

Stellungnahme des EDSA nach Artikel 64 DSGVO



Stellungnahme 27/2024 zu den Brand Compliance-Zertifizierungskriterien in Bezug auf ihre Genehmigung als Europäisches Datenschutzsiegel gemäß Artikel 42 Absatz 5 (DSGVO) durch den Ausschuss

Angenommen am 2. Dezember 2024

INHALTSVERZEICHNIS

1	ZUSAMMENFASSUNG DES SACHVERHALTS	5
2	BEWERTUNG	5
3	ZUSÄTZLICHE KRITERIEN FÜR DAS EUROPÄISCHE DATENSCHUTZSIEGEL	8
4	SCHLUSSFOLGERUNGEN/EMPFEHLUNGEN	8
5	ABSCHLIESSENDE BEMERKUNGEN	9

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 63, Artikel 64 Absatz 2 und Artikel 42 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 (im Folgenden „DSGVO“),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum (im Folgenden „EWR“), insbesondere auf Anhang XI und das Protokoll 37, in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung¹,

gestützt auf die Artikel 10 und 22 seiner Geschäftsordnung.

- (1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Europäische Datenschutzausschuss (im Folgenden „EDSA“ oder „Ausschuss“) und die Europäische Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren (im Folgenden „Zertifizierungsverfahren“) sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass die DSGVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird, wobei den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen Rechnung getragen wird.² Darüber hinaus kann die Einführung von Zertifizierungsverfahren die Transparenz erhöhen und den betroffenen Personen einen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.³
- (2) Die Zertifizierungskriterien sind integraler Bestandteil eines Zertifizierungsverfahrens. Deshalb sieht die DSGVO Genehmigungserfordernisse vor, wobei die Kriterien – im Falle eines nationalen Zertifizierungsverfahrens – der Genehmigung durch die zuständige Aufsichtsbehörde (Artikel 42 Absatz 5 und Artikel 43 Absatz 2 Buchstabe b DSGVO) oder – im Falle eines Europäischen Datenschutzsiegels – der Genehmigung durch den EDSA (Artikel 42 Absatz 5 und Artikel 70 Absatz 1 Buchstabe o DSGVO) bedürfen.
- (3) Beabsichtigt eine Aufsichtsbehörde (im Folgenden „AB“), vorzuschlagen, dass der EDSA ein Europäisches Datenschutzsiegel gemäß Artikel 42 Absatz 5 DSGVO genehmigt, sollte die Aufsichtsbehörde angeben, dass der Verfahrensverantwortliche das Zertifizierungsverfahren in allen Mitgliedstaaten anzubieten beabsichtigt. In diesem Falle besteht die Rolle des EDSA im Wesentlichen darin, die einheitliche Anwendung der DSGVO sicherzustellen, und zwar durch das in den Artikeln 63, 64 und 65 DSGVO vorgesehene Kohärenzverfahren. In diesem Rahmen genehmigt der EDSA die Zertifizierungskriterien gemäß Artikel 64 Nummer 2 DSGVO.
- (4) Diese Stellungnahme soll sicherstellen, dass die DSGVO, was die zu entwickelnden zentralen Elemente von Zertifizierungsverfahren angeht, einheitlich angewendet wird, auch von den Aufsichtsbehörden, Verantwortlichen und Auftragsverarbeitern. Die Bewertung durch den EDSA erfolgt insbesondere auf

¹ Soweit in dieser Stellungnahme auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.

² Artikel 42 Absatz 1 DSGVO.

³ Erwägungsgrund 100 DSGVO.

Grundlage der „Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679“ (im Folgenden „Leitlinien“) und dem dazugehörigen Anhang „Leitlinien für die Überprüfung und Bewertung von Zertifizierungskriterien“ (im Folgenden „Zusatz“).

