of the data subjects for communication for direct marketing purposes. However, even in the event that the given category refers to the selection for download communication for direct marketing is included in "any customer preferences (where needed)" of group "A. Customer Data" of the policy, the given this should be deleted at the end of the contract.

5

25. However, the Defendant did not delete his data in question complainant, nor the other data subjects, a total of 332 data subjects. Therefore, Kathy did not apply the specific one policy. Therefore, she did not apply an appropriate policy and, in general, appropriate technical and organizational measures in order to ensure and be able to prove that the processing is carried out in accordance with the Regulation, v violation of Article 24(1) and (2) thereof.

28.

Taking into account all the above elements, as they are cited, and based on the powers granted to me I find that there is prima facie infringement by Epic Ltd:

(...)

(b)

of article 24(1) and (2) of the Regulation, because the Defendant did not apply the data deletion policy and, in general, appropriate technical and organizational measures in order to ensure and be able to demonstrate that the processing is carried out in accordance with the Regulation, as a result of which they continue to there are 332 of Kathy's former clients on her client list."

7.3.3. Regarding the admission of the Defendant, which is mentioned in paragraph 19.1 of my prima facie Decision, dated October 10, 2022, Ms.

states that he admitted that the data was erroneously included in the List and not that Kathy wrongly retained the data.

She refers to the following paragraph of my prima facie Decision, dated 10 October 2022:

"19.1. There is also the admission of the Court that "incorrectly" according to termination of services the particular number was not removed from the catalog and that it was not her intention to disturb or further process them personal data of the complainant."

7.3.4. Regarding the policy review, it was reported that the policy has completed and that any changes made do not affect the subject matter of sub case investigation. I note at this point, that the revised policy data retention policy (Data Retention Policy, V.1.3, dated 24 October 2022) has been submitted to my Office.

7.3.4.1. This policy includes the following categories of personnel data character ("Personal Data categories"):

"A. Customer Data and Billing Data - name, surname, national identification number / passport number, email address, residence and billing address, contact

number(s), payment records, invoices issued per service per month, details of authorized representatives per contract, direct debit details (where needed), debit or credit card details (where needed), any customer preferences and/or consents (where needed), any other documentation related to the customer, details of modem data.

B. Telecommunication / Traffic and Location data – Location data, called subscriber number, date, starting time and duration of the calls made and/or the

6
data volume transmitted, IP address, internet browsing, number of identification of subscriber devices.

*Call includes SMS

C. CCTV data - Closed Circuit Surveillance System processing in Epic stores and other premises where needed for security purposes.

D. Voice Recordings»

7.3.4.2. The retention period of the data belonging to category A. Customer and Billing Data, are:

"Retain the data throughout the validity of the contract.

Upon contract termination data are maintained for a minimum period of six (6) years:

(a) For the purposes of taxation legislation (Law 95(I)/2000 and Law 4/1978), and up until a tax clearance is provided.

(b) For the purposes of protecting Epic's legitimate interest (e.g. legal disputes between Epic and the customer, unpaid balances), or until the legitimate purpose is completed."

7.4. Regarding the violation of articles 24(1) and 24(2) of the Regulation, and as regarding the technical and organizational measures, the Client states that she has admitted that the including the data in a list of existing customers for telephone calls;

concerning information to upgrade their services, was isolated

case, where the technical and organizational measure of removing former customers from the list didn't work due to human error.

7.4.1. The list for phone calls is fed from Kathy's base, on a monthly basis

basis (at the beginning of each month). Then, during the relevant month,

"customers who have terminated this month are removed, in order to ensure the updating the monthly list".

7.4.2. The error in the case under investigation was due to the human factor.

Specifically, the error resulted from entering an incorrect date in the criteria for extracting the list. As mentioned, the month March 2020 was entered, instead of the month March 2021. 7.4.3. To strengthen the safeguards in this process, the monthly

process of extracting the list for telephone calls has been automated, to minimize human intervention. 7.5. Regarding the

reasons and circumstances that must be taken into account in the context and for the purposes of imposing an administrative

sanction, the Defendant stated the following: 7.5.1 The violation of Article 6(1) of the Regulation is due to the fact that, in this

specific on a single occasion, the technical and organizational measures taken by Kathy when creating the list failed due to

human error. There was, as mentioned, no decision to include in the list former clients and actively and/or 7 willfully infringe the

provisions of Article 6(1) of the Regulation. The telephone calls concerned existing subscribers of the Defendant, therefore the

calls to the 332 data subjects had no purpose, object or effect of commercial promotion and were stopped immediately. 7.5.2

