Stellungnahme 1/2022 zum Entwurf eines Beschlusses der luxemburgischen Aufsichtsbehörde in Bezug auf die Zertifizierungskriterien für GDPR-CARPA

Angenommen am 1. Februar 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. Im Einklang mit Artikel 42 Absatz 5 der DSGVO und den Leitlinien wurden von der luxemburgischen Aufsichtsbehörde die „Zertifizierungskriterien für GDPR-CARPA“ (im Folgenden „Entwurf der Zertifizierungskriterien“ oder „Zertifizierungskriterien“) ausgearbeitet.

2. Die luxemburgische Aufsichtsbehörde hat ihren Entwurf eines Beschlusses zur Genehmigung der Zertifizierungskriterien für GDPR-CARPA vorgelegt und den EDSA am 1. Oktober 2021 um eine Stellungnahme gemäß Artikel 64 Absatz 1 Buchstabe c der DSGVO ersucht. Der Beschluss über den Abschluss der Akte erging am 28. Oktober 2021.

   Die vorliegende Zertifizierung ist keine Zertifizierung gemäß Artikel 46 Absatz 2 Buchstabe f der DSGVO für internationale Übermittlungen personenbezogener Daten und bietet 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. 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 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 der luxemburgischen Aufsichtsbehörde auslässt, sollte das so verstanden werden, dass der Ausschuss keine Anmerkungen hat und die luxemburgische Aufsichtsbehörde nicht auffordert, weitere Maßnahmen zu ergreifen.

2.1 Allgemeine Bemerkungen

4. Der Ausschuss stellt fest, dass die im gesamten Dokument verwendeten Begriffe teilweise verwirrend sein können. Ein Beispiel für die mangelnde Konsistenz der Terminologie findet sich in Abschnitt I-13, wo auf „Betroffene“ Bezug genommen wird, was durch „betroffene Personen“ ersetzt werden sollte. Daher fordert der Ausschuss die luxemburgische Aufsichtsbehörde auf, dafür zu sorgen, dass der verwendete Begriff im gesamten Entwurf der Zertifizierungskriterien konsistent ist.

5. Der Ausschuss regt an, die Bedeutung einiger der in den Zertifizierungskriterien verwendeten Begriffe zu klären, wie z. B. das „befugte“ Management der Einrichtung, das die Umsetzung des von ihrem Datenschutzbeauftragten unterstützten Mechanismus für internationale Datenübermittlungen überwachen muss, um die Einhaltung der DSGVO sicherzustellen (siehe Kriterien II-a-18 und III-13, aber auch I-1), sowie die von der Einrichtung durchzuführende „förmliche Bewertung“, die im Entwurf der Kriterien mehrfach erwähnt wird (z. B. Abschnitt II-a-10).

6. Im Entwurf der Kriterien heißt es in mehreren Abschnitten, dass „die Einrichtung die förmliche Stellungnahme ihres Datenschutzbeauftragten berücksichtigt hat“ (z. B. Abschnitte II-a-18 und III-13). Der Ausschuss fordert die luxemburgische Aufsichtsbehörde auf, in einem

Vermerk im Entwurf der Kriterien klarzustellen, dass der Datenschutzbeauftragte trotz der Tatsache, dass er eine wichtige Rolle bei der Überwachung der Einhaltung der Vorschriften bei den Verarbeitungsvorgängen der Einrichtung gemäß Artikel 39 der DSGVO spielt, nicht dafür zuständig sein sollte, die Umsetzung der Maßnahmen zur Gewährleistung dieser Einhaltung zu bewerten.

7. Der Ausschuss stellt fest, dass die von der luxemburgischen Aufsichtsbehörde vorgelegten Zertifizierungskriterien keine Informationen über die geplanten Bewertungsmethoden enthalten. Nach Angaben der luxemburgischen Aufsichtsbehörde lassen sich diese (teilweise) aus der Norm ISAE 3000 (International Standard on Assurance Engagements) ableiten, die Teil des Zertifizierungsverfahrens ist, da sie im Zusammenhang mit der Akkreditierung verwendet wird. Auf der Grundlage der von der Aufsichtsbehörde bereitgestellten Informationen wurde diese Norm vom International Auditing and Assurance Standards Board (IAASB) entwickelt und befasst sich mit anderen Bestätigungsaufträgen als Abschlussprüfungen oder Überprüfungen historischer Finanzinformationen. Der EDSA fordert die luxemburgische Aufsichtsbehörde auf, klarzustellen, dass die Norm ISAE 3000 für die Zertifizierungskriterien keine Bedeutung hat, da sie kein Teil davon ist, dass sie aber für das Zertifizierungsverfahren relevant ist. In diesem Zusammenhang erinnert der EDSA an die Empfehlungen, die er bereits in seiner Stellungnahme zu den Akkreditierungsanforderungen für Zertifizierungsstellen der luxemburgischen Aufsichtsbehörde ausgesprochen hat[4].

