EDSA-Dokument über das zu einer gemeinsamen Zertifizierung („Europäisches Datenschutzsiegel“) führende Verfahren zur Genehmigung von Zertifizierungskriterien durch den EDSA

angenommen am 28. Januar 2020

Inhalt

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 42 Absatz 5, Artikel 64 Absatz 2 und Artikel 70 Absatz 1 Buchstabe o der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, im Folgenden „DSGVO“),

gestützt auf das EWR-Abkommen und insbesondere Anhang XI und Protokoll 37, zuletzt geändert durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018,[1]

gestützt auf die Artikel 3 und 22 seiner Geschäftsordnung vom 25. Mai 2018 –

HAT FOLGENDES DOKUMENT ANGENOMMEN

1. Genehmigung EU-weiter Zertifizierungskriterien (Europäisches Datenschutzsiegel) durch den EDSA: Überprüfung, Vorlage, Zulässigkeit und Annahme

1.1. Vorlage

Programmeigner (d. h. Organisationen oder private Unternehmen, die selber nicht für die Erteilung von Zertifikaten zuständig sind) oder Zertifizierungsstellen sollten ihre EU-weiten Zertifizierungskriterien in folgender Anwendungsreihenfolge bei den betreffenden zuständigen Aufsichtsbehörden förmlich einreichen:

1) bei der für den Sitz derProgrammeigner[2] zuständigen Aufsichtsbehörde,
2) bei der Aufsichtsbehörde, die für den Sitz einer das Zertifizierungsverfahren durchführenden Zertifizierungsstelle zuständig ist[3], nach Maßgabe der Frage, in welchem Mitgliedstaat voraussichtlich die meisten Zertifikate erteilt werden.

Zudem können die zuständigen Behörden von sich aus Zertifizierungskriterien für ein EU-weites Zertifizierungsverfahren ausarbeiten[4].

Aufsichtsbehörden können gemäß Artikel 63 und Artikel 70 Absatz 1 Buchstabe o beim EDSA Kriterien für ein EU-weites Zertifizierungsverfahren nach Artikel 42 Absatz 5 zur Genehmigung einreichen[5]. Jede

[1] Soweit in dieser Stellungnahme auf die „EU“ Bezug genommen wird, ist dies als Bezugnahme auf den „EWR“ zu verstehen.
[2] Programeigner kann auch eine Zertifizierungsstelle sein.
[3] Die Akkreditierung der Zertifizierungsstelle (entweder durch die nationale Akkreditierungsstelle oder durch die zuständige Aufsichtsbehörde) schließt auch eine Bewertung des Zertifizierungsverfahrens ein und insbesondere die Prüfung der Frage, ob die vorgeschlagenen Bewertungsmethoden den genehmigten Zertifizierungskriterien angemessen sind. Gemäß Absatz 44 der vom EDSA veröffentlichten Leitlinien 1/2018 hat die Akkreditierung auch an dem Ort zu erfolgen, an dem die Zertifizierungsstelle ihren Sitz hat.
[4] In diesem Fall fungiert die Aufsichtsbehörde als Programmeigner.
[5] Eine Aufsichtsbehörde kann Zertifizierungskriterien nur dann zur Genehmigung einreichen, wenn sie bereits ihre Akkreditierungsanforderungen zur Genehmigung eingereicht hat.

Aufsichtsbehörde hat dabei nach Maßgabe der Zertifizierungsleitlinien des EDSA[6] zu überprüfen, ob die vorgeschlagenen Zertifizierungskriterien den in der DSGVO festgelegten Anforderungen an EU-weite Zertifizierungskriterien genügen. Zur Vereinfachung ihrer Überprüfung sollte die zuständige Aufsichtsbehörde die vom EDSA angenommene Vorlage für die Bewertung von Zertifizierungskriterien vollständig ausfüllen (dies gilt sowohl für den nationalen Teil der Vorlage als auch für den EU-spezifischen Teil). Dieses Dokument darf dem EDSA nur vorgelegt werden, wenn die zuständige Aufsichtsbehörde der Auffassung ist, dass die Kriterien vom EDSA genehmigt werden könnten (siehe Schritt 3a)[7].