There was no other greater risk of processing the data subjects' data, as the processing stopped at the telephone call for each

subject, there was no repeat call to the subjects or call to other data subjects later, without a legal basis. 7.5.3 On receipt of the

information regarding the complaint submitted to my Office, Ms. acted immediately and gave instructions to re-check customer

lists for telephone calls, the procedures followed and to investigate the facts, to avoid such incidents. 7.5.4 No other data of the

332 subjects was processed, apart from their name, address and telephone number. 7.5.5 The scope of the processing

involved a small number of subjects compared to the number of subscribers of Ms. (who are over XXX) or former subscribers

of Ms. (who amount to around XXX per year) or calls (6 845 data subjects included in the list). 7.5.6. Only one complaint was

submitted by a data subject. 7.5.7 The purpose of the telephone calls concerned existing subscribers and there was no benefit

for the Defendant (financial or otherwise), as no attempt was made to market any product or service to the 332 subjects.

Similarly, the calls were not made with a view to avoiding any harm which the Defendant would have suffered had she not made the calls. 7.5.8. The processing did not cause physical, material or non-material damage to the 332 subjects. Kathy acknowledges, however, that some data subjects felt discomfort, however she emphasizes again that there was only one complaint, and there have been no others. 7.5.9. Kathy has reviewed the technical and organizational measures and added new ones in order to minimize human intervention in this process. Also, the specific issue has not been repeated. 7.5.10. There is no previous Judgment of mine against the Defendant for a breach of personal data, who, as mentioned, cooperated fully with me in the investigation of the complaint. 7.6. Kathy fully respects the provisions of the Regulation and takes her compliance with it seriously. The incident is isolated and Kathy reacted immediately, by taking additional measures, to avoid similar incidents in the future, there was no malice or financial gain. She also apologizes for any inconvenience she caused to the 332 data subjects who received a call. 8 Legal Aspect 7.7. Taking into account the above and especially the type of violation and its unintentional nature, the type of data of the 332 subjects that were included in the list and her immediate and serious response, the Defendant requested that no "financial penalty" be imposed on her (administrative fine), but reprimand. 7.8. Kathy's turnover for the financial year 2021 was €XXX, while she employs XXX people. B. 8. According to article 4 of the Regulation, 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 ID 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". 9. Pursuant to article 4 of the Regulation, processing is considered "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 the collection, registration, organization, structuring, the storage, adaptation or alteration, retrieval, retrieval of information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, restriction, deletion or destruction". 10. As a data controller, in article 4 of the Regulation, it is defined as "the natural or legal person, public authority, agency or other entity that, alone or jointly with others, determines the purposes and manner of processing personal data; 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 for by Union law or the law of a Member State." 11. Article 4 of the Regulation defines that the consent of the data subject is "any indication of will, free, specific, explicit and in full knowledge, with which the data subject manifests that he

agrees, by statement or by a clear positive action, to be the object of processing the personal data concerning it". 12. With regard to the principles that must govern the processing of personal data, Article 5, paragraph 1 of the Regulation states that: Personal data: "1. are processed lawfully and legitimately in a transparent manner in a) relation to the data subject ("legality, objectivity and transparency"), 9 ("minimization of which they are processed are appropriate, relevant and limited to what is necessary for the purposes of the collected for specified, explicit and legitimate purposes and are not b) further processed in a manner incompatible with those purposes; further processing for archiving purposes in the public interest or scientific or historical research or statistical purposes is not considered incompatible with the original purposes in accordance with Article 89 paragraph 1 ("limitation of purpose"), c) for data", d) are accurate and, where necessary, updated; all reasonable steps must be taken to promptly delete or correct personal data the which is 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 the processing of the personal data; the personal data may be stored for longer periods, as long as the personal data will only be processed for archiving purposes in the public interest, for the purposes of scientific or historical research or for statistical purposes, in accordance with Article 89 paragraph 1 and as long as the appropriate technical and organizational measures required by this regulation to safeguard the rights and freedoms of the data subject ("limitation of the storage period"), f) are processed in a way that guarantees the appropriate security of personal data, including their protection from unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality")." Regarding the legality of a processing of personal data, 13. article 6, paragraph 1, of the Regulation, provides that: The processing is lawful only if and as long as at least one of "1. the following conditions: a) the data subject has consented to the processing of his personal data for one or more specific purposes, 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 controller, d) the data subject or another natural person, e) the processing is necessary for the fulfillment of a task performed in the public interest or in the exercise of public power he has entrusted to the data controller, the processing is necessary for the purposes of the legal interests f) pursued by the data controller or a third party, unless these interests are overridden by the interest or fundamental rights and freedoms of the processing is necessary for the preservation of vital in the interest of the processing is necessary to comply with a legal obligation 10 of the data subject that imposes the protection of personal data, in particular if the data subject is a child. Item f) of the first paragraph does not