2.2 Anwendungsbereich des Zertifizierungsverfahrens und Evaluationsgegenstand (EVG)

8. Das Zertifizierungssystem „GDPR-CARPA“ ist ein allgemeines System, das sich nicht auf einen bestimmten Sektor oder eine bestimmte Art der Verarbeitung bezieht. Nach den von der luxemburgischen Aufsichtsbehörde bereitgestellten Informationen sind der Hauptgegenstand des Anwendungsbereichs der Zertifizierung die Datenschutzpflichten des Verantwortlichen/Auftragsverarbeiters (Grundsatz der Rechenschaftspflicht). Aus diesem Grund enthält GDPR-CARPA Anforderungen, die sich auf die Datenschutz-Governance in der Organisation für die im EVG enthaltenen Verarbeitungstätigkeiten konzentrieren, sowie spezifische Kriterien, die diese Verarbeitungstätigkeiten unmittelbar betreffen. Die luxemburgische Aufsichtsbehörde hat jedoch einige Einschränkungen/Ausschlüsse für den Anwendungsbereich festgelegt, um klarzustellen, welche (Arten von) Verarbeitungstätigkeiten im Rahmen des Zertifizierungssystems GDPR-CARPA zertifiziert bzw. nicht zertifiziert werden können. Insbesondere ist GDPR-CARPA nicht geeignet für:

- die Zertifizierung der Verarbeitung personenbezogener Daten speziell für Minderjährige unter 16 Jahren,
- die Zertifizierung von Verarbeitungstätigkeiten im Rahmen einer gemeinsamen Verantwortlichkeit,

[4] Siehe Stellungnahme 5/2020 des EDSA zum Entwurf des Beschlusses der zuständigen Aufsichtsbehörde Luxemburgs zur Genehmigung der Anforderungen an die Akkreditierung von Zertifizierungsstellen nach Artikel 43 Absatz 3 DSGVO, angenommen am 29. Januar, Nummer 8.

- die Zertifizierung von Verarbeitungstätigkeiten im Zusammenhang mit Artikel 10 der DSGVO,
- Einrichtungen, die keinen offiziellen Datenschutzbeauftragten benannt haben (Artikel 37 der DSGVO).

In diesem Zusammenhang stellt der Ausschuss fest, dass der Ausschluss von Verarbeitungstätigkeiten, die unter die Artikel 85 bis 89 der DSGVO fallen, nicht im System GDPR-CARPA erwähnt wird. Der Ausschuss geht jedoch davon aus, dass relevante Aspekte der Einhaltung der DSGVO in Bezug auf die Verarbeitungsvorgänge, die unter diese Artikel fallen, von den Zertifizierungskriterien abgedeckt werden sollen. Beispielsweise betrifft Abschnitt II-a-9 des Entwurfs der Zertifizierungskriterien die Verarbeitung besonderer Kategorien personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken, enthält jedoch keine geeigneten und spezifischen Maßnahmen zum Schutz der Grundrechte und Interessen der betroffenen Personen gemäß Artikel 89 Absatz 1 der DSGVO. Daher empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, spezifische Kriterien für Verarbeitungstätigkeiten gemäß den Artikeln 85 bis 89 der DSGVO aufzunehmen.

Darüber hinaus empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, aufzunehmen, dass die Einrichtung eine Analyse der einschlägigen Rechtsvorschriften durchführt, aus der hervorgeht, dass spezifische und geeignete Maßnahmen ergriffen wurden, um die Grundrechte und Interessen der betroffenen Personen gemäß Artikel 89 der DSGVO zu wahren.

