Opinion 28/2022 on the Europrivacy criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to Article 42.5 (GDPR)

Adopted on 10 October 2022

The European Data Protection Board

Having regard to Article 63, Article 64(2) and Article 42 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Articles 10 and 22 of its Rules of Procedure.

(1) Member States, supervisory authorities, the European Data Protection Board (hereinafter "the EDPB or the Board") and the European Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms(hereinafter "certification mechanisms") and of data protection seals and marks, for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors, taking into account the specific needs of micro, small and medium-sized enterprises.[2] In addition, the establishment of certification mechanisms can enhance transparency and allow data subjects to assess the level of data protection of relevant products and services.[3]

(2) The criteria of certification form an integral part of a certification mechanism. Consequently, the GDPR requires the approval of the criteria of a national certification mechanism by the competent supervisory authority (Articles 42(5) and 43(2)(b) of the GDPR), or in the case of a European Data Protection Seal, by the EDPB (Articles 42(5) and 70(1)(o) of the GDPR).

(3) When a supervisory authority (hereinafter "SA") intends to propose the approval by the EDPB of a European data protection seal pursuant to article 42(5) of the GDPR, the SA should state the intention of the scheme owner to offer the certification mechanism in all Member States. In this case, the main role of the EDPB is to ensure the consistent application of the GDPR, through the consistency mechanism referred to in Articles 63, 64 and 65 of the GDPR. In this framework, according to Article 64(2) of the GDPR, the EDPB is approving the criteria of certification.

(4) This Opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors in the light of the core elements, which certification mechanisms have to develop. In particular, the EDPB assessment is carried out on the basis "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation" (hereinafter the "Guidelines") and their Addendum providing "Guidance on certification criteria assessment" (hereinafter the "Addendum"), for which the public consultation period expired on 26 May 2021.

(5) Accordingly, the EDPB acknowledges that each certification mechanism should be addressed individually and is without prejudice to the assessment of any other certification mechanism.

[1] References to "Member States" made throughout this Opinion should be understood as references to "EEA Member States".
[2] Article 42(1) of the GDPR.
[3] Recital 100 of the GDPR.

(6) Certification mechanisms should enable controllers and processors to demonstrate compliance with the GDPR. Therefore, its criteria should properly reflect the requirements and principles concerning the protection of personal data laid down in the GDPR and contribute to its consistent application.

(7) At the same time, scheme owner should ensure the alignment and conformity of the certification mechanism with any included or leveraged ISO standards and certification practices.

(8) As a result, certifications should add value to controllers and processors by helping to implement standardized and specified organizational and technical measures that demonstrably facilitate and enhance processing operation compliance to the GDPR, taking account of sector-specific requirements.

(9) The EDPB welcomes the efforts made by scheme owners to elaborate certification mechanisms, which are practical and potentially cost-effective tools to ensure greater consistency with the GDPR and foster the right to privacy and data protection of data subjects by increasing transparency.

(10) The EDPB recalls that certifications are voluntary accountability tools, and that the adherence to a certification mechanism does not reduce the responsibility of controllers or processors for compliance with the GDPR or prevent supervisory authorities from exercising their tasks and powers pursuant to the GDPR and the relevant national laws.

(11) In this Opinion, the EDPB addresses issues, such as the scope of the criteria, the applicability and relevance of the criteria in all Member States.

(12) This Opinion focusses on the certification criteria. In case the EDPB requires high level information on the evaluation methods in order to be able to thoroughly assess the auditability of the criteria in the context of its Opinion thereof, the latter does not encompass any kind of approval of such evaluation methods.

(13) The Opinion of the EDPB shall be adopted, pursuant to Article 64(2) of GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter. If the opinion of the EDPB concludes that the criteria cannot be approved at stake, the SA may resubmit the criteria for approval when the concerns expressed in the initial EDPB Opinion are addressed.

HAS ADOPTED THE FOLLOWING OPINION:

SUMMARY OF THE FACTS

1. In accordance with Article 42(5) of the GDPR and the Guidelines, the Europrivacy v.60 criteria (hereinafter the “draft certification criteria”, “certification criteria” or “criteria”) was drafted by European Center for Certification and Privacy (hereinafter the “scheme owner”).

2. The Supervisory Authority of Luxemburg (hereinafter the “LU SA”) has submitted the Europrivacy criteria of certification to the EDPB for approval pursuant to Article 64(2) GDPR on 28 September 2022. The decision on the completeness of the file was taken on 28 September 2022.