apply to the processing carried out by public authorities in the exercise of their duties." Regarding the responsibility of the data controller, article 24 of Regulation 14. provides, among other things, that: "1. Taking into account the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and freedoms of natural persons, the controller implements appropriate technical and organizational measures in order to ensure and can demonstrate that the processing is carried out in accordance with this regulation. These measures are reviewed and updated when deemed necessary. 2. Where justified in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.' 15. Regarding the security of the processing, article 32(1) of the Regulation provides that: "1. Taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and freedoms of natural persons, the controller and the executor the processing implement appropriate technical and organizational measures in order to ensure the appropriate level of security against risks, including, among others, where applicable: a) pseudonymization and encryption of personal data, b) availability and reliability of systems and services processing on an ongoing basis, c) the possibility of restoring the availability and access to personal data in a timely manner in the event of a physical or technical event, d) a procedure for the effectiveness of technical and organizational measures to ensure the security of processing." the ability to ensure assessment and evaluation of integrity, confidentiality, regular testing, on 16. Pursuant to article 58, paragraph 2, of the Regulation, the Commissioner for Personal Data Protection has the following corrective powers: "a) to issue warnings to the data controller or to the data processor that intended processing operations are likely to violate the provisions of this regulation, 11 to instruct the data controller to announce the violation to impose a temporary or definitive restriction, including reprimanding the data controller or the data controller b) processing when processing operations have violated the provisions of this regulation, c) to instruct the controller or the processor to comply with the data subject's requests for the exercise of his rights in accordance with this regulation, d) to instruct to the controller or the processor to make the processing operations in accordance with the provisions of this regulation, if necessary, in a specific way and within a certain period, e) personal data to the data subject, f) prohibition of processing, to give an order to correct or delete personal data g) or to restrict processing pursuant to articles 16, 17 and 18 and an order to notify such actions to recipients to whom the personal data was disclosed pursuant to article 17 paragraph 2 and article 19 h) to withdraw the certification or order the certification body to withdraw a certificate issued in accordance with

articles 42 and 43 or order the certification body not to issue certification if the certification requirements are not met or are no longer met, i) impose an administrative fine under of article 83, in addition to or instead of the measures referred to in this paragraph, depending on the circumstances of each individual case, j) a third country or an international organization." to give an order to suspend the circulation of data to a recipient in Regarding the general conditions for imposing administrative fines, in article 83, 17. paragraph 2, of the Regulation, the following are provided: "2. Administrative fines, depending on the circumstances of each individual case, are imposed in addition to or instead of the measures referred to in Article 58(2)(a) to (h) and Article 58(2)(j). When deciding on the imposition of an administrative fine, as well as on the amount of the administrative fine for each individual case, the following shall be duly taken into account: a) the nature, gravity and duration of the infringement, taking into account the nature, extent or purpose of the relevant processing, as well as the number of data subjects affected by the breach and the degree of damage they suffered, the intent or negligence that caused the breach, b) any actions taken by the controller or c) of the processor to mitigate the damage suffered by the data subjects, d) the degree of responsibility of the controller or processor, taking into account the technical and organizational measures they apply pursuant to Articles 25 and 32, e) of the processor the processing, any related previous violations of the controller or 12 the observance of approved codes of conduct in accordance with article 40 or the degree of cooperation with the control authority for the correction of the categories of personal data affected by f) violation and the limitation of possible of its adverse effects, g) breach, h) the way in which the supervisory authority was informed of the breach, in particular if and to what extent the data controller or processor notified the breach, in case the measures were previously ordered to be taken) referred to in Article 58 paragraph 2 against the controller involved or the processor in relation to the same object, the compliance with said measures, j) approved certification mechanisms in accordance with Article 42 and k) any other aggravating or mitigating factor arising from the circumstances of the particular case, such as the financial benefits obtained or losses avoided, directly or indirectly, from the infringement. 3. In the event that the controller or processor, for the same or related processing operations, violates several provisions of this regulation, the total amount of the administrative fine does not exceed the amount set for the most serious violation. 4. Violations of the following provisions shall attract, in accordance with paragraph 2, administrative fines of up to EUR 10 000 000 or, in the case of undertakings, up to 2 % of the total worldwide annual turnover of the previous financial year, whichever is higher: a) the obligations of the controller and the processor in accordance with Articles 8, 11, 25 to 39 and 42 and 43, the obligations of the certification body in accordance with Articles 42 and 43, b) c) the obligations of the monitoring

