Stellungnahme des EDSA nach Artikel 64 DSGVO

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

Translations proofread by EDPB Members.
This language version has not yet been proofread.

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 der Geschäftsordnung des Europäischen Datenschutzausschusses

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 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 der DSGVO) oder – im Falle eines Europäischen Datenschutzsiegels – der Genehmigung durch den EDSA (Artikel 42 Absatz 5 und Artikel 70 Absatz 1 Buchstabe o der DSGVO) bedürfen.

(3) Wenn eine Aufsichtsbehörde (im Folgenden „Aufsichtsbehörde“) beabsichtigt, 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 abzugeben zum Entwurf eines Beschlusses der Aufsichtsbehörde zur Genehmigung der Zertifizierungskriterien.

[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.

(4) Diese 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 auf 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 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, die Einhaltung der DSGVO nachzuweisen; 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) Deshalb sollten Zertifizierungen Organisationen 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 Verfahrensverantwortlichen, Zertifizierungsmechanismen auszuarbeiten, die praktikable und potenziell kosteneffektive Instrumente zur Gewährleistung einer größeren DSGVO-Konformität darstellen und, indem sie für mehr Transparenz sorgen, das Recht der betroffenen Personen auf Schutz ihrer Privatsphäre und auf Datenschutz stärken.

(10) Der EDSA erinnert daran, dass Zertifizierungen Instrumente einer freiwilligen Selbstkontrolle sind und dass die Einhaltung eines Zertifizierungsverfahrens weder eine Reduzierung der Verantwortung der Verantwortlichen und der Auftragsverarbeiter für die Einhaltung der DSGVO bewirkt, noch die Aufsichtsbehörden an der Wahrnehmung ihrer sich aus der DSGVO und den einschlägigen nationalen Gesetzen ergebenden Aufgaben und Befugnisse hindert.

(11) Die Stellungnahme des EDSA ist gemäß Artikel 64 Absatz 1 Buchstabe c der 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.

(12) Der Schwerpunkt der Stellungnahme des EDSA liegt auf den Zertifizierungskriterien. Sollte der EDSA abstrakte Informationen über die Bewertungsmethoden anfordern, um die Überprüfbarkeit der im Entwurf vorgesehenen Zertifizierungskriterien im Zusammenhang mit seiner diesbezüglichen Stellungnahme gründlich bewerten zu können, so bedeutet dies nicht, dass Letztere eine Art Genehmigung der betreffenden Bewertungsmethoden beinhaltet –

HAT FOLGENDE STELLUNGNAHME ERLASSEN:

1 ZUSAMMENFASSUNG DES SACHVERHALTS

1. Der „Kriterienkatalog für die Zertifizierung von IT-gestützter Verarbeitung personenbezogener Daten gemäß Artikel 42 DSGVO (‚DSGVO – information privacy standard')" (im Folgenden „Entwurf der Zertifizierungskriterien" oder „Zertifizierungskriterien") wurde von der datenschutz cert GmbH (im Folgenden „Datenschutz cert"), einer juristischen Person deutschen Rechts, gemäß Artikel 42 Absatz 5 der DSGVO verfasst und dem Landesbeauftragten für Datenschutz Bremen vorgelegt, welcher die zuständige deutsche Aufsichtsbehörde in Bremen ist (im Folgenden „deutsche Aufsichtsbehörde (Bremen)").

2. Am 9. Oktober 2024 hat die deutsche Aufsichtsbehörde (Bremen) ihren Entwurf des Beschlusses zur Billigung der Zertifizierungskriterien der Datenschutz cert, den Entwurf der Kriterien für ein nationales Zertifizierungsverfahren, dem EDSA vorgelegt und den EDSA um eine Stellungnahme gemäß Artikel 64 Absatz 1 Buchstabe c der DSGVO ersucht. Der Beschluss über die Vollständigkeit des Dossiers erging am 12. November 2024.

3. Da die vorliegende Zertifizierung keine Zertifizierung gemäß Artikel 46 Absatz 2 Buchstabe f der DSGVO für die Übermittlung personenbezogener Daten ins Ausland ist, enthält sie keine geeigneten Garantien im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen, so wie diese in Artikel 46 Absatz 2 Buchstabe f vorgesehen sind. Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation ist nämlich nur zulässig, wenn die Bestimmungen von Kapitel V DSGVO eingehalten werden.

2 BEWERTUNG

4. Der Ausschuss hat seine Bewertung gemäß der in Anhang 2 der Leitlinien (im Folgenden „Anhang") und dem dazugehörigen Addendum vorgesehenen Gliederung vorgenommen. Soweit diese Stellungnahme keine Anmerkungen zu einem bestimmten Abschnitt der Entwurfsfassung der Zertifizierungskriterien enthält, ist davon auszugehen, dass der Ausschuss dazu nichts anzumerken hat und die deutsche Aufsichtsbehörde (Bremen) um keine weiteren Maßnahmen ersucht.

