Stellungnahme 25/2022 zu den EuroPriSe-Zertifizierungskriterien für Verarbeitungsvorgänge von Auftragsverarbeitern

Angenommen am 13. September 2022

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 Protokoll 37, geändert durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018[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 Einrichtung von Datenschutzzertifizierungsverfahren (im Folgenden „Zertifizierungsverfahren“) und von Datenschutzsiegeln und -prüfzeichen, um die Einhaltung der DSGVO bei Verarbeitungsvorgängen durch Verantwortliche und Auftragsverarbeiter nachzuweisen, wobei den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen Rechnung zu tragen ist.[2] Darüber hinaus kann die Einführung von Zertifizierungen die Transparenz erhöhen und es den betroffenen Personen ermöglichen, das Datenschutzniveau einschlägiger Produkte und Dienstleistungen zu bewerten.[3]

(2) Die Zertifizierungskriterien sind ein fester Bestandteil eines jeden Zertifizierungsverfahrens. Folglich wird in der DSGVO die Genehmigung nationaler Zertifizierungskriterien für ein Zertifizierungsverfahren durch die zuständige Aufsichtsbehörde (Artikel 42 Absatz 5 und Artikel 43 Absatz 2 Buchstabe b der DSGVO) oder im Falle eines Europäischen Datenschutzsiegels durch den EDSA (Artikel 42 Absatz 5 und Artikel 70 Absatz 1 Buchstabe o der DSGVO) verpflichtend festgelegt.

(3) Beabsichtigt eine Aufsichtsbehörde, eine Zertifizierung gemäß Artikel 42 Absatz 5 der DSGVO zu genehmigen, besteht die Hauptaufgabe des EDSA darin, die einheitliche Anwendung der DSGVO durch das in den Artikeln 63, 64 und 65 der DSGVO genannte Kohärenzverfahren sicherzustellen. In diesem Rahmen ist der EDSA gemäß Artikel 64 Absatz 1 Buchstabe c der DSGVO verpflichtet, eine Stellungnahme zum Entwurf eines Beschlusses der Aufsichtsbehörde zur Genehmigung der Zertifizierungskriterien abzugeben.

(4) Mit dieser Stellungnahme soll die einheitliche Anwendung der DSGVO sichergestellt werden, auch durch die Aufsichtsbehörden, Verantwortlichen und Auftragsverarbeiter im Lichte der Kernelemente, die Zertifizierungsverfahren enthalten müssen. Die Bewertung des EDSA

[1] Soweit in dieser Stellungnahme auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.
[2] Artikel 42 Absatz 1 der DSGVO.
[3] Erwägungsgrund 100 der DSGVO.

erfolgt insbesondere auf der 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 ihres Addendums mit „Leitlinien zur Bewertung der Zertifizierungskriterien“ (im Folgenden „Addendum“), für die die Frist für die öffentliche Konsultation am 26. Mai 2021 endete.

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

(6) Zertifizierungsverfahren sollten es den Verantwortlichen und Auftragsverarbeitern ermöglichen, die Einhaltung der DSGVO nachzuweisen; daher sollten die Zertifizierungskriterien den in der DSGVO festgelegten Anforderungen und Grundsätzen in Bezug auf den Schutz personenbezogener Daten angemessen Rechnung tragen und zu ihrer einheitlichen Anwendung beitragen.

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

(8) In diesem Zusammenhang sollten Zertifizierungen einen Mehrwert für eine Organisation schaffen, indem sie zur Umsetzung standardisierter und spezifischer organisatorischer und technischer Maßnahmen beitragen, die die Einhaltung der Vorschriften bei Verarbeitungsvorgängen unter Berücksichtigung sektorspezifischer Anforderungen nachweislich erleichtern und verbessern.

(9) Der EDSA begrüßt die Bemühungen der Systeminhaber, Zertifizierungsverfahren auszuarbeiten, die praktische und potenziell kosteneffiziente Instrumente sind, um eine größere Kohärenz mit der DSGVO zu gewährleisten und das Recht der betroffenen Personen auf Privatsphäre und Datenschutz durch mehr Transparenz zu fördern.

(10) Der EDSA weist darauf hin, dass Zertifizierungen Instrumente der freiwilligen Rechenschaftspflicht sind und dass die Einhaltung eines Zertifizierungsverfahrens weder die Verantwortung der Verantwortlichen oder Auftragsverarbeiter für die Einhaltung der DSGVO einschränkt noch die Aufsichtsbehörden daran hindert, ihre Aufgaben und Befugnisse gemäß der DSGVO und den einschlägigen nationalen Rechtsvorschriften wahrzunehmen.

(11) Gemäß Artikel 64 Absatz 1 Buchstabe c der DSGVO in Verbindung mit Artikel 10 Absatz 2 der Satzung des EDSA hat die Annahme der Stellungnahme des EDSA binnen acht Wochen ab dem ersten Werktag, nachdem der Vorsitz und die zuständige Aufsichtsbehörde beschlossen haben, dass die Akte abgeschlossen ist, zu erfolgen. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit auf Beschluss des Vorsitzes um weitere sechs Wochen verlängert werden.