body in accordance with Article 41 paragraph 4. 5. Violations of the following provisions shall attract, in accordance with paragraph 2, administrative fines of up to EUR 20 000 000 or, in the case of undertakings, up to 4 % of the total global annual turnover of the previous financial year, depending whichever is higher: a) apply to approval, in accordance with Articles 5, 6, 7 and 9, b) to 22, c) or to an international organization in accordance with Articles 44 to 49, d) which are established under chapter IX, e) non-compliance with an order or temporary or permanent restriction of processing or suspension of data circulation imposed by the supervisory authority pursuant to Article 58 paragraph 2 or failure to provide access in violation of Article 58 paragraph 1." the transmission of personal data to a recipient in a third country the basic principles for the processing, including the conditions that the rights of the data subjects in accordance with articles 12 any obligations according to the law of the member state the 13 Rationale C. Purpose of the processing 18. In the case under investigation, the Defendant has the role of the controller, since she herself has determined the purpose of the processing. This purpose is achieved by a telephone call to the data subjects, possibly also in other ways, which however do not relate to the case under investigation. 19. As stated in her letter dated November 7, 2022, the call to the complainant's number was made to "inform about an upgrade of his services". However, in the same letter, the Defendant stated that "The purpose of the calls was to inform existing customers about the possibility of upgrading their services". The update to upgrade services is not entirely consistent with the possibility of upgrading services, in which, as it turns out, the customer has the possibility to decide whether or not he wishes to upgrade the services he receives. 20. Having said that, positions have been put before me which are not completely consistent with each other, but without any relevant explanation and/or reference from the Defendant, which clarifies the real purpose of the processing, which in any case will it had to be correctly and clearly formulated before the processing was carried out. 21. It is also not known whether the upgrade or the ability to upgrade services would have any change in the terms of the services customers received (such as a change in duration, fees, etc.). 22. The Defendant in her letter, dated November 7, 2022, stated that the calls "had no substantive content or promotional activity was carried out during the calls, as the purpose of the calls was only to existing customers" and that the According to her "he did not take advantage of the accidental call for promotional action". He also stated that "the purpose of the phone calls was to existing subscribers, so no promotional action could be taken nor was it done." 23. Because as a result the service upgrade has not been effective, it does not mean that the calls had no substantial content or that no promotional action has necessarily been carried out. Notification of a service upgrade or the possibility of a service upgrade could only be justified in relation to existing customers.

