Stellungnahme 19/2024 zu den EuroPriSe-Zertifizierungskriterien in Bezug auf ihre Genehmigung als Europäisches Datenschutzsiegel gemäß Artikel 42 Absatz 5 (DSGVO) durch den Ausschuss

Angenommen am 16. Juli 2024

Inhalt

1. ZUSAMMENFASSUNG DES SACHVERHALTS 5

2. BEWERTUNG 5

2.1 Anwendungsbereich des Zertifizierungsverfahrens und Evaluierungsgegenstand (Target of Evaluation, ToE) 5

2.2 Verarbeitungsvorgänge 6

2.3 Rechtmäßigkeit und Grundsätze der Datenverarbeitung 6

2.4 Allgemeine Verpflichtungen der Verantwortlichen und Auftragsverarbeiter 6

2.5 Rechte der betroffenen Personen 7

2.6 Risiken für Rechte und Freiheiten 7

2.7 Schutz garantierende technische und organisatorische Maßnahmen 7

2.8 Kriterien für den Nachweis des Vorhandenseins geeigneter Garantien für die Übermittlung personenbezogener Daten 7

3. ZUSÄTZLICHE KRITERIEN FÜR DAS EUROPÄISCHE DATENSCHUTZSIEGEL 8

FAZIT/EMPFEHLUNGEN 8

SCHLUSSBEMERKUNGEN 8

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 Fassung[1],

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“), für den die Anhörungsfrist im Rahmen der öffentlichen Konsultation am 26. Mai 2021 abgelaufen ist.

(5) Dementsprechend 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 sollten Verfahrensverantwortliche sicherstellen, dass das Zertifizierungsverfahren mit allen ISO-Normen und Zertifizierungspraktiken, die im Zertifizierungsverfahren enthalten sind oder auf die sich das Zertifizierungsverfahren stützt, übereinstimmt.

(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 das Recht von betroffenen Personen auf den Schutz ihrer Privatsphäre und auf Datenschutz durch mehr Transparenz 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 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. Im Einklang mit Artikel 42 Absatz 5 der DSGVO und den Leitlinien wurde der Entwurf des „EuroPriSe-Kriterienkatalog[s] für die Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern (Anwendungsbereich: EU) v1.5“ (im Folgenden „Entwurfsfassung der Zertifizierungskriterien“, „Zertifizierungskriterien“ oder „Kriterien“) von der EuroPriSe Cert GmbH (im Folgenden „Verfahrensverantwortlicher“), einer in Deutschland ansässigen juristischen Person, ausgearbeitet und der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, der zuständigen deutschen Aufsichtsbehörde in Nordrhein-Westfalen (im Folgenden „AB DE-NRW“), vorgelegt.

2. Die AB DE-NRW hat die Entwurfsfassung der Zertifizierungskriterien am 29. April 2024 dem EDSA gemäß Artikel 64 Absatz 2 der DSGVO zur Genehmigung vorgelegt. Der Beschluss über die Vollständigkeit des Dossiers erging am 29. Mai 2024.

3. Das EuroPriSe-Zertifizierungsverfahren ist keine Zertifizierung gemäß Artikel 46 Absatz 2 Buchstabe f der DSGVO, die für die grenzüberschreitende Übermittlung personenbezogener Daten vorgesehen ist, und enthält deshalb keine geeigneten Garantien im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen, unter den in Artikel 46 Absatz 2 Buchstabe f genannten Bedingungen. Jede Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation ist nur zulässig, wenn die Bestimmungen von Kapitel V der DSGVO eingehalten werden.

2. BEWERTUNG

4. Der EDSA hat seine Bewertung der Zertifizierungskriterien im Hinblick auf deren Genehmigung im Sinne von Artikel 42 Nummer 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. Der EuroPriSe-Zertifizierungsmechanismus enthält Zertifizierungskriterien für ein EU-weites Zertifizierungssystem für die Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern. Gegenstand von Zertifizierungen, auf die dieser Kriterienkatalog Anwendung findet, sind Verarbeitungsvorgänge, die in Produkten, Prozessen und Dienstleistungen oder mithilfe von (auch mehreren) Produkten und Dienstleistungen erbracht werden, und bezüglich derer der Zertifizierungskunde als Auftragsverarbeiter agiert. Die Hauptkriterien dieses Zertifizierungsverfahrens sind in drei Kategorien unterteilt, und zwar in Anforderungen aus rechtlicher Sicht (Kategorie 1), Anforderungen aus der Perspektive technischer und organisatorischer Maßnahmen (Kategorie 2) und Anforderungen aus der Perspektive der Rechte der betroffenen Personen (Kategorie 3).