(12) Der Schwerpunkt der Stellungnahme des EDSA liegt auf den Zertifizierungskriterien. Für den Fall, dass der EDSA umfassende Informationen über die Bewertungsmethoden benötigt, um die Überprüfbarkeit des Entwurfs der Zertifizierungskriterien im Rahmen seiner Stellungnahme gründlich bewerten zu können, umfasst Letzteres keinerlei Genehmigungen solcher Bewertungsmethoden —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 ZUSAMMENFASSUNG DES SACHVERHALTS

1. Gemäß Artikel 42 Absatz 5 der DSGVO und den Leitlinien wurden die „EuroPriSe-Zertifizierungskriterien für Verarbeitungsvorgänge von Auftragsverarbeitern“ (im Folgenden „Entwurf der Zertifizierungskriterien“ oder „Zertifizierungskriterien“) von der EuroPriSe Cert GmbH (im Folgenden „EuroPriSe“), einer juristischen Person in Deutschland, ausgearbeitet und der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, der zuständigen deutschen Aufsichtsbehörde in Nordrhein-Westfalen (im Folgenden „deutsche Aufsichtsbehörde (aus NRW)“), vorgelegt.

2. Die deutsche Aufsichtsbehörde (aus NRW) hat den Entwurf der Kriterien für ein nationales Zertifizierungsprogramm dem EDSA vorgelegt und am 2. Juni 2022 um eine Stellungnahme des Ausschusses gemäß Artikel 64 Absatz 1 Buchstabe c der DSGVO ersucht. Die Entscheidung über die Vollständigkeit des Vorgangs wurde am 7. Juli 2022 getroffen.

2 BEWERTUNG

3. Der Ausschuss hat seine Bewertung im Einklang mit der Struktur durchgeführt, die in Anhang 2 der Leitlinien (im Folgenden „Anhang“) und ihrem Addendum vorgesehen ist. Soweit diese Stellungnahme einen bestimmten Abschnitt des Entwurfs der Zertifizierungskriterien auslässt, sollte das so verstanden werden, dass der Ausschuss keine Anmerkungen hat und die deutsche Aufsichtsbehörde (aus NRW) nicht auffordert, weitere Maßnahmen zu ergreifen.

2.1 Allgemeine Bemerkungen

4. Nach Ansicht des Ausschusses ist der Anwendungsbereich des Zertifizierungsprogramms nicht hinreichend klar. Ungeachtet der Tatsache, dass der Anwendungsbereich des Programms in Klammern („(Anwendungsbereich: DE)“) auf der Titelseite des Dokuments angegeben ist, enthält diese Seite auch die Formulierung („European Privacy Seal“), die trotzdem den Eindruck erwecken kann, dass das Programm einen europäischen Anwendungsbereich hat. Daher regt der Ausschuss an, den Anwendungsbereich des Zertifizierungsprogramms im Einleitungstext des Dokuments klarzustellen.

5. Bei der vorliegenden Zertifizierung handelt es sich nicht um eine Zertifizierung gemäß Artikel 46 Absatz 2 Buchstabe f der DSGVO, die für die internationale Übermittlung personenbezogener Daten bestimmt ist. Sie bietet keine angemessenen Garantien im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen gemäß den in Artikel 46 Absatz 2 Buchstabe f genannten Bedingungen. Die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf nur dann erfolgen, wenn die Bestimmungen in Kapitel V der DSGVO eingehalten werden.

2.2 Verarbeitungsvorgänge durch einen Auftragsverarbeiter

6. Nach Ansicht des Ausschusses ist die Beurteilung, ob der Antragsteller ein Auftragsverarbeiter ist, Teil der Antragsprüfung (und nicht der Kriterien nach Artikel 42 Absatz 5 der DSGVO). Die Zertifizierungsstelle muss die Rolle anhand der Informationen und Unterlagen bewerten, die

der Antragsteller bei der Beantragung einer Zertifizierung vorlegt. Daher empfiehlt der Ausschuss, Abschnitt 1 aus den Kriterien gemäß Artikel 42 Absatz 5 der DSGVO zu streichen und ihn in das Antragsverfahren aufzunehmen.

7. Der Ausschuss stellt ferner fest, dass das derzeitige Programm Kriterien gemäß Artikel 28 der DSGVO hinsichtlich des Verhältnisses des Auftragsverarbeiters zum Verantwortlichen (in Abschnitt 2.2 des Programms) und des Verhältnisses des Auftragsverarbeiters zu anderen Auftragsverarbeitern[4] (Unterauftragsverarbeitern) (in Abschnitt 2.3.3 des Programms) vorsieht, die es zu erfüllen gilt. Um klarzustellen, dass dies nicht bedeutet, dass ein solcher Unterauftragsverarbeiter im Rahmen dieses Programms zertifiziert werden kann und dass nur die im Namen des Antragstellers durchgeführten Verarbeitungsvorgänge der Zertifizierung unterliegen, empfiehlt der EDSA, auch in der Einleitung zu präzisieren, dass Unterauftragsverarbeiter nicht im Rahmen des EuroPriSe-Zertifizierungsprogramms zertifiziert werden können.

2.3 Anforderungen aus rechtlicher Sicht

2.3.1 Verzeichnis der Verarbeitungstätigkeiten

8. Die Anforderung der Führung eines Verzeichnisses der Verarbeitungstätigkeiten gemäß Artikel 30 Absatz 2 der DSGVO ist in Abschnitt 2.1.1 der Zertifizierungskriterien festgelegt. Laut EuroPriSe gilt diese Anforderung „immer“. Der Ausschuss regt jedoch an, klarzustellen, ob die Ausnahmen nach Artikel 30 Absatz 5 der DSGVO in Einzelfällen weiterhin gelten könnten oder ob – um die Kriterien des EuroPriSe-Programms zu erfüllen – ein solches Verzeichnis der Verarbeitungstätigkeiten unabhängig von den Ausnahmen stets von einem Zertifizierungskunden geführt werden muss.

