Stellungnahme des EDSA nach Artikel 64 DSGVO

Stellungnahme 16/2025 zum Entwurf des Beschlusses der für Nordrhein-Westfalen zuständigen deutschen Aufsichtsbehörde in Bezug auf die Zertifizierungskriterien für die Datenschutz-Zertifizierung Trusted Site Privacy (TÜV IT)

Angenommen am 8. Juli 2025

Inhaltsverzeichnis

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 63, Artikel 64 Absatz 1 Buchstabe c 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 Artikel 64 Absatz 1 Buchstabe c der DSGVO und die Artikel 10 und 22 seiner Geschäftsordnung.

In Erwägung nachstehender Gründe:

(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Europäische Datenschutzausschuss (im Folgenden „EDSA") 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 Zertifizierungen die Transparenz erhöhen und den betroffenen Personen einen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.[3]

(2) Die Zertifizierungskriterien sind integraler Bestandteil jedes Zertifizierungsverfahrens. Deshalb sieht die DSGVO Genehmigungserfordernisse vor, wobei die Zertifizierungskriterien – 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 „Aufsichtsbehörde"), eine Zertifizierung gemäß Artikel 42 Absatz 5 DSGVO zu genehmigen, besteht die Aufgabe 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 ist der EDSA gemäß Artikel 64 Absatz 1 Buchstabe c der DSGVO verpflichtet, zum Entwurf eines Beschlusses der Aufsichtsbehörde zur Genehmigung der Zertifizierungskriterien Stellung zu nehmen.

[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.

(4) Die Stellungnahme soll sicherstellen, dass die DSGVO in Bezug auf die zu entwickelnden zentralen Elemente von Zertifizierungsverfahren von den Aufsichtsbehörden, Verantwortlichen und Auftragsverarbeitern einheitlich angewendet wird. Die Bewertung durch den EDSA erfolgt insbesondere gemäß den „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 Addendum „Leitlinien für die Überprüfung und Bewertung von Zertifizierungskriterien“ (im Folgenden „Addendum“).

(5) Dementsprechend erkennt der EDSA an, dass jedes Zertifizierungsverfahren einzeln zu betrachten ist und die Bewertung anderer Zertifizierungsverfahren unberührt lässt.

(6) Zertifizierungsmechanismen sollten es den für die Verarbeitung Verantwortlichen und den Auftragsverarbeitern ermöglichen, Nachweis für die Einhaltung der DSGVO zu erbringen; daher sollten die Zertifizierungskriterien die in der DSGVO festgelegten Anforderungen und Grundsätze für den Schutz personenbezogener Daten ordnungsgemäß wiedergeben und zu deren einheitlicher Anwendung beitragen.

(7) Gleichzeitig sollten die Zertifizierungskriterien andere Standards wie ISO-Normen und Zertifizierungsverfahren berücksichtigen und gegebenenfalls mit diesen interoperabel sein.

(8) Zertifizierungen sollten Organisationen also einen Mehrwert bieten, indem sie dabei helfen, standardisierte und spezifizierte organisatorische und technische Maßnahmen einzurichten, die die Konformität von Verarbeitungsvorgängen nachweislich erleichtern und verbessern, wobei sektorspezifischen Anforderungen Rechnung getragen wird.

(9) Der EDSA begrüßt die Bemühungen der Programmeigner, Zertifizierungsmechanismen auszuarbeiten, die als praktikable und potenziell kosteneffektive Instrumente mehr DSGVO-Konformität gewährleisten und durch mehr Transparenz 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 die Verantwortung der Verantwortlichen und der Auftragsverarbeiter für die Einhaltung der DSGVO reduziert, noch die Aufsichtsbehörden daran hindert, ihre Aufgaben und Befugnisse aus der DSGVO und den einschlägigen nationalen Gesetzen wahrzunehmen.

(11) Die Stellungnahme des EDSA wird gemäß Artikel 64 Absatz 1 Buchstabe c 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 angenommen. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit auf Beschluss des Vorsitzes um weitere sechs Wochen verlängert werden.

(12) Gegenstand dieser Stellungnahme des EDSA sind die Zertifizierungskriterien. Sollte der EDSA im Zusammenhang mit seiner diesbezüglichen Stellungnahme abstrakte Informationen über die Bewertungsmethoden benötigen, um die Überprüfbarkeit der im Entwurf vorgesehenen Zertifizierungskriterien gründlich bewerten zu können, beinhaltet diese Stellungnahme keine Genehmigung der betreffenden Bewertungsmethoden –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. ZUSAMMENFASSUNG DES SACHVERHALTS

1. Der „*Trusted Site Data Privacy Criteria Catalogue for Inspecting the Conformity of an IT Solution with the European General Data Protection Regulation*“ („Trusted Site Privacy Datenschutz-Kriterienkatalog für die Prüfung der DSGVO-Konformität von IT-Lösungen“) (im Folgenden „*draft certification criteria*“ („Entwurfsfassung der Zertifizierungskriterien“) oder „*certification criteria*“ („Zertifizierungskriterien“)) wurde von der TÜV NORD CERT GmbH (im Folgenden „TÜV NORD“), einer juristischen Person in Deutschland, gemäß Artikel 42 Absatz 5 DSGVO und den Leitlinien ausgearbeitet und der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (im Folgenden „DE-AB“ oder „zuständige AB“), der für Nordrhein-Westfalen zuständigen deutschen Aufsichtsbehörde, vorgelegt.

