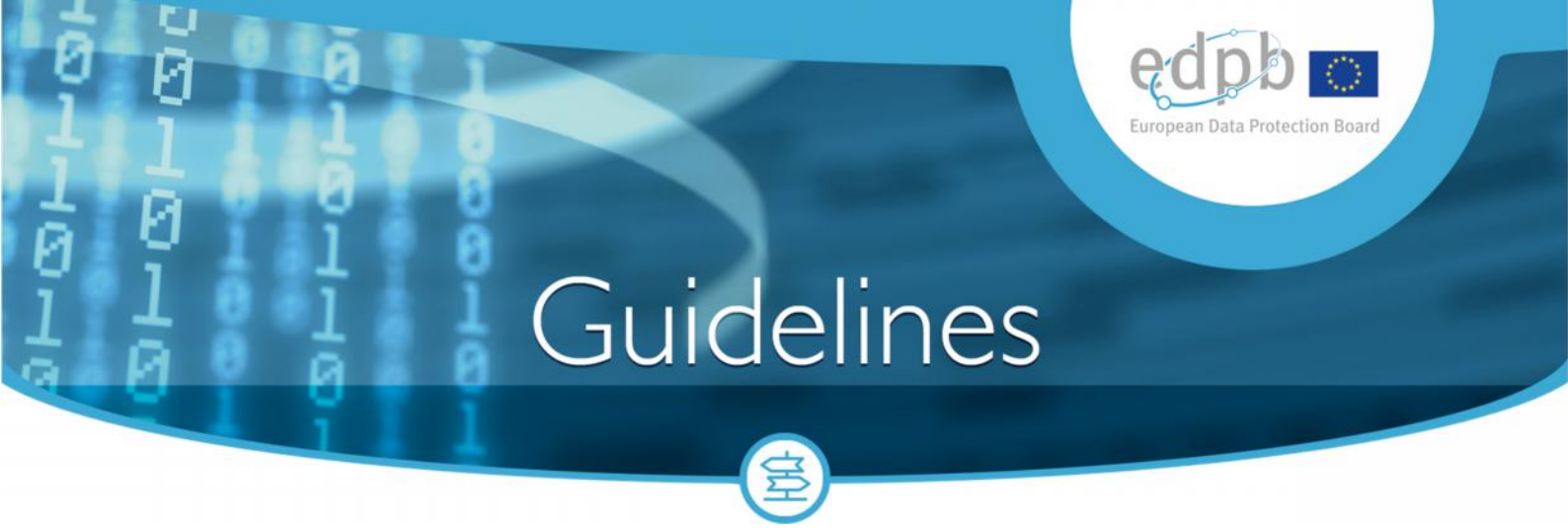

Annex 2

on the review and assessment of certification criteria pursuant to Article 42(5)

to the Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679

Version for public consultation

Adopted on 23 January 2019

adopted

Table of contents

ANNEX 2

1 INTRODUCTION

Annex 2 provides guidance for review and assessment of certification criteria pursuant to Article 42(5). It identifies topics that a data protection supervisory authority and the EDPB will consider and apply for the purpose of approval of certification criteria of a certification mechanism. The questions should be considered by certification bodies and scheme owners who wish to draft and present criteria for approval. The list is not exhaustive, but presents the minimum topics to be considered. Not all questions will be applicable, however they should be considered when drafting criteria and reasoning may be needed to explain why criteria do not cover specific aspects. Some questions are repeated, as they are from different perspectives. This guidance should be considered in accordance with the legal requirements provided by the GDPR and, where applicable, by national legislation.

2 SCOPE AND TOE

a. Is the scope for which the data protection criteria shall be used clearly described?

b. Is the scope meaningful to its addressed audience and not misleading?

- *Example: A "Trusted Company Seal" suggests that the processing activities of an entire company have been audited, even though only specified processing operations, e.g. the online payment process, are actually subject to certification.*

c. Does the scope include all relevant aspects of processing operations that are addressed by it?

- *Example: A "Privacy Health Mark" shall not exclude from evaluation data concerning health in order to circumvent requirements pursuant to Article 9.*

d. Does the scope allow meaningful data protection certification taking into account its nature, content, risk and the scope of processing?