1.2. Vorläufige Zulässigkeit der Zertifizierungskriterien

Falls die zuständige Aufsichtsbehörde der Auffassung ist, dass die vorgeschlagenen Kriterien nicht akzeptabel sind, teilt sie dies dem Programmeigner mitsamt der Gründe für ihre Entscheidung mit (siehe Schritt 3b).

Falls die zuständige Aufsichtsbehörde der Auffassung ist, dass die vorgeschlagenen Kriterien akzeptabel sind, teilt sie dem Programmeigner schriftlich mit, dass sie zur nächsten Verfahrensphase übergehen und die vorgeschlagenen Kriterien bewerten wird. Dadurch beginnt das nachfolgend beschriebene informelle Verfahren der Zusammenarbeit bei der Bewertung der Kriterien im Hinblick auf deren Genehmigung.

1.3. Zusammenarbeit (informelle Kooperationsphase auf Ebene der Aufsichtsbehörden)

Die Phase der informellen Zusammenarbeit ist eine wesentliche Voraussetzung für ein effizientes Genehmigungsverfahren des EDSA. Sie ermöglicht der besagten zuständigen Aufsichtsbehörde, die Bewertung der Kriterien vorzunehmen und dem Programmeigner die geforderte Rückmeldung zu geben. Die zuständige Aufsichtsbehörde hat den Programmeigner zeitnah über den jeweiligen Stand der einzelnen Phasen zu informieren.

Sie muss allen Aufsichtsbehörden den neuesten Stand mitteilen und um freiwillige Unterstützung durch maximal zwei Co-Reviewer bei der inhaltlichen Bewertung der Kriterien ersuchen (siehe Schritt 4). Die Anfrage bezüglich der Co-Reviewer ist per E-Mail an das Sekretariat des EDSA zu richten. Der E-Mail ist die von der zuständigen Aufsichtsbehörde ausgefüllte Bewertungsvorlage des EDSA beizufügen.

Die informelle Kooperationsphase (Schritte 4 bis 6) kann erst beginnen, wenn nachstehende Dokumente in englischer Sprache vorliegen und somit an andere Aufsichtsbehörden weitergeleitet werden können:

- die von der zuständigen Aufsichtsbehörde vollständig ausgefüllte Bewertungsvorlage des EDSA mit Angaben darüber, wie allen einschlägigen nationalen Rechtsvorschriften Rechnung getragen wurde und wie die geplante Einführung in den Mitgliedstaaten erfolgen soll, und
- eine Kopie der Zertifizierungskriterien einschließlich etwaiger sachdienlicher Anhänge.

Zertifizierungskriterien, die sich auf einschlägige mitgliedstaatliche Rechtsvorschriften beziehen, können, falls verfügbar, in der betreffenden Landessprache vorgelegt werden.

[6] Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679.
[7] Siehe Abschnitt 4.2 (Absätze 35 bis 45) der vom EDSA veröffentlichten Leitlinien für Zertifizierungskriterien.

Die Aufgabe der Co-Reviewer besteht darin, die zuständige Aufsichtsbehörde bei der Bewertung der vorgeschlagenen Zertifizierungskriterien zu unterstützen. Die Co-Reviewer haben Sachverständige für den jeweiligen Zertifizierungsbereich zurate zu ziehen. Nach erfolgter Bestätigung der Co-Reviewer sind deren Anmerkungen zu den Kriterien binnen dreißig Tagen nach Übermittlung der Dokumente an die Co-Reviewer vorzulegen. Die zuständige Aufsichtsbehörde berücksichtigt diese Anmerkungen bei ihrer anschließenden Bewertung. Die Überprüfung befasst sich hauptsächlich mit der Frage, ob die Zertifizierungskriterien technisch akzeptabel sind (siehe Schritt 5).