- (5) Danach erkennt der EDSA an, dass jedes Zertifizierungsverfahren einzeln zu betrachten ist und die Bewertung anderer Zertifizierungsverfahren unberührt lässt.
- (6) Zertifizierungsverfahren sollten den Verantwortlichen und den Auftragsverarbeitern den Nachweis der Einhaltung der DSGVO ermöglichen. Ihre Kriterien sollten deshalb die Anforderungen und Grundsätze des in der DSGVO niedergelegten Schutzes personenbezogener Daten ordnungsgemäß widerspiegeln und zur deren einheitlicher Anwendung beitragen.
- (7) Gleichzeitig sollte der Verfahrensverantwortliche darauf achten, dass das Zertifizierungsverfahren allen ISO-Normen und Zertifizierungspraktiken, die im Zertifizierungsverfahren enthalten sind oder auf die sich das Zertifizierungsverfahren stützt, angepasst ist und mit diesen konform ist.
- (8) Deshalb sollten Zertifizierungen den Verantwortlichen und den Auftragsverarbeitern einen Mehrwert bieten, indem sie dabei helfen, standardisierte und spezifizierte organisatorische und technische Maßnahmen zu ergreifen, die die DSGVO-Konformität von Verarbeitungsvorgängen nachweislich erleichtern und verbessern, wobei sektorspezifische Anforderungen berücksichtigt werden.
- (9) Der EDSA begrüßt die Bemühungen der Verfahrensverantwortlichen, Zertifizierungsverfahren auszuarbeiten, die praktikable und potenziell kosteneffektive Instrumente zur Gewährleistung einer größeren DSGVO-Konformität darstellen und- indem sie für mehr Transparenz sorgen - das Recht der betroffenen Personen auf Schutz ihrer Privatsphäre und auf Datenschutz stärken.
- (10) Der EDSA erinnert daran, dass Zertifizierungen Instrumente einer freiwilligen Selbstkontrolle sind und dass die Einhaltung eines Zertifizierungsverfahrens weder dazu führt, dass sich die Verantwortung der Verantwortlichen und der Auftragsverarbeiter für die Einhaltung der DSGVO reduziert, noch dazu, dass die Aufsichtsbehörden gehindert wären, ihre sich aus der DSGVO und den einschlägigen nationalen Gesetzen ergebenden Aufgaben und Befugnisse wahrzunehmen.
- (11) In dieser Stellungnahme geht der EDSA auf Themen wie den Anwendungsbereich der Kriterien sowie die Anwendbarkeit der Kriterien und ihre Relevanz für alle Mitgliedstaaten ein.
- (12) Der Schwerpunkt dieser Stellungnahme liegt auf den Zertifizierungskriterien. Sollte der EDSA im Zusammenhang mit seiner diesbezüglichen Stellungnahme abstrakte Informationen über die Bewertungsmethoden anfordern, um die Überprüfbarkeit der Kriterien gründlich bewerten zu können, so bedeutet dies nicht, dass die Stellungnahme eine Art Genehmigung der betreffenden Bewertungsmethoden beinhaltet.
- (13) Die Stellungnahme des EDSA ist gemäß Artikel 64 Absatz 2 DSGVO in Verbindung mit Artikel 10 Absatz 2 der Geschäftsordnung des EDSA binnen acht Wochen ab dem ersten Arbeitstag nach dem Beschluss des Vorsitzes und der zuständigen Aufsichtsbehörde über die Vollständigkeit des Dossiers anzunehmen. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit auf Beschluss des Vorsitzes um weitere sechs Wochen verlängert werden. Gelangt der EDSA in seiner Stellungnahme zu dem Schluss, dass die in Rede stehenden Kriterien nicht genehmigt werden können, kann die Aufsichtsbehörde die Kriterien erneut zur Genehmigung vorlegen, wenn die Aspekte, die in der ersten Stellungnahme des EDSA beanstandet wurden, behoben sind.

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 ZUSAMMENFASSUNG DES SACHVERHALTS

1. In Übereinstimmung mit Artikel 42 Absatz 5 DSGVO und den Leitlinien wurde der Entwurf „DSGVO-Zertifizierungsstandard und -kriterien, BC 5701:2024, Version 0.7“ (im Folgenden der „Entwurf der Zertifizierungskriterien“, „Zertifizierungskriterien“ oder „Kriterien“) von Brand Compliance B.V., einer juristischen Person in den Niederlanden (im Folgenden der „Verfahrensverantwortliche“), ausgearbeitet und der Autoriteit Persoonsgegevens, der zuständigen Aufsichtsbehörde der Niederlande (im Folgenden die „NL-AB“), vorgelegt.
2. Die NL-AB hat die Entwurfsfassung der Zertifizierungskriterien am 29. September 2024 dem EDSA gemäß Artikel 64 Absatz 2 der DSGVO zur Genehmigung vorgelegt. Der Beschluss über die Vollständigkeit des Dossiers erging am 12. November 2024.
3. Das Brand Compliance-Zertifizierungsverfahren ist keine Zertifizierung gemäß Artikel 46 Absatz 2 Buchstabe f DSGVO, die für die Übermittlung personenbezogener Daten ins Ausland vorgesehen ist, und es enthält deshalb keine geeigneten Garantien im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen, so wie diese in Artikel 46 Absatz 2 Buchstabe f vorgesehen sind. Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation ist nämlich nur zulässig, wenn die Bestimmungen von Kapitel V DSGVO eingehalten werden.

