Io

Athens, 27-03-2020

PRINCIPLE FOR DATA PRIVACY

FOR OPIC CHARACTER

Prot. No.: G/EX/2297/27-03-2020

A P O F A S H 06/2020

The Personal Data Protection Authority met, after

invitation of its President, in a regular meeting at its headquarters on Tuesday

25.02.2020 and time 10:00, in order to examine the case referred to in

history of the present. The President of the Authority, Konstantinos, was present

Menoudakos and the regular members of the Pyridon Authority Vlachopoulos, Konstantinos

Lambrinoudakis, Eleni Martsoukou and Grigorios Tsolias, substitute member

of the Authority, as rapporteur, in place of regular member Charalampou

Anthopoulos, who, although he was legally summoned, did not appear, due to obstruction. present,

without the right to vote, was Chariklia Latsiu, legal auditor - lawyer, as

assistant rapporteur and Irini Papageorgopoulou, employee of the department

of administrative affairs, as secretary.

The Authority took into account the following:

With the date of 23.07.2019 (and with prot. no. APDPCH G/EI /5141/23.07.2019)

complaint, as it was completed with the one from 09.10.2019 (and with No. prot.

C/EI /6110/10.09.2019) application, A complains that the AXA insurance company does not

satisfied the right to erasure in personal data that

concern. specifically, complains that the AXA insurance company did not satisfy

his request from ... regarding deletion from the company's records

personal data of himself and his family members, which

were collected by the AXA insurance company pursuant to the application from ...

insurance during the pre-contractual stage of concluding a relevant insurance contract,

which, in the end, due to the relevant terms of the insurance policy, no

accepted and never signed. The Authority, while examining the complaint, called

2

with the under no. prot. C/EX/5141-1/10.09.2019 document AXA insurance company

such as submitting explanations on the complaints and clarifying, in particular, the reasons

for which he did not satisfy the right of deletion submitted by A with the

from … email message. in response to her above document

Authority, the AXA insurance company with the from 27.09.2019 (under prot. no.

C/EI /6546/30.09.2019) her application clarified that the complainant submitted the...

health insurance application for himself, his wife and their two minor children and

on … he and his wife submitted both individually and on behalf of the

of his minor children in specific questions from the company Advance

Medical Health Care Management Services S.A. (I was editing), which

has contracted with the AXA insurance company for the assessment of the insurance policy

risk of the health programs through an interview that takes place

by telephone and recorded with the consent of the candidate concerned

insured. according to the AXA insurance company, during

telephone interview, personal data is collected, especially of special categories

(health data), the data subject is informed about their processing

data and his consent is expressly requested. specifically, the interested party

candidate insured before the start of the interview is informed, between

others, for the purpose of collecting personal data, their recipients

data, their retention period (i.e. for 5 years, and in case

of concluding a contract for the entire period of its validity), as well as for

his rights, including the right to erasure. His answer

prospective insured, the call is also recorded in case of refusal

is terminated, without collecting additional personal data. In that way

according to AXA insurance company, the obligation to obtain consent is satisfied

of the data subject, as the recording is a document with it

evidentiary power conferred on him by law (article 444 par. 1 c of the Civil Code). According to

AXA insurance company, both the complainant and his wife agreed with

the above way in the processing of their personal data and

were informed – in the case of the insurance application that does not develop into

insurance contract – to maintain them for 5 years. Subsequently, due to

exceptions imposed on the above-mentioned insurance coverage

program, A refused the insurance and requested it by e-mail

the deletion of his and his family's personal data, which

had been collected in accordance with the above, during the pre-contractual stage. On ...

AXA insurance company responded to his request via e-mail,

by informing him again about the policy of keeping personal data, them

processing purposes, including avoidance and

combating insurance fraud, as well as maintaining data for

a 5-year period in case of not concluding an insurance contract. Finally, on ... the AHA

insurance company sent, via e-mail, the following

answer to A: "In connection with our telephone communication I repeat to you

and in writing that according to the policy of our company, the personal data

of candidates for our customer insurance are kept for five (5) years from

date of submission of their application for insurance, for reasons of prevention

insurance fraud. You have already received and consented to this information

orally in the online processing of your personal data. In each case

and in order to satisfy your request, we inform you that we will proceed to

anonymization of your application, i.e. the deletion of any personal data that

is written on it". according to the claims of AXA insurance company,

the preservation of the complainant's data was necessary, according to article 17

par. 1 item a' of the GDPR, to satisfy the purpose of "avoidance and

combating insurance fraud". The insurance is invoked, in particular

company the "Code of Ethics for the processing of personnel data

character from the insurance companies" submitted by the Union

of Insurance Companies of Greece and is pending at the Authority for approval. Furthermore, the