2. Am 28. April 2025 hat die DE-AB dem EDSA den Entwurf der Kriterien für ein nationales Zertifizierungssystem vorgelegt und den Ausschuss um Stellungnahme gemäß Artikel 64 Absatz 1 Buchstabe c DSGVO ersucht. Der Beschluss über die Vollständigkeit des Dossiers erging am 17. Juni 2025.

3. Die vorliegenden Zertifizierungskriterien haben einen allgemeinen Anwendungsbereich und sind nicht auf bestimmte Verarbeitungsvorgänge beschränkt. Die Zertifizierung von Verantwortlichen und Auftragsverarbeitern ausgeführter Verarbeitungsvorgänge ist möglich.

4. Die Zertifizierung gemeinsam Verantwortlicher im Sinne von Artikel 26 DSGVO ist aus dem Anwendungsbereich der Zertifizierungskriterien ausgeschlossen. Die Zertifizierung wird auch nicht angeboten für Unternehmen ohne Niederlassung im EWR.

5. Der EDSA merkt an, dass es sich bei der vorliegenden Zertifizierung nicht um eine für die internationale Übermittlung personenbezogener Daten vorgesehene Zertifizierung im Sinne von Artikel 46 Absatz 2 Buchstabe f DSGVO handelt. Nicht darin vorgesehen sind geeignete Garantien im Sinne von Artikel 46 Absatz 2 Buchstabe f für die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen. Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation ist vielmehr nur zulässig, wenn die Bestimmungen von Kapitel V DSGVO eingehalten werden.

2. BEWERTUNG

6. Der Ausschuss hat seine Bewertung nach der Gliederung in Anhang 2 der Leitlinien (im Folgenden „Anhang“) und deren Addendum vorgenommen. Soweit diese Stellungnahme zu einem bestimmten Abschnitt der Entwurfsfassung der Zertifizierungskriterien schweigt, ist davon auszugehen, dass der Ausschuss dazu nichts anzumerken hat und die DE-AB um keine weiteren Maßnahmen ersucht.

2.1. ALLGEMEINE HINWEISE

7. Der Ausschuss merkt an, dass mehrere Kriterien nicht mehr zutreffende Querverweise auf gelöschte Punkte enthalten (z. B. verweist DP06.15 auf DP06.18), was einer zutreffenden

Bewertung entgegenstehen könnte. Der Ausschuss empfiehlt der DE-AB, vom Programmeigner die Überprüfung und Berichtigung aller Verweisungen zu verlangen, damit diese ausschließlich auf bestehende und gültige Kriterien verweisen.

8. Der Ausschuss stellt fest, dass in Kriterium DP01.01 die Wendung „*The IPS is documented to a sufficient extent and it is sufficiently up to date*“ („Das IPS ist in hinreichendem Umfang dokumentiert und hinreichend aktuell“) verwendet wird. Weiter heißt es in dem Kriterium, dass „*[t]he processor must communicate changes to the IPS … with sufficient notice (at least 14 days) …*“ („der Auftragsverarbeiter muss Änderungen des IPS … rechtzeitig (mindestens 14 Tage) im Voraus ankündigen …“). Der Begriff „*sufficient*“ („hinreichend“) erscheint auch in anderen Kriterien (beispielsweise in DP02.01 und DP02.04), ohne dass jedoch seine genaue Bedeutung jeweils definiert wäre. Die Überprüfbarkeit dieser Anforderungen ist deshalb möglicherweise nicht in allen Fällen sichergestellt. Der Ausschuss empfiehlt der DE-AB, zu verlangen, dass der Programmeigner die genaue Bedeutung von „*sufficient*“ („hinreichend“) für den jeweiligen Kontext klarstellt.

9. Des Weiteren wird im Kriterium DP02.02, wie auch in anderen ähnlichen Fällen, auf „*appropriate processes*“ („geeignete Prozesse“) Bezug genommen, ohne zu definieren, was diese Prozesse vorsehen. Der Ausschuss ist der Ansicht, dass dies die Klarheit beeinträchtigt und zu uneinheitlichen Auslegungen führen kann. Der Ausschuss empfiehlt der DE-AB deshalb, vom Programmeigner zu verlangen, dass dieser, wo immer „*appropriate processes*“ („geeignete Prozesse“) verwendet wird, die für die volle Überprüfbarkeit des Kriteriums erforderlichen spezifischen Prozesselemente festlegt.

2.2. ANWENDUNGSBEREICH DES ZERTIFIZIERUNGSVERFAHRENS UND EVALUIERUNGSGEGENSTAND (TARGET OF EVALUATION, TOE)

10. Der EDSA erinnert daran, dass ein Unterauftragsverarbeiter, der von einem nach dem TÜV-Zertifizierungssystem zertifizierten Auftragsverarbeiter eingesetzt wird, nicht geltend machen kann, nach dem TÜV-Zertifizierungssystem zertifiziert worden zu sein. In einem solchen Fall sind nur Verarbeitungsvorgänge, die vom ursprünglichen und zertifizierten Auftragsverarbeiter durchgeführt werden, von der Zertifizierung gedeckt.

