European Data Protection Board

Anu Talus
Chair of the European Data Protection Board

Accredia
Dr. Emanuele Riva
Vice General Director

Brussels, 01 August 2023

by e-mail only
Ref: OUT2023-0061

Subject: Reply to Accredia Letter [Ref: DC2023SPM054]

Dear Dr. Riva,

Thank you for your letter of 3 May 2023, by which Accredia contacted the European Data Protection Board ("the Board" or the "EDPB") in the context of the Europrivacy criteria of certification.

The Board appreciates your efforts to clarify the roles and competences of the different actors involved in certification and accreditation procedures under Regulation (EU) 2016/679 ("the GDPR")[1].

Please find below the approach of the EDPB regarding the different questions raised by Accredia.

[1] Regulation (EU) 2016/679 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 (General Data Protection Regulation).

Question 1 – Competence, adequacy, and effect of the EDPB Opinion

We received a comment that "only the EU Commission owns the legal authority to establish mechanisms for the recognition of certification procedures, data protection seals and marks by means of implementing acts." Could you clarify if this is the case and alternatively confirm that:

a) the EDPB is competent to adopt a European Data Protection Seal, without requiring the adoption of an implementing act by the EU Commission?

Yes, the European Data Protection Board (EDPB) is competent to approve the criteria for a European Data protection seal, without the prior adoption of an implementing act by the European commission.

Pursuant to Articles 42 (5) and 70 (1) (o) of the General Data Protection Regulation ((EU) 2016/679 (GDPR)), the European Data Protection Board (EDPB) has the authority to approve the criteria of a certification scheme intended to be used in all EEA Member States: a European Data Protection Seal.

The authority of the EDPB to approve a European Data Protection Seal is not dependent on the prior adoption of a delegated or an implementing act of the European Commission (EC), pursuant to Articles 43(8) and (9) GDPR.

For instance, the Europrivacy certification criteria have been approved by the EDPB as European Data Protection Seal in its Opinion 28/2022[2].

b) the GDPR and EDPB Guidelines allow for a scheme owner, like ECCP, to submit its certification criteria to Art. 42 GDPR without being itself an accredited certification body under Art. 43 GDPR?

Yes.

The EDPB's Guidelines 7/2022 define a certification scheme owner as an identifiable organisation which has set up certification criteria and the requirements against which conformity is to be assessed[3]. The scheme owner may coincide with a certification body accredited pursuant to Art. 43(1) GDPR, but there is no requirement for the two entities to be same[4].

[2] Opinion 28/2022 on the Europrivacy criteria of certification. Available at: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282022-europrivacy-criteria-certification.

[3] Guidelines 07/2022 on certification as a tool for transfers (07.02.2023) p. 11. Available at: https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202207_certificationfortransfers_en_1.pdf.

[4] EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals (2023) p. 2. Available at: https://edpb.europa.eu/system/files/2023-02/edpb_document_procedure_for_the_adoption_edpb_opinions_regarding_national_criteria_for_certification_european_data_protection_seals_en.pdf.

It should be noted that a scheme owner seeking approval of its certification criteria must always apply to a supervisory authority (SA), regardless of whether the certification scheme is intended to become a European Data Protection Seal or is only valid nationally[5].

For example, the Luxembourgish supervisory authority (LU SA), following its own assessment of the Europrivacy certification criteria drafted by the European Centre for Certification and Privacy (ECCP), submitted the Europrivacy certification criteria to the EDPB for approval, pursuant to 64 (2) GDPR, as a European Data Protection Seal. However, the approved criteria only become operational following accreditation of a certification body.

c) the EDPB Opinion 28/2022 is not limited to provide guidance to the Luxembourgish supervisory authority, but it constitutes a formal decision by EDPB that is valid, effective, and applicable to all EU and EEA Members States?

d) The Europrivacy criteria have been formally approved to serve as European Data Protection Seal that can be used in all EU and EEA Member States.

Please note that the answer replies to both points c) and d).

Yes, assuming that in relation to your question 1(d) you mean that the Europrivacy criteria have been formally approved to serve as *criteria* for a European Data Protection Seal that can be used in all EU and EEA Member States. It is important to note that the approved criteria are not identical to the data protection seal itself, since the criteria only become operational following the accreditation of a certification body.

According to Art. 42(5) GDPR, which refers to Art. 63 GDPR, the approval of a certification mechanism by the EDPB must follow the consistency procedure in Art. 64 GDPR.

