PRINCIPLE OF DATA PROTECTION

OF A PERSONAL CHARACTER

Athens, 16-10-2018

Prot. No.: G/EX/8187/16-10-2018

A P O F A S H 65/2018

The Personal Data Protection Authority met in composition

Plenary meeting at its headquarters on Tuesday 9-10-2018 following the invitation of its President,

in order to examine the issue of maintaining or modifying the plan

of a list of the details of the processing operations that are subject to the requirement for

carrying out an impact assessment regarding data protection following the

number 7/2018 of the relevant opinion issued by the European Protection Council

Data (ESPDN). The President of the Authority, Constantnos Menoudakos, was present

and the regular members Constantos Christodoulou, Antonios Symvonis, Spyrdon

Vlachopoulos, Constantos Lambrinoudakis, as rapporteur, Charalambos Anthopoulos

and Eleni Martsoukou, also as rapporteur. Present at the meeting, no

with the right to vote, was Ephrosyne Siugle, auditor, as assistant rapporteur and

Irini Papageorgopoulou, employee of the Department of Administrative Affairs, as

secretary.

The Authority took into account the following:

With its Decision No. 53/2018, the Authority decided to draw up a draft

of a list of the details of the processing operations that are subject to the requirement for

carrying out a data protection impact assessment (DPA) based

of article 35 par. 4 of the General Data Protection Regulation (EU) 679/2016

(GDPR). The Authority, before issuing the said list, implemented, according to

provided for in article 35 par. 6 of the GDPR, the coherence mechanism which

referred to in article 63 by announcing the draft list to the ESA. The ESPD

during the plenary session of September 25, 2018 issued the opinion

7/20181 regarding the Authority's EAPD list draft based on article 64 paragraph 1

of the GDPR. With this opinion, for which the Authority was informed electronically

way on October 2, 2018, the EDPS requests the Authority to amend the

draft list based on the recommendations included therein.

The Authority, after hearing the rapporteurs and the assistant rapporteur and after thorough

discussion,

SEVENTH E ACCORDING TO THE LAW

1. According to article 35, paragraph 1 of the GDPR:

"When a type of processing, i.e. using new technologies and taking into account the

nature, scope, context and purposes of our processing, may

poses a high risk to the rights and freedoms of natural persons,

the person in charge of processing carried out, before the processing, an evaluation of them

effects of the planned processing operations on data protection

of a personal nature. In an assessment, a set of similar ones can be considered

processing operations that involve similar high risks".

2. According to article 35 par. 3 of the GDPR, the EAPD is required in particular as

following cases:

"(...) a) systematic and extensive assessment of personal aspects regarding

natural persons, which is based on automated

processing,

including profile training, and on which decisions are based

produce legal results regarding the natural person or entity they affect

1 The opinion 7/2018 of the EDPS is available at the online address: https://edpb.europa.eu/our-

work-tools/our-documents/opinion-board-art-64/opinion-greece-sas-dpia-list_en

significantly the natural person,

b) a large amount of processing of the special categories of data that

referred to in Article 9 paragraph 1 or personal data which

concern criminal convictions and offenses referred to in article 10 or

c) systematic monitoring of the public as an accessible space on a large scale

(…)".

3. To provide a coherent interpretation of our processing operations in such

due to the high risk posed by the Group, it is required to carry out an EAPD

Our Article 29 Committee issued the "Guidelines for the assessment of

impact on data protection (DPA) and determination of

whether the processing "may entail a high risk" for its purposes

of regulation 2016/679" (WP248)2, which were approved by the EDPS during the first

its entirety. These guidelines are primarily aimed at

clarification of the concept of high risk and set the criteria for it

compilation of the lists to be approved by the Data Protection Authorities

based on article 35 par. 4 of the GDPR. Also, the purpose of the above text is yes or no

facilitation of the work of EPSD and the facilitation of our processors

which have the obligation to carry out an impact assessment.