2.1 ALLGEMEINE BEMERKUNGEN

5. Nach Ansicht des Ausschusses wird der nationale Anwendungsbereich des Zertifizierungsverfahrens nicht hinreichend deutlich. Diese Stellungnahme ist als Voraussetzung für den Verwaltungsakt, mit dem die deutsche Aufsichtsbehörde (Bremen) die Billigung erteilt und der nur einen nationalen Anwendungsbereich haben kann, an die deutsche Aufsichtsbehörde (Bremen) gerichtet; dennoch wird in dem Verfahrensdokument mehrfach der Begriff „mitgliedstaatliches Recht" verwendet, was den Eindruck erwecken kann, dass das Zertifizierungsverfahren einen unionsweiten Anwendungsbereich im Sinne von Artikel 42 Absatz 5 Satz 2 der DSGVO hätte. Im Hinblick darauf empfiehlt der Ausschuss der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dass in der Einleitung des Dokuments klargestellt wird, dass das Zertifizierungsverfahren nur national anwendbar ist. Darüber hinaus regt der Ausschuss an, dass die zuständige Aufsichtsbehörde vom Verfahrensverantwortlichen verlangt, den Begriff „mitgliedstaatliches Recht" durch „deutsches Datenschutzrecht" zu ersetzen.

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

6. Das Zertifizierungsverfahren gilt für Verantwortliche und Auftragsverarbeiter und für alle IT-gestützten Verarbeitungsvorgänge. Das Zertifizierungsverfahren sieht keine Kriterien für gemeinsame Verantwortlichkeit vor; für Verarbeitungsvorgänge, die unter gemeinsamer Verantwortlichkeit erfolgen, ist eine Zertifizierung nach diesem Zertifizierungsverfahren deshalb nicht möglich. Der EDSA empfiehlt der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dass im Abschnitt über den Anwendungsbereich klargestellt wird, dass Verarbeitungsvorgänge unter gemeinsamer Verantwortlichkeit davon ausgenommen sind.

7. In Abschnitt 4.7.1 enthält der Katalog Kriterien für Datenübermittlungen an Drittländer. Der EDSA merkt an, dass diese Kriterien in den Katalog aufgenommen sind, um sicherzustellen, dass zertifizierte Verarbeitungsvorgänge auch dann, wenn sie mit Datenübermittlungen an Drittländer verbunden sind, DSGVO-konform sind. Der EDSA empfiehlt der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dass im Abschnitt über den Anwendungsbereich des Zertifizierungsverfahrens klargestellt wird, dass die Zertifizierung kein Instrument für die Übermittlung gemäß Artikel 46 Absatz 2 Buchstabe f der DSGVO ist.

2.3 RECHTMÄßIGKEIT DER VERARBEITUNG

2.3.1 RECHTSGRUNDLAGE – EINWILLIGUNG

8. In Bezug auf die Einwilligung (4.1.4 (P 1.4)) heißt es in dem Verfahrensdokument, dass die Einwilligung nur dann als Rechtsgrundlage verwendet werden kann, wenn, falls die Einwilligung widerrufen werden sollte, der Beendigung der Verarbeitung nichts entgegensteht. Der EDSA regt an, dass die zuständige Aufsichtsbehörde vom Verfahrensverantwortlichen verlangt, in diesen Absatz die in Artikel 17 Absatz 3 der DSGVO genannten Ausnahmen aufzunehmen, um für Fälle, in denen nach der DSGVO im Fall des Widerrufs keine sofortige Löschung erforderlich ist, die auf die Einwilligung gestützte Datenverarbeitung zu gestatten. In diesem Zusammenhang regt der EDSA an, dass die zuständige Aufsichtsbehörde vom Verfahrensverantwortlichen verlangt, den Satz klarer zu formulieren, indem doppelte Verneinungen oder doppelte Wenn-Klauseln vermieden werden.

9. In Bezug auf von Kindern erteilte Einwilligungen regt der EDSA an, dass die zuständige Aufsichtsbehörde vom Verfahrensverantwortlichen verlangt, in die Kriterien eine Verweisung auf den Verbindlichen Beschluss 2/2023 der EDSA zu TikTok aufzunehmen.

2.3.2 VERARBEITUNG BESONDERER KATEGORIEN PERSONENBEZOGENER DATEN

10. In Bezug auf die Verarbeitung besonderer Kategorien personenbezogener Daten sind in Abschnitt 4.1.8 (P 1.8) für Verantwortliche und Auftragsverarbeiter dieselben Anforderungen vorgesehen; in einer Anmerkung wird erklärt, dass für den Auftragsverarbeiter die

Verpflichtung besteht, Verfahren zu haben, die den Kunden (in seiner Eigenschaft als Verantwortlicher) in Bezug auf dessen Pflichten unterstützen. Der EDSA empfiehlt der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, Beispiele für die spezifischen Verpflichtungen der Auftragsverarbeiter in Bezug auf die verschiedenen in diesem Abschnitt aufgeführten Kriterien aufzuführen sowie eine Verweisung auf die Kriterien aus Abschnitt 4.4.1 (P 4.1) (Vertrag über die in Auftrag gegebene Verarbeitung personenbezogener Daten) aufzunehmen. Der Auftragsverarbeiter muss sich zumindest der Kategorien der verarbeiteten Daten bewusst sein.

2.4 GRUNDSÄTZE GEMÄß ARTIKEL 5

2.4.1 ZWECKBINDUNG

11. In Kapitel 4.2.3 (P 2.3) des Verfahrensdokuments sind die Anforderungen in Bezug auf den Zweckbindungsgrundsatz festgelegt. Unter Bezugnahme auf Artikel 6 Absatz 4 der DSGVO werden in der Anforderung Verarbeitungsvorgänge untersagt, die zu Zwecken erfolgen, die mit den Zwecken, zu denen die Daten ursprünglich erhoben wurden, nicht vereinbar sind. Die in Artikel 6 Absatz 4 der DSGVO vorgesehenen Bestimmungen für die Vereinbarkeitsprüfung sind nicht in vollem Umfang aufgenommen. Der EDSA empfiehlt der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dass die detaillierten Anforderungen an die Vereinbarkeitsprüfung in das Verfahrensdokument aufgenommen werden.