24. As the complainant mentioned, when he informed the Accused, at number 136, about the calls he was receiving, he received the answer that this number belongs to the Accused's sales department. This position of the complainant was communicated to her in letters from my Office, dated May 26, 2021, September 3, 2021 and January 4, 2022. In her letter, dated June 9, 2021, Ms. sales team that the number does not belong to an existing 14 customer of ours and immediately stopped making calls to this number and removed it from the customer list." 25. Despite the above, apart from the letter dated November 7, 2022, Ms. did not attempt to point out to my Office that the calls did not relate to the sale of a service, i.e. to a promotional action, despite the fact that reference is made by complainant to "sales department" and from the same to "sales team". Also, the subject of the aforementioned last two letters from my Office was "Complaint/Complaint about Unsolicited Marketing Call - Sp. 27/2021" and "Complaint about unsolicited marketing call - Sp. 27/2021", without however the Defendant trying to clarify that "no promotional action was carried out", as she pointed out in her letter dated November 7, 2022. 26. The Defendant stated that there was no benefit (financial or other) as no attempt was made to market a product or service to the data subjects. Even if I accept that there would be no financial benefit to the upgrade or the ability to upgrade the services, the Defendant has not provided me with evidence to demonstrate that she would have no other benefit from any upgrade of the services of the subjects who received the call, therefore I cannot accept this position as a mitigating factor when imposing and measuring an administrative sanction. 27. However, I accept as a mitigating factor the Defendant's position that the calls were not made with a view to avoiding any harm which the Defendant would have suffered had she not made the calls. 28. Taking into account the positions submitted to my Office by the Ms., and especially the purposes of the calls which she mentioned, I consider that the Ms. has not submitted sufficient information so that the communication to the complainant and others 331 data subjects who received a call and no longer had a customer relationship with the Client, not to be considered a communication for promotional purposes. Legal basis of processing For each act of processing there must be an appropriate legal basis, as 29. provided for in article 6(1) of the Regulation. The legal basis must be valid at all times. The controller must be able to demonstrate the lawfulness of the processing at all times. Therefore, special attention must be paid in case there is a change in conditions and/or situations that concern and/or affect the processing. 30. As stated by the Defendant, the complainant was a client of the Defendant. However, as of July 2020, the telephone number held by the complainant was transferred to another telecommunications provider. Therefore, from the moment the telephone number was transferred to another provider, there was no longer a customer relationship between the complainant and the Defendant. 31. It cannot be

considered that the communication made by the Defendant rests on the legal basis of consent, as provided for in Article 6(1)(a) of Regulation 15, or that it is necessary for the execution of the contract of which the complainant is a contracting party or for measures to be taken at his request before the conclusion of a contract, as provided for in article 6(1)(b) of the Regulation, since by transferring the telephone number to another provider, the services received by the complainants from the Defendant and therefore the customer relationship between them is terminated. Nor can it be assumed that as a former customer of the Plaintiff he expected to continue to receive specific updates or services from the Plaintiff. 32. In addition to the above, it cannot be considered that the act of processing carried out by the Defendant can be based on any other legal basis of Article 6 of the Regulation. 33. Based on the above, it follows that the communication of the Defendant with the complainant, for the purposes that the Defendant herself mentioned, even if these purposes, as put before me, are not completely consistent with each other, cannot to rely on a legal basis, in violation of article 6 of the Regulation. 33.1. The same conclusion applies to the communication of the Defendant with the other 331 persons who received a call from her. 34. The above applies not only to the communication, but also to the "creation of the List" and/or the "inclusion" of the complainant and the other 331 data subjects in the list, since these actions constitute processing, pursuant to Article 4 of the Regulation. 35. Therefore, the essence of paragraphs 17, 18, and 19 of my prima facie Decision, dated October 10, 2022, is not negated, since the inclusion of the complainant in a list or list for notification for upgrading or for the possibility of upgrading his services , as well as communication for these purposes, is not based on a legal basis, as provided for in article 6(1) of the Regulation. Directory - Base - List of customers of Kathy 36.1. The Attorney in her letter dated June 9, 2021, stated that the complainant's telephone number "was in the telephone directory of the Client" of the Attorney "and erroneously upon termination of services the particular number was not removed from the directory and therefore they have phone calls were made", while after establishing that the complainant's number did not belong to an existing customer, it was "removed from the customer list". 36.2. The Defendant in her letter, dated September 10, 2021, stated that in the specific customer list "numbers of customers whose customer relationship" with the Defendant "had been terminated" were included by mistake. 36.3. In her letter, dated January 17, 2022, Kathleen noted that "a call was made to all 332 numbers that were mistakenly included in the list." 37. Based on the above information, but also by studying the letters of the Professor, dated June 9, 2021, September 10, 2021 and January 17, 2022, it appears 16 clearly that no reference was made by the Professor to the "basis" of the Professor and/or on an "existing customer list for telephone calls", terms which were first set out in Kat's letter dated November 7, 2022. 38.