AXA insurance company citing article 34 par. 3 of law 4624/2019

argues that five years can be understood as a contractual retention period,

since by providing the complainant's consent to the recording

interview, in the context of the insurance product application, was concluded between

party agreement regarding the terms of personal data processing

in accordance with the provisions of article 192 of the Civil Code. Furthermore, the AXA insurance company

invokes recital 47 of GDPR 2016/679, in which "(...) the

processing of personal data, to the extent that it is strictly necessary

for fraud prevention purposes, it also constitutes his legitimate interest

concerned data controller (…)". Following this, AXA concludes

insurance company that the complainant's right was duly satisfied,

given that following the anonymization of personal data, which

were included in his application, it becomes impossible to identify him.

in addition to the above answer, the AXA insurance company with the

03.10.2019 (under no. prot. ADDPX G/EI /6671/04.10.2019) her application informed the
Principle: "(...) Using the customer's identification data (name,
VAT number and insurance application number) found in the information systems (back
offices, CRM) of the company, all records related to the customer's request and
through the technical tools of each system we proceeded to anonymize them.
All identification details of the customer and his/her dependents
containing alphabetic letters were replaced with "XXX..." and any of them
containing numbers were replaced with "999...". Locating the customer at
information systems of our company with any identification element
now impossible. The anonymization process took time on …. Furthermore, the
complainant was informed again today ... about the satisfaction of his request (...)".
Subsequently, the Authority called under no. prot. ADDPHX C/EX/5141-2/18.10.2019
document the AXA insurance company to provide additional explanations on
specific issues. in response, the AXA insurance company with the
04.11.2019,
05.11.2019
and
05.11.2019
(and
with
No.
first APDPH
G/EI /7564/05.11.2019, G/EI /7573/05.11.2019 and G/EI / 7610/06.11.2019) documents
informed, among other things, the Authority that the sole legal basis of the processing
is the consent of the data subject, pursuant to article 9 par. 2
item a' of GDPR 2016/679 and the invocation of recital 47 of GDPR

2016/679 aimed at further explaining the purpose of processing, which consisted

to avoid and combat insurance fraud and legality

of this, as well as that the company never used any other legal basis than that

consent. Furthermore, according to the AXA insurance company: "(...) 2. H

avoiding and combating insurance fraud consists in avoiding submission

of a future insurance application from the same data subject with false (in other words,

differentiated) in relation to the original health data insurance application. The energy

this constitutes deceiving the insurance company in order to obtain insurance

risk, which would be excluded from insurance if the subject had submitted truthfully

data or the subject would pay a premium for said coverage. The above

practice is detrimental not only to the insurance company but also to the whole

of the (bona fide) insured as long as the amount of the annual premiums each

insurance program is formed each time based on the amount of damages that

4

5

covered by the insurance company in the previous year. In the case of compliance

of personal data collected during the pre-contractual stage, achieved comfortably o

above purpose, as long as the subject returns to a future role and submits

new insurance application with different insurance details compared to the existing ones

submitted in the first instance, the insurance company may recognize it

insurance fraud and deny insurance'. (…) 6. It is attached to the subject of

given the possibility of withdrawing his consent even in the pre-contract

insurance application stage. Specific information can be found on the application form

insurance (…) as well as in the verbal information he receives during the unwritten

telephone medical interview (…) 7. Our company informed the subject of

data for the reasons that anonymization of his data was chosen instead of her

deletion, through telephone communication with the Protection Officer

Personal Data of our Company. This fact is also proven by

pending the termination of the data subject, where this is mentioned

communication as well as informing the subject about its process

anonymization (…)".

Subsequently, the Authority with sub. No. prot. C/EX/5141-4/12.12.2019 and C/EX/5141-

3/12.12.2019 documents called the AXA insurance company and the complainant A,

respectively, as presented at a meeting of the Authority's Plenary on Tuesday

21.01.2020 at 10:00 a.m. in order to discuss the aforementioned complaint. THE

A, following the aforementioned call, informed the Authority with the from

29.12.2019 (and with no. prot. APDPH G/EI /53/07.01.2020) his application that he will not

attend the above meeting. the meeting of the Authority on 21.01.2020

Aikaterini – Nikoleta Pavli (AM DD A ...) appeared, as attorney-at-law

of the AXA insurance company, which presented the company's views and gave

clarifications following relevant questions from the members, while Michael was also present

Dermitzakis, lawyer, Data Protection Officer of AXA Insurance

company.