2 BEWERTUNG

4. Der EDSA hat seine Bewertung der Zertifizierungskriterien im Hinblick auf deren Genehmigung im Sinne von Artikel 42 Absatz 5 DSGVO nach der in Anhang 2 der Leitlinien (im Folgenden „Anhang“) vorgesehen Gliederung nebst Zusatz vorgenommen.

2.1 Anwendungsbereich des Zertifizierungsverfahrens und Evaluierungsgegenstand (Target of Evaluation, ToE)

5. Das Brand Compliance-Zertifizierungsverfahren beinhaltet Zertifizierungskriterien zur Zertifizierung von Verarbeitungsvorgängen im Zusammenhang mit personenbezogenen Daten durch Verantwortliche oder Auftragsverarbeiter mit Sitz in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR).
6. Die Hauptkriterien dieses Zertifizierungsverfahrens sind in sechs Anforderungsgruppen unterteilt, nämlich: Kontext der Datenverarbeitung, einschließlich der Einhaltung der einschlägigen Rechtsvorschriften der EU oder des Mitgliedstaats (Gruppe 1), organisatorische Rahmenbedingungen (Gruppe 2), Grundlagen der Verarbeitungstätigkeiten, einschließlich der Grundsätze für die Verarbeitung personenbezogener Daten (Gruppe 3), technischer und organisatorischer Schutz (Gruppe 4), operative Durchführung, einschließlich der Rechte der betroffenen Personen (Gruppe 5), und Verwaltungssystem (Gruppe 6).
7. Bei den Antragstellern im Rahmen dieses Zertifizierungsverfahrens muss es sich um Verantwortliche oder Auftragsverarbeiter handeln. Dies schließt Auftragsverarbeiter sowie Unterauftragsverarbeiter

ein, die direkt mit der Verarbeitung personenbezogener Daten durch einen Verantwortlichen im Sinne von Artikel 4 Absatz 7 DSGVO betraut sind. Verarbeitungsvorgänge, die (teilweise) als Unterverarbeitung durchgeführt werden, werden in der organisatorischen Eigenschaft eines Auftragsverarbeiters zertifiziert.

8. Der Ausschuss stellt fest, dass das Zertifizierungsverfahren nicht zur Zertifizierung von Verarbeitungsvorgängen verwendet werden kann, bei denen zwei oder mehr für die Verarbeitung Verantwortliche gemeinsam die Zwecke und Mittel gemäß Artikel 26 Absatz 1 DSGVO festlegen (gemeinsame Verantwortliche). Das Zertifizierungsverfahren kann nicht zur Zertifizierung von Verarbeitungsvorgängen durch eine Organisation mit Sitz außerhalb der EU oder des EWR verwendet werden. Darüber hinaus kann das Zertifizierungsverfahren nicht als Übermittlungsinstrument im Sinne von Artikel 42 Absatz 2 und Artikel 46 Absatz 2 Buchstabe f DSGVO verwendet werden.

2.2 Verarbeitungsvorgänge

9. Das Zertifizierungsverfahren kann auf die Verarbeitung personenbezogener Daten angewandt werden, unabhängig von der Art und Größe der Organisation und von der Art der von ihr angebotenen Produkte oder Dienstleistungen. Daher ist der Anwendungsbereich des Zertifizierungsverfahrens nicht auf bestimmte Arten von Verarbeitungsvorgängen beschränkt und ermöglicht die Zertifizierung aller Verarbeitungsvorgänge durch einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter. Deshalb ist es von fundamentaler Bedeutung, dass die methodischen Vorgaben beachtet werden, weil nur so eine einheitliche Anwendung der Zertifizierungskriterien und ein vergleichbares Maß an Prüftiefe über verschiedene Zertifizierungsverfahren hinweg sichergestellt werden können. Letztlich geht es darum, Vergleichbarkeit und Reproduzierbarkeit der erteilten Zertifizierungen und ihrer Ergebnisse zu garantieren.

2.3 Rechtmäßigkeit der Verarbeitung

10. Die Kriterien erfordern eine Prüfung dahingehend, ob die Verarbeitungsvorgänge eines Verantwortlichen den Bestimmungen von Artikel 6 (Abschnitt 6.1.2 der Kriterien) und gegebenenfalls Artikel 9 (Abschnitt 6.1.2.h der Kriterien) sowie Artikel 10 DSGVO (Abschnitt 6.1.2.i der Kriterien) entsprechen. Auch wenn die Einhaltung des Grundsatzes der Rechtmäßigkeit der Verarbeitung eine Pflicht des Verantwortlichen darstellt, muss der Auftragsverarbeiter in diesem Zusammenhang dennoch bestimmte Anforderungen erfüllen (Abschnitt 6.2 der Kriterien). Diese Anforderungen zielen insbesondere darauf ab, sicherzustellen, dass die Genehmigung für die Datenverarbeitung rechtmäßig vom Verantwortlichen erlangt wird und dass der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung der DSGVO, einschließlich des Grundsatzes der Rechtmäßigkeit, unterstützt.