4. According to articles 35 par. 4 and par. 6 of the GDPR:

"(par. 4) The supervisory authority prepares and publishes a list of the names of

processing operations that are subject to the requirement to carry out an evaluation

impact on data protection pursuant to paragraph 1. H

supervisory authority announces the list in question to the Protection Council

Data referred to in article 68".

"(par. 6) Before issuing the lists referred to in paragraphs 4

and 5, the competent supervisory authority applies the coherence mechanism which

referred to in Article 63, if those lists include activities

process related to the offer of goods or services to

2 The WP248 guidelines are available online

https://edpb.europa.eu/node/70 and http://ec.europa.eu/newsroom/article29/item-

detail.cfm?item_id=611236.

data subjects or by monitoring their behavior in

more than one Member State or which may significantly affect it

free circulation of personal data in the Union".

5. According to article 64 par. 1, 3, 6, 7 and 8 of the GDPR:

"(par. 1) The Council issues an opinion whenever a competent supervisory authority intends to

adopt any of the following measures. For this purpose, the competent authority

supervisory authority announces the draft decision to the Council, when: a) purpose

in the approval of a list of processing operations subject to the requirement for

carrying out a data protection impact assessment under

of article 35 paragraph 4 (…)".

"(par. 3) In the cases referred to in paragraphs 1 and 2, the Council

Data Protection issues an opinion on the subject matter submitted to it,

since it has not already issued an opinion on the matter. This opinion is issued

within a period of eight weeks by a simple majority of the members of the Council

Let's protect Data. This deadline could be extended by six more

weeks, taking into account the complexity of the matter(...)".

"(par. 6) The competent supervisory authority does not approve the draft decision referred to

in paragraph 1 within the deadline referred to in paragraph 3".

"(par. 7) The supervisory authority referred to in paragraph 1 receives in particular

taking into account the opinion of the Data Protection Officer and, within two weeks

upon receipt of the opinion, informs the President of the Council

Let's protect Data by electronic means whether to keep or not

amend the draft decision and, if applicable, the amended one

draft decision, using a standard format'.

"(par. 8) When the supervisory authority concerned informs its President

Data Protection Advisor, within the deadline referred to in

paragraph 7 of this article, that he does not intend to follow his opinion

Our Data Protection Advisor, in whole or in part, providing the relevant

reason a, Article 65 paragraph 1 shall apply".

6. In accordance with the recommendations contained in opinion 7/2018, the EDPS requests

by the Authority to amend the draft EAPD list as follows:

a. Regarding reference to WP248 guidelines: to add

that the draft catalog is based on the WP248 guidelines for

the impact assessment, which it supplements and further specifies.

b. Regarding the meaning of the big kl maca: to delete the quantitative ones

criteria and to add a reference to the definitions of the large kl maca

as listed in the guidelines for the Responsible

Data Protection (WP243) and impact assessment (WP248).

c. About the data processing that is carried out with the use

implant: to state that only the processing of health data with

use of an implant is subject to the requirement to perform an excision

impact.

7. In view of the above, the Authority, after taking into account and examining the above

recommendations, considers unanimously that the opinion 7/2018 of the EDPS should be accepted, to

make the necessary changes to the draft list he has submitted

initially to the EMS and to announce the amended list to the EMS.

8. For this purpose a) mention is added that the EAPD list is based on

WP248 guidelines, which it complements and further specifies,

b) the quantitative criteria included in the original plan are removed

directory to define the large processing load and is added

reference to the relevant definitions of the WP243 guidelines and

WP248 and c) item 2.2.5 of the catalog is amended by removing the

prediction for the use of implants given that the processing of data

health with the use of implants is covered by point 2.1 and in combination

with reference to 3.1.