During the meeting, AXA insurance company received, upon request,

deadline until 10.02.2020 for the submission of a memorandum document. Then

therefore, the AXA insurance company submitted by deadline to the Authority the from

10.02.2020 (and with prot. no. ADDPCH G/EI /1087/10.02.2020) document reminder,

with which he informed, among other things, the Authority about the conservation policy

personal data of the company in general, and provided information on the technique

of the anonymization adopted in satisfaction of A.'s deletion request.

The Authority, after examining the elements of the file, after hearing him

rapporteur and the clarifications from the assistant rapporteur, who was present without the right to attend

vote and withdrew after the discussion of the case and before the conference

and making a decision, after a thorough discussion,

IN ACCORDANCE WITH THE LAW

1. Because, from the provisions of articles 51 and 55 of the General Regulation

of Data Protection (Regulation 2016/679) and Article 9 of Law 4624/2019

(Government Gazette A' 137) it appears that the Authority has the authority to supervise the implementation of

provisions of the GDPR, this law and other regulations concerning

protection of the individual from the processing of personal data. In particular, from

the provisions of articles 57 par.1 item f of the GDPR and 13 par. 1 item g' of the law

4624/2019 it follows that the Authority has the authority to deal with A's complaint

against the AXA insurance company for non-satisfaction of the right

erasure of personal data concerning him and to exercise,

respectively, the powers granted to it by the provisions of articles 58 thereof

GDPR and 15 of Law 4624/2019.

2. Because Article 5 of the GDPR defines the processing principles that govern the

processing of personal data. specifically, defined in

paragraph 1 that the personal data, among others: "a) are submitted

in lawful and fair processing in a transparent manner in relation to the subject of

data

("legality, objectivity, transparency"), b) are collected

for

defined, express and legal purposes and are not subjected to further

processed in a manner incompatible with these purposes (…), c) are appropriate,

relevant and limited to what is necessary for the purposes for which they are submitted

in processing ("data minimization"), (…) e) are kept in a form that

allows the identification of data subjects only for the period that

required for the purposes of processing personal data; ta

personal data may be stored for longer periods,

since the personal data will be processed only for

purposes of ranking in the public interest, for purposes of scientific or

historical research or for statistical purposes, in accordance with article 89 paragraph 1 and

6

7

as long as the appropriate technical and organizational measures required herein are applied

regulation to ensure the rights and freedoms of the subject of

data ("restriction of the storage period") (...)'.

3. Because, in accordance with the provisions of article 5 paragraph 2 of the GDPR

the controller bears responsibility and must be able to prove it

its compliance with the processing principles established in paragraph 1

of article 5. As the Authority1 has judged, a new model was adopted with the GDPR

compliance, a central dimension of which is the principle of accountability in the framework

of which the controller is obliged to design, implement and in general

takes the necessary measures and policies, in order to process the data

to be in accordance with the relevant legislative provisions. In addition, the person in charge

processing is burdened with the further duty to prove by itself and per

at all times its compliance with the principles of article 5 par. 1 GDPR.

4. Because, in accordance with the provisions of article 4 par. 1 of the GDPR

are understood as personal data "any information concerning

identified or identifiable natural person ("data subject"); the

an identifiable natural person is one whose identity can

be ascertained, directly or indirectly, in particular by reference to an identifier

ID, such as name, ID number, location data, online

identity identifier or to one or more factors specific to

physical, physiological, genetic, psychological, economic, cultural or social

identity of the natural person in question"2. Also, in article 4 par. 5 of the GDPR

2016/679 is defined as pseudonymization: "the processing of personnel data

1 See Authority decision 26/2019, paragraph 8, available on its website.

2 In addition, recital 26 of GDPR 2016/679 underlines that: "The advantages of the protection

should apply to any information that concerns an identified or identifiable

individual. Personal character data that has undergone pseudonymization, which will

could be attributed to a natural person by stating additional information, it should

are considered information relating to an identifiable natural person. To judge whether a natural

person is identifiable, consideration should be given to all means which are reasonably likely

that they will be formalized, such as its appointment, either by the data controller or

by a third party for the direct or indirect verification of the identity of the natural person. To find out

whether any means are reasonably likely to be formalized to verify identity

of the natural person, all objective factors, such as costs, should be taken into account

and the ron required for identification, taking into account the technology it is

available during processing and technological developments. The virtues of protection

data protection should therefore not apply to anonymous information, i.e. information that does not

are directed to an identified or identifiable natural person or personal data

which have been made anonymous in such a way that the identity of the data subject cannot

or can no longer be ascertained. This regulation therefore does not concern the processing of such

anonymous information, not for statistical or research purposes among others".

character in such a way that the data can no longer be attributed to

specific subject

of hourly data

the saying of complements

information, as long as said supplementary information is kept permanently

and are subject to technical and organizational measures to ensure that they do not

can be attributed to an identified or identifiable natural person"3.