11. Des Weiteren merkt der Ausschuss an, dass aus den Zertifizierungskriterien nicht klar hervorgeht, ob Unterauftragsverarbeiter nach dem Zertifizierungsprogramm zertifiziert werden können. Insbesondere sehen die Zertifizierungskriterien keine spezifischen Kriterien für Unterauftragsverarbeiter vor. In Fällen, in denen die Zertifizierung nach dem Programm von einem Unterauftragsverarbeiter beantragt wird, wären einige Kriterien nach Ansicht des Ausschusses nicht anwendbar. Beispielsweise wäre im Falle einer Datenschutzverletzung das Kriterium DP09.01 nicht anwendbar; es sollte deshalb auf die Zertifizierung von Unterauftragsverarbeitern abgestimmte spezifische Kriterien geben, die vorsehen, dass der Unterauftragsverarbeiter den Auftragsverarbeiter benachrichtigen muss. Für den Fall, dass die Zertifizierung von Unterauftragsverarbeitern zulässig ist, empfiehlt der Ausschuss der DE-AB deshalb, vom Programmeigner zu verlangen, dass spezifische Kriterien ausgearbeitet

werden, die die Besonderheiten der Unterverarbeitung berücksichtigen[4]. Dies würde auf ein eigenständiges und unabhängiges Verfahren hinauslaufen[5].

2.3. ALLGEMEINE ANFORDERUNGEN

12. Der Ausschuss merkt an, dass die Kriterien DP04.08, DP06.03, DP06.07 ff. wie auch D10.04 bestimmen, dass der Auftragsverarbeiter den Verantwortlichen unterstützt – zum Beispiel im Zusammenhang mit dem Einwilligungsmanagement, der Ausübung der Rechte betroffener Personen und der Durchführung der Datenschutz-Folgenabschätzung. Der Wortlaut wirkt jedoch recht allgemein gehalten und es gibt keine detaillierten Kriterien mit genauen Angaben dazu, was mit dieser Unterstützungspflicht verbunden ist. Deshalb ist die Überprüfbarkeit dieser Anforderungen möglicherweise nicht sichergestellt[6]. Der Ausschuss empfiehlt der DE-AB deshalb, vom Programmeigner zu verlangen, dass er die Unterstützungspflichten der Auftragsverarbeiter in Bezug auf das jeweilige Kriterium genauer klarstellt.

2.4. RECHTMÄSSIGKEIT DER VERARBEITUNG

13. Der Ausschuss stellt fest, dass gemäß dem Kriterium DP03.01, das die Rechtmäßigkeit der Verarbeitung betrifft, „*[t]he controller provides for Lawful Processing of PD only in accordance with one or more of the following conditions*“ („[d]er Verantwortliche ... die rechtmäßige Verarbeitung nur gemäß einer oder mehrerer der folgenden Bedingungen [vorsieht]“), bevor dann im Weiteren die Rechtsgrundlagen für die Verarbeitung aufgezählt werden. Diese Formulierung gibt jedoch den Wortlaut von Artikel 6 Absatz 1 DSGVO nicht zutreffend wider, der bestimmt, dass „*[p]rocessing shall be lawful only if and to the extent that at least one of the following applies*“ („[d]ie Verarbeitung … nur rechtmäßig (ist), wenn mindestens eine der nachstehenden Bedingungen erfüllt ist“). Um die Übereinstimmung mit der DSGVO sicherzustellen, empfiehlt der Ausschuss der DE-AB, zu verlangen, dass der Programmeigner das Kriterium DP03.01 so ändert, dass es enger an den Wortlaut des Artikel 6 Absatz 1 angelehnt ist.

14. Der Ausschuss begrüßt, dass im Kriterium DP02.02, Randnummer 14 auf die vernünftigen Erwartungen der betroffenen Personen Bezug genommen wird (ähnlich auch in der „*Evaluation note*“ (Bewertungserläuterung) zu DP03.07 und DP10.01 sowie in der Begriffsbestimmung für „*Fairness and transparency*“ („Verarbeitung nach Treu und Glauben, Transparenz“)). Der Ausschuss stellt fest, dass zum Beispiel im Kriterium DP02.02, Randnummer 14 die Zertifizierungskriterien vorsehen, dass zu berücksichtigen ist, „*whether the data subjects can reasonably foresee at the time of the collection of the personal data and the circumstances of the processing that processing may take place for this purpose*“ („ob für

[4] Vgl. EDSA, Stellungnahme 15/2023 über den Entwurf des Beschlusses der niederländischen Aufsichtsbehörde betreffend die Brand Compliance-Zertifizierungskriterien, angenommen am 19. September 2023, Randnummer 15.