2.3.2 Antragsteller, die Artikel 3 Absatz 2 der DSGVO unterliegen

9. Der Ausschuss stellt fest, dass Auftragsverarbeiter, die keine Niederlassung in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) haben, gemäß Abschnitt 2.1.3 einen Vertreter nach Artikel 27 der DSGVO benennen müssen. Folglich geht der Ausschuss davon aus, dass das EuroPriSe-Zertifizierungsprogramm für Zertifizierungskunden anwendbar ist, die außerhalb der EU oder des EWR ansässig sind.

10. Da dies bedeuten könnte, dass ein solcher Auftragsverarbeiter mit Sitz außerhalb der EU/des EWR auch personenbezogene Daten außerhalb der EU/des EWR verarbeiten könnte, empfiehlt der Ausschuss, in Abschnitt 2.1.3 klarzustellen, dass immer dann, wenn eine „Übermittlung“ im Sinne von Artikel 44 der DSGVO an einen Auftragsverarbeiter mit Sitz außerhalb der EU oder des EWR erfolgt, die in Kapitel V der DSGVO festgelegten Pflichten vollumfänglich einzuhalten sind. Darüber hinaus empfiehlt der Ausschuss, in Abschnitt 2.1.3 klarzustellen, dass es sich bei dem vorliegenden Programm nicht um ein Programm im Sinne von Artikel 46 Absatz 2 Buchstabe f der DSGVO handelt. Der Ausschuss empfiehlt, in Abschnitt 2.1.3. klarzustellen, dass der Antragsteller nicht berechtigt ist, die Zertifizierung in einer Weise zu nutzen, die den Eindruck erwecken könnte, dass es sich bei der Zertifizierung selbst um ein Übermittlungsinstrument nach Artikel 46 Absatz 2 Buchstabe f der DSGVO handelt. Die Verantwortlichen sollten ungeachtet des Vorliegens des Zertifizierungssiegels dennoch eine Bewertung der Rechtsvorschriften des Empfängerlands vornehmen, bevor sie

[4] Andere Auftragsverarbeiter im Sinne von Artikel 28 Absätze 2 und 4 der DSGVO.

Daten an den DSGVO-zertifizierten Auftragsverarbeiter außerhalb der EU übermitteln. Für den Fall, dass die Rechtsvorschriften kein angemessenes Schutzniveau vorsehen, sollten zusätzliche Maßnahmen ergriffen werden.[5]

11. Ein Auftragsverarbeiter sollte keine Zertifizierung beantragen, wenn ihm bekannt ist, dass seine Rechtsvorschriften ihn daran hindern würden, die im Zertifizierungsprogramm verankerten Grundsätze der DSGVO einzuhalten.

2.4 Verhältnis des Verantwortlichen zum Auftragsverarbeiter

12. Der Ausschuss stellt fest, dass in den Abschnitten 2.2 und 2.3 der EuroPriSe-Zertifizierungskriterien auf die Anforderungen im Sinne von Artikel 28 der DSGVO Bezug genommen wird. In Abschnitt 2.2.1 der Zertifizierungskriterien geht es um das Vorhandensein von Vertragsklauseln, die alle Anforderungen des Artikels 28 der DSGVO erfüllen. In diesem Zusammenhang heißt es in der Orientierungshilfe, dass der Auftragsverarbeiter eine Vorlage für einen Auftragsverarbeitungsvertrag erstellt, die alle Anforderungen des Artikels 28 der DSGVO erfüllt. Ungeachtet der Tatsache, dass in der Orientierungshilfe auch darauf hingewiesen wird, dass die Vorlage nicht verwendet werden muss, empfiehlt der Ausschuss, diese Orientierungshilfe ausführlicher zu formulieren, um klarzustellen, dass eine solche Vorlage für einen Auftragsverarbeitungsvertrag das Recht des Verantwortlichen unberührt lässt, die Klauseln nach Artikel 28 der DSGVO mit dem Auftragsverarbeiter festzulegen oder auszuhandeln, ohne dass sich dies auf die Zertifizierung auswirkt.

13. Darüber hinaus heißt es in Abschnitt 2.2.1, dass diese Anforderung zu ändern ist, wenn die einschlägige Auftragsverarbeitung nicht auf der Grundlage eines Vertrags, sondern auf der Grundlage eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erfolgt. Gibt es jedoch andere Rechtsinstrumente, so ist die Anforderung des Abschnitts 2.2.1 nicht anwendbar. In diesen Fällen sind solche Vertragsklauseln nicht erforderlich. Der Ausschuss empfiehlt, den Wortlaut entsprechend zu ändern.

14. In Abschnitt 2.2.1 wird die Zertifizierungsstelle angewiesen, zu prüfen, ob das betreffende Rechtsinstrument die Anforderungen nach Artikel 28 der DSGVO erfüllt, ergänzt durch eine Fußnote, in der es heißt: „Diese Konstellation wird in dieser v2.1 des Kriterienkatalogs wegen fehlender praktischer Relevanz nicht näher betrachtet.“ Wenn bestimmte Kriterien in der Praxis nicht relevant sind, sollten sie nicht Teil des Kriterienkatalogs sein. Der Ausschuss empfiehlt daher, diese Sätze aus Abschnitt 2.2.1 zu streichen.

15. Die Anforderung in Abschnitt 2.2.1 Nummer 2 Buchstabe e der Kriterien im Detail sollte nicht nur den Wortlaut von Artikel 28 wiedergeben; vielmehr empfiehlt der Ausschuss, die Unterstützung näher zu spezifizieren, die der Auftragsverarbeiter leisten sollte oder könnte, um dem Verantwortlichen bei der Erfüllung seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Personen zu helfen. Dies soll die tatsächlichen Handlungsmöglichkeiten des Auftragsverarbeiters und des Verantwortlichen widerspiegeln, d. h. inwieweit der Verantwortliche bei der Ausübung der Rechte der betroffenen Person praktisch auf die Unterstützung des Auftragsverarbeiters angewiesen ist (Unterstützung ist zwingend erforderlich) oder ob der Verantwortliche lediglich (irgendeine Art von)

[5] Siehe EDSA-Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten: https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de).