12. Der EDSA merkt an, dass bei den Kriterien im ersten Absatz dieses Abschnitts, der mit „*The client (as controller) shall ensure that the processes (PRC) or the applications (APPL) and all other relevant assets (PO, IT, INFRA, EXT) processing personal only permit …*“ („Der Kunde (als der Verantwortliche) stellt sicher, dass die Verfahren (PRC) oder die Anwendungen (APPL) und alle sonstigen relevanten Assets (PO, IT, INFRA, EXT), die personenbezogene verarbeiten, lediglich gestatten …“) beginnt, ein geringfügiger Fehler unterlaufen ist. Der EDSA regt an, dass die zuständige Aufsichtsbehörde vom Verfahrensverantwortlichen verlangt, zwischen „*personal*“ und „*only*“ das Wort „*data*“ [„Daten“] einzufügen.

2.4.2 RICHTIGKEIT DER DATEN

13. In Kapitel 4.2.5 (P 2.5) des Verfahrensdokuments sind die Anforderungen in Bezug auf den Richtigkeitsgrundsatz im Sinne von Artikel 5 Absatz 1 Buchstabe d der DSGVO festgelegt. Der EDSA empfiehlt der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dass spezifische Elemente in die Kriterien aufgenommen werden, anhand derer sich die Richtigkeit der Datenverarbeitung bestimmen und überprüfen lässt, so wie dies z. B. in Kapitel 3.6 der Leitlinien 4/2019 zu Artikel 25 DSGVO („Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“) vorgesehen ist.

2.4.3 VERARBEITUNG NACH TREU UND GLAUBEN

14. In Kapitel 4.2.7 (P 2.7) des Verfahrensdokuments sind die Anforderungen in Bezug auf den Grundsatz der Verarbeitung nach Treu und Glauben bestimmt. Der EDSA empfiehlt der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dass in die

Kriterien spezifische Elemente aufgenommen werden, anhand derer sich überprüfen lässt, dass die Verarbeitung personenbezogener Daten nach Treu und Glauben erfolgt, so wie dies z. B. in Kapitel 3.3 der Leitlinien 4/2019 zu Artikel 25 DSGVO – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen vorgesehen ist.

2.5 ALLGEMEINE VERPFLICHTUNGEN DER VERANTWORTLICHEN UND AUFTRAGSVERARBEITER

15. Das Zertifizierungsverfahren ist auf Verantwortliche und Auftragsverarbeiter anwendbar. Die DSGVO-Anforderungen an die Datenverarbeitung sind je nach der Rolle, die einem Unternehmen in Bezug auf die Verarbeitung zukommt, verschieden. Folglich wird in dem Zertifizierungsverfahren danach unterschieden, ob der Zertifizierungskunden als Verantwortlicher oder als Auftragsverarbeiter handelt, um die Kriterien der jeweiligen Rolle anzupassen. Da diese detaillierten Klarstellungen in der Regel in Fließtext erfolgen, besteht die Gefahr, dass sie übersehen werden könnten. Um diesem Risiko entgegenzuwirken, gibt es für jedes Kriterium einen gesonderten Absatz mit der Überschrift „*Applicability according to SOA*“ („Anwendbarkeit gemäß der Anwendbarkeitsklausel“), wo allgemein angegeben ist, ob das jeweilige Kriterium für den Verantwortlichen, den Auftragsverarbeiter oder für beide gilt. Der EDSA merkt an, dass das Zertifizierungsverfahren vorsieht, dass der Auftragsverarbeiter verpflichtet ist, dem Verantwortlichen in Bezug auf die Einhaltung der DSGVO Unterstützung und Hilfe zu leisten; deshalb gibt es eine Vielzahl von Kriterien, die als sowohl auf Verantwortliche als auch auf Auftragsverarbeiter anwendbar gekennzeichnet sind. Ob die Verpflichtungen des Auftragsverarbeiters in Bezug auf das jeweilige Kriterium die gleichen sind wie die des Verantwortlichen oder ob sie eher Unterstützungscharakter haben, geht dann erst aus der Prüfung des Wortlauts für das Kriterium hervor. Der EDSA regt an, dass die zuständige Aufsichtsbehörde vom Verfahrensverantwortlichen verlangt, zu ermöglichen, dass schneller feststellbar ist, welche Verpflichtungen der Zertifizierungskunde in seiner jeweiligen Rolle als Verantwortlicher oder Auftragsverarbeiter hat; beispielsweise, indem dem Verfahrensdokument ein Referenzbogen oder eine Referenzmatrix beigefügt wird oder indem im Abschnitt „*applicability according to SOA*“ („Anwendbarkeit gemäß der Anwendbarkeitsklausel“) zu jedem Kriterium ein Hinweis hinzugefügt wird, der klarstellt, ob der Kunde dieses im vollem Umfang einhalten muss oder ob er lediglich seine Rolle als Unterstützer erfüllen muss.

16. In Abschnitt 4.6.2 (P 6.2) geht es unter anderem um die Bestellung des Datenschutzbeauftragten (DSB). In Bezug auf die erforderlichen Qualifikationen eines DSB heißt es lediglich allgemein, dass für die Bestellung des DSB auf dessen „*qualifications and expertise in data protection matters*“ („Qualifikationen und Fachwissen in Datenschutzangelegenheiten“) abzustellen ist. In dieser Hinsicht empfiehlt der EDSA der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dass der Wortlaut auf die in Artikel 37 Absatz 5 der DSGVO genannten Anforderungen abgestimmt wird; dort heißt es, dass der Datenschutzbeauftragte „auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt [wird], das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt …“.