Im Anschluss an die gemeinsam mit den Co-Reviewern durchgeführte Überprüfung leitet die zuständige Aufsichtsbehörde die vorgeschlagenen Kriterien allen Aufsichtsbehörden weiter. Das Sekretariat des EDSA kann die Kommunikation zwischen den Aufsichtsbehörden unterstützen (siehe Schritt 6). Alle betroffenen Aufsichtsbehörden haben binnen 30 Tagen zu antworten. Wichtige Fragen können der zuständigen Untergruppe des EDSA zur Diskussion vorgelegt werden. Die Überprüfung dient dazu, sich darüber Gewissheit zu verschaffen, dass den nationalen Rechtsvorschriften in geeigneter Weise Rechnung getragen wurde. Sie schließt zudem eine Analyse der Frage ein, inwieweit die Kriterien mit den nationalen Rechtsvorschriften vereinbar sind. Reagieren die Aufsichtsbehörden nicht, wird die nächste Verfahrensphase in Bezug auf die Kriterien eingeleitet.

Die zuständigen Aufsichtsbehörden können erforderlichenfalls beschließen, die Schritte 5 und 6 zu wiederholen.

Die zuständige Aufsichtsbehörde kann dem Programmeigner nach jedem Schritt der informellen Kooperationsphase Gelegenheit geben, die Zertifizierungskriterien unter Berücksichtigung der Anmerkungen der Aufsichtsbehörden zu überarbeiten.

Im Anschluss an Schritt 6 kann die zuständige Aufsichtsbehörde um eine Zusammenkunft der EDSA-Untergruppe zwecks Erörterung der zu prüfenden Kriterien ersuchen, falls sie sich davon ein positives Ergebnis verspricht (siehe Schritt 7). Die zentralen Ergebnisse der Zusammenkunft werden von der zuständigen Aufsichtsbehörde in die Bewertungsvorlage des EDSA eingetragen. Die zuständige Aufsichtsbehörde kann etwaige in der Zusammenkunft angeregte Maßnahmen vorantreiben und der Programmeigner die Kriterien entsprechend überarbeiten.

Die zuständige Aufsichtsbehörde kann am Ende der informellen Kooperationsphase (in Absprache mit dem Programmeigner) entscheiden, ob sie die Zertifizierungskriterien dem EDSA zur förmlichen Genehmigung vorlegt. Dabei liegt die endgültige Entscheidung, ob die vorgeschlagenen Kriterien dem EDSA gemäß Artikel 63 DSGVO zur Annahme vorgelegt werden, bei ihr. Falls sie beschließt, die Zertifizierungskriterien dem EDSA nicht vorzulegen, ist das Verfahren damit beendet (siehe Schritt 8b). Falls die Zertifizierungskriterien zu einem späteren Zeitpunkt erneut vorgelegt werden, ist ein neues Prüfverfahren durchzuführen.

Der Programmeigner hat sich an der Überprüfung in der informellen Phase zu beteiligen. Die zuständige Aufsichtsbehörde informiert den Programmeigner über die in der Kooperationsphase erfolgten Anmerkungen und gibt ihm Gelegenheit, um Präzisierungen zu bitten und zu erwidern[8].

1.4. Förmliche Vorlage und Genehmigung (EDSA-interne Phase)

Die Genehmigung eines Europäischen Datenschutzsiegels erfolgt im Wege des Verfahrens zur Annahme einer Stellungnahme nach Artikel 64 Absatz 2.

[8] Die zuständige Aufsichtsbehörde muss sicherstellen, dass dem Programmeigner diese Möglichkeit bekannt ist und ihm diese Gelegenheit gegeben wird.

Es wird ersucht, dass die zuständige Aufsichtsbehörde jeweils den Arbeitsplan der CEH-Fachuntergruppe berücksichtigt, wenn sie ihre Vorlage über die IMI-Plattform vornimmt.

Die förmliche Vorlage hat über die IMI-Plattform zu erfolgen (Schritt 8a). Damit sie vom EDSA zugelassen werden kann, müssen folgende Zulässigkeitskriterien erfüllt sein:

- Sämtliche Dokumente sind in englischer Sprache einzureichen,
- die EDSA-Bewertungsvorlage muss von der zuständigen Aufsichtsbehörde vollständig ausgefüllt eingereicht werden (die Vorlage muss um die Ergebnisse der ersten Überprüfung ergänzt worden sein), und
- es ist eine Kopie der Zertifizierungskriterien einschließlich etwaiger Anhänge einzureichen.

