Athens, 27-04-2020

Prot. no.: G/EX/2883/27-04-2020

PRINCIPLE FOR DATA PRIVACY

FOR OPIC CHARACTER

A P O F A S H 8 /2020

The Personal Data Protection Authority met, after

invitation of its President, to a regular meeting via teleconference on 07-

04-2020 following the meetings of 25.02.2020, 03.03.2020 and 10.03.2020

at its seat, in order to examine the question concerning the definition

additional requirements for the accreditation of the organizations that grant

certifications to controllers and processors in accordance with

articles 42 and 43 of Regulation (EU) 2016/679 on the protection of natural

persons against the processing of personal data (General

Data Protection Regulation – GDPR). They were attended by the President,

Constantinos Menudakos, and the regular members Pyridon Vlachopoulos,

Konstantinos Lambrinoudakis, Charalambos Anthopoulos, as rapporteur and Eleni

Martsoukou, also as rapporteur. they also attended the meeting by mandate

of the President, without the right to vote, the expert scientists Euphrosyne Yugle and

Konstantinos Limniotis, informatics, as assistant lecturers, who provided

clarifications and left before the conference and decision making, as well

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

as secretary.

The Authority took into account the following:

Article 42 paragraph 1 of the GDPR provides that the Member States, the supervisory

authorities, the European Data Protection Board (EDPB) and the Commission

encourage the establishment of data protection certification mechanisms. And this
because the establishment of these voluntary accountability tools can improve the
transparency and compliance with the GDPR and to allow their subjects
data to assess the level of data protection of the relevant
products and services (recital 100 GDPR).
In particular, compliance with an approved certification mechanism may
be used as evidence of compliance with obligations
of the data controller (Article 24 par. 3 GDPR) or as evidence to prove
that the processor provides sufficient assurances in accordance with par. 1
and 4 of article 28 (article 28 par. 5 GDPR). It is also taken into account during
making a decision regarding the imposition of an administrative fine as well as regarding
the amount of the administrative fine (Article 83 paragraph 2 letter j) GDPR).
The certification is granted by a certification body accredited for this purpose,
based on article 43 of the GDPR, to a controller or executor
processing, who has submitted the relevant processing to the mechanism
certification. The accreditation of certification bodies is of particular importance as
provides official confirmation of the relevant competence of these bodies
making it possible to develop trust in the certification mechanism. THE
accreditation of a certification body is carried out by the competent supervisory authority or
the national accreditation body or by both of these bodies (Article 43
par. 1 GDPR) and is granted for a maximum period of five years, and may
revised under the same conditions, provided that the certification body
meets the requirements of article 43 (article 43 par. 4 GDPR). If the accreditation
carried out by the national accreditation body according to the EN-
ISO/IEC 17065/2012
(ISO 17065), the

additional requirements set by the competent supervisory authority.

The Authority after hearing the rapporteurs, as well as the assistant rapporteurs, the

who then withdrew, and after a thorough discussion,

2

SEVENTH E ACCORDING TO THE LAW

1. article 43 paragraph 1 of the GDPR provides that "With the reservation of the duties

and the powers of the competent supervisory authority in accordance with articles 57 and 58,

the certification bodies that set the appropriate level of expertise in

in relation to data protection, after informing the supervisory authority

in order to be able to exercise its powers under Article 58

paragraph 2 in point h) where they request, grant and renew permits. The

member state ensures that the accreditation of said certification bodies

do one or both of the following:

a) the supervisory authority that is competent pursuant to articles 55 or 56,

b) the national accreditation body designated in accordance with Regulation (EC)

no. 765/2008 of the European Parliament and of the Council (20), in accordance with

the EN-ISO/IEC 17065/2012 standard and in accordance with the supplementary requirements

that have been appointed by the supervisory authority that is competent by virtue of article 55 or

56."

2. article 43 par. 3 of the GDPR provides that "The trust of the bodies

verification as mentioned in paragraphs 1 and 2 of this article

carry out on the basis of the requirements that have been approved by the supervisory authority that

is competent under article 55 or 56, or by the Data Protection Board

pursuant to article 63. In the case of d trust pursuant to point b) of

paragraph 1 of this article, the aforementioned claims complement the

fraud provided for in Regulation (EC) No. 765/2008 and technical

rules describing the methods and duties of the certification bodies".

3. article 37 par. 1 of Law 4624/2019 provides that "The trust of the institutions

which grant grants in accordance with Article 42 of the GDPR carried out by

the National Credit System

(E.SY.D.) based

the standard EN-

ISO/IEC17065:2012 and in accordance with additional requirements defined

from beginning.".

4. article 43 paragraph 6 of the GDPR provides that "The fraud of paragraph 3

of this article and the provisions referring to article 42 paragraph 5

public from the supervisory authority in an easily accessible form. The supervisor Mr

3

authorities are also reporting these frauds and crimes to the Council

Data Protection".

5. article 64 par. 1 of the GDPR provides that "1. The Council issues an opinion

whenever a competent supervisory authority purports to adopt any of the following

measures. For this purpose, the competent supervisory authority shall announce the draft decision

to the Council, when:

(..) c) aims at approving claims for body accreditation in accordance with

Article 41 paragraph 3, certifying body in accordance with Article 43 paragraph

3 or the verification criteria of article 42 paragraph 5 (…)".

6. The EP issued the guidelines 4/2018 entitled "Directors

lines 4/2018 related to the accreditation of certification bodies based on the article

43 of the General Data Protection Regulation (2016/679)"1. their interest

is to provide guidance on how to interpret and apply them

provisions of article 43 of the GDPR in order to establish a coherent and

harmonized reference basis for the accreditation of certification bodies that

issue certifications in accordance with the GDPR. In particular, in the annex of

of these guidelines guidance is provided on ways

definition of additional accreditation requirements and are proposed

requirements that supervisory authorities and national accreditation bodies must

review to ensure GDPR compliance.

FOR THOSE REASONS

The Authority decides the definition of supplements, in relation to the ISO standard

17065, requirements for the accreditation of certification bodies to fulfill it

of its obligation as derived from article 43 par. 1 item b) and par. 3 of

GDPR as well as article 37 par. 1 of Law 4624/2019. These supplements

accreditation requirements are based on the guidelines 4/2018 of the European Commission

1 Available at the link https://edpb.europa.eu/our-work-tools/our-

documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

and are implemented by the E.Y.D. during the process of accreditation of the bodies

certification in combination with the above standard.

These supplementary accreditation requirements are submitted to

Data protection in accordance with the mechanism provided for in Article 63 of the GDPR

coherence and are not made public by the Authority until its completion

said procedure.

.

The president

The Secretary

Constantinos Menoudakos

Irini Papageorgopoulou

5