17. In Abschnitt 4.6.2 (P 6.2) wird zumindest einmal der Begriff „*data privacy officer*“ verwendet. Der EDSA empfiehlt der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu

verlangen, dass durchgehend der Begriff „*data protection officer*“ („Datenschutzbeauftragter“) im Sinne der Definition in der DSGVO verwendet wird.

18. Des Weiteren ist in Abschnitt 4.6.2 (P 6.2) bestimmt, dass der DSB „*shall report directly to the highest management level of the client (as controller or processor) and shall not receive instructions*“ („direkt der höchsten Leitungsebene des Kunden (als Verantwortlicher oder Auftragsverarbeiter) unterstellt ist und keine Anweisungen erhält“). Der EDSA empfiehlt der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dass der Wortlaut entsprechend Artikel 38 Absatz 3 der DSGVO dahin gehend präzisiert wird, dass der DSB „*… shall not receive any instructions regarding the exercise of his tasks*“ („… bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Wahrnehmung dieser Aufgaben erhält“) (womit die in Artikel 39 der DSGVO genannten Aufgaben gemeint sind).

19. Der EDSA merkt an, dass es in Abschnitt 4.6.4 (P 6.4) heißt: „*The processor's, or where applicable, the controller's representative, Record of processing activities (ROPA) shall contain at least the following information …*“ (Das vom Auftragsverarbeiter bzw. vom Vertreter des Verantwortlichen geführte Verzeichnis von Verarbeitungstätigkeiten (ROPA) enthält mindestens folgende Angaben …). Da sich dies auf Anforderungen an Auftragsverarbeiter bezieht, sollte dieser Satz dahin gehend geändert werden, dass er sich auf den „Vertreter des Auftragsverarbeiters“ bezieht. Der EDSA empfiehlt der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dies entsprechend zu ändern.

2.5.1 Verarbeitungsvorgänge (PO) und Prozesse (PRC) als Asset-Kategorien sowie Prozesse als (zusätzliche) Anforderungen in den Kriterien

20. In der Einleitung des Verfahrensdokuments werden verschiedene Asset-Kategorien eingeführt, die Teil des Evaluierungsgegenstands sind. Zusätzlich zu den Verarbeitungsvorgängen (PO), in denen personenbezogene Daten verarbeitet werden, werden im Verfahrensdokument Prozesse (PRC) definiert als Tätigkeiten, die Inputs verwenden, um ein für die Datenverarbeitung erforderliches beabsichtigtes Ergebnis zu erzielen. In mehreren Kriterien wird ausdrücklich auf diese Prozesse als (zusätzliche) Anforderungen an die Kriterienerfüllung Bezug genommen; in mehreren Fällen kommt zu den für Verantwortliche geltenden Kriterien die Anforderung hinzu, dass ein Prozess eingerichtet sein muss, der die kontinuierliche Erfüllung des Kriteriums sicherstellt. In Bezug auf Auftragsverarbeiter sieht das Verfahrensdokument wiederholt die Anforderung vor, dass sie Prozesse eingerichtet haben müssen, die die Verantwortlichen bei der Erfüllung ihrer für Verantwortliche geltenden rechtlichen Pflichten unterstützen. Deshalb enthalten die Kriterien eine Mischung aus rechtlichen und technischen Pflichten und Prozessen, die erforderlich sind, um sicherzustellen, dass diese Verpflichtungen kontinuierlich erfüllt werden, bzw. Prozesse, die der Auftragsverarbeiter eingerichtet haben muss, um den Verantwortlichen zu unterstützen. Der EDSA merkt an, dass diese unterschiedlichen Anforderungen nicht immer in derselben Reihenfolge aufgeführt sind, und er regt an, dass die zuständige Aufsichtsbehörde vom Verfahrensverantwortlichen verlangt, die Orientierung innerhalb des Verfahrensdokuments durch eine einheitlichere Reihenfolge zu erleichtern, die idealerweise mit der für den Verantwortlichen geltenden rechtlichen oder technischen Anforderung beginnen sollte, ergänzt um die Anforderung an die Prozesse, die erforderlich sind, um die kontinuierliche Erfüllung sicherzustellen, und mit abschließender Angabe der für den Auftragsverarbeiter geltenden Anforderungen.

2.5.2 Für Auftragsverarbeiter geltende Pflichten

21. In Abschnitt 4.4.1 (P 4.1) des Verfahrensdokuments sind die Anforderungen an den Vertrag gemäß Artikel 28 der DSGVO niedergelegt, wobei zwischen dem Vertrag zwischen Verantwortlichem und Auftragsverarbeiter sowie dem Vertrag zwischen Auftragsverarbeiter und Unterauftragsverarbeiter unterschieden wird. Im anschließenden Abschnitt (4.4.2 (P 4.2)) geht es um die Umsetzung der Maßnahmen im Vertrag zwischen Verantwortlichem und Auftragsverarbeiter. In dem Abschnitt fehlen Anforderungen an Maßnahmen im Vertrag zwischen Auftragsverarbeiter und Unterauftragsverarbeiter. Auch wenn diese Maßnahmen den Maßnahmen im Vertrag zwischen Verantwortlichem und Auftragsverarbeiter ähnlich sein mögen, empfiehlt der EDSA der zuständigen Aufsichtsbehörde dennoch, vom Verfahrensverantwortlichen zu verlangen, dass die Maßnahmen ausdrücklich angegeben werden.