5. Because, in accordance with article 8 par. 1 of the Charter of the Fundamental

Rights of the European Union, the article

9A

of the regiment and the

recital 4 of the GDPR, the right to data protection

of a personal nature is not absolute, but must be evaluated in relation to

his functioning in society and to be weighed against other fundamental rights,

according to the principle of proportionality. The GDPR respects all fundamentals

rights and observes the freedoms and principles recognized in the Charter, in particular

respect for private and family life, residence and communications,

the protection of personal data, freedom of thought,

conscience and religion, the freedom of expression and information, the

business freedom, the right to a real and impartial remedy

court and cultural, religious and linguistic diversity.

6. Because, with regard to the right to erasure, Article 17 of the GDPR,

provides, among other things: "1. The data subject has the right to request

by the controller the deletion of personal data that the

sometimes involve unjustified delay and the data controller is liable

to delete personal data without undue delay, if

is one of the following reasons: a) the personal data is not

longer necessary in relation to the purposes for which they were collected or submitted

otherwise processed, b) the data subject revokes the

consent on which the processing is based in accordance with Article 6 paragraph

1 point a) or Article 9 paragraph 2 point a) and there is no other legal basis

for processing (…)". Next, the provision of paragraph 3 of the same article

provides for derogations from the right to erasure, defining, among other things: "3. The

3 recital 28 provides that: "The provision of pseudonymisation in personnel data

actor can reduce risks for data subjects and facilitate them

controllers and processors to comply with the relevant procedures regarding

data protection. The explicit introduction of "pseudonymization" in this regulation does not

is intended to preclude any other data protection measure'.

8

9

paragraphs 1 and 2 do not apply to the extent that the processing is necessary:

(…) b) to comply with a legal obligation that imposes the processing based on it

Union law or the law of the Member State to which the person responsible belongs

processing or for the fulfillment of a duty performed in the public interest

or in the exercise of public authority delegated to the controller,

c) for reasons of public interest in the field of public health in accordance with the article

9 paragraph 2 points h) and i), as well as article 9 paragraph 3 d) for purposes

numbering in the public interest, for purposes of scientific or historical research

or for statistical purposes in accordance with Article 89 paragraph 1, if the right

referred to in paragraph 1 is likely to make impossible or hinder

to a large extent the achievement of purposes of said processing, or e) for the establishment,

exercising or supporting legal claims".

Accordingly, Article 34 of Law 4624/2019 introduces, pursuant to Article 23 of

GDPR limits the right to erasure and provides: "1. If the delete in

case of non-automated processing due to its particular nature

storage is not possible or is only possible with a disproportionately large effort and

the interest of the data subject for the erasure is not considered important,

the subject's right and the controller's obligation do not exist

to delete personal data in accordance with article 17 paragraph

1 of the GDPR, except for the exceptions mentioned in article 17 paragraph 3 thereof

GDPR. In this case, the deletion is replaced by its limitation

processing in accordance with Article 18 of the GDPR. The above paragraphs do not apply,

if the personal data has been processed illegally (...) 3.

In addition to Article 17 paragraph 3 letter b) of the GDPR, paragraph 1 applies

according to the case of article 17 paragraph 1 letter a) of the GDPR, if the

deletion will occur when in conflict with legal or contractual retention periods".