Unterstützung durch den Auftragsverarbeiter in dieser Angelegenheit bevorzugt (Unterstützung ist optional). Ferner sollte in der Anforderung darauf hingewiesen werden, dass solche Klauseln mit der in der DSGVO festgelegten Verantwortung des Verantwortlichen in Bezug auf die Rechte der betroffenen Personen im Einklang stehen und diese Verantwortung nicht über Gebühr auf den Auftragsverarbeiter übertragen werden sollte.[6] Der EDSA empfiehlt, die Anforderung 2.2.1 dahin gehend zu ändern, dass berücksichtigt wird, inwieweit der Verantwortliche tatsächlich vom Auftragsverarbeiter und dessen Unterstützung in Bezug auf die Rechte der betroffenen Personen abhängig ist.

16. In Abschnitt 2.2.2 (Nummer 8 der Kriterien im Detail) heißt es, dass der Auftragsverarbeiter alle „erforderlichen Informationen“ zum Nachweis der Einhaltung von Artikel 28 der DSGVO zur Verfügung stellt. Es ist nicht ganz klar, auf welche Dokumente sich diese Anforderung konkret bezieht, da die Liste der Dokumente nicht beschränkt und der Begriff „erforderliche Informationen“ eher vage ist. Der Ausschuss empfiehlt daher, eine erschöpfende Liste der Dokumente/Informationen zu erstellen, die von der Zertifizierungsstelle zu prüfen ist, um zu beurteilen, ob dieses Kriterium erfüllt wird oder nicht. Darüber hinaus sollte in diesem Kriterium klargestellt werden, dass diese Dokumente/Informationen der Zertifizierungsstelle vorzulegen sind.

17. In Abschnitt 2.3.2 heißt es weiter, dass der Auftragsverarbeiter mit allen weiteren Auftragsverarbeitern Verträge schließen muss, die diesen weiteren Auftragsverarbeitern dieselben Datenschutzpflichten auferlegen, die in dem Vertrag/den Verträgen zwischen dem/den Verantwortlichen und dem Auftragsverarbeiter festgelegt sind. Für eine bessere Lesbarkeit empfiehlt der Ausschuss, den mittleren Teil des Satzes geringfügig zu ändern. So könnte z. B. „weiteren Auftragsverarbeitern“ in „Unterauftragsverarbeitern“ geändert werden.

18. In Abschnitt 2.3.2 (Nummer 1a der Anforderung im Detail) ist festgelegt, dass der genaue Zeitraum oder die Kriterien, nach denen er bestimmt wird, anzugeben sind. Aus Gründen der Klarheit empfiehlt der Ausschuss, in diese Anforderung aufzunehmen, dass diese Angaben zur Dauer der Verarbeitung im Einklang mit den einschlägigen Bestimmungen des Auftragsverarbeitungsvertrags, der zwischen dem Verantwortlichen und dem Auftragsverarbeiter geschlossen wurde, stehen müssen.

2.5 Anforderungen bezüglich spezieller Arten von Verarbeitungsvorgängen

2.5.1 Gesetzliche Geheimhaltungspflichten, Berufsgeheimnisse und besondere Amtsgeheimnisse, die nicht auf gesetzlichen Vorschriften beruhen

19. Der Ausschuss stellt fest, dass die Anforderung in Abschnitt 2.4.1 nur anwendbar ist, wenn die zu zertifizierenden Verarbeitungsvorgänge ausschließlich bzw. mehrheitlich von Verantwortlichen in Anspruch genommen werden, die besonderen Geheimhaltungs-/Verschwiegenheitspflichten unterliegen. Nach Ansicht des Ausschusses ist unklar, ob diese Anforderung für den Fall gilt, dass nur wenige Verantwortliche, die besonderen Pflichten unterliegen, die Verarbeitungsvorgänge des zertifizierten Auftragsverarbeiters in Anspruch nehmen. Darüber hinaus ist unklar, unter welchen Umständen der Begriff „mehrheitlich“ erfüllt ist. Daher empfiehlt der Ausschuss, Abschnitt 2.4.1 entsprechend zu präzisieren.

[6] Dieser Absatz ist in Verbindung mit den Absätzen 35, 36 und 37 zu lesen.

20. Zusätzlich zu Fußnote 63 des EuroPriSe-Zertifizierungsprogramms regt der Ausschuss an, in der „Orientierungshilfe“ von Abschnitt 2.4.1 weitere Beispiele dafür zu nennen, wie spezielle Geheimhaltungspflichten nach EU-Recht oder dem Recht von Mitgliedstaaten in die Vorlage für einen Auftragsverarbeitungsvertrag aufgenommen werden können.[7]

2.5.2 Übermittlung personenbezogener Daten an Drittländer

21. Der Ausschuss stellt fest, dass in Abschnitt 2.4.2 Anforderungen in Bezug auf Kapitel V der DSGVO festgelegt sind. Die EuroPriSe-Zertifizierung ist jedoch selbst kein Übermittlungsinstrument für die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen gemäß Artikel 46 Absatz 2 Buchstabe f der DSGVO. In diesem Zusammenhang empfiehlt der Ausschuss, in Abschnitt 2.4.2 klarzustellen, dass das EuroPriSe-Zertifizierungsprogramm selbst kein Übermittlungsinstrument im Sinne von Artikel 46 Absatz 2 Buchstabe f der DSGVO darstellt, da es keine geeigneten Garantien im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen gemäß den in Artikel 46 Absatz 2 Buchstabe f genannten Bedingungen bietet. Darüber hinaus empfiehlt der Ausschuss, die Pflicht des Zertifizierungsantragstellers aufzunehmen, den Verantwortlichen darüber zu informieren, dass das EuroPriSe-Zertifizierungsprogramm selbst kein Übermittlungsinstrument nach Artikel 46 Absatz 2 Buchstabe f der DSGVO ist.