2.6 RECHTE BETROFFENER PERSONEN

22. In Abschnitt 4.8 geht es um die Rechte betroffener Personen im Sinne von Kapitel III der DSGVO. Der EDSA merkt an, dass in diesem Abschnitt die möglichen Ausnahmen gemäß Artikel 23 der DSGVO, die unter bestimmten Voraussetzungen gewisse Beschränkungen dieser Rechte zulassen, nicht erwähnt sind. Vor diesem Hintergrund empfiehlt der EDSA der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dass Kriterien aufgestellt werden für die Prüfung, ob die im deutschen mitgliedstaatlichen Recht vorgesehenen Beschränkungen der Rechte betroffener Personen auf die Verarbeitungsvorgänge des Evaluierungsgegenstands anwendbar sind und damit in Einklang stehen.

23. Des Weiteren merkt der EDSA an, dass die in Artikel 12 der DSGVO vorgesehenen Modalitäten für die Rechte betroffener Personen im betreffenden Kapitel von Abschnitt 4.8 für jedes der Rechte betroffener Personen wiederholt werden. Auch wenn dies nicht dazu führt, dass die Kriterien unvollständig aufgeführt sind, kann es doch sein, dass die Lesbarkeit und insgesamt die Klarheit dadurch beeinträchtigt werden. Der EDSA regt deshalb an, dass die zuständige Aufsichtsbehörde vom Verfahrensverantwortlichen verlangt, die Modalitäten gemäß Artikel 12 der DSGVO am Anfang von Abschnitt 4.8 anzugeben, statt sie für jedes einzelne Recht betroffener Personen zu wiederholen.

24. Insoweit als in Abschnitt 4.8 die Kriterien aufgeführt sind, die Auftragsverarbeiter in Bezug auf die Rechte betroffener Personen erfüllen müssen, merkt der EDSA an, dass die Bestimmungen lediglich allgemeinen Charakter haben. Diese Kriterien sehen vor, dass „*the client (as processor) shall implement processes (PRC) to assist the controller in fulfilling this obligation …*“ (der Kunde (als Auftragsverarbeiter) Prozesse (PRC) implementiert, um den Verantwortlichen bei der Erfüllung dieser Verpflichtung zu unterstützen …). Es gibt jedoch keine spezifischen Bestimmungen, in denen im Einzelnen angegeben wird, auf welche Weise diese Unterstützungspflicht in Bezug auf jedes der einzelnen Rechte betroffener Personen implementiert werden könnte; dies lässt Bedenken im Hinblick auf die Überprüfbarkeit dieser Kriterien aufkommen. Der EDSA empfiehlt der zuständigen Aufsichtsbehörde deshalb, vom Verfahrensverantwortlichen zu verlangen, dass für jedes Recht betroffener Personen spezifischere Kriterien für die Unterstützungspflicht der Auftragsverarbeiter aufgenommen werden.

25. Im Zusammenhang mit dem Auskunftsrecht in Abschnitt 4.8.1 (P 8.1) wird unter anderem auf „*the origin of the data*“ („die Herkunft der Daten“) als Teil der zu machenden Angaben Bezug genommen. Der EDSA empfiehlt der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dass der Wortlaut an Artikel 15 Absatz 1 Buchstabe g der DSGVO angepasst wird, wo es heißt, dass „*any available information as to their source*“ [„alle verfügbaren Informationen über die Herkunft der Daten“] zu liefern sind.

26. In Abschnitt 4.8.1 (P 8.1) wird auch auf Artikel 12 Absatz 5 der DSGVO verwiesen. Es gibt jedoch keine Kriterien dafür, wann Anfragen betroffener Personen als „*manifestly unfounded or excessive*“ („offenkundig unbegründet oder exzessiv“) zu bewerten sind. Der EDSA empfiehlt der zuständigen Aufsichtsbehörde deshalb, vom Verfahrensverantwortlichen zu verlangen, dass Kriterien für eine solche Bewertung angegeben werden. In seinen „Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht“ (6.3.2) hat der EDSA einige Kriterien angegeben, die diesbezüglich in Betracht kommen könnten.

27. In Abschnitt 4.8.7 (P 8.7) des Verfahrensdokuments sind die Kriterien für das Widerspruchsrecht gemäß Artikel 21 der DSGVO aufgeführt. Dabei sind alle relevanten Aspekte berücksichtigt, wobei das Kriterium jedoch nicht der Gliederung in Artikel 21 folgt, was zu Verwirrung führen kann. Der EDSA empfiehlt der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, das Kriterium gemäß der Gliederung in Artikel 21 umzuformulieren.

28. In Abschnitt 4.8.8 (P 8.8) geht es um „*revocation of consent*“ („Widerruf der Einwilligung“). Unter anderem ist dort die Anforderung vorgesehen, dass der Widerruf der Einwilligung zur Beendigung der Datenverarbeitung führt, es sei denn, es gibt alternative Rechtsgrundlagen. Zur Vermeidung von Uneindeutigkeit empfiehlt der EDSA der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, in diesem Zusammenhang eine Bezugnahme auf Artikel 17 Absatz 1 Buchstabe b der DSGVO aufzunehmen.