[5] Siehe EDSA, Stellungnahme 19/2024 zu den EuroPriSe-Zertifizierungskriterien in Bezug auf ihre Genehmigung als Europäisches Datenschutzsiegel durch den Ausschuss, angenommen am 16. Juli 2024, Randnummer 7.

[6] Vgl. Stellungnahme 26/2024 des EDSA zum Entwurf des Beschlusses der Aufsichtsbehörde der Freien Hansestadt Bremen betreffend den von der datenschutz cert GmbH vorgelegten „Kriterienkatalog für die Zertifizierung von IT-gestützter Verarbeitung personenbezogener Daten gemäß Artikel 42 DSGVO (‚DSGVO – information privacy standard‘)“, angenommen am 2. Dezember 2024, Randnummer 24.

die betroffenen Personen in dem Zeitpunkt, in dem die personenbezogenen Daten erhoben werden, und unter den Umständen der Verarbeitung vernünftigerweise erkennbar ist, dass eine Verarbeitung zu diesem Zweck erfolgen könnte“). Was die vernünftigen Erwartungen der betroffenen Personen angeht, ist der Ausschuss der Auffassung, dass die Beziehung der betroffenen Personen zum Verantwortlichen („z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht“) ein Kriterium ist, das sich unmittelbar aus den Erwägungsgründen 47 und 50 DSGVO ergibt. Um die Einhaltung der DSGVO wie auch die Überprüfbarkeit der Zertifizierungskriterien sicherzustellen, empfiehlt der Ausschuss deshalb, dass die DE-AB vom Programmeigner verlangt, die Bestimmungen der Erwägungsgründe 47 und 50 DSGVO zu berücksichtigen, um die Kriterien weiter auszuarbeiten und zu garantieren, dass für die Bewertung der vernünftigen Erwartungen der betroffenen Personen die Beziehung der betroffenen Personen zum Verantwortlichen ordnungsgemäß berücksichtigt wird.

15. In Bezug auf das Entwurfskriterium DP04 über „*Consent*“ („Einwilligung“) weist der Ausschuss auf einige Unstimmigkeiten im Wortlaut hin, die zu Verwirrung über die Art der in den Artikeln 7 und 8 DSGVO verankerten rechtlichen Pflichten führen könnten. Der Ausschuss stellt fest, dass im Abschnitt „*Definition of requirements*“ (Bestimmung der Anforderungen) Sätze verwendet werden wie „*The declaration of consent used is provided in easily accessible, clear and plain language, visibly separated from other matters*“ („Die verwendete Einwilligungserklärung wird in zugänglicher, klarer und einfacher Sprache, erkennbar von anderen Regelungsgegenständen getrennt, bereitgestellt“) (Kriterium DP04.02) oder „*There is a process for providing proof that the data subject has given consent*“ („Es gibt ein Verfahren für die Erbringung des Nachweises, dass die betroffene Person ihre Einwilligung erteilt hat“) (Kriterium DP04.03). Dagegen heißt es beispielsweise in Kriterium DP04.08, dass „*[i]n the case of an information society service offered directly to a child, the processing of the child's personal data is lawful if the child has reached the age of sixteen and the child has given consent to the processing*“ („[i]m Fall eines Angebots von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, … die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig (ist), wenn das Kind das 16. Lebensjahr vollendet hat und das Kind in die Verarbeitung eingewilligt hat“). Diesbezüglich regt der EDSA an, dass die DE-AB vom Programmeigner verlangt, das Kriterium DP04 anzupassen, um sicherzustellen, dass der Wortlaut der einschlägigen Abschnitte die Art und den Umfang der Pflichten in Artikel 7 DSGVO (Bedingungen für die Einwilligung) und Artikel 8 DSGVO (Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft) wiedergibt.

2.5. GRUNDSÄTZE, ARTIKEL 5

16. In Bezug auf Abschnitt DP02 („*Principles relating to processing*“ (Grundsätze in Bezug auf die Verarbeitung)) merkt der Ausschuss an, dass in den einzelnen Kriterien nicht durchgehend einheitlich und ausdrücklich auf die in Artikel 5 DSGVO genannten Grundsätze Bezug genommen wird, was die Lesbarkeit und Verständlichkeit des Kriteriums beeinträchtigen könnte[7]. Beispielsweise werden die Anforderungen an eine Verarbeitung, die in einer „*fair*

[7] Vgl. EDSA, Stellungnahme 15/2023 über den Entwurf des Beschlusses der niederländischen Aufsichtsbehörde betreffend die Brand Compliance-Zertifizierungskriterien, angenommen am 19. September 2023, Randnummer 24.

and transparent manner“ („fairen und transparenten Weise“) erfolgt (Kriterium DP02.02), im Zertifizierungsprogramm festgelegt, ohne dass auf den Grundsatz von Treu und Glauben (Fairness) als gemäß Artikel 5 Absatz 1 Buchstabe a unabhängig zu prüfendes eigenständiges Element eingegangen wird[8]. Der Ausschuss empfiehlt deshalb, dass die DE-AB vom Programmeigner verlangt, in ausdrücklicherer Weise auf die Grundsätze in Artikel 5 DSGVO Bezug zu nehmen und spezifische, genaue und überprüfbare Kriterien auszuarbeiten, die auf den Elementen beruhen, die in Abschnitt 3.3 der am 20. Oktober 2020 angenommenen EDSA-Leitlinien 4/2019 zu Artikel 25 DSGVO Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen aufgeführt sind.