6. Bei den Antragstellern im Rahmen dieses Zertifizierungsverfahrens muss es sich um Auftragsverarbeiter handeln. Dies schließt Auftragsverarbeiter ein, die direkt mit der Verarbeitung personenbezogener Daten durch einen Verantwortlichen im Sinne von Artikel 4 Absatz 7 DSGVO

betraut sind. Zertifizierungsantragsteller können jedoch auch Auftragsverarbeiter im Sinne von Artikel 28 Absätze 2 und 4 DSGVO sein (Unterauftragsverarbeiter).

7. Wenn ein nach dem EuroPriSe-Zertifizierungssystem zertifizierter Auftragsverarbeiter einen Unterauftragsverarbeiter einsetzt, kann dieser nicht geltend machen, dass er nach dem EuroPriSe-Zertifizierungssystem zertifiziert ist. Nur Verarbeitungsvorgänge, die vom ursprünglichen und zertifizierten Auftragsverarbeiter durchgeführt werden, fallen in einem solchen Fall unter die Zertifizierung. Allerdings können auch Unterauftragsverarbeiter eine Zertifizierung beantragen, was zu einem eigenständigen und unabhängigen Verfahren führen würde.

8. Der Ausschuss stellt fest, dass das EuroPriSe-Verfahren nach den von der AB DE-NRW vorgelegten Unterlagen über den Anwendungsbereich des Zertifizierungsverfahrens auf Auftragsverarbeiter Anwendung findet, die in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) niedergelassen sind.

2.2 Verarbeitungsvorgänge

9. Der Anwendungsbereich dieser Kriterien ist nicht auf bestimmte Arten von Verarbeitungsvorgängen beschränkt. Es geht vielmehr um die Methodik, die einer EuroPrise-Bewertung zugrunde liegt, die eine Zertifizierung jeglicher Verarbeitungsvorgänge durch die Verarbeiter ermöglicht. Es handelt sich folglich um einen allgemeingültigen methodischen Ansatz, auf dessen Grundlage eine Vielzahl sehr verschiedener Verarbeitungsvorgänge zertifiziert werden können. Deshalb ist es von fundamentaler Bedeutung, dass die methodologischen 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 und Grundsätze der Datenverarbeitung

10. Nach den Kriterien ist zu prüfen, ob die zu zertifizierenden Verarbeitungen den Grundsätzen des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen entsprechen (Abschnitt 1.5 der Kriterien), was die Mitwirkung des Antragstellers an der Unterstützung des für die Verarbeitung Verantwortlichen bei der Umsetzung dieser Grundsätze voraussetzt. Dies ermöglicht eine Beurteilung der Einhaltung von Artikel 25 DSGVO in Verbindung mit Artikel 5 DSGVO. Zwar gibt es keine Kriterien, die unmittelbar auf die Einhaltung von Artikel 6 DSGVO abzielen – da der für die Verarbeitung Verantwortliche für die Rechtmäßigkeit der Verarbeitung verantwortlich ist –, doch zielen die Kriterien darauf ab sicherzustellen, dass antragstellende Auftragsverarbeiter die zu zertifizierenden Verarbeitungsvorgänge so gestalten, dass sie den für die Verarbeitung Verantwortlichen die Umsetzung der Datenschutzgrundsätze nach Artikel 5 DSGVO, einschließlich des Grundsatzes der Rechtmäßigkeit der Verarbeitung, erleichtern.

2.4 Allgemeine Verpflichtungen der Verantwortlichen und Auftragsverarbeiter

11. Die Kriterien spiegeln die Beziehung zwischen dem Auftragsverarbeiter und dem für die Verarbeitung Verantwortlichen wider. Insbesondere sehen die Kriterien vor, dass der Auftragsverarbeiter über eine Vorlage für einen Auftragsverarbeitungsvertrag mit dem Verantwortlichen verfügen muss, der alle Anforderungen von Artikel 28 DSGVO umfasst (Abschnitt 1.2 der Kriterien).

12. Nach den Kriterien müssen Antragsteller einen Datenschutzbeauftragten (DSB) gemäß Artikel 37 DSGVO ernennen und die Benennung des DSB dokumentieren (z. B. durch eine Benennungsurkunde). Nach den Kriterien wird geprüft, ob der DSB den sich aus den Artikeln 37 bis 39 ergebenden Anforderungen genügt (Kategorie 1 Abschnitt 1.1 der Kriterien).

13. Die Kriterien enthalten Anforderungen an den Inhalt des Verzeichnisses der Verarbeitungstätigkeiten gemäß Artikel 30 DSGVO (Kategorie 1 Abschnitt 1.1 der Kriterien).