- *Example: A scope focussing only on specific aspects of processing such as the collection of data but not on the further processing, excluding e.g. processing for the purpose of creating advertising profiles or the management of data subject's rights is generally not meaningful for those addressed by the certification, e.g. the data subject.*

e. Does the scope cover personal data processing in the relevant country of application or does it address cross border processing and/or transfers?

f. Do the scope and/or the criteria require a clearly described individual Target of Evaluation (ToE)?

- *Example: A "Privacy Seal" offering a general scope only requiring "a specification of the processing subject to certification" would not provide clear enough guidance on how to set and describe a ToE. E.g., a ToE describing processing operations, such as the*

"processing of personal data carried out by company "C" offering a social network" would be too general and do not clearly describe the particular processing operation(s).

- *Example: A (specific) scope, "The Privacy Vault Seal", addressing secure storage should describe in detail the requirements to meets this scope in its criteria, e.g. definition of vault, system requirements, mandatory technical and organisational measures (TOMs).*

g. Do the criteria require the ToE to include an identification of all relevant processing operations, illustration of data flows and a determination of the ToE's area of application?

- *Example: A certification mechanism offers certification of processing operations of controllers under the GDPR without specifying further the area of application (general scope). The criteria used by the mechanism require the applicant controller to determine the targeted processing operation (ToE) in terms of data types, systems and processes deployed.*

h. Do the criteria require from the applicant to make clear where the processing that is subject to evaluation starts and ends? Do the criteria require the ToE to include interfaces where interdependent processing operations are not included as part of the ToE? And is this satisfactorily justified?

- *Example: A ToE describing in sufficient detail the processing operation of a web based service such as including the registration of users, the provision of service, invoicing, logging of IP-addresses, interfaces to users and to third parties and excluding server hosting (yet including processing and TOM agreements).*

i. Do the criteria guarantee that the (individual) ToEs are understandable to its audience, including data subjects where relevant?

3 GENERAL REQUIREMENTS

a. Are all relevant terms used in the criteria catalogue identified, explained and described?

b. Are all normative references identified?

c. Do the criteria include the definition of data protection responsibilities, procedures and processing covered by the scope?

4 PROCESSING OPERATION, ARTICLE 42(1)

a. With respect to the scope (general or specific), are all relevant components of the processing operations (data, systems, and processes) addressed by the criteria?

b. Do criteria require identification of the valid legal bases of processing with respect to the ToE?

c. With respect to the ToE, do the criteria recognize the relevant phases of processing and the whole life-cycle of data including the deletion and or anonymisation?

d. With respect to the ToE, do the criteria require data portability?

e. With respect to the ToE, do the criteria allow identifying and reflecting special types of processing operations, e.g. automated decision making, profiling?

f. With respect to the ToE, do the criteria allow identifying special categories of data?

g. Do the criteria allow and require assessing the risk of the individual processing operations and the protection needs for the rights and freedoms of data subjects?

h. Do the criteria allow and require adequate account of the risks to the rights and freedoms of natural persons?

5 LAWFULNESS OF PROCESSING

a. Do the criteria require checking the lawfulness of processing for individual processing operations with respect to purpose and necessity of processing?

b. Do the criteria require checking all the requirements of a legal basis for individual processing operations?

c. …

6 PRINCIPLES, ARTICLE 5

a. Do the criteria adequately address all data protection principles pursuant to Article 5?

b. Do the criteria require demonstration of data minimisation for the individual ToE?

c. …

7 GENERAL OBLIGATIONS OF CONTROLLERS AND PROCESSORS

a. Do the criteria require proof of contractual agreements between processors and controllers?

b. Are controller processor agreements subject to evaluation?

c. Do the criteria reflect the obligations of the controller pursuant to Chapter IV?

d. Do the criteria require proof of review and updating of technical and organisational measures implemented by the controller pursuant to Article 24(1)?

e. …

8 RIGHTS OF THE DATA SUBJECTS

a. Do the criteria adequately address data subject's right to information and require respective measures to be put in place?

b. Do the criteria require that data subjects are granted adequate or even greater access and control of their data including data portability?