Therefore, by Kat's letter dated November 7, 2022, they have put before me positions which are not consistent with the Defendant's previous answers, without the Defendant attempting to make a reference, clarification or justification for the differentiation of her answers. 39. Furthermore, in the letters dated June 9, 2021, September 10, 2021 and January 17, 2022, the Defendant had never noted that the client list referred to was not her existing client list or part of it or a special list created to satisfy specific purposes. 40. In her letter dated November 7, 2022, the Attorney General stated that she admitted that the data was erroneously included in the referenced list and not that she erroneously retained the data. For this position, it refers to paragraph 19.1. of my prima facie Decision dated October 10, 2022, according to which: "19.1. There is also the Defendant's admission that "erroneously" when terminating the services, the specific number was not removed from the list and that it was not her intention to disturb or further process the personal data of the complainant." 40.1. The mentioned paragraph 19.1. arose from the Plaintiff's letter dated June 9, 2021, according to which the complainant's telephone number "was in the Plaintiff's" customer phone book "and erroneously upon termination of services the particular number was not removed from the list and therefore phone calls have been made." 41. In the mentioned paragraph 19.1. there was no mention of the word conservation. However, taking into account the admission of the Court in the letter dated June 9, 2021, that the complainant's number was wrongly not removed, it appears that the complainant's number, since it was not removed, was retained. After all, taking into account that the complainant's personal data was included in a list, it follows that the non-maintenance and, therefore, processing of this data for the specific purposes was not prevented. 42. In the letter dated November 7, 2022, the Court stated that the data subjects' data was included in a specific list of existing customers for telephone calls. However, it said that the technical and organizational measure to remove former customers did not work due to human error. He also noted that the list is fed from Kathy's database at the beginning of each month, on a monthly basis, and during the month, "customers who have terminated that month are removed to ensure the monthly list is updated." and that the error resulted from entering an incorrect date (March 2020 instead of March 2021) in the criteria for deriving the list and that technical and organizational measures failed when creating the list. 17 43. Based on the information presented to me by Kathleen, it is not clear how the list works. That is, it is not clear whether there is a specific list in which new customer data is included / added on a monthly basis, which is removed when the customers in a given month have terminated their relationship with the Client, or whether it is created or created, in specific intervals, list or lists which concern active customers based on criteria determined at the given time by the Customer. 43.1. Since the complainant terminated his services during

July 2020, the position that the error arose from entering an incorrect date (March 2020 instead of March 2021) is not substantiated, since the complainant did not terminate his services in any of these months. I therefore do not accept as a mitigating factor that the alleged human error did not remove former customers from that list during the material time. 43.2. However, the failure to fully clarify and explain how the list works does not negate or diminish the breach committed by Ms. Data deletion / retention policy 44. The controller's data retention policy indicates the period of time for which personal data of data subjects is or may be retained, for the purpose or purposes determined by the controller and which purposes are included in this policy. In many cases, it turns out that there is the possibility of fulfilling another purpose, which is not included in the policy, by processing personal data which are referred to in the policy and are intended to be kept in it for the fulfillment of a specific purpose or purposes. In this case, because the data is kept for the fulfillment of a specific purpose or purposes, it does not imply that the fulfillment of any other purpose, which is not included in the policy, is legalized, especially when there is no legal basis for the intended processing act. 45. Therefore, none of the data of customers whose customer relationship has been terminated, even if the same data or the same categories of data relate to another purpose or purposes, should not be retained and used, and therefore processed, for upgrade purposes or the possibility of upgrading services. The fact that the complainant was included in a specific list of existing customers for telephone calls, indicates that for these purposes this data was retained for a period of time beyond that prescribed. That is, despite the fact that it appears that specific data of the complainant had to be kept for other purposes, a fact which I consider acceptable, it was not prevented from being kept for the purposes of updating information for an upgrade or for the possibility of upgrading services, a fact which shows that no Kathy's data retention policy was applied. At this point I note that in the letter dated January 17, 46, 2022, she referred to a data deletion policy (Data Retention Policy, V1.2, dated September 9, 2020), while in the letter dated November 7, 2022, referred to a data retention policy (Data 18 Retention Policy, V1.3 dated October 24, 2022). In this Decision, the terms data retention policy and data deletion policy are used, without any distinction between them, unless explicitly stated. 47. From the Customer's data deletion policy (Data Retention Policy, V1.2, dated September 9, 2020), it follows that the data relating exclusively to the fact that a data subject is a customer of the Customer, and related to the services offered to it, are included in category A. Customer Data. The data related to the services offered to customers do not fall into category B. Telecommunication / traffic and Billing data – location data, category C. CCTV data or category D. Voice Recordings. The data of category A. Customer Data, based on the policy, exists for 48. the entire duration of the contract for active customers. If the