17. Der Ausschuss stellt fest, dass die im Entwurf genannten Kriterien (z. B. DP02.01, DP02.02 und DP06.07) unter anderem darauf abzielen, die Informationen zu regeln, die zur Einhaltung der in Artikel 5 Absatz 1 Buchstabe a DSGVO genannten Grundsätze den betroffenen Personen zu übermitteln sind. In den Kriterien ist jedoch nicht immer klar angegeben, wann und auf welche Weise die erforderlichen Informationen zu übermitteln sind, da sich die Kriterien jeweils auf unterschiedliche Zeitrahmen beziehen[9]. In den Kriterien DP02.01 und DP02.02 gibt es dagegen keinerlei Angaben zum Zeitpunkt. Der Ausschuss erinnert an die Bestimmungen der Artikel 13 und 14 DSGVO, die genauere Angaben zu den Pflichten der Verantwortlichen vorsehen, sowie an seine früheren Leitlinien in Bezug auf „zentrale Aspekte der Technikgestaltung und der Voreinstellung in Bezug auf den Grundsatz der Transparenz“[10]. Zudem stellt der Ausschuss fest, dass das Kriterium DP02.02 in Bezug auf Profiling bestimmt, dass „*the information must be provided at the time the PD is collected or, in the case of indirectly collected data, the time frame pursuant to Art. 14 para. 3 lit. a to c GDPR must be ensured*“ („die Informationen zu dem Zeitpunkt zu übermitteln sind, zu dem die personenbezogenen Daten erhoben werden, oder dass, wenn es sich um indirekt erhobene Daten handelt, die Einhaltung der in Artikel 14 Absatz 3 Buchstabe a DSGVO genannten Frist sicherzustellen ist“). Insoweit ist dem Ausschuss nicht klar, ob diese Pflicht auf Profiling-Situationen beschränkt ist oder ob sie für alle Verarbeitungsvorgänge gilt. Der Ausschuss empfiehlt der DE-AB deshalb, vom Programmeigner zu verlangen, dass er in die Kriterien weitere Informationen und Detailangaben dazu aufnimmt, wann und auf welche Weise der Verantwortliche die sich aus der DSGVO ergebenden Informationspflichten erfüllen muss.

18. In Bezug auf Kriterium DP02.05, welches die weitere Verarbeitung betrifft, stellt der Ausschuss fest, dass der Programmeigner bei der Auflistung der für die Implementierung in Betracht

[8] Vgl. zum Beispiel die Aspekte, die bei der Verarbeitung nach Treu und Glauben zu berücksichtigen sind, die der Ausschuss in Randnummer 70 seiner am 20. Oktober 2020 angenommenen Leitlinien 4/2019 zu Artikel 25, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, aufgelistet hat; vgl. auch EDSA, Stellungnahme 18/2024 zum Entwurf eines Beschlusses der Österreichischen Aufsichtsbehörde zu den Zertifizierungskriterien der DSGVO-zt GmbH, angenommen am 16. Juli 2024, Randnummer 22; EDSA, Stellungnahme 26/2024 zum Entwurf des Beschlusses der Aufsichtsbehörde der Freien Hansestadt Bremen betreffend den von der datenschutz cert GmbH vorgelegten „Kriterienkatalog für die Zertifizierung von IT-gestützter Verarbeitung personenbezogener Daten gemäß Artikel 42 DSGVO (‚DSGVO – information privacy standard‘)“, angenommen am 2. Dezember 2024, Randnummer 14.

[9] So heißt es zum Beispiel in Kriterium DP06.04, dass die Informationen „*before collection*“ („vor der Erhebung“) zu übermitteln sind, wohingegen die Übermittlung gemäß DP06.07 „*without undue delay, and in any case within one month of receipt of the request*“ („unverzüglich, auf jeden Fall jedoch innerhalb von einem Monat nach Antragseingang“) erfolgen muss.

[10] EDSA, Leitlinien 4/2019 zu Artikel 25, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, angenommen am 20. Oktober 2020, insbesondere der Umstand, dass „[d]ie Informationen … zum maßgeblichen Zeitpunkt und in der geeigneten Form bereitgestellt werden [sollten]“, Rn. 66.

kommenden technischen und organisatorischen Maßnahmen unter anderem „*Access and authorisation concept*“ („Zugang und Autorisierungskonzept“) und „*Access and access controls*“ („Zugang und Zugangskontrollen“) aufführt. Der Ausschuss merkt an, dass sich diese beiden Maßnahmen nicht klar voneinander abgrenzen lassen. Der EDSA hält es auch für unklar, was der Programmeigner mit der Definition von „*data protection concept*“ („Datenschutzkonzept“) meint. Der Ausschuss regt deshalb an, dass die zuständige AB vom Programmeigner verlangt, die Unterschiede zwischen „*Access and authorisation concept*“ („Zugang und Autorisierungskonzept“) und „*Access and access controls*“ („Zugang und Zugangskontrollen“) klarzustellen. Des Weiteren regt der Ausschuss an, dass die DE-AB vom Programmeigner verlangt, die Bedeutung von „*data protection concept*“ („Datenschutzkonzept“) zu erklären.

