Opinion 19/2024 on the EuroPrise criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to Article 42.5 (GDPR)

Adopted on 16 July 2024

Contents

The European Data Protection Board

Having regard to Article 63, Article 64(2) and Article 42 of 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) GDPR), or in the case of a European Data Protection Seal, by the EDPB (Articles 42(5) and 70(1)(o) 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) 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 GDPR. In this framework, according to Article 64(2) 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) GDPR.
[3] Recital 100 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) 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:

1. SUMMARY OF THE FACTS

1. In accordance with Article 42(5) GDPR and the Guidelines, the draft "EuroPriSe Criteria Catalogue for the certification of processing operations by processors (scope: EU) v1.5" (hereinafter the "draft certification criteria", "certification criteria" or "criteria") was drafted by EuroPriSe Cert GmbH (hereinafter the "scheme owner"), a legal entity in Germany, and submitted to the Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, the competent German supervisory authority in North Rhine-Westphalia (hereinafter "DE-NRW SA").

2. The Supervisory Authority of Germany (hereinafter the "DE SA") has submitted the draft certification criteria to the EDPB for approval pursuant to Article 64(2) GDPR on 29 April 2024. The decision on the completeness of the file was taken on 29 May 2024.

3. The EuroPrise certification mechanism is not a certification according to article 46(2)(f) 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 GDPR are respected.

2. ASSESSMENT

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

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

5. The EuroPrise certification mechanism contains certification criteria of an EU-wide certification scheme for the certification of processing by processors. The subject of certifications to which the criteria catalogue applies are processing operations performed in products, processes and services or with the aid of (also several) products and services and with regard to which the certification applicant is acting as a processor. The main criteria of this certification mechanism are divided into the three sets of requirements, namely: from a legal perspective (set 1), from a technical and organisational measures perspective (set 2), and from the rights of the data subjects perspective (set 3).

6. Certification applicants under this scheme must be processors. This includes processors who are directly entrusted with the processing of personal data by a controller within the meaning of Article 4(7) GDPR. However, certification applicants may also be processors within the meaning of Article 28(2) and (4) GDPR (sub-processors).

7. When a processor - certified under the EuroPrise certification scheme - uses a sub-processor, the latter cannot claim that it has been certified under EuroPrise certification scheme. Only processing operations performed by the initial and certified processor are covered by the certification in such a case. However, sub-processors can also apply for certification, which would result in a stand-alone and independent procedure.

8. The Board notes in the documentation related to the scope of the certification mechanism provided by the DE SA that the EuroPrise scheme applies to processors established in the European Union (EU) or in the European Economic Area (EEA).

2.2 Processing operations

9. The scope of these criteria is not limited to certain types of processing operations. It is rather the methodology underlying a EuroPrise evaluation, which allows for certification of any processing operations by processors. It is, therefore, a universal methodological approach on the basis of which a large number of very different processing operations can be certified. Hence, it is of fundamental importance that the methodological requirements are adhered to, as this is the only way to ensure a uniform application of the certification criteria and a comparable level of testing across different certification procedures. The aim is to ensure comparability and reproducibility of the certifications issued and their results.

2.3 Lawfulness and principles of data processing

10. The criteria require the examination of whether the processing operations to be certified comply with the principles of data protection by design and by default (section 1.5 of the criteria), entailing the participation of the applicant in assisting the controller in the implementation of these principles. This allows assessing compliance with Article 25 GDPR, read in conjunction with Article 5 GDPR. While there is no criteria directly aiming at compliance with Article 6 GDPR - given the fact that the controller is responsible for the lawfulness of the processing - the criteria aim at ensuring that processors-applicants design the processing operations to be certified in a way that facilitates controllers' implementation of Article 5 GDPR data protection principles, including the principle of lawfulness of processing.

2.4 General obligations of controllers and processors

11. The criteria reflect the relationship between the processor and the controller. In particular, the criteria provide the obligation of the processor to have in place a template of data processing agreement with the controller, which includes all the requirements of Article 28 GDPR (section 1.2 of the criteria).

12. The criteria require applicants to appoint a Data Protection Officer (DPO) according to Article 37 GDPR and provide a proof of the appointment of the DPO (e.g. certificate of appointment). The criteria check that the DPO meet the requirements under Articles 37 to 39 (set 1, section 1.1 of the criteria).

13. The criteria check the content of the records of processing of activities in accordance with Article 30 GDPR (set 1, section 1.1 of the criteria).

2.5 Rights of the data subjects

14. The criteria adequately address data subject's right to information in accordance with Chapter III 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 (set 3 of the criteria).

2.6 Risks for the rights and freedom

15. The criteria require the processor to be aware of the possible risks to the rights and freedoms of natural persons for the data processing involved in the ToE. If the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons, several criteria ensure that the applicant demonstrates that the requirements of Article 35 GDPR are fulfilled in accordance with Article 35 GDPR (section 1.2.2 of the criteria, requirement n°6, section 1.3.2 of the criteria, section 1.3.3 of the criteria, section 2.1.5.1 of the criteria, section 2.1.5.9 pf the criteria).

2.7 Technical and organisational measures guaranteeing protection

16. 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 GDPR (section 1.5 of the criteria, section 2.1 of the criteria/other documents).

17. 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 GDPR (section 1.2.2 of the criteria, requirement n°6).

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

18. 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 GDPR (section 1.4 of the criteria).

3. ADDITIONAL CRITERIA FOR A EUROPEAN DATA PROTECTION SEAL

19. 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 4 of the criteria requires the applicant to comply with applicable national and relevant sector-specific data protection law. Furthermore, the Board understands that a "national law compliance report" - assessing in particular the compliance of the target of evaluation with applicable national data protection law requirements - shall be prepared by legal experts, provided that these experts have demonstrated the necessary level of expertise in the applicable national law.

CONCLUSIONS / RECOMMENDATIONS

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

21. The EDPB will register the "EuroPriSe Criteria Catalogue for the certification of processing operations by processors" certification mechanism in the public register of certification mechanisms and data protection seals and marks pursuant to Article 42(8).

FINAL REMARKS

22. This Opinion is addressed to the German supervisory authority in North Rhine-Westphalia and will be made public pursuant to Article 64(5)(b) GDPR.

For the European Data Protection Board

The Chair
Anu Talus