Das Sekretariat des EDSA prüft jeweils, ob sämtliche erforderlichen Dokumente vollständig vorliegen. Es kann die zuständige Aufsichtsbehörde bitten, ihm binnen eines bestimmten Zeitraums zusätzliche Informationen zu übermitteln, um die Akte zu vervollständigen. Unbeschadet etwaiger Übersetzungen, die von Rechts wegen oder aus anderen Gründen erforderlich sind, gilt, dass der Antragsteller generell alle einschlägigen Dokumente sowohl in der Landessprache der zuständigen Aufsichtsbehörde als auch auf Englisch vorzulegen hat. Erforderlichenfalls werden die von der zuständigen Aufsichtsbehörde vorgelegten Dokumente (beispielsweise nicht von der Aufsichtsbehörde stammende bzw. erstellte Unterlagen) unverzüglich vom Sekretariat übersetzt. Wenn in derartigen Fällen die zuständige Behörde die Übersetzung gutheißt und der Vorsitz des EDSA und die zuständige Aufsichtsbehörde beschließen, dass das Verfahren somit abgeschlossen ist, übermittelt das Sekretariat die Akte den Mitgliedern des EDSA.

Die Stellungnahme des EDSA muss binnen acht Wochen, nachdem sein Vorsitz und (gegebenenfalls) die zuständige Aufsichtsbehörde beschlossen haben, dass das Verfahren abgeschlossen ist, angenommen werden. Die Annahmefrist kann unter Berücksichtigung der Komplexität des Gegenstands der Stellungnahme auf eigenen Beschluss des Vorsitzes oder auf Antrag mindestens eines Drittels der EDSA-Mitglieder um sechs Wochen verlängert werden.

Alle dem EDSA zur Abstimmung vorgelegten Stellungnahmen-Entwürfe müssen vom Sekretariat (und, falls vom Vorsitz so beschlossen, in Zusammenarbeit mit einem Berichterstatter und Mitgliedern der Fachuntergruppen) vorbereitet und ausgearbeitet werden. Je nach Umfang des Zertifizierungsverfahrens können Sachverständige anderer Untergruppen des EDSA für die Erstellung der Stellungnahmen herangezogen werden.

Je nach dem Zeitpunkt der Vorlage kann auf Beschluss des Vorsitzes per E-Mail oder im Rahmen einer CEH-Sitzung ein Team zusammengestellt werden, das den Entwurf erstellt. Der Aufruf nach Freiwilligen für das Entwurfsteam erfolgt durch das Sekretariat in Zusammenarbeit mit den Koordinatoren der CEH-Fachgruppen. Um Interessenkonflikte zu vermeiden, sollten dem Kern des Entwurfsteams keine Mitarbeiter der zuständigen Aufsichtsbehörde angehören. Gleichwohl kann dieses Kernteam jederzeit Fragen an die zuständige Aufsichtsbehörde richten.

Das Sekretariat und gegebenenfalls das Entwurfsteam prüfen die vorgeschlagenen Kriterien und die diesbezüglich eingereichten Dokumente einschließlich der Bewertungsvorlage und erstellen sodann den Stellungnahmen-Entwurf. Im Sinne der Konsistenz sind dabei stets die in früheren Stellungnahmen zum selben Thema getroffenen Feststellungen zu berücksichtigen. Bei der Erstellung des Stellungnahmen-Entwurfs kann die von der zuständigen Aufsichtsbehörde eingereichte Bewertungsvorlage des EDSA als interne Arbeitsunterlage verwendet werden. Diese Überprüfung muss innerhalb der geltenden Fristen für Stellungnahmen erfolgen.

1.5. Stellungnahme nach Artikel 64 Absatz 2 DSGVO

Der EDSA hat gemäß Artikel 64 Absatz 2 und Artikel 70 Absatz 1 Buchstabe o Stellungnahmen zu den in Artikel 42 Absatz 5 DSGVO beschriebenen Sachverhalten abzugeben bzw. über diesbezügliche Genehmigungen zu entscheiden (siehe Schritt 9)[9].