19. Der Ausschuss begrüßt das Kriterium DP02.06, das Datenminimierung betrifft, sowie die Bezugnahme auf die mit diesem Grundsatz verbundenen Pflichten. Der Ausschuss merkt allerdings auch an, dass zwar wichtige Aspekte wie Pseudonymisierung und Anonymisierung erwähnt werden und überprüfbar zu sein scheinen, dass aber andere Aspekte allgemeiner gehalten sind (vgl. die Gliederungspunkte unter Kriterium DP02.06)[11]. Im Interesse der Vollständigkeit und Überprüfbarkeit regt der Ausschuss deshalb an, dass die DE-AB vom Programmeigner verlangen sollte, weitere spezifische, genaue und überprüfbare Kriterien für die Datenminimierung auszuarbeiten.

2.6. RECHTE DER BETROFFENEN PERSON

20. Kriterium DP06.05 betrifft die Informationspflicht aus Artikel 14 DSGVO. In dem Kriterium ist jedoch nicht der genaue Zeitpunkt angegeben, zu dem die Informationen gemäß Artikel 14 Absatz 3 DSGVO zu erteilen sind. Der Ausschuss empfiehlt deshalb, dass die DE-AB vom Programmeigner verlangt, sicherzustellen, dass die Kriterien die in Artikel 14 Absatz 3 DSGVO genannten Anforderungen widerspiegeln.

21. Im Kriterium DP06.06 geht es um Informationspflichten gemäß den Artikeln 13 Absatz 3 und 14 Absatz 4 DSGVO. In diesem Zusammenhang wird im Kriterium Artikel 14 Absatz 3 DSGVO erwähnt. Der Ausschuss empfiehlt, dies zu korrigieren, damit auf Artikel 14 Absatz 4 DSGVO verwiesen wird. Hinsichtlich der Bestimmung in Kriterium DP06.06, wonach der Verantwortliche „*documents a consideration in which it states that the processing for the other purpose is compatible with that for which the PD were originally collected, cf. requirement DP03.08*“ („eine Erwägung dokumentiert, in der er angibt, dass die Verarbeitung für den anderen Zweck mit demjenigen, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, vgl. Anforderung DP03.08“), empfiehlt der Ausschuss, dass die DE-AB vom Programmeigner verlangt, klar anzugeben, wer in diesem Zusammenhang die betroffenen Personen sind.

22. Des Weiteren enthält Kriterium DP06.08 die Anforderungen an die Zurverfügungstellung einer Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, im Sinne von Artikel 15 Absatz 3 DSGVO. Nach Ansicht des EDSA ist das Verfahren für die Zurverfügungstellung der Kopie der personenbezogenen Daten nicht ganz klar, und der

[11] Vgl. nähere Ausführungen dazu in EDSA, Leitlinien 4/2019 zu Artikel 25, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, angenommen am 20. Oktober 2020, Abschnitt 3.5.

Ausschuss empfiehlt, dass die DE-AB vom Programmeigner verlangt, klarzustellen, auf welche Weise die Kopie zur Verfügung gestellt werden wird[12].

23. Gemäß Kriterium DP06.15 (Widerspruchsrecht) bedarf es einer „*definition of personnel responsibilities to ensure that an objection to the processing of personal data is realized within one month*“ („Festlegung der Personalzuständigkeiten, um sicherzustellen, dass ein Widerspruch gegen die Verarbeitung personenbezogener Daten innerhalb von einem Monat realisiert wird“). Der Ausschuss findet diese Formulierung ungenau, und zwar insbesondere den Begriff „*realized*“ („realisiert“), da die Pflichten aus Artikel 12 Absätze 3 und 4 DSGVO („stellt … Informationen über die … ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung“) mit der sich aus Artikel 21 DSGVO ergebenden Pflicht zur Einstellung der Verarbeitung vermengt wird. Der Ausschuss empfiehlt der DE-AB deshalb, vom Programmeigner zu verlangen, DP06.15 genauer zu fassen, indem Kriterien ausgearbeitet werden, die die verschiedenen Maßnahmen, die zu ergreifen sind, um dem Widerspruchsrecht Genüge zu tun, und die damit verbundenen Informationspflichten berücksichtigen.