2.4 Datenverarbeitungsgrundsätze

11. Die Kriterien enthalten spezifische Anforderungen für die Bewertung aller Grundsätze im Zusammenhang mit der Verarbeitung personenbezogener Daten im Sinne von Artikel 5 DSGVO (Abschnitt 6 der Kriterien). Was die Anforderungen an Auftragsverarbeiter betrifft, so müssen in diesem Zusammenhang gesonderte Kriterien bewertet werden (Abschnitt 6.2 der Kriterien). Wie bereits erwähnt, zielen die Anforderungen an die Auftragsverarbeiter in erster Linie darauf ab, den Verantwortlichen bei der Einhaltung der Grundsätze zu unterstützen.

2.5 Allgemeine Verpflichtungen der Verantwortlichen und Auftragsverarbeiter

12. Die Kriterien spiegeln die Beziehung zwischen den Verantwortlichen und Auftragsverarbeitern wider. Die Kriterien legen insbesondere die Verpflichtung für Verantwortliche und Auftragsverarbeiter fest, die Anforderungen im Zusammenhang mit der Auslagerung von Verarbeitungstätigkeiten zu erfüllen, wozu unter anderem die Einhaltung der Bestimmungen von Artikel 28 Absatz 3 DSGVO gehört (Abschnitt 8.5 der Kriterien). Was Auftragsverarbeiter betrifft, müssen sie auch die spezifischen Anforderungen an die Verarbeitung unter der Aufsicht eines Verantwortlichen erfüllen (Abschnitt 8.6 der Kriterien). Darüber hinaus werden weitere Anforderungen festgelegt, um den Umständen der Unterverarbeitung Rechnung zu tragen (Abschnitt 6.2.e und insbesondere Abschnitt 8.6.g der Kriterien).
13. Die Kriterien enthalten Anforderungen an den Inhalt des Verzeichnisses der Verarbeitungstätigkeiten gemäß Artikel 30 DSGVO (Abschnitt 5.4 der Kriterien). In diesem Zusammenhang wird zwischen dem erforderlichen Inhalt eines Verzeichnisses der Verarbeitungstätigkeiten für Verantwortliche und Auftragsverarbeiter gemäß Artikel 30 Absätze 1 und 2 DSGVO unterschieden.
14. Nach den Kriterien müssen Antragsteller einen Datenschutzbeauftragten (DSB) gemäß Artikel 37 DSGVO benennen. Darüber hinaus stellen die Kriterien sicher, dass die Anforderungen der Artikel 37 bis 39 DSGVO erfüllt sind (Abschnitt 5.3.2 der Kriterien).
15. In Bezug auf den Grundsatz der Rechenschaftspflicht gemäß Artikel 5 Absatz 2 und Artikel 24 DSGVO werden Anforderungen an die Organisation von Datenschutz- und Meldemechanismen (Abschnitt 5.1 und 5.3 der Kriterien) sowie an die Umsetzung von Datenschutzstrategien (Abschnitt 5.2 der Kriterien) festgelegt.

2.6 Rechte der betroffenen Personen

16. Gemäß Kapitel III DSGVO enthalten die Kriterien angemessene Anforderungen für die Rechte der betroffenen Personen. Zunächst werden die Anforderungen an transparente Information, Kommunikation und die Modalitäten für die Ausübung der Rechte der betroffenen Personen behandelt, gefolgt von einer detaillierten Prüfung der jeweiligen Rechte der betroffenen Personen (Abschnitt 8.4 der Kriterien). Was die Anforderungen an die Auftragsverarbeiter betrifft, so sind besondere Bestimmungen für die Unterstützungspflichten enthalten (Abschnitt 8.4.11 der Kriterien).

2.7 Risiken für Rechte und Freiheiten

17. Nach den Kriterien muss sich der Verantwortliche der möglichen Risiken für die Rechte und Freiheiten natürlicher Personen bei der Datenverarbeitung im Zusammenhang mit dem Evaluierungsgegenstand bewusst sein. Wenn die Verarbeitung personenbezogener Daten wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, gewährleisten mehrere Kriterien, dass der Antragsteller nachweist, dass die Anforderungen von Artikel 35 DSGVO erfüllt sind (Abschnitt 7.3 der Kriterien). Darüber hinaus werden spezifische Anforderungen an die Unterstützungspflichten der Auftragsverarbeiter gemäß Artikel 35 DSGVO festgelegt.