22. Des Weiteren empfiehlt der Ausschuss, in Abschnitt 2.4.2 klarzustellen, dass diese spezifischen Anforderungen nur gelten, wenn der Zertifizierungsantragsteller (als Auftragsverarbeiter) personenbezogene Daten an einen Datenempfänger in einem Drittland übermittelt. Außerdem sollte eine Anforderung festgelegt werden, dass Zertifizierungsantragsteller ihre Wahl eines bestimmten Übermittlungsinstruments gemäß Kapitel V der DSGVO begründen und dokumentieren müssen.

23. Abschnitt 2.4.2.1 enthält allgemeine Anforderungen an die Übermittlungsinstrumente im Sinne von Kapitel V der DSGVO.[8] Nach Ansicht des Ausschusses sind solche allgemeinen Anforderungen nicht überprüfbar und können zu Inkonsistenzen bei der Anwendung des EuroPriSe-Zertifizierungsprogramms führen. Während es „Use Cases“ als Beispiele für die Anwendung des EuroPriSe-Zertifizierungsprogramms gibt, stellt der Ausschuss fest, dass solche „Use Cases“ und „Orientierungshilfen“ laut EuroPriSe nicht zu den normativen Kriterien gehören. Daher enthält diese Stellungnahme keine Schlussfolgerungen zur korrekten Anwendung der DSGVO gemäß den in Abschnitt 2.4.2 genannten „Use Cases“.

24. Da die Use Cases ergänzende Maßnahmen betreffen, empfiehlt der Ausschuss daher, weitere Einzelheiten für die Bewertung der Einhaltung der in Kapitel V festgelegten Pflichten des Datenexporteurs aufzunehmen. Insbesondere sollte in Bezug auf die Umsetzung ergänzender

[7] Die Beispiele können den „Use Cases“ in Abschnitt 2.4.2.1 ähneln.

[8] *„Hier MUSS im Einzelfall und gegebenenfalls in Zusammenarbeit mit dem Empfänger personenbezogener Daten im Drittland geprüft (und dokumentiert) werden, ob das Recht oder die Praxis des Drittlandes die Wirksamkeit der in den Übermittlungsinstrumenten nach Artikel 46 DSGVO enthaltenen angemessenen Garantien beeinträchtigt. Ist dies der Fall, MUSS der Auftragsverarbeiter ergänzende Maßnahmen treffen (und dokumentieren), um diese Schutzlücken zu schließen und das Schutzniveau auf das vom EU-Recht geforderte Niveau zu bringen. In Betracht kommen insoweit technische Maßnahmen, organisatorische Maßnahmen und zusätzliche vertragliche Maßnahmen, wobei es im Einzelfall erforderlich sein kann, verschiedene dieser Maßnahmen zu kombinieren.“*

Maßnahmen auf die Empfehlungen des EDSA zu Maßnahmen zur Ergänzung von Übermittlungstools verwiesen werden.[9]

25. Schließlich stellt der Ausschuss fest, dass in Abschnitt 2.4.2.1 Anforderungen in Bezug auf Artikel 49 der DSGVO festgelegt sind. In diesem Zusammenhang empfiehlt der Ausschuss, die Anforderung an den Antragsteller aufzunehmen, der Zertifizierungsstelle spezifische Informationen darüber vorzulegen, in welchen Fällen und unter welchen Bedingungen sich der Antragsteller auf die Ausnahme nach Artikel 49 der DSGVO berufen würde.

2.6 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

26. In Abschnitt 2.5.3 heißt es, dass diese Anforderung keine Anwendung auf Verarbeitungsvorgänge von Auftragsverarbeitern findet, die von deren Auftraggebern (Verantwortlichen) zu *vielen* verschiedenen Zwecken in Anspruch genommen werden. Der Begriff „viele" ist zu offen, um von einer Zertifizierungsstelle zur Überprüfung der Konformität verwendet zu werden. Der Ausschuss empfiehlt daher, genauer anzugeben, wann diese Anforderung anwendbar ist und wann nicht, indem beispielsweise die Anzahl der Zwecke quantifiziert wird, ab der die Anwendung dieser Anforderung unmöglich wird (z. B.: „zu drei oder mehr Zwecken").