2.7. SCHUTZ GARANTIERENDE TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

24. Der Ausschuss stellt fest, dass in den Kriterien ausdrücklich angegeben ist, dass diese mit den Grundanforderungen internationaler Normen an technische und organisatorische Maßnahmen (wie ISO/IEC 27001 und BSI-IT-Grundschutz), die ein förmliches Verfahren für die Durchführung von Penetrationstests vorsehen, in Einklang stehen. Des Weiteren stellt der Ausschuss fest, dass gemäß Kriterium DP08.01 der Verantwortliche und der Auftragsverarbeiter die Wirksamkeit der implementierten Maßnahmen durch dokumentierte Penetrationstests überprüfen müssen, die durch Schwachstellen-Scans, Konfigurationsanalysen und Tests auf Anwendungsebene ergänzt werden. Soweit es jedoch in dem Kriterium heißt, dass „*the results of these tests must be analysed, evaluated, and prioritised*“ [*in the context of penetration test results*] („die Ergebnisse dieser Tests [im Zusammenhang mit den Penetrationstestergebnissen] analysiert, evaluiert und priorisiert“ werden müssen“), ist für den Ausschuss nicht klar ersichtlich, ob diese Pflicht Bestandteil des „*risk management plan*“ („Risikomanagementplans“) ist, auf den später im Zusammenhang mit Schwachstellen-Scans Bezug genommen wird. Der Ausschuss merkt an, dass Scannen, Bewertung, Priorisierung, Behebung, Überprüfung und Dokumentation von Schwachstellen sämtlich ein Prozess sind, der von einem allgemeineren Plan für Risiko- und Risikominderungsmanagement umfasst sein muss. Der Ausschuss regt an, dass die DE-AB den Programmeigner auffordert, klarzustellen, wie die Linearität des Risikominderungsverfahrens gestaltet ist und ob der Prozess für die Analyse der Penetrationstestergebnisse Teil eines allgemeineren Risikomanagementplans ist oder ob er spezifisch für die einzelnen Verfahren der Schwachstellen-Scans gilt.

25. In Bezug auf die Kriterien DP08.01 und DP08.02 verweist der Programmeigner auf die BSI-Norm, deren Risikokategorien in der Bewertungserläuterung ausdrücklich festgelegt sind[13] In

[12] Vgl. auch EuGH, Urteil vom 4. Mai 2023, Rechtssache C-487/21, *F.F. gegen Österreichische Datenschutzbehörde and CRIF GmbH* (ECLI:EU:C:2023:369).

[13] Vgl. EDSA, Stellungnahme 25/2022 zu den EuroPriSe-Zertifizierungskriterien für Verarbeitungsvorgänge von Auftragsverarbeitern, angenommen am 13. September 2022, Randnummer 30, wo es heißt, dass der Programmeigner die Risiken nach den verschiedenen Arten kategorisieren muss.

Bezug auf die Verpflichtung zur Durchführung jährlicher Penetrationstests ist laut dem Kriterium eine „*high protection requirement*“ („hohe Schutzanforderung“) erforderlich; insoweit ist dem Ausschuss nicht klar, ob es sich um dieselbe Risikoniveau-Nomenklatur wie die für die Schwachstellenbewertung verwendete handelt. Sollte dies nicht der Fall sein, so sollten die Kriterien die in der Risikobewertungsmatrix verwendeten Niveaus enthalten, um einen Vergleich zwischen verschiedenen Schutzanforderungen zu ermöglichen. Der Ausschuss regt deshalb an, dass der DE-AB den Programmeigner auffordert, die verwendeten Begrifflichkeiten klarzustellen und eine kriterienübergreifend einheitliche Risikokategorisierung sicherzustellen, um Uneindeutigkeit bei der Umsetzung und Bewertung zu vermeiden.

3. SCHLUSSFOLGERUNGEN / EMPFEHLUNGEN

26. Abschließend stellt der EDSA fest, dass die vorliegenden Zertifizierungskriterien zu einer uneinheitlichen Anwendung der DSGVO führen könnten und dass folgende Änderungen erforderlich sind, um die Anforderungen aus Artikel 42 DSGVO, so wie diese sich im Licht der Leitlinien und des Addendums ergeben, zu erfüllen.

1. In Bezug auf die „*general remarks*“ („allgemeinen Bemerkungen“) empfiehlt der Ausschussder DE-AB, zu verlangen, dass der Programmeigner:

a. sämtliche im Zertifizierungsprogramm enthaltenen Bezugnahmen überprüft und berichtigt;

b. im gesamten Zertifizierungsprogramm die genaue Bedeutung klarstellt, die dem Wort „*sufficient*“ („hinreichend“) im jeweiligen Zusammenhang zukommt;

c. für die Zwecke der Überprüfbarkeit im gesamten Zertifizierungsprogramm festlegt, welche spezifischen Prozesselemente der Begriff „*appropriate processes*“ („geeignete Prozesse“), wo immer dieser vorkommt, umfasst.

2. In Bezug auf den „*scope of the certification mechanism and target evaluation (ToE)*“ („Anwendungsbereich des Zertifizierungsverfahrens und Evaluierungsgegenstand (Target of Evaluation, ToE)“) empfiehlt der Ausschuss der DE-AB, zu verlangen, dass der Programmeigner:

a. in das Zertifizierungsprogramm spezifische Kriterien aufnimmt, die die Besonderheiten der Unterauftragsverarbeitung berücksichtigen, oder, alternativ, im Einleitungsteil angibt, dass Unterauftragsverarbeiter nicht nach dem Zertifizierungsprogramm zertifiziert werden können.