As explained in the answer to question 1.b, when the competent SA receives an application for a certification mechanism intended to become a European Data Protection Seal, it will, after its assessment, refer the matter to the EDPB for an opinion, pursuant to Art. 64(2) GDPR.

Then, pursuant to Art. 64(3) GDPR, the EDPB will adopt an opinion that either approves or rejects that the certification criteria fulfil the requirements of the GDPR, interpreted in line with the EDPB Guidelines 1/2018 on certification[6].

---

[5] EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals (2023) p. 2.

[6] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation (Version 3.0), p. 36, available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf;
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) (10.10.2022), pp. 3, and 25-27. EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals (2023) p. 34 and Annex A.

Therefore, following the adoption of EDPB's opinion 28/2022, the Europrivacy certification criteria can be applied in all EEA Member States, without any additional criteria, by certification bodies – accredited in compliance with Art. 43 GDPR by the respective competent NAB or SA – to conduct certification under these criteria[7].

Question 2 – Competent authority for delivering national accreditation under art. 43 GDPR

Could you confirm that the accreditation/agreement procedures under Art. 43 GDPR are performed in principle by the competent authority of the country where the certification body is located?

Yes.

Accreditation for a European Data Protection Seal shall occur in the Member State where the certification body intending to operate the scheme has its' headquarters. Where other establishments or offices manage and perform certifications autonomously, each of these establishments or offices will require separate accreditation in the Member State where they are based[8].

In other words, if a certification body wants to issue certificates in Member State, in line with Art. 43 (1) GDPR, the certification body has to become accredited in accordance with the requirements for accreditation adopted by the SA of that Member State, pursuant to Art. 43 (3) GDPR.

According to art. 43(1), the accreditation process of certification bodies may be conducted either by the SA or the national accreditation body (NAB) or both.

Question 3 – Ability of EA to support Art. 43 GDPR Accreditation procedures

Can EA conduct a further and additional evaluation (fulfilling the EA-1/22 A 2020 requirements), to assess whether the Europrivacy scheme is an accreditable scheme under ISO/IEC 17065, in compliance with GDPR?

The assessment conducted by the SAs and the EDPB for the approval of the certification criteria for a European Data Protection Seal focuses on whether the criteria are compliant with the GDPR, interpreted in line with Guidelines 1/2018. The scope of the EDPB Opinion 28/2022 does not cover the accreditability of the Europrivacy certification scheme under EN-ISO/IEC 17065.

It should be noted that the EDPB, in its internal procedure for handling applications for approving certification criteria, recommends SAs, that do not accredit certification bodies themselves, to collaborate with their NAB[9]. Whilst this is not a requirement that stems from the GDPR, it is encouraged by the EDPB to facilitate the accreditability of certification mechanisms.

As to the evaluation of the accreditability by the EA, the EDPB considers that it is outside its mandate to determine whether such an evaluation may take place or not. Nevertheless, the EDPB welcomes all

[7] Guidelines 1/2018, p. 43.
[8] Guidelines 1/2018, p. 44.
[9] EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals (2023) p. 12.

initiatives aiming at harmonizing the approach adopted by NABs so as to ensure a consistent evaluation of the accreditability of European Data Protection Seals.

In this regard, the EDPB invites the EA to consider how the NAB that takes the lead for the assessment of the accreditability of a European Data Protection Seal could liaise with national SAs that perform accreditation of certification bodies, in accordance with Art. 43(1) (a) GDPR. The EDPB would also be open to exchange views and best practices with the EA, concerning the accreditability of certification mechanisms pursuant to the GDPR.

Question 4 – European Cooperation in Accreditation Procedures

a) Can a National Accreditation Body, recognized by Reg. 765, accredit for a GDPR European scheme a certification Bodies not established in its country? For example, could Accredia accredit a certification body established in another country for the Europrivacy scheme, if the National Accreditation Body of the other country agrees with such approach?

b) If yes, should Accredia apply for this accreditation the national criteria established by Italian DPA, or the additional criteria established by the other country's Supervisory Authority?

Please note that the answer replies to both points a) and b).

According to Art. 6 (3) of Reg. 765/2008: "national accreditation bodies shall be permitted to operate across national borders, within the territory of another Member State, either at the request of a conformity assessment body in the circumstances set out in Art. 7(1), or, if they are asked to do so by a national accreditation body in accordance with Art. 7(3), in cooperation with the national accreditation body of that Member State."