27. Gemäß Unterabschnitt 2.5.3.1 ist der Verantwortliche verpflichtet, ein Merkblatt zu verwenden, das Informationen zu relevanten Datenschutzaspekten enthält. Unter Nummer 2 heißt es, dass das Merkblatt Informationen zur Benennung möglicher Rechtsgrundlagen enthalten muss, auf die sich der Verantwortliche gegebenenfalls stützen kann. Der Ausschuss empfiehlt, diesen Punkt aus dem Kriterienkatalog zu streichen, da er in die Verantwortung des Verantwortlichen eingreift, die geeignete Rechtsgrundlage zu bestimmen und sicherzustellen, dass alle Bedingungen für diese Rechtsgrundlage erfüllt sind. Dies gilt unbeschadet der Pflicht des Auftragsverarbeiters gemäß Artikel 28 Absatz 3 DSGVO, den Verantwortlichen unverzüglich zu unterrichten, wenn eine Anweisung seiner Ansicht nach gegen diese Verordnung oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

28. Unterabschnitt 2.5.3.1 enthält die Pflicht des Auftragsverarbeiters, die Unterstützungsleistungen für die Beantwortung von Anträgen auf Wahrnehmung von Rechten der betroffenen Personen im Merkblatt zu benennen. Aus Gründen der Klarstellung und zur Angleichung an Artikel 28 Absatz 3 Buchstabe e der DSGVO empfiehlt der Ausschuss, diesen Satz wie folgt zu ändern: „Benennung der Dienste des Auftragsverarbeiters zur Unterstützung des Verantwortlichen bei der Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Personen …"

29. Unterabschnitt 2.5.3.2 enthält eine Pflicht zur Erstellung eines Musterformulars für eine Einwilligungserklärung oder zur Befreiung von der Geheimhaltung, wenn die Einwilligung die einzige Rechtsgrundlage für die Nutzung der zu zertifizierenden Verarbeitungsvorgänge ist. Dieselbe Pflicht gilt, wenn die zu zertifizierenden Verarbeitungsvorgänge die Übermittlung

[9] Siehe EDSA Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de.

personenbezogener Daten in Drittländer umfassen und die Einwilligung als Legitimation für diese Übermittlung dient. Obwohl ein solches Muster für einige Verantwortliche, insbesondere kleine und mittlere Unternehmen, hilfreich sein könnte, empfiehlt der Ausschuss, diese spezifische Anforderung zu streichen, da das Einholen der Einwilligung nicht in die Zuständigkeit des Auftragsverarbeiters, sondern des Verantwortlichen fällt und daher nicht als Kriterium für den Auftragsverarbeiter dienen kann, um die Einhaltung der DSGVO nachzuweisen, was letztlich der Zweck der DSGVO-Zertifizierung ist.

2.7 Technische und organisatorische Maßnahmen

30. Der Ausschuss stellt fest, dass beim Verweis auf die Risikoanalyse in den Abschnitten 3.1.1.1 und 3.1.5.1 nicht ganz klar ist, auf welche Risiken eingegangen wird (z. B. die der betroffenen Personen). Der Ausschuss empfiehlt daher, zu präzisieren, dass die Risiken für die Rechte und Freiheiten der betroffenen Personen angegangen werden. Darüber hinaus wird in dem Dokument in den Leitlinien zu mehreren Anforderungen auf eine Klassifizierung der Risiken Bezug genommen, wobei diese Klassifizierung jedoch in keiner der Anforderungen näher erläutert wird. Aus Gründen der Klarheit empfiehlt der Ausschuss daher, in den Abschnitten 3.1.1.1 und 3.1.5.1 einen Verweis auf die Klassifizierung der Risiken in Bezug auf die verschiedenen Arten von Risiken für die betroffenen Personen aufzunehmen.

31. Was Abschnitt 3.1.1.3 betrifft, so erkennt der Ausschuss an, dass EuroPriSe die Bedeutung der Einrichtung von Zugriffskontrollmechanismen bei der Interaktion mit webbasierten Diensten hervorheben möchte. Die derzeitige Formulierung „*dies ist insbesondere bei der Interaktion mit webbasierten Diensten sichergestellt*“ könnte jedoch darauf hindeuten, dass diese Kontrollmechanismen in allen anderen Fällen nicht so wichtig oder obligatorisch sind. Der Ausschuss empfiehlt daher, diesen Teilsatz entweder zu streichen oder ihn entsprechend umzuformulieren.

32. Die Anforderung in Abschnitt 3.1.2.1 sieht vor, dass der Auftragsverarbeiter nachweisen muss, dass „die Speicherdauer der Protokolldaten konfiguriert werden kann bzw. so konfiguriert ist, dass das bestehende bzw. ein angenommenes Risiko berücksichtigt ist“. Der Ausschuss stellt jedoch fest, dass die Speicherdauer gemäß Artikel 5 Absatz 1 Buchstabe c der DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der verarbeiteten Daten notwendige Maß beschränkt sein muss. Der Ausschuss empfiehlt daher, einen Verweis aufzunehmen, um nicht nur die Risiken, sondern auch den Zweck der Verarbeitung zu berücksichtigen.

33. Der Ausschuss stellt ferner fest, dass die Abschnitte 3.1.2.1 und 3.1.2.2 dieselbe „Anforderung in Kürze“ aufweisen, obwohl sich die Anforderungen „im Detail“ auf verschiedene Aspekte beziehen. Aus Gründen der Klarheit empfiehlt der Ausschuss, diese Unterscheidung auch in den „*Anforderungen in Kürze*“ zu treffen.

2.8 Rechte der betroffenen Personen

34. Infolge der Empfehlungen des Ausschusses zu den Abschnitten 2.2.1 und 2.2.2 in Bezug auf Vertragsklauseln über die Unterstützung, die der Auftragsverarbeiter dem Verantwortlichen zu leisten hat, um die Wahrnehmung der Rechte der betroffenen Personen zu erleichtern, empfiehlt der Ausschuss außerdem, diese relevanten Unterschiede in den Vertragsklauseln in Kapitel IV des EuroPriSe-Programms aufzunehmen und zu berücksichtigen. Ferner empfiehlt der Ausschuss, denselben Ansatz in den Anforderungen (4.1-4.8) für alle Rechte der

betroffenen Personen (4.2-4.8) zu ändern, die im Allgemeinen als Pflicht des Auftragsverarbeiters zum Ergreifen „technischer und organisatorischer Maßnahmen“ ohne weitere Spezifizierung dieser Maßnahmen formuliert werden. Diese Änderungen sollten die erheblichen Unterschiede zwischen den verschiedenen Rechten der betroffenen Personen widerspiegeln, da einige dieser Rechte immer anwendbar sind (a), einige von einer weiteren rechtlichen Bewertung des Falls abhängen (b) und einige von einer inhaltlichen Beurteilung abhängen (c). Folglich müssen die Zuständigkeiten des Verantwortlichen und des Auftragsverarbeiters in Bezug auf die Buchstaben b und c in den Vertragsklauseln präzisiert werden.