29. In Abschnitt 4.3.1 (P 3.1) des Verfahrensdokuments sind die Kriterien für die Pflicht zur Information betroffener Personen festgelegt. Die Anforderungen gemäß den Artikeln 13 und 14 der DSGVO sind im selben Kapitel enthalten. Der EDSA regt an, dass die zuständige Aufsichtsbehörde vom Verfahrensverantwortlichen verlangt, diese Kriterien in verschiedene Kapitel zu untergliedern, um den Überblick zu erleichtern und die Lesbarkeit und Überprüfbarkeit zu verbessern.

30. Im Hinblick auf die Informationspflichten im Fall von nicht bei den betroffenen Personen erhobenen Daten (Artikel 14) weisen die Anforderungen auf die in Artikel 14 Absatz 5 vorgesehenen Ausnahmen von der Informationspflicht hin. Der EDSA regt an, dass die zuständige Aufsichtsbehörde vom Verfahrensverantwortlichen verlangt, Kriterien für die Überprüfung der Verhältnismäßigkeit des damit verbundenen Aufwands aufzustellen und zu definieren, wann die Mitteilung der Informationen an die betroffene Person möglich bzw. nicht möglich ist.

2.7 RISIKEN FÜR DIE RECHTE UND FREIHEITEN DER BETROFFENEN PERSONEN UND SCHUTZ GARANTIERENDE TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

31. Was die Umsetzung technischer und organisatorischer Maßnahmen (TOMs) durch den Auftragsverarbeiter angeht, enthält Abschnitt 4.5.1 (P 5.1) keine Angaben zu den vom Verantwortlichen erteilten Anweisungen sowie insbesondere zu Artikel 28 Absatz 3 Buchstabe c der DSGVO. Der Ausschuss merkt jedoch an, dass der „Vertrag zwischen Verantwortlichem und Auftragsverarbeiter" auch die Umsetzung risikobasierter TOMs durch einen Auftragsverarbeiter berührt. Vor diesem Hintergrund empfiehlt der EDSA der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dass in den vorgenannten Abschnitt 4.5.1 (P 5.1) eine Bezugnahme auf die Kriterien aus Abschnitt 4.4.1 (P 4.1) („Vertrag über die in Auftrag gegebene Verarbeitung personenbezogener Daten") aufgenommen wird.

32. In Abschnitt 4.5.1 (P 5.1) geht es um die Bestimmung geeigneter technischer und organisatorischer Maßnahmen. Laut diesem Abschnitt ist der erste Schritt eine Analyse der Datenverarbeitung im Ganzen, die sämtliche Assets umfasst. Dieser Abschnitt enthält allgemeine Bedingungen für die Durchführung einer solchen Analyse, jedoch keine weiteren Informationen über die Methodik. Der EDSA regt deshalb an, dass die zuständige Aufsichtsbehörde vom Verfahrensverantwortlichen verlangt, dass klargestellt wird, dass der Antragsteller anerkannte Methodiken der Risikoabschätzung anwendet.

33. In Abschnitt 4.5.5 (P 5.5), wird im ersten Aufzählungspunkt der Begriff „organization" („Organisation") verwendet, der sich ersichtlich auf den Kunden (den zu zertifizierenden Verantwortlichen oder Auftragsverarbeiter) bezieht. Zur Vermeidung von Missverständnissen und Sicherstellung einheitlicher Terminologie regt der EDSA an, dass die zuständige Aufsichtsbehörde vom Verfahrensverantwortlichen verlangt, in diesem Kontext den Begriff „*client*" („Kunde") anstelle des Begriffs „*organization*" („Organisation") zu verwenden.

34. Des Weiteren geht es in Abschnitt 4.6.5 (P 6.5) um die Anforderungen in Bezug auf die Erforderlichkeit der Durchführung einer Datenschutz-Folgenabschätzung (DSFA). Es gibt eine Bezugnahme auf die Listen im Sinne von Artikel 35 Absätze 4 und 5 der DSGVO, diese sind jedoch nicht im Einzelnen angegeben. Der EDSA empfiehlt daher der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dass klargestellt wird, dass nur die Listen der für den Verantwortlichen oder Auftragsverarbeiter zuständigen (deutschen) Aufsichtsbehörde zu berücksichtigen sind.

2.8 KRITERIEN FÜR DEN NACHWEIS DES VORHANDENSEINS GEEIGNETER GARANTIEN FÜR DIE ÜBERMITTLUNG PERSONENBEZOGENER DATEN

35. Im Zusammenhang mit Datenübermittlungen an Drittländer gemäß Abschnitt 4.7.1 (P 7.1) weist der EDSA darauf hin, dass laut seinen „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus

für personenbezogene Daten“ der erste Schritt für die Bewertung der Zulässigkeit derartiger Übermittlungen stets in der Aufzeichnung und Erfassung aller derartigen Datenübermittlungen besteht („Know your transfers“). Der EDSA empfiehlt der zuständigen Aufsichtsbehörde deshalb, vom Verfahrensverantwortlichen zu verlangen, dass diese Anforderung ausdrücklich aufgenommen wird. Sollte diese Anforderung bereits anderswo in den vorliegenden Kriterien geregelt sein, empfiehlt der EDSA der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dass ein Querverweis auf Abschnitt 4.7.1 (P 7.1) aufgenommen wird.

36. Des Weiteren merkt der EDSA an, dass gemäß Abschnitt 4.7.1 (P 7.1) sicherzustellen ist, dass Datenübermittlungen an Drittländer *„permitted“* („gestattet“) sind. Im Interesse größerer Klarheit regt der EDSA an, dass die zuständige Aufsichtsbehörde vom Verfahrensverantwortlichen verlangt, vorzugeben, dass Datenübermittlungen an Drittländer *„shall always be carried out in accordance with the provisions of Chapter V of the GDPR“* („stets gemäß den Bestimmungen in Kapitel V der DSGVO durchzuführen sind“).