The EDPB considers that the legal situation of cross-border accreditation of certification bodies within the scope of the GDPR is inconclusive[10] and would invite the EA to discuss the topic further. In this matter, the EDPB reiterates that the accreditation of a certification body for a European Data Protection Seal shall be granted in the Member State where the certification body that is intending to operate the certification scheme has its' headquarters, or in the Member State where the certification body has other establishments or offices managing or performing certification autonomously. The competence over a certifying body is thus *not* dependent on where the accrediting NAB is located, which entails that the additional accreditation requirements that apply for the accreditation of the certification body are those approved by the certification body's competent SA.

[10] The EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) state that the fact that Art. 43 (1) GDPR allows accreditation by SAs is a derogation from the general principle that accreditation is to be conducted exclusively by NABs, means that the GDPR is *lex specialis* in relation to Art. 2(11) of Regulation. (EC) 765/2008. See para. 33 of the Guidelines 4/2018 (Version 3.0). Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf.

Question 5 – Possibility to Use Europrivacy for Voluntary Certifications

Would it be possible to use the Europrivacy criteria on a voluntary basis, for assessing compliance of data processing activities and delivering certification outside of the scope of Art. 42 and 43 GDPR [in non-EEA jurisdictions]?

No, the Europrivacy criteria as approved in Opinion 28/2022, the EuroPrivacy name, trade mark or brand and the approved EuroPrivacy Seal or any names or seals likely to be confused with it cannot be used for certification outside the scope of Art. 42 and 43 GDPR (see below), but this does not preclude the use of the Europrivacy criteria for self-assessment without any attestation of conformity.

First, it should be noted that GDPR certification pursuant to Articles 42 and 43 is a voluntary tool. Data controllers and processors are not required to hold a certification but they may use it as an element to demonstrate compliance with their obligations under the GDPR, as stipulated in Articles 24(3), 25(3), 28(5) and 32(3) GDPR. To that end, only certification criteria approved by a SA or the EDPB, may be relied upon to demonstrate compliance with the GDPR.

Accordingly, the use of certification criteria outside of the scope of Articles 42 and 43 GDPR would not have any of the legal effects anticipated by the GDPR. Whilst this does not preclude a controller or processor from using approved certification criteria as a tool for self-assessment of compliance with the GDPR, the data controller or processor could not in such a case refer to a certification, seal or mark as a certification pursuant to Articles 42 and 43 GDPR.

As to the Europrivacy certification criteria, it should be noted that the scope, as approved in Opinion 28/2022, is limited to controllers and processors established in the EU and the EEA. In this regard, the criteria cover – *inter alia* – obligations to assess compatibility with EEA Member State legislation complementary to the GDPR (cf. criteria G1.1.3 – National Regulation Compliance) and include requirements to notify competent SAs in certain situations, for example in case of a data breach (cf. criteria G7 – Management of data breaches). Hence, controllers or processors that are established outside the EU/EEA and outside the scope of the GDPR, are not in a position to comply with the entirety of the Europrivacy criteria and can therefore not obtain the Europrivacy European Data Protection Seal.

Finally, EDPB Guidelines 4/2018 clarify that data protection certificates, seals and marks "shall only be used" in compliance with Articles 42 and 43 GDPR and Guidelines 1/2018[11]. The purpose of this requirement is to ensure transparency and to enable other stakeholders and especially data subjects to quickly assess the level of data protection of relevant products and services provided by a certified controller or processor[12]. By contrast, the use of certification under the Europrivacy label outside the scope of the GDPR and the scope of the Europrivacy criteria approved in Opinion 28/2022, could create a situation of unfair competition, as entities certified under the label could be seen as having obtained a certification that demonstrates compliance with the GDPR. In the view of the EDPB, this

[11] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) (Version 3.0) Annex 1, section 4.1.3.
[12] Recital 100 GDPR.

could jeopardise the validity of and trust in the system of accreditation and certification under the GDPR.

However, reusing some of the Europrivacy criteria within a certification mechanism outside the scope of application of GDPR would be possible, if such use is without prejudice to any other applicable law (including intellectual property rights). Additionally it shall be clearly stated that the use of the criteria results in a certification which is different from the EuroPrivacy name, trade mark or brand and the approved EuroPrivacy Seal or any names or seals likely to be confused with it. Lastly, it shall be clearly underlined that it is not a GDPR certification.

Yours sincerely

Anu Talus

European Data Protection Board
Rue Wiertz, 60
1047 Brussels