2.3 Verfahren zur Festlegung eines Evaluationsgegenstands (EVG)

9. Nach den von der luxemburgischen Aufsichtsbehörde bereitgestellten Informationen muss der EVG für die Zertifizierung gemäß den Anforderungen für die „Planung und Durchführung des Auftrags“ der Norm ISAE (International Standard on Assurance Engagements), die Teil des Zertifizierungsverfahrens ist, festgelegt werden. Wie in den EDSA-Leitlinien 1/2018 dargelegt, sollte jedoch in den Zertifizierungskriterien selbst hinreichend beschrieben werden, wie der EVG zu definieren ist (siehe Anhang 2 der EDSA-Leitlinien 1/2018, Abschnitt 2 Buchstabe f). Dies scheint für das Zertifizierungssystem GDPR-CARPA nicht der Fall zu sein, das sich in dieser Hinsicht auf die Norm ISAE stützt, aber Leitlinien für die Definition des EVG im Zertifizierungsprogramm umfasst. In diesem Zusammenhang empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, zu Beginn des Entwurfs der Zertifizierungskriterien in einem eigenen Abschnitt ausreichende Informationen über die Kriterien für die Definition des EVG aufzunehmen.

2.4 Zertifizierungskriterien

10. Der Ausschuss stellt fest, dass bei einer Vielzahl der Kriterien nicht klar ist, was geprüft werden muss und von wem. Der Ausschuss betont vielmehr, dass dies aus den Kriterien selbst eindeutig hervorgehen sollte. Insbesondere wird das Instrument der „Selbstbewertung“ durch den Antragsteller in vielen Kriterien verwendet. Diesbezüglich stellt der Ausschuss fest, dass die luxemburgische Aufsichtsbehörde in den Kriterien nicht immer die Elemente festlegt, auf deren Grundlage der Antragsteller die Selbstbewertung durchführen sollte, um klarzustellen, welche Nachweise vom Antragsteller erwartet und von der Zertifizierungsstelle geprüft werden. So wird beispielsweise in den Abschnitten II-a-I und II-a-4 über die Ermittlung einer

gültigen Rechtsgrundlage bzw. die Datenverarbeitung auf der Grundlage eines Vertrags nicht angegeben, welche Faktoren der Antragsteller bei der Bewertung der Ermittlung der Rechtsgrundlage berücksichtigen sollte, wie z. B. die Notwendigkeit der Verarbeitung in Bezug auf die verfolgten Zwecke und die Eignung der Rechtsgrundlage unter Berücksichtigung der Verarbeitungstätigkeiten je nach Art, Kontext, Umfang und Zweck der Verarbeitung. Gleiches gilt für die anderen Kriterien für die übrigen Rechtsgrundlagen (d. h. II-a-3 und II-a-5-8).

In diesem Zusammenhang ist zu vermeiden, dass die Zertifizierungsstelle die Bewertung des Antragstellers übernimmt, ohne sie in Bezug auf die genannten, in den Kriterien aufzuführenden Faktoren zu überprüfen oder zumindest kritisch zu hinterfragen. Dies gilt insbesondere für die nachstehend aufgeführten Kriterien:

- Abschnitt II-a-I und Abschnitte II-a-3 bis II-a-8 in Bezug auf die oben genannten Faktoren zur Bewertung der Ermittlung der Rechtsgrundlage der Datenverarbeitung.
- Abschnitt I-14 über Datenschutzverletzungen in Bezug auf die Faktoren, die bei der vorgeschriebenen Bewertung zu berücksichtigen sind.
- Ebenso in Abschnitt I-15 über die Meldung von Datenschutzverletzungen an den Verantwortlichen unter Bezugnahme auf die Faktoren, die bei der Bewertung dieser Verletzungen zu berücksichtigen sind.
- Abschnitt II-a-11 über das Recht auf Einschränkung der Verarbeitung in Bezug auf die zu berücksichtigenden Faktoren, um die Unmöglichkeit oder Unverhältnismäßigkeit der Mitteilung an die Empfänger, denen personenbezogene Daten offengelegt wurden, nachzuweisen.
- Ebenso in Abschnitt II-a-14 in Bezug auf die zu berücksichtigenden Faktoren, um festzustellen, ob sich die Auskunft an betroffene Personen gemäß Artikel 14 der DSGVO als unmöglich erweist oder einen unverhältnismäßigen Aufwand mit sich bringen würde.
- Abschnitt II-a-18 betreffend Übermittlungen an Drittländer, siehe die spezifische Empfehlung in Nummer 22 der vorliegenden Stellungnahme.
- Abschnitt II-b-2 über die Vereinbarkeit des Zwecks, siehe die spezifische Empfehlung in Nummer 23 der vorliegenden Stellungnahme.
- Abschnitt II-c-2 über alternative Mittel in Bezug auf die Faktoren, die bei der Beurteilung der Frage zu berücksichtigen sind, ob die Zwecke nicht durch einen