35. Die Anforderung in Abschnitt 4.1 ist unspezifisch im Hinblick darauf, welche Informationen für die Informationspflichten des Verantwortlichen gegenüber den betroffenen Personen relevant sind und somit vom Auftragsverarbeiter zur Verfügung gestellt werden müssen. Der Ausschuss empfiehlt eine weitere Spezifizierung unter Berücksichtigung der Elemente, die in den Artikeln 13 und 14 der DSGVO angeführt sind.

36. In Bezug auf die Anforderung in Abschnitt 4.8 ist der Ausschuss der Auffassung, dass der Verantwortliche für die Entscheidung über die Zwecke und Mittel der Verarbeitung zuständig ist, sodass dies nicht in den Zuständigkeitsbereich eines Auftragsverarbeiters zu fallen scheint. Daher empfiehlt der Ausschuss, genauer festzulegen, welche Art von Unterstützung der Auftragsverarbeiter in Bezug auf die Wahrnehmung des Rechts, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, leisten sollte.

3 SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

37. Abschließend ist der EDSA der Auffassung, dass die EuroPriSe-Zertifizierungskriterien zu einer uneinheitlichen Anwendung der DSGVO führen können und die folgenden Änderungen vorzunehmen sind, um die Anforderungen nach Artikel 42 der DSGVO im Lichte der Leitlinien und des Addendums zu erfüllen:

38. In Bezug auf den „Anwendungsbereich des Programms“ empfiehlt der Ausschuss:

    1) Abschnitt 1 der Kriterien gemäß Artikel 42 Absatz 5 der DSGVO zu streichen und in das Antragsverfahren aufzunehmen,

    2) in der Einleitung klarzustellen, dass Unterauftragsverarbeiter nicht im Rahmen des EuroPriSe-Zertifizierungsprogramms zertifiziert werden können.

39. In Bezug auf die „Antragsteller, die Artikel 3 Absatz 2 der DSGVO unterliegen“, empfiehlt der Ausschuss:

    1) in Abschnitt 2.1.3 daran zu erinnern, dass immer dann, wenn eine „Übermittlung“ im Sinne von Artikel 44 der DSGVO an einen Auftragsverarbeiter mit Sitz außerhalb der EU oder des EWR erfolgt, die in Kapitel V der DSGVO festgelegten Pflichten in vollem Umfang einzuhalten sind,

    2) in Abschnitt 2.1.3 klarzustellen, dass es sich bei dem vorliegenden Programm nicht um ein Programm im Sinne von Artikel 46 Absatz 2 Buchstabe f der DSGVO handelt,

3) in Abschnitt 2.1.3 zu präzisieren, dass der Antragsteller nicht berechtigt ist, die Zertifizierung in einer Weise zu nutzen, die den Eindruck erwecken könnte, dass es sich bei der Zertifizierung selbst um ein Übermittlungsinstrument nach Artikel 46 Absatz 2 Buchstabe f der DSGVO handelt.

40. In Bezug auf das „Verhältnis des Verantwortlichen zum Auftragsverarbeiter" empfiehlt der Ausschuss:

1) den Wortlaut der Anforderung in Abschnitt 2.2.1 so anzupassen, dass klar daraus hervorgeht, dass die Anforderung in Abschnitt 2.2.1 nicht anwendbar ist, wenn andere Rechtsinstrumente vorhanden sind,

2) Sätze in Abschnitt 2.2.1 in Bezug auf „fehlende praktische Relevanz" zu streichen,

3) die Anforderung 2.2.1 dahin gehend zu ändern, dass berücksichtigt wird, inwieweit der Verantwortliche tatsächlich von der Unterstützung des Auftragsverarbeiters in Bezug auf die Rechte der betroffenen Personen abhängig ist,

4) in Abschnitt 2.2.2 (Punkt 8 der Anforderung im Detail) eine erschöpfende Liste der Dokumente zu erstellen, die von der Zertifizierungsstelle zu prüfen sind, um zu beurteilen, ob dieses Kriterium erfüllt wird oder nicht. Darüber hinaus sollte in diesem Kriterium klargestellt werden, dass diese Informationen der Zertifizierungsstelle vorzulegen sind,

5) in Abschnitt 2.3.2 (Nummer 1a der Anforderung im Detail) aufzunehmen, dass die Angaben zur Dauer der Verarbeitung im Einklang mit den einschlägigen Bestimmungen des Auftragsverarbeitungsvertrags, der zwischen dem Verantwortlichen und dem Auftragsverarbeiter geschlossen wurde, stehen müssen.

41. In Bezug auf die „gesetzlichen Geheimhaltungspflichten, Berufsgeheimnisse und besonderen Amtsgeheimnisse, die nicht auf gesetzlichen Vorschriften beruhen" empfiehlt der Ausschuss:

1) eine Erläuterung des Begriffs „mehrheitlich von Verantwortlichen in Anspruch genommen" in Abschnitt 2.4.1 aufzunehmen.