37. Allgemein merkt der EDSA zu diesem Abschnitt an, dass der Abschnitt mehrere Artikel umfasst. Diese enthalten zwar sämtliche relevanten Aspekte, der Abschnitt ist jedoch nicht klar gegliedert. Der EDSA regt deshalb an, dass die zuständige Aufsichtsbehörde vom Verfahrensverantwortlichen verlangt, den Abschnitt neu zu gliedern oder zur Untergliederung Überschriften zwischen den verschiedenen Übermittlungsinstrumente einzufügen.

3 SCHLUSSFOLGERUNGEN / EMPFEHLUNGEN

Der EDSA gelangt zu folgenden Schlussfolgerungen und Empfehlungen:

38. In Bezug auf den „Anwendungsbereich des Zertifizierungsverfahrens und Evaluierungsgegenstand (Target of Evaluation, ToE)“ empfiehlt der Ausschuss, dass die deutsche Aufsichtsbehörde (Bremen) vom Verfahrensverantwortlichen Folgendes verlangt:

    1. Klarstellung in der Einleitung des Dokuments, dass das Zertifizierungsverfahren einen nationalen Anwendungsbereich hat;

    2. Klarstellung im Abschnitt „Anwendungsbereich“, dass Verarbeitungsvorgänge unter gemeinsamer Verantwortlichkeit ausgenommen sind;

    3. Klarstellung im Abschnitt „Anwendungsbereich“ des Verfahrensdokuments, dass die Zertifizierung kein Instrument für die Übermittlung gemäß Artikel 46 Absatz 2 Buchstabe f der DSGVO ist;

39. in Bezug auf die „Rechtmäßigkeit der Verarbeitung“ empfiehlt der Ausschuss, dass die deutsche Aufsichtsbehörde (Bremen) vom Verfahrensverantwortlichen Folgendes verlangt:

    1. Beispiele für die spezifischen Verpflichtungen der Auftragsverarbeiter in Bezug auf die verschiedenen in diesem Abschnitt aufgeführten Kriterien aufzuführen und eine Verweisung auf die Kriterien aus Abschnitt 4.4.1 (P 4.1) (Vertrag über die in Auftrag gegebene Verarbeitung personenbezogener Daten) aufzunehmen;

40. in Bezug auf die „Grundsätze des Artikels 5 der DSGVO“ empfiehlt der Ausschuss, dass die deutsche Aufsichtsbehörde (Bremen) vom Verfahrensverantwortlichen Folgendes verlangt:

1. Aufnahme der detaillierten Anforderungen an die Vereinbarkeitsprüfung gemäß Artikel 6 Absatz 4 der DSGVO;

2. Aufnahme spezifischer Elemente, anhand derer sich die Richtigkeit der Datenverarbeitung bestimmen und überprüfen lässt, in die Kriterien, so wie dies z. B. in Kapitel 3.6 der Leitlinien 4/2019 zu Artikel 25 DSGVO – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen vorgesehen ist;

3. Aufnahme spezifischer Elemente, anhand derer sich überprüfen lässt, dass die Verarbeitung nach Treu und Glauben erfolgt, in die Kriterien, so wie dies z. B. in Kapitel 3.3 der Leitlinien 4/2019 zu Artikel 25 DSGVO – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen vorgesehen ist;

41. in Bezug auf die „allgemeinen Verpflichtungen der Verantwortlichen und Auftragsverarbeiter" empfiehlt der Ausschuss, dass die deutsche Aufsichtsbehörde (Bremen) vom Verfahrensverantwortlichen Folgendes verlangt:

    1. Anpassung des Wortlauts an die in Artikel 37 Absatz 5 der DSGVO genannten Anforderungen, wo es heißt, dass der Datenschutzbeauftragte „auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt (wird), das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt …";

    2. einheitliche Verwendung des Begriffs „Datenschutzbeauftragter" entsprechend der Begriffsbestimmung in der DSGVO;

    3. klarere Formulierung, aus der hervorgeht, dass der DSB „*… shall not receive any instructions regarding the exercise of his tasks*" („… bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Wahrnehmung dieser Aufgaben erhält") (womit die in Artikel 39 der DSGVO genannten Aufgaben gemeint sind);

    4. Änderung des Satzes „*The processor's, or where applicable, the controller's representative, Record of processing activities (ROPA) shall contain at least the following information …*" (Das vom Auftragsverarbeiter bzw. vom Vertreter des Verantwortlichen geführte Verzeichnis von Verarbeitungstätigkeiten (ROPA) enthält mindestens folgende Angaben …), sodass er sich auf den „*processor's representative*" („Vertreter des Auftragsverarbeiters") bezieht;

    5. ausdrückliche Angabe der Maßnahmen im Vertrag zwischen Auftragsverarbeiter und Unterauftragsverarbeiter;

42. in Bezug auf die „Rechte betroffener Personen" empfiehlt der Ausschuss, dass die deutsche Aufsichtsbehörde (Bremen) vom Verfahrensverantwortlichen Folgendes verlangt:

    1. Aufstellung der Kriterien für die Prüfung, ob die Beschränkungen der Rechte betroffener Personen, die im deutschen mitgliedstaatlichen Recht vorgesehen sind, auf die Verarbeitungsvorgänge des Evaluierungsgegenstands anwendbar sind und damit in Einklang stehen;