2.5 Rechte der betroffenen Personen

14. Die Kriterien berücksichtigen in angemessener Weise das Recht der betroffenen Person auf Information gemäß Kapitel III der DSGVO und verlangen die Ergreifung entsprechender Maßnahmen. Nach den Kriterien sind auch Vorkehrungen zu treffen, die es ermöglichen in den Verarbeitungsvorgang einzugreifen, um die Rechte der betroffenen Personen zu garantieren und Berichtigungen, Löschungen oder Einschränkungen zu ermöglichen (Kategorie 3 der Kriterien).

2.6 Risiken für Rechte und Freiheiten

15. Nach den Kriterien muss sich der Auftragsverarbeiter der möglichen Risiken für die Rechte und Freiheiten natürlicher Personen bei der Datenverarbeitung im Zusammenhang mit dem Evaluierungsgegenstand bewusst sein. Ist davon auszugehen, dass die Verarbeitung personenbezogener Daten ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt, stellen mehrere Kriterien sicher, dass der Antragsteller nachweist, dass die Anforderungen von Artikel 35 DSGVO gemäß Artikel 35 DSGVO erfüllt sind (Abschnitt 1.2.2 der Kriterien, Anforderung Nr. 6, Abschnitt 1.3.2 der Kriterien, Abschnitt 1.3.3 der Kriterien, Abschnitt 2.1.5.1 der Kriterien, Abschnitt 2.1.5.9.pf der Kriterien).

2.7 Schutz garantierende technische und organisatorische Maßnahmen

16. Nach den Kriterien sind technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit, der Integrität und der Verfügbarkeit der Verarbeitungsvorgänge zu ergreifen. Nach den Kriterien sind auch technische Maßnahmen zur Implementierung von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gemäß den Artikeln 25 und 32 DSGVO zu treffen (Abschnitt 1.5 der Kriterien, Abschnitt 2.1 der Kriterien/Sonstige Dokumente).

17. Die Kriterien sehen vor, dass Maßnahmen zu ergreifen sind, die sicherstellen, dass im Fall von Verletzungen des Schutzes personenbezogener Daten die betreffenden Melde- und Benachrichtigungspflichten rechtzeitig und in vollem Umfang gemäß Artikel 33 DSGVO erfüllt werden (Abschnitt 1.2.2 der Kriterien, Anforderung 6).

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

18. Nach den Kriterien ist es erforderlich, dass alle den Evaluierungsgegenstand betreffenden Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen zu identifizieren sind und die Wahl, die hinsichtlich des geeignete Garantien bietenden Datenübermittlungsmechanismus getroffen wurde, begründet wird, wie in Kapitel V DSGVO vorgesehen (Abschnitt 1.4 der Kriterien).

3. ZUSÄTZLICHE KRITERIEN FÜR DAS EUROPÄISCHE DATENSCHUTZSIEGEL

19. 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 der Kriterien muss der Antragsteller das geltende nationale und einschlägige branchenspezifische Datenschutzrecht einhalten. Darüber hinaus geht der Ausschuss davon aus, dass Rechtssachverständige einen „Bericht über die Einhaltung nationaler Rechtsvorschriften“ – in dem insbesondere bewertet wird, ob der Evaluierungsgegenstand den geltenden Anforderungen des nationalen Datenschutzrechts entspricht – erstellen werden, sofern diese Fachleute das erforderliche Maß an Fachwissen im geltenden nationalen Recht nachgewiesen haben.

FAZIT/EMPFEHLUNGEN

20. Der EDSA gelangt abschließend zu dem Ergebnis, dass die Entwurfsfassung der Zertifizierungskriterien mit der DSGVO in Einklang steht, und genehmigt diese in Wahrnehmung seiner in Artikel 70 Absatz 1 Buchstabe o DSGVO vorgesehenen Aufgabe; dies führt zur allgemeinen Zertifizierung (dem Europäischen Datenschutzsiegel).

21. Der EDSA wird das Zertifizierungsverfahren „EuroPriSe-Kriterienkatalog für die Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern“ in das öffentliche Register der Zertifizierungsverfahren und Datenschutzsiegel und -zeichen gemäß Artikel 42 Absatz 8 eintragen.

SCHLUSSBEMERKUNGEN

22. Diese Stellungnahme richtet sich an die deutsche Aufsichtsbehörde in Nordrhein-Westfalen und wird gemäß Artikel 64 Absatz 5 Buchstabe b DSGVO veröffentlicht.

Für den Europäischen Datenschutzausschuss

Der Vorsitz
Anu Talus