42. In Bezug auf die „Übermittlung personenbezogener Daten an Drittländer" empfiehlt der Ausschuss:

1) in Abschnitt 2.4.2 daran zu erinnern, dass das EuroPriSe-Zertifizierungsprogramm selbst keine Zertifizierung gemäß Artikel 46 Absatz 2 Buchstabe f der DSGVO für die internationale Übermittlung personenbezogener Daten darstellt und daher keine geeigneten Garantien im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen gemäß den in Artikel 46 Absatz 2 Buchstabe f genannten Bedingungen bietet,

2) die Pflicht des Zertifizierungsantragstellers aufzunehmen, den Verantwortlichen darüber zu informieren, dass das EuroPriSe-Zertifizierungsprogramm selbst kein Übertragungsinstrument gemäß Artikel 46 Absatz 2 Buchstabe f der DSGVO ist,

3) in Abschnitt 2.4.2 klarzustellen, dass diese Anforderungen nur gelten, wenn der Zertifizierungsantragsteller (als Auftragsverarbeiter) personenbezogene Daten an einen Datenempfänger in einem Drittland übermittelt. Außerdem sollte eine Anforderung festgelegt werden, dass Zertifizierungsantragsteller ihre Wahl eines

bestimmten Übermittlungsinstruments gemäß Kapitel V der DSGVO begründen und dokumentieren müssen,

4) weitere Einzelheiten für die Bewertung der Einhaltung der in Kapitel V genannten Pflichten des Datenexporteurs aufzunehmen. Insbesondere sollte in Bezug auf die Umsetzung ergänzender Maßnahmen auf die Empfehlungen des EDSA zu Maßnahmen zur Ergänzung von Übermittlungstools verwiesen werden,

5) in Abschnitt 2.4.2 die Anforderung aufzunehmen, dass der Zertifizierungsantragsteller der Zertifizierungsstelle spezifische Informationen darüber vorlegen muss, in welchen Fällen und unter welchen Bedingungen er sich auf die Ausnahme nach Artikel 49 der DSGVO berufen würde.

43. In Bezug auf Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen empfiehlt der Ausschuss:

1) genauer anzugeben, wann die Anforderung von Abschnitt 2.5.3 anwendbar ist,

2) aus dem Kriterienkatalog in Abschnitt 2.5.3.1 unter Nummer 2 den Teil zu streichen, in dem es heißt, dass das Merkblatt Informationen zur Benennung möglicher Rechtsgrundlagen enthalten muss, auf die sich der Verantwortliche stützen kann,

3) in Unterabschnitt 2.5.3.2 die Pflicht zur Erstellung eines Musterformulars für eine Einwilligungserklärung oder zur Befreiung von der Geheimhaltung zu streichen, wenn die Einwilligung die einzige Rechtsgrundlage für die Nutzung der zu zertifizierenden Verarbeitungsvorgänge ist.

44. In Bezug auf „technische und organisatorische Maßnahmen“ empfiehlt der Ausschuss:

1) in den Abschnitten 3.1.1.1 und 3.1.5.1 zu präzisieren, dass die Risiken für die Rechte und Freiheiten der betroffenen Personen angegangen werden,

2) in den Abschnitten 3.1.1.1 und 3.1.5.1 einen Verweis auf die Klassifizierung der Risiken in Bezug auf die verschiedenen Arten von Risiken für die betroffenen Personen aufzunehmen.

45. In Bezug auf die Rechte der betroffenen Personen empfiehlt der Ausschuss:

1) diese relevanten Unterschiede in Bezug auf die Unterstützung des Auftragsverarbeiters (siehe Empfehlungen zu den Abschnitten 2.2.1 und 2.2.2) in den Vertragsklauseln in Kapitel IV des EuroPriSe-Programms aufzunehmen und zu berücksichtigen,

2) denselben Ansatz in den Anforderungen (4.1-4.8) für alle Rechte der betroffenen Personen (4.2-4.8) zu ändern, die im Allgemeinen als Pflicht des Auftragsverarbeiters zum Ergreifen „technischer und organisatorischer Maßnahmen“ ohne weitere Spezifizierung dieser Maßnahmen formuliert werden,

3) die Anforderung 4.1 (Recht auf Information) unter Berücksichtigung der in den Artikeln 13 und 14 der DSGVO angeführten Elemente weiter zu spezifizieren,

4) die Art der Unterstützung, die der Auftragsverarbeiter leisten sollte, in Anforderung 4.8 genauer festzulegen.

4 ABSCHLIEßENDE BEMERKUNGEN

46. Diese Stellungnahme ist an die deutsche Aufsichtsbehörde (aus NRW) gerichtet und wird gemäß Artikel 64 Absatz 5 Buchstabe b der DSGVO veröffentlicht.

47. Gemäß Artikel 64 Absätze 7 und 8 der DSGVO hat die deutsche Aufsichtsbehörde (aus NRW) dem Vorsitz binnen zwei Wochen nach Eingang der Stellungnahme auf elektronischem Wege mitzuteilen, ob sie ihren Beschlussentwurf beibehalten oder ändern wird. Innerhalb derselben Frist übermittelt sie den geänderten Beschlussentwurf oder gibt, wenn sie nicht beabsichtigt der Stellungnahme des EDSA zu folgen, die maßgeblichen Gründe an, aus denen sie nicht beabsichtigt, dieser Stellungnahme ganz oder teilweise zu folgen.

48. Der EDSA weist darauf hin, dass die deutsche Aufsichtsbehörde (aus NRW) gemäß Artikel 43 Absatz 6 der 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 der DSGVO übermitteln muss.

Für den Europäischen Datenschutzausschuss
Die Vorsitzende

(Andrea Jelinek)