Die Annahme einer Stellungnahme des EDSA erfolgt nach Maßgabe von Artikel 10 seiner Geschäftsordnung[10]. Die die Stellungnahme nach Artikel 64 Absatz 2 beantragende Aufsichtsbehörde hat ihren Antrag laut Artikel 10 Absatz 3 der Geschäftsordnung schriftlich zu begründen. Im Hinblick auf die Genehmigung der zu einem Europäischen Datenschutzsiegel führenden Zertifizierungskriterien durch den EDSA muss die zuständige Aufsichtsbehörde eine Stellungnahme nach Artikel 64 Absatz 2 zu einer Angelegenheit mit Auswirkungen in mehr als einem Mitgliedstaat beantragen.

Das vom EDSA durchgeführte Genehmigungsverfahren endet jeweils mit der Genehmigung oder Ablehnung des eingereichten Antrags zur Genehmigung der vorgeschlagenen, zu einem Europäischen Datenschutzsiegel führenden Zertifizierungskriterien. Etwaige Folgemaßnahmen zu der vom EDSA abgegebenen Stellungnahme sind in Artikel 64 Absatz 2 nicht vorgesehen.

Die vom EDSA abgegebenen Stellungnahmen nach Artikel 64 Absatz 2 sind in allen Mitgliedstaaten anwendbar[11].

1.6. Weitere Schritte nach der Stellungnahme des EDSA

Nachdem der EDSA seine Stellungnahme zu den zu einem Europäischen Datenschutzsiegel führenden Kriterien angenommen hat, sind folgende Schritte zu unternehmen:

- Das Sekretariat veröffentlicht die vom EDSA abgegebene Stellungnahme mit der Genehmigung bzw. Ablehnung des Datenschutzsiegels.

Falls der EDSA den Antrag auf ein Europäisches Datenschutzsiegel im Wege einer positiven Stellungnahme genehmigt, gilt Folgendes:

- Die zuständige Aufsichtsbehörde teilt dem Programmeigner das Ergebnis des Antrags auf Genehmigung eines Europäischen Datenschutzsiegels mit.
- Die federführende bzw. koordinierende zuständige Aufsichtsbehörde stellt sicher, dass dem Sekretariat alle erforderlichen Dokumente für die Veröffentlichung im öffentlichen Register des EDSA zugeleitet werden.

Falls der EDSA den Antrag auf ein Europäisches Datenschutzsiegel im Wege einer negativen Stellungnahme ablehnt, gilt Folgendes:

[9] Artikel 64 Absatz 2 DSGVO sieht vor, dass jede Aufsichtsbehörde eine Stellungnahme zu einer Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat beantragen kann. Da das EU-Datenschutzsiegel EU-weite Auswirkungen hat, fällt die diesbezügliche Stellungnahme des EDSA nicht unter Artikel 64 Absatz 1, sondern unter Artikel 64 Absatz 2.