    2. Aufnahme spezifischerer Kriterien für die Unterstützungspflicht der Auftragsverarbeiter in Bezug auf die einzelnen Rechte betroffener Personen;

3. Anpassung des Wortlauts, wo es heißt, dass Informationen über „*… any available information as to their source*“ („alle verfügbaren Informationen über die Herkunft der Daten“) zu liefern sind, an Artikel 15 Absatz 1 Buchstabe g der DSGVO;

4. Aufnahme der Kriterien für die Bewertung von Anträgen als „*manifestly unfounded or excessive*“ („offenkundig unbegründet oder exzessiv“);

5. Neugliederung des Abschnitts über das „Widerspruchsrecht“ gemäß der Gliederung in Artikel 21 der DSGVO;

6. Aufnahme einer Bezugnahme auf Artikel 17 Absatz 1 Buchstabe b der DSGVO im Zusammenhang mit dem Widerruf der Einwilligung;

43. In Bezug auf „*risks for the rights and freedoms of natural persons*“ („Risiken für die Rechte und Freiheiten betroffener Personen“) und „*technical and organisational measures guaranteeing protection*“ („Schutz garantierende technische und organisatorische Maßnahmen“) empfiehlt der Ausschuss, dass die deutsche Aufsichtsbehörde (Bremen) vom Verfahrensverantwortlichen Folgendes verlangt:

    1. Aufnahme einer Bezugnahme auf die Kriterien aus Abschnitt 4.4.1 (P 4.1) (Vertrag über die in Auftrag gegebene Verarbeitung personenbezogener Daten) im Abschnitt 4.5.1 (P 5.1). (Durchführung technischer und organisatorischer Maßnahmen (TOM) durch einen Auftragsverarbeiter);

    2. Klarstellung, dass, was die in Artikel 35 Absätze 4 und 5 der DSGVO vorgesehenen Listen angeht, nur die Listen der für den Verantwortlichen oder Auftragsverarbeiter zuständigen (deutschen) Aufsichtsbehörde zu berücksichtigen sind;

44. in Bezug auf die „*criteria for the purpose of demonstrating the existence of appropriate safeguards for transfer of personal data*“ („Kriterien für den Nachweis des Vorhandenseins geeigneter Garantien für die Übermittlung personenbezogener Daten“) empfiehlt der Ausschuss, dass die deutsche Aufsichtsbehörde (Bremen) vom Verfahrensverantwortlichen Folgendes verlangt:

    1. Aufnahme der Anforderung, dass der erste Schritt für die Bewertung der Zulässigkeit derartiger Übermittlungen stets in der Aufzeichnung und Erfassung aller derartigen Datenübermittlungen besteht („Know your transfers“). Sollte diese Anforderung bereits anderswo in den vorliegenden Kriterien geregelt sein, empfiehlt der EDSA der zuständigen Aufsichtsbehörde, vom Verfahrensverantwortlichen zu verlangen, dass ein Querverweis auf Abschnitt 4.7.1 (P 7.1) aufgenommen wird.

45. Abschließend erinnert der EDSA an die Leitlinien, nach denen die deutsche Aufsichtsbehörde (Bremen) im Falle von Abänderungen des „*Catalogue of Criteria for the Certification of IT-supported Processing of Personal Data pursuant to Art. 42 GDPR ('GDPR – information privacy standard')*“ („Kriterienkatalog für die Zertifizierung von IT-gestützter Verarbeitung personenbezogener Daten gemäß Artikel 42 DSGVO ('DSGVO – information privacy standard')“), die erhebliche Änderungen mit sich bringen[4], die abgeänderte Fassung gemäß Artikel 42 Absatz 5 und Artikel 43 Absatz 2 Buchstabe b der DSGVO dem EDSA vorlegen muss.

[4] Siehe Abschnitt 9 des Addendums zu den Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679, die „*Guidance on*

4 SCHLUSSBEMERKUNGEN

46. Diese Stellungnahme richtet sich an die deutsche Aufsichtsbehörde (Bremen) und wird gemäß Artikel 64 Absatz 5 Buchstabe b der DSGVO veröffentlicht.

47. Nach Artikel 64 Absätze 7 und 8 der DSGVO muss die deutsche Aufsichtsbehörde (Bremen) dem Vorsitz binnen zwei Wochen nach Eingang der Stellungnahme auf elektronischem Weg mitteilen, ob sie den Beschlussentwurf beibehalten oder ändern wird. Innerhalb derselben Frist übermittelt sie den geänderten Entwurf oder teilt unter Angabe der maßgeblichen Gründe mit, dass sie beabsichtigt, der Stellungnahme des Ausschusses insgesamt oder teilweise nicht zu folgen.

48. Gemäß Artikel 70 Absatz 1 Buchstabe y der DSGVO teilt die deutsche Aufsichtsbehörde (Bremen) dem EDSA den endgültigen Beschluss mit zwecks Aufnahme in das Register der Beschlüsse, die Gegenstand des Kohärenzverfahrens waren.

49. Der EDSA erinnert daran, dass die deutsche Aufsichtsbehörde (Bremen) gemäß Artikel 43 Absatz 6 der DSGVO die Zertifizierungskriterien der Datenschutz cert in leicht zugänglicher Form veröffentlichen und sie 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

Der Vorsitz
Anu Talus

certification criteria assessment“ [„Leitlinien für die Überprüfung und Bewertung von Zertifizierungskriterien“] bieten.