contract expires, and if there is no reason to retain them, as stated in the relevant paragraph 2, these data must be deleted.

49. As the Client stated in the letter dated November 7, 2022, when a customer terminates their relationship with the Client, their data continues to be retained in accordance with the Client's database retention policy, the which is uniform and clearly shows whether a customer's contract has been terminated. Also, the Client stated that according to the data retention policy, the Client retains all data of category A. Customer Data (including the preferences of each subject), because there are reasons for retention, for the purposes and periods referred to in the policy and for this reason considers that it has correctly implemented the policy in terms of data retention on its basis. 50. As a result and taking into account that the contract / contract that the complainant had with the Defendant had been terminated, the data of category A. Customer Data for which at least one of the sub-paragraphs 2 applied had to be preserved or not deleted (a) to (d) of this category and if they are subject to processing, beyond their retention, to be used exclusively and solely to achieve the purpose or purposes referred to in one or more of the sub-paragraphs 2(a) to 2(d) . 51. None of the Defendant's intended purposes relate to the cases of sub-paragraphs 2(a) to (d). The notification for upgrading or for the possibility of upgrading the services of the complainant does not concern and/or is not related to law enforcement purposes (subparagraph 2(a)), tax legislation purposes (subparagraph 2(b)), legal interest purposes (subparagraph 2 (c)) nor for payment information purposes (subsection 2(d)). 52. The Court, in her letter dated 7 November 2022, stated that she disagreed with paragraphs 24 and 25 of my prima facie Decision, dated 10 October 2022, specifically that she did not correctly apply the data retention policy at its base. First of all, I would like to repeat that in my prima facie Decision the term "basis" was not used, since this term 19 was used for the first time in the letter of the Court, dated November 7, 2022. 52.1. With regard to the mentioned paragraph 24, as I mentioned in para28 of this Decision, I believe that the Defendant has not submitted sufficient evidence anyway so that the communication to the complainant and to the other 331 subjects of data not to be considered communication for promotional purposes. However, even if the communication for information about an upgrade or for the possibility of upgrading services does not concern communication for direct marketing, this communication does not falls, in any case, in the cases of sub-paragraphs 2(a) to 2(d) of category A. Customer Data.

52.2. Also, I do not consider that the Defendant's disagreement with paragraph 25 has any basis

of my prima facie Decision, since the data of the complainant and of other 331 data subjects, were used for another purpose, which is not foreseen in the policy, and for which there was no legal basis, since it had terminate their customer relationship with Kathy.

53. Based on the above data, I conclude that the Defendant did not apply it then applicable data retention policy. Therefore, Kathy did not apply appropriately data protection policy, in violation of Article 24(2) thereof

Regulation, therefore appropriate organizational measures in order to ensure and to can prove that the processing is carried out in accordance with the Regulation, v violation of Article 24(1) thereof.

of the above, I confirm that the changes that have

54. Regardless

carried out in the new data retention policy (Data Retention Policy, V1.3, with date of issue on October 24, 2022) are not related to its content case under investigation, as well as the Defendant's admission that any changes were made they do not affect the subject of this research.

Technical and organizational security measures

55. Since both existing customers and customers with whom it has terminate the client relationship with the Client, coexist on the same basis, must all those security steps are taken, so that the data every subject to the data included in the base, not be able to be used for any other purpose than that or those which are included in the policy, for the relevant processing operations provided that these are based on the legal basis of article 6(1) of the Regulation and for which they are observed the processing authorities, as defined in article 5(1) of the Regulation.

56. If the data of customers who had terminated their customer relationship

with Kathy were included exclusively and only on a separate basis, then they will not list could be created, which includes concurrent data existing customer and former customer data.