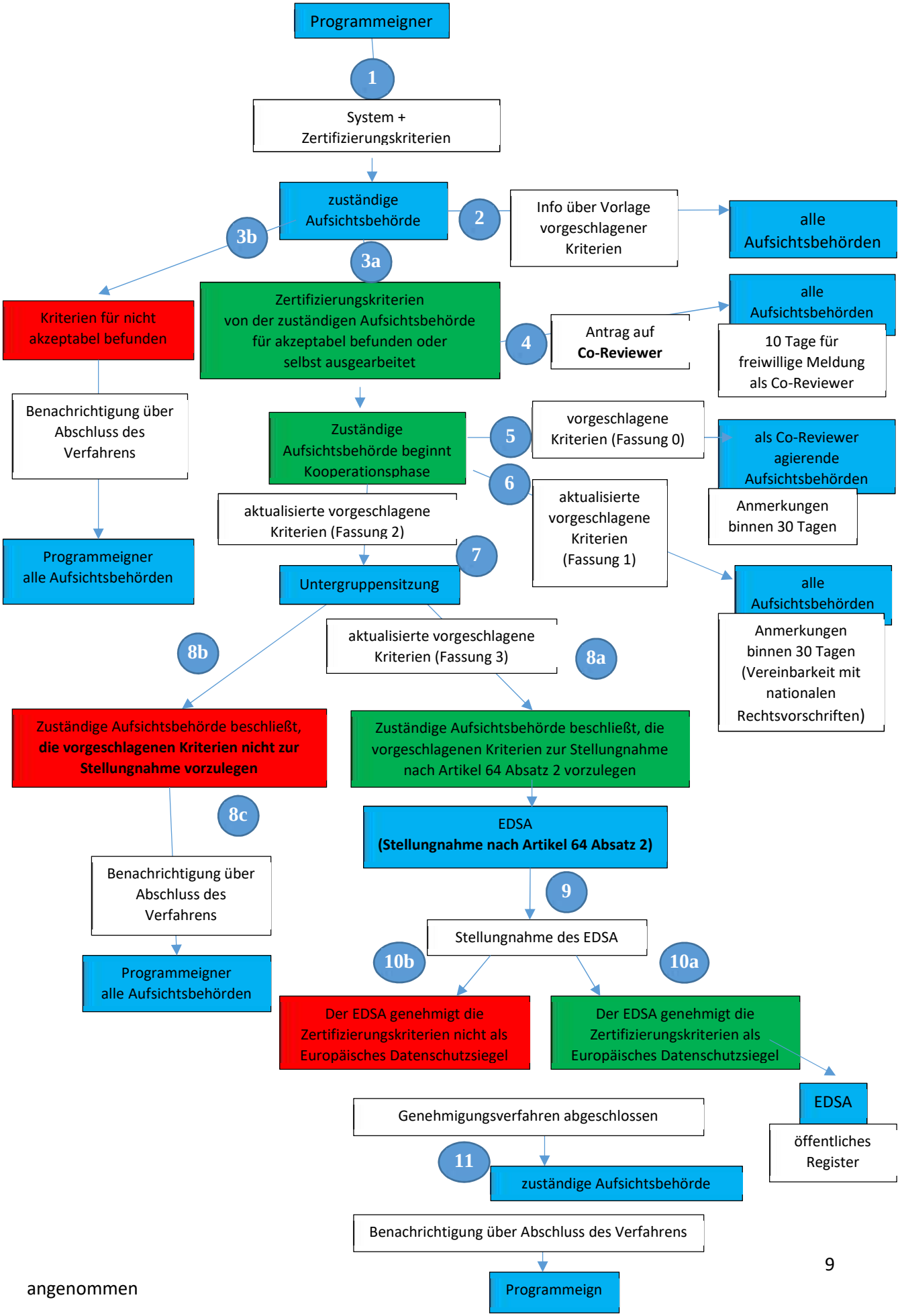
[10] Zudem sei darauf hingewiesen, dass mit den Stellungnahmen ausschließlich eine endgültige Genehmigung bzw. Ablehnung erteilt werden kann, da es zu Missverständnissen kommen könnte, wenn ein Datenschutzsiegel genehmigt würde, bei dem es noch ungeklärte Aspekte gäbe.

[11] Wenn eine Aufsichtsbehörde einer solchen Stellungnahme nicht Folge leistet, kann gemäß Artikel 65 Absatz 1 Buchstabe c DSGVO jede andere Aufsichtsbehörde oder die Kommission die Angelegenheit dem EDSA vorlegen, um einen verbindlichen Beschluss zu erwirken[11].

- Die zuständige Aufsichtsbehörde teilt dem Programmeigner mit, dass das vorgeschlagene Zertifizierungsverfahren laut der Stellungnahme des EDSA nicht den Anforderungen für eine Genehmigung durch den EDSA genügt.
- Die zuständige Aufsichtsbehörde kann beschließen, einen weiteren Antrag auf Genehmigung der zu einem Europäischen Datenschutzsiegel führenden Zertifizierungskriterien zu stellen. Diesbezüglich kann sie wiederum beschließen, entweder zunächst eine neue informelle Kooperationsphase einzuleiten oder aber die vorgeschlagenen Kriterien direkt zur Stellungnahme nach Artikel 64 Absatz 2 vorzulegen.

Bezüglich der Befugnisse der Europäischen Kommission gemäß Artikel 43 Absätze 8 und 9 werden zu gegebener Zeit ergänzende Leitlinien einschließlich etwaiger zusätzlicher Anforderungen an Kriterien für internationale Datenübermittlungen veröffentlicht werden.

Prozessübersicht des EDSA-internen Verfahrens zur Genehmigung von zu einem Europäischen Datenschutzsiegel führenden Zertifizierungskriterien



angenommen