3. The Europrivacy certification mechanism is not a certification according to article 46(2)(f) of the GDPR meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international

organisations under the terms referred to in letter (f) of Article 46(2). Indeed, any transfer of personal data to a third country or to an international organisation, shall take place only if the provisions of Chapter V of the GDPR are respected.

2 ASSESSMENT

4. The EDPB has conducted its assessment of the criteria of certification for their approval under Articles 42(5) of the GDPR in line with the structure foreseen in Annex 2 to the Guidelines (hereinafter "Annex") and its Addendum.

5. The EDPB notes that the implementing guidance and suggested means of verification of the certification mechanism provided by the scheme owner are not always consistent throughout the catalogue of criteria. For instance, section T.2.3.2 requires that rules, policies, procedures or mechanisms are in place to detect and report intrusions (e.g. an intrusion detection system that monitors network traffic for suspicious activity and alerts when such activity is discovered), whereas the suggested means of verification refer to inspection and penetration test (required in section T.2.3.1). Although such inconsistencies do not fall under the scope of its assessment, the EDPB underlines that they may be a barrier to the accreditation of the certification body, unless rectified by the scheme owner.

2.1 Scope of the certification mechanism and Target of Evaluation (ToE)

6. The Europrivacy certification mechanism is a general scheme in that it targets a large range of different processing operations performed by controllers and processors from various sectors of activity. The main criteria of this certification mechanism are composed of the "Core criteria" and of the "TOMs checks and controls" concerning technological and organisational measures set in place to secure the processed personal data. A set of the "TOMs checks and controls" criteria are only applicable if the Target of Evaluation (hereinafter "ToE") processes special categories of data, criminal offense related data, or personal data of a child.

7. Additionally, the criteria also include "Complementary contextual checks and controls" that aim to ensure that the data processing involved in the ToE comply with domain-specific and technology-specific requirements. An informative matrix provided by the scheme owner describes to which categories of data processing operations, each set of the "Complementary contextual checks and controls" criteria apply.

8. The EDPB welcomes general schemes that include specific criteria so to make them scalable and applicable to specific processing operations or sector of activity. However, the EDPB also wishes to clarify that in the context of a general scheme, the completeness of the criteria relating to specific processing operations is not required and thus was not assessed in the context of this Opinion. In addition, the EDPB recalls that when it publishes documents related to specific processing activities, such documents shall be taken into account by the scheme owner and the accredited certification bodies.

9. The criteria applicable to the specification of the ToE are defined in the requirements available in A.2.1.1. The specific rules applicable to the process to be followed by the applicant and by the certification body in order to define the ToE are specified by the Europrivacy scheme (10.2 - Pre-certification Activities).

10. The Board notes in the documentation related to the scope of the certification mechanism provided by LU SA that the Europrivacy scheme applies to controllers and processors established in the European Union (EU) or in the European Economic Area (EEA). The applicability of the criteria is defined depending on the role and responsibilities of the applicant

11. The Board notes that a data controller can submit to the Europrivacy certification process a ToE which is subject to joint-controllership (criteria A.2.7.1). In case the ToE is subject to joint-controllership, the Board wishes to underline that the the accredited certification body will have to carefully conduct the application process to ensure that the ToE is meaningful and that the applicant is fully responsible for the compliance of the ToE with all obligations under the GDPR that the certification mechanism aims at demonstrating. As a consequence, the arrangement concluded between the applicant and the other joint controllers involved in the ToE with regards to their respective responsibilities for compliance with the obligations under the GDPR[4] might might – depending on the context of the processing activities of the ToE - prevent the applicant to fulfil the criteria of certification.

12. The Board notes that the data processing of genetic data is excluded from the scope of the Europrivacy certification mechanism. As a consequence, the assessment of the criteria conducted by the Board does not cover the suitability of the criteria for ToE that would include such data processing.

2.2 Processing operations

13. The criteria address the relevant components of the processing operations (data, systems, and processing) with respect to the general scope of the certification mechanism. In particular, the criteria allow identifying special categories of data as defined in Article 9 of the GDPR (section G.2 of the criteria - Special Data Processing).