7. Because, in the case under consideration, from the data in the case file,

it follows that the AXA insurance company, as data controller, in accordance with

those defined in the provision of article 4 par. 7 of the GDPR, should in principle have

satisfy A's request from ... regarding deletion from her records

company's personal data and members of his family, which

were collected in the name of the complainant himself by AXA insurance

company with his consent, in accordance with the provisions of article 9

par. 2 item a' of the GDPR, pursuant to the insurance application from ...

pre-contractual stage of concluding a relevant insurance contract, which, in the end,

due to the relevant terms of the insurance policy the complainant did not

accepted and never signed. In this case, the AXA insurance company, as
data controller, due, in accordance with the provisions of article 17
par. 1 item b' of the GDPR, to satisfy the aforementioned deletion request
Ah, since the latter with his request from ... essentially revoked the positive
declaration of intent that he had provided to the insurance company in question for the
collection of his personal data for the purpose of the insurance application and not
there is another legal basis for the specific processing. Besides, it doesn't happen
case of legal deviation from the right of erasure to maintain the
of personal data, in accordance with the provisions of article 17 par. 3
of the GDPR, not even in this case the exercise of the right to erasure
replaced by the possible anonymization of the collected personnel data
character. Furthermore, AXA's claim is rejected as unfounded
insurance company for a contractual period of retention of the data in question,
pursuant to articles 34 par. 3 of law 4624/2019 and 192 of the Civil Code, since the
aforementioned provision of Law 4624/2019 regarding deletion in case
non-automated processing, does not apply in this case to
automated processing carried out by AXA in its information
systems.
8. Because following these, the Authority taking into account, among others, in particular, the
Opinions 15/2011 "regarding the definition of consent" and 5/2014 "regarding the
anonymization principles' and the guidelines 'concerning consent
based on regulation 2016/679" of the working group of article 294, as well as the
relevant directives of the European Network Security Agency and
of Information (ENISA)5, considers that in this particular case it was on its part
AXA insurance company violation of A's right to erasure according to article
17 of the GDPR. Furthermore, regardless of the issue of the relationship between the deletion

and the anonymization of personal data without the possibility

4 WP187 from 13.07.2011, WP216 from 10.04.2014 and WP259 rev.1 as finally revised and

were issued on 10.04.2018, respectively, available on the website http://ec.europa.eu/justice/data-

protection/index_en.htm

5 In particular, Pseudonymisation techniques and best practices from 03.12.2019 available on the website

https://www.enisa.europa.eu.

identification of the specific natural person6, however, AXA insurance

company, as controller, does not prove but neither does it invoke

existence of a reason, based on the GDPR, for the non-satisfaction of the right

the deletion of personal data and its substitution

deletion by anonymizing them. On the one hand, the relative does not constitute such a reason

provision and invocation of the personal data management policy

character to the extent that it is not supported by the GDPR, on the other hand, the choice of

technical specifications of the information system of AXA insurance

company to the extent that it is not supported by the GDPR. The Authority, during its exercise

corrective power, in such a way as to impose, if the case arises, the

effective, proportionate and deterrent measure according to article 83 of the GDPR, according to

and with the Guidelines "for the implementation and determination of administrative

of fines for the purposes of regulation 2016/679" of the working group of the article

297, when evaluating the data in order to select the appropriate one

corrective measure, considering, in particular, that the specific violation referred to

processing of a special category of personal data (health data)

constitutes an individual case (article 83 par. 2 letter a) and evaluates as

mitigating circumstance (article 83 par. 2 letter k) the fact that AXA insurance

company followed a practice harmonized with the provisions of the Code

Code of Conduct of the Association of Insurance Companies for the preservation of personal

data of the prospective insured for five years, in case of non-contract

insurance contract, which, however, due to the fact that it has not been approved by the Authority,

cannot be used as evidence of its compliance with

GDPR (article 24 par. 3). The legality of the above provision of the draft Code

will be decided by the Authority when examining the Code as a whole.

The beginning

FOR THOSE REASONS

a) considers that the AXA insurance company, as a data controller, has violated it

6 Compare relevant decision of the Austrian Supervisory Authority from 05.12.2018 (Geschäftszahl DSB-D123.270/0009-DSB/2018), available on the website https://www.ris.bka.gv.at.

7 WP 253 from 03.10.2017, available at https://edpb.europa.eu

exercise of A's right of deletion in accordance with the provisions of articles 5 and

17 of the GDPR and addresses, pursuant to article 58 par. 2 item. II of the GDPR,

reprimand the insurance company in question for violating these provisions

and

b) reserves the right to judge the legality of the retention of personal data

of prospective insureds for five years from their collection on

pre-contractual stage for the purpose of avoiding and combating insurance

fraud in the context of the examination of the draft Union Code of Conduct

of Insurance Companies that has been submitted for approval to the Authority, in accordance with

defined in the provision of article 40 par. 5 of the GDPR.

The president

The Secretary

Constantinos Menoudakos

Irini Papageorgopoulou

12