FOR THOSE REASONS

The Authority unanimously decides to amend the draft list with the

of the processing operations that are subject to the requirement to carry out an evaluation

impact based on the recommendations of opinion 7/2018 of the EDPS and its announcement

of a modified list in the ESA. Following this, the amended list

is structured as follows:

disproportionate to the types of processing operations they are subject to

in the requirement to carry out a protection impact assessment

of data in accordance with article 35 par. 4 of the 3rd PD

Legal basis

In accordance with Article 35 para. 4 of the GDPR, the supervisory authority also prepares

publish a list of the details of the processing operations subject to

request for a data protection impact assessment

(EAPD) pursuant to par. 1 and announces this list to the European

Data Protection Board (DPA).

If this list includes processing activities such as

are related to the offer of goods or services to data subjects or with

the monitoring of their behavior in more than one member state or the

which may significantly affect the free circulation of data

in the Union, the coherence mechanism referred to in Article 63 shall apply.

Square

The DPA is required when a type of processing, namely with the use of new

technologies and taking into account the nature, the field of application, the context and the

purposes of our processing, may pose a high risk to the rights and

the freedoms of natural persons (article 35 par. 1 of the GDPR). Indicative

cases in which an EAPD is required are listed in article 35 paragraph 3

of the GDPR.

To provide a more coherent set of processing operations that require

carrying out EARP due to the high risk involved, its Working Group

Article 29 issued the guidelines with the title "Guidelines for

the data protection impact assessment (DPA) and

determining whether the processing "may entail a high risk" for

the purposes of regulation 2016/679" (WP248 rev.01). The above guidelines

lines define nine criteria that managers should use

process to determine whether or not an EAP should be carried out.

Definition of the large kl maka

In determining whether processing is carried out on a large scale

it is recommended that the following parameters be specifically taken into account based on

of the aforementioned WP248 guidelines as well as the guidelines

of lines with the line "Guidelines on data protection officers

data" (WP243):

a. the number of data subjects involved, specifically

number as a percentage of the relevant population;

b. the volume of data and/or the range of different data items that

undergo processing;

c. the duration or permanent nature of our data processing activity;

d. the geographical scope of our processing activity.

Processing operations subject to a GDPR requirement

This list groups and further specifies the details of the acts

of processing that are subject to the requirement to carry out a DPA with quotation and

indicative examples. This list is not exhaustive and it is not

the obligation to carry out an EAPD in each case is neither preserved nor changed

compliance with the conditions of article 35 par. 1 of the GDPR. The directory in question

is based on article 35 of the GDPR and its paragraphs 1 and 3 as well as on

impact assessment guidelines (WP248), which complement

and specializes further.

The criteria for carrying out EAPD are grouped into the following three

blame:

-

-

-

1st category: based on the data and purposes of processing.

2nd category: based on the type of data and/or their categories

subjects.

3rd category a: based on the additional features and/or those used

through processing let's.

The implementation of EAPD is considered mandatory when at least one of the following is met

criteria of the 1st or 2nd category let. Yes, it is also mandatory when one occurs

at least criterion for the 3rd category and the processing concerns especially

1st

charge, and/or with public data and/or charges

processing purposes

subjects of the 2nd category let.

1st category: first and purpose of processing

1.1 Systematic assessment, grading, prediction, prognosis and training

profl, id as aspects concerning the financial situation, the health, the

personal preferences or interests, credibility or behavior, position

or the movements or creditworthiness of the data subjects.

Related examples are yes the case, when a financial

strictly checks its customers based on creditworthiness data or

data for the fight against money laundering

activities and terrorist financing or data on

fraud crimes, or the event, in which a biotechnology company provides

direct to consumers genetic tests to assess and predict

the risks of disease/health.

1.2 Systematic data processing aimed at receiving automated

decisions, which produce legal results regarding the subjects

of the data or significantly affect the data subjects by

in a similar way and may lead to exclusion or discrimination against him

natural person.

Related examples include the automatic denial of an online credit card

or electronic recruitment practices without human intervention (ref. 71 of

GDPR) or the automatic refusal of insurance provision.

1.3 Systematic data processing that may prevent the subject from

exercise his rights or use a service or contract, i.e.

when data collected by them are taken into account.