2.8 Schutz garantierende technische und organisatorische Maßnahmen

18. Die Kriterien erfordern die Anwendung technischer und organisatorischer Maßnahmen auf der Grundlage eines Sicherheitsstandards, der die Vertraulichkeit, Integrität und Richtigkeit der

verarbeiteten personenbezogenen Daten und die Resilienz des Verarbeitungssystems gewährleistet. Die Kriterien erfordern auch die Anwendung von Maßnahmen zur Umsetzung des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gemäß Artikel 25 DSGVO (Abschnitt 7.4 der Kriterien). Die Kriterien enthalten spezifische Anforderungen an die Verantwortlichen in Bezug auf die Bewertung der Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde und, erforderlichenfalls, die Benachrichtigung der betroffenen Person über eine solche Verletzung des Schutzes personenbezogener Daten gemäß den Artikeln 33 und 34 DSGVO (Abschnitt 8.8 der Kriterien). In diesem Zusammenhang werden auch spezifische Verpflichtungen für Auftragsverarbeiter dargelegt, insbesondere in Bezug auf die Erkennung einer Verletzung des Schutzes personenbezogener Daten und die Kommunikation mit dem Verantwortlichen (Abschnitte 8.8.1 und 8.8.4 der Kriterien).

2.9 Kriterien für den Nachweis des Vorhandenseins geeigneter Garantien für die Übermittlung personenbezogener Daten

19. Nach den Kriterien ist es erforderlich, alle den Evaluierungsgegenstand betreffenden Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen anzugeben und die Wahl, die hinsichtlich des geeigneten Garantien bietenden Datenübermittlungsverfahrens getroffen wurde, zu substantiieren, so wie in Kapitel V DSGVO vorgesehen (Abschnitt 8.7 der Kriterien). Die Kriterien sehen ein Verfahren zur Bewertung der beabsichtigten Übermittlungen vor, z. B. zur Überwachung ihrer Rechtmäßigkeit.

3 ZUSÄTZLICHE KRITERIEN FÜR DAS EUROPÄISCHE DATENSCHUTZSIEGEL

20. Gemäß den Leitlinien umfasst die Bewertung die Frage, ob „die Kriterien dazu geeignet [sind], auch den Datenschutzvorschriften oder -szenarien der Mitgliedstaaten Rechnung zu tragen“. Gemäß Abschnitt 4.3 der Kriterien muss der Antragsteller das geltende nationale und einschlägige branchenspezifische Datenschutzrecht einhalten. Die Organisation muss die einschlägigen nationalen oder sektorspezifischen Gesetze und Vorschriften, die für die Verarbeitung personenbezogener Daten im Rahmen des Evaluierungsgegenstands gelten, korrekt und umfassend ermitteln, analysieren und dokumentieren. In den Dokumenten ist anzugeben, welche Person(en) für die Darlegung des nationalen oder sektorspezifischen Rechtsrahmens, der für den Evaluierungsgegenstand relevant ist, verantwortlich ist/sind, sowie deren juristische Fachkenntnisse. Darüber hinaus geht der Ausschuss davon aus, dass die Angemessenheit der Ermittlung und Darlegung dieses Rechtsrahmens von der Zertifizierungsstelle festgestellt wird.

4 SCHLUSSFOLGERUNGEN/EMPFEHLUNGEN

21. Der EDSA gelangt abschließend zu dem Ergebnis, dass die Brand Compliance-Zertifizierungskriterien mit der DSGVO in Einklang stehen, und genehmigt diese in Wahrnehmung seiner in Artikel 70 Absatz 1 Buchstabe o DSGVO vorgesehenen Aufgabe; dies führt zur gemeinsamen Zertifizierung (dem Europäischen Datenschutzsiegel).

22. Der EDSA wird das Zertifizierungsverfahren „DSGVO-Zertifizierungsstandard und -kriterien, BC 5701:2024, Version 0.7“ in das öffentliche Register der Zertifizierungsverfahren und Datenschutzsiegel und -zeichen gemäß Artikel 42 Absatz 8 eintragen.

5 ABSCHLIESSENDE BEMERKUNGEN

23. Diese Stellungnahme richtet sich an die NL-AB und wird gemäß Artikel 64 Absatz 5 Buchstabe b DSGVO veröffentlicht.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende
Anu Talus