57. From the result, it follows that the information on the single basis that the a customer's contract has been terminated did not work as a security measure for the non processing without a legal basis.

20

58. In her letter, dated November 7, 2022, Ms inclusion of the complainant's data in a list of existing customers for phone calls related to updating their services was a single case, where the technical and organizational measure of removal ex customers from the list did not work due to human error. He also mentioned that the error related to an incorrect date entry in the criteria for extracting the list and that in order to strengthen the security barriers in the procedure followed, it has the monthly process of exporting the list for telephone numbers is now automated calls for minimizing human intervention.

59. Based on the positions of the Defendant, I accept, as well as her admission, that the non-operation of a technical and organizational measure led to its inclusion complainant to a list of existing customers. This fact resulted in the telephone call to the complainant, as well as to the other 331 subjects of the data that received a call for the purposes in question.

60. There were, therefore, measures which the Defendant could take and which they could have prevented the incident.

61. Based on the above, it is established that during the essential time he was not in implementation of appropriate technical and organizational measures to ensure the appropriate level of security against risks, in breach of Article 32(1) thereof

Regulation.

62. It also appears that the Defendant did not apply appropriate technical and organizational measures in order to ensure and be able to prove that the processing is carried out according to the Regulation, in violation of Article 24(1) of the Regulation.

63. Taking into account that calls have been made to 332 subjects of data, I accept as a mitigating factor the fact that he has been subjected to My office complaint only from a data subject.

63.1. However, due to the absence of technical and organizational measures that would prevented the violation, the fact cannot be taken as a mitigating factor that the scope of the processing included, as Cathy mentioned, a small number of data subjects compared to the number of subscribers, the number of former subscribers of the Customer or the calls made.

D.

64. Taking into account all the above elements, as they have been set, and with based on the powers granted to me under Article 57(1)(f) of the Regulation, I find that there is a violation by Epic Ltd:

(a)

of article 6(1) of the Regulation, due to the absence of a legal basis for telephone Kat's communication with 332 of her former clients, including him complainant,

Conclusion

21

the fact that the data processed was only the the non-existence during the essential time of technical and organizational measures that will the submission to my Office, by Ms., of positions which do not of article 24(1) and (2) of the Regulation, because the Defendant did not apply the

(b)

data retention policy and, in general, appropriate technical and organizational measures in order to ensure and be able to prove that the processing is carried out according to the Regulation, and

(c)

of Article 32(1) of the Regulation, because the Defendant did not apply it properly technical and organizational measures to ensure the appropriate level security against risks.

65. Based on the provisions of article 83 of the Regulation, regarding the conditions imposition of administrative fines, to the extent that they are applied in the specific case case, when calculating the administrative fine, I took them into account following aggravating (a) – (b) and mitigating (c) – (h) factors:

(a)

they prevented the violation that was committed by Kathy.

(b)

documented, contradictory and inconsistent with each other,

(c)

name, address and telephone number,

(d)

that the processing has not caused physical, material or non-material damage to data subjects and that there was no other greater processing risk of data, after the call stopped on the first successful call in each data subject,

(e)

that Ms., following the letter from my Office, dated May 26, 2021, acted immediately, giving instructions to recheck the list and procedures that

instructions were also followed to investigate the facts,

(f)

making the calls,

(g)

(the)

that 332 of her former clients received a call.

66. Having taken into account and considered:

(a)

in the provisions of article 58(2) and article 83 of the Regulation,

(b)

before me based on all existing correspondence,

(c)

bearing in mind the above facts, the legal aspect on which the

this Decision and the analysis as explained above, exercising them

powers granted to me by article 58(2)(i) of the Regulation,

the non-existence of my previous Decision against the Defendant,

the fact that only one complaint was lodged with my Office, notwithstanding

all the circumstances and factors raised by the complainant and the Defendant

the taking of corrective technical and organizational measures by the Customer after

the applicable legislative basis regarding the prescribed administrative sanctions

the above mitigating and aggravating factors,

22

I decided

at my discretion and subject to the above provisions:

to impose on Epic Ltd an administrative fine of three thousand two hundred and fifty

euros (€3 250) for violation of the above articles of Regulation (EU) 2016/679.

Irini Loizidou Nikolaidou

Protection Commissioner

Personal Data

February 3, 2023

23