Relevant examples are the case, when the bank controls them

its customers using a credit rating database to

to decide whether to grant them a loan or not, the registration of the subject in

"black" network, such as the network of mobile phone providers (telephones), the

registration of the subject in whistleblowing systems.

1.4 Systematic data processing concerning the preparation of profiles for the purpose

of the promotion of products and services if the data is combined with

data collected by them.

1.5 Systematic and large-scale processing for monitoring, the

observation or control of natural persons using data that

collected through video surveillance systems or through networks or by any

another medium in public space, public as accessible space or private accessible space

to an unlimited number of people. Includes tracking of movements

or the location/geographical location in real time or not of identified or

identifiable natural persons.

Related examples are the use of cameras in a shopping center or in stations

means of mass transport, or the processing of passenger location data in

airport or on public transport. Also, tracking via wi-fi

systems (wi-fi tracking) of visitors to shopping centers or processing a

data via drones.

1.6 Large-scale systematic processing of personal data

concerning health and public health for purposes of public interest,

such as the introduction and use of electronic prescription systems and

introduction and use of an electronic file or an electronic health card.

1.7 Large-scale systematic processing of personal data with

for the purpose of introducing, organizing, providing and controlling the use of services

electronic governance, as defined in article 3 of Law 3979/2011 as

apply.

kl makas

2nd category: type of data and/or categories of subjects

2.1 Megalis

process a

data

(including genetic and biometric for the purpose of

indisputable identification of a person) referred to in article 9 par. 1 and

of the data referred to in article 10 of the GDPR.

of exceptional character as

2.2 Systematic and large-scale processing of particularly important data or

categories

of

specialists

2.2.1 social welfare data (data on poverty,

unemployed, social work, etc.),

2.2.2 electronic communications data, including data

content such as e-mail, metadata and

of geographic location/location data, with the exception of

recording of telephone conversations in accordance with article 4 par. 3 thereof

Law 3471/2006,

2.2.3 data relating to a national identity number or other identifier

general application identification number or change of conditions and

terms of processing and use of these and related data

personal,

2.2.4 data included in personal documents, diaries,

notes from an electronic reader (e-reader) and in applications

life logging, which offer monitoring capabilities

notes and very personal information,

2.2.5 data collected or generated by devices (such as those with

sensors) i.e. through the applications of the 'internet of things' -

IoT' (such as smart TVs, smart home devices, connected

games, smart cities, smart energy meters, etc.) and/or with

use of other means.

2.3 Systematic monitoring – if it is permissible – of the position/location

as well as the content and metadata of their communications

employees with the exception of the records for security reasons if n

processing is limited to absolutely necessary data and is specific

documented. A relevant example that falls under the obligation to carry out an EAPD

was the use of DLP systems.

Systematic processing of biometric data of employees for the purpose of

indisputable identification of a person as well as their genetic data

workers.

3rd category: additional features and/or used means of our processing

3.1 Innovative use or application of new technologies or organizational solutions, such as

may include new forms of data collection and use, with

possible high risk for the rights and freedoms of individuals

of persons such as the combined use of fingerprints and

facial recognition for improved physical access control, or applications

mhealth or other "smart" applications, from which profiles are created

users (e.g. daily habits), or artificial intelligence applications or

publicly accessible blockchain technologies that include personal

data.

3.2 Combining and/or correlating personal data from multiple sources or sources,

from two or more processing operations implemented for different

purposes and/or by different controllers let us process in a way that will

could exceed the reasonable expectations of the data subject.

3.3 In case the processing concerns data, which have not been collected by

the subject and the information of the subjects in accordance with Article 14 GDPR

proves impossible or would require a disproportionate effort or is likely to

make impossible or seriously impair the achievement of its purposes

let's edit.

Revision of the directory

The above list is subject to a regular review every two years or an extraordinary one

revision in case of significant developments at a technological level or at

business models, as well as in the event of a change in its purposes

let's process since the young people for this purpose involve a high risk.

The president

The Secretary

Constantinos Menoudakos

Irini Papageorgopoulou