3. In Bezug auf die „*general requirements*“ („allgemeinen Bemerkungen“) empfiehlt der Ausschuss der DE-AB, zu verlangen, dass der Programmeigner:

a. spezifischere Kriterien für die Unterstützungspflichten der Auftragsverarbeiter in Bezug auf das jeweilige Kriterium aufnimmt.

4. In Bezug auf die „*lawfulness of processing*“ („Rechtmäßigkeit der Verarbeitung“) empfiehlt der Ausschuss, dass die DE-AB verlangt, dass der Programmeigner:

a. das Kriterium DP03.01 so ändert, dass es enger an den Wortlaut des Artikel 6 Absatz 1 DSGVO angelehnt ist;

b. die Kriterien genauer ausarbeitet und garantiert, dass für die Bewertung der vernünftigen Erwartungen der betroffenen Personen, wie in den Erwägungsgründen 47 und 50 DSGVO vorgesehen, die Beziehung der betroffenen Personen zum Verantwortlichen ordnungsgemäß berücksichtigt wird.

5. In Bezug auf die „*principles, Article 5*“ („Grundsätze, Artikel 5“) empfiehlt der Ausschuss, dass die DE-AB verlangt, dass der Programmeigner:

a. in Abschnitt DP02 der Zertifizierungskriterien in ausdrücklicherer Weise auf die Grundsätze in Artikel 5 DSGVO Bezug nimmt und spezifische, genaue und überprüfbare Kriterien ausarbeitet, die auf den Elementen beruhen, die in den am 20. Oktober 2020 angenommenen EDSA-Leitlinien 4/2019 zu Artikel 25 DSGVO über Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen aufgeführt sind;

b. in die Kriterien weitere Informationen und Detailangaben dazu aufnimmt, wann und auf welche Weise der Verantwortliche die sich aus der DSGVO ergebenden Informationspflichten – insbesondere diejenigen aus den Artikeln 13 und 14 DSGVO und aus den EDSA-Leitlinien 4/2019 zu Artikel 25 DSGVO über Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, angenommen am 20. Oktober 2020 – erfüllen muss.

6. In Bezug auf die „*rights of the data subject*“ („Rechte betroffener Personen“) empfiehlt der Ausschuss, dass die DE-AB verlangt, dass der Programmeigner:

a. sicherstellt, dass das Kriterium DP06.05 die in Artikel 14 Absatz 3 DSGVO genannten Anforderungen widerspiegelt;

b. in Kriterium DP06.06 die Bezugnahme auf Artikel 14 Absatz 3 DSGVO streicht und diese Bezugnahme berichtigt, sodass sie auf Artikel 14 Absatz 4 DSGVO verweist;

c. in Kriterium DP06.06, wo es heißt, dass der Verantwortliche „*documents a consideration in which it states that the processing for the other purpose is compatible with that for which the PD were originally collected, cf. requirement DP03.08*“ („eine Erwägung dokumentiert, in der er angibt, dass die Verarbeitung für den anderen Zweck mit demjenigen, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, vgl. Anforderung DP03.08“), klar angibt, wer in diesem Zusammenhang die betroffenen Personen sind;

d. in Kriterium DP06.08, wo die Anforderungen an die Zurverfügungstellung einer Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, angegeben sind, klarstellt, wie die Kopie übermittelt werden wird;

e. für das Kriterium DP06.15 Kriterien ausarbeitet, die die verschiedenen Maßnahmen, die zu ergreifen sind, um dem Widerspruchsrecht Genüge zu tun, und die damit verbundenen Informationspflichten des Verantwortlichen gemäß den Artikeln 12 Absätze 3 und 4 und 21 DSGVO berücksichtigen.

Abschließend erinnert der EDSA im Einklang mit den Leitlinien auch daran, dass die DE-AB im Fall von Änderungen der Zertifizierungskriterien der Trusted Site Privacy (TÜV IT), die wesentliche Änderungen mit sich bringen, gemäß Artikel 42 Absatz 5 und Artikel 43 Absatz 2 Buchstabe b der DSGVO verpflichtet ist, dem EDSA die geänderte Fassung vorzulegen.

4. SCHLUSSBEMERKUNGEN

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

28. Nach Artikel 64 Absätze 7 und 8 DSGVO muss die DE-AB dem Vorsitz binnen zwei Wochen nach Eingang der Stellungnahme auf elektronischem Weg mitteilen, ob sie den Beschlussentwurf beibehalten oder ändern wird. Innerhalb derselben Frist muss sie den geänderten Entwurf übermitteln oder, falls sie beabsichtigt, der Stellungnahme des Ausschusses insgesamt oder teilweise nicht zu folgen, die maßgeblichen Gründe dafür mitteilen.

29. Der EDSA erinnert daran, dass die DE-AB gemäß Artikel 43 Absatz 6 DSGVO die Zertifizierungskriterien in leicht zugänglicher Form veröffentlichen und dem Ausschuss zur Aufnahme in das öffentliche Register der Zertifizierungsverfahren und Datenschutzsiegel gemäß Artikel 42 Absatz 8 DSGVO übermitteln muss.

Für den Europäischen Datenschutzausschuss

Der Vorsitz

(Anu Talus)