c. Do criteria require measures put in place providing for the possibility to intervene in the processing operation in order to guarantee data subjects' rights and allow corrections, erasure or restrictions?

d. …

9 RISKS FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS

a. Do the criteria allow and require assessing the risk to the rights and freedoms of natural persons?

b. Do the criteria provide or require a recognized risk assessment methodology? If appropriate, is it commensurate?

c. Do the criteria allow and require assessing the impact of the envisaged processing operations for the rights and freedoms of natural persons?

d. Do the criteria, , require prior consultation concerning the remaining risks that could not be mitigated, based on the results of the DPIA?

e. …

10 TECHNICAL AND ORGANISATIONAL MEASURES GUARANTEEING PROTECTION

a. Do criteria require technical and organisational measures providing for confidentiality of processing operations?

b. Do criteria require technical and organisational measures providing for integrity of processing operations?

c. Do criteria require technical and organisational measures providing for availability of processing operations?

d. Do criteria require measures providing for transparency of processing operations with respect to

    (1) Accountability?

    (2) Data subjects rights?

(3) Assessment of individual processing operations, e.g. for algorithmic transparency?

e. Do criteria require technical and organisational measures guaranteeing data subjects' rights, e.g. the ability to provide information, or to data portability?

f. Do criteria require technical and organisational measures providing for the ability to intervene into the processing operation in order to guarantee data subjects right and allow corrections, erasure orrestrictions?

g. Do criteria require measures providing for the ability to intervene into the processing operation in order to patch or check the system or the process?

h. Do criteria require measures providing for unlinkability or separation of data (anonymisation or pseudonymisation) or isolation of systems?

i. Do criteria require technical measures to implement data protection by default?

j. Do criteria require technical and organisational measures implementing data protection by design, e.g. a data protection management system to demonstrate, inform, control and enforce data protection requirements?

k. Do criteria require technical and organisational measures implementing appropriate periodic training and education for the personnel having permanent or regular access to personal data?

l. Do criteria require reviewing measures?

m. Do criteria require self-assessment/ internal audit?

n. Do criteria require measure to ensure that personal data breach notification duties are carried out in due time and scope?

o. Do criteria require monitoring of evolving privacy and technology issues and updating of the scheme as required?

p. …

11 OTHER SPECIAL DATA PROTECTION FRIENDLY FEATURES

a. Do the criteria require the implementation of data protection enhancing techniques?

b. Do the criteria require the implementation of enhanced data subjects controls to facilitate self-determination and choice?

c. …

12 CRITERIA FOR THE PURPOSE OF DEMONSTRATING THE EXISTENCE OF APPROPRIATE SAFEGUARDS FOR TRANSFER OF PERSONAL DATA

1. Criteria will be addressed in forthcoming guidelines on Article 42(2).
2. …

13 ADDITIONAL CRITERIA FOR A EUROPEAN DATA PROTECTION SEAL

a. Do the criteria envisage covering all Member States?

b. Are the criteria customizable to Member State data protection law or scenarios?

c. Do the criteria require an evaluation of the individual ToE with respect to sector specific Member State data protection law?

d. Do the criteria require the controller or processor to provide information to data subjects and business partners in the languages of Member States

   (1) On the processing/ToE?

   (2) Documentation of the processing/ToE?

   (3) The results of the evaluation?

e. …

14 OVERALL EVALUATION OF CRITERIA

a. Do the criteria reflect the scope adequately? Is the scope adequately reflected in the criteria?

b. Are the criteria commensurate with the size of the processing operation being addressed by the scope of the certification mechanism, the sensitivity of information and the risk of processing?

c. Is the certification statement in comparison with the criteria likely to make misleading representations of data protection standards,e.g. “gold standard” when in fact the processing merely meets state of the art?

- *Example: A mechanism called “Privacy Gold Standard” should not only provide criteria that allow controllers and processors to pass certification successfully, but is only compliant with the minimum requirements set by the GDPR.*

d. Are the criteria likely to improve data protection compliance of controllers and processors?

e. Will data subjects benefit in respect of their information rights, including explaining desired outcomes to data subjects?

f. …

For the European Data Protection Board

The Chair

(Andrea Jelinek)