2.3 Lawfulness of processing

14. The criteria require checking the lawfulness of the data processing for each individual processing operations in the ToE and require checking the requirements of a legal basis as defined in Article 6 of the GDPR (section G.1 of the criteria - Lawfulness of Data Processing).

2.4 Principles of data processing

15. The criteria adequately address the data protection principles pursuant to Article 5 of the GDPR. In particular, the criteria require the applicant to demonstrate that the personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

2.5 General obligations of controllers and processors

16. The criteria reflect the obligations of the controller pursuant to article 24 of the GDPR (G.4 - Data Controller Responsibility) and require the evaluation of processor-controller contractual agreements

[4] *The determination of their respective responsibilities must in particular regard the exercise of data subjects' rights and the duties to provide information. In addition to this, the distribution of responsibilities should cover other controller obligations such as regarding the general data protection principles, legal basis, security measures, data breach notification obligation, data protection impact assessments, the use of processors, third country transfers and contacts with data subjects and supervisory authorities* (Guidelines 07/2020 on the concepts of controller and processor in the GDPR)

in accordance with Article 28 of the GDPR (section G.5 of the criteria - Data Processors or sub Processors).

17. The criteria require all applicants to appoint a Data Protection Officer (DPO) even in the case where the applicant is not required to designate a DPO according to Article 37 of the GDPR. The criteria check that the DPO meet the requirements under Articles 37 to 39 (section G.9 of the criteria - Data Protection Officer).

18. The criteria check the content of the records of processing of activities in accordance with Article 30 of the GDPR (section G.5.3 of the criteria - Records of processing activities).

2.6 Rights of the data subjects

19. The criteria adequately address data subject's right to information in accordance with Chapter III of the GDPR and require respective measures to be put in place. The criteria also 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 (section G.3 of the criteria - Rights of the Data Subjects).

2.7 Risks for the rights and freedom

20. The criteria require assessing the risk to the rights and freedoms of natural persons of the data processing involved in the ToE in accordance with Article 35 of the GDPR (section G.8 of the criteria - Data Protection Impact Assessment).

2.8 Technical and organisational measures guaranteeing protection

21. The criteria require the application of technical and organisational measures providing for confidentiality, integrity and availability of processing operations. The criteria also require the application of technical measures to implement data protection by design and by default in accordance with Article 25 and Article 32 of the GDPR (section G.6 of the criteria - Security of Processing and Data Protection by Design, Section T.1/T.2 of the criteria – Core Security Requirements/Extended Security Requirements).

22. The criteria require the application of measure to ensure that personal data breach notification duties are carried out in due time and scope in accordance with Article 33 and 34 of the GDPR (section G.7 of the criteria - Management of Data Breaches).

2.9 Criteria for the purpose of demonstrating the existence of appropriate safeguards for transfer of personal data

23. The criteria require identifying all personal data transfers to third countries and to international organizations involved in the ToE and substantiating the choice made regarding the data transfer mechanism providing for appropriate safeguards, pursuant to Chapter V of the GDPR (section G.10 of the criteria - Transfers of personal data to third countries or international organisations).

3. ADDITIONAL CRITERIA FOR A EUROPEAN DATA PROTECTION SEAL

24. According to the Guidelines, the assessment shall include the question on "whether the criteria are able to take into account Member State data protection laws or scenarios". Section G.1.1.3 of the criteria requires the applicant to provide such an assessment in a National Obligations Compliance Assessment Report (NOCAR). The Board notes that such report shall include an assessment of the

national obligations applicable to the ToE and will document the measures taken by the applicant to comply with applicable rules and, possibly, ongoing corrective actions. The applicant shall not use the key complementary national requirements list provided by the scheme owner for each country as an exhaustive list of national obligations relevant for the ToE. The indicative list of minimal complementary checks and controls requirement provided by the scheme owner are not criteria of certification in the scope of this Opinion.

CONCLUSIONS / RECOMMENDATIONS

25. By way of conclusion, the EDPB considers that the Europrivacy criteria of certification are consistent with the GDPR and approves them pursuant to the task of the Board defined in article 70(1)(o) of the GDPR, resulting in a common certification (European Data Protection Seal).

26. The EDPB will register the Europrivacy certification mechanism in the public register of certification mechanisms and data protection seals and marks pursuant to Article 42(8).

FINAL REMARKS

27. This Opinion is addressed to the LU SA and will be made public pursuant to Article 64(5)(b) of the GDPR.

For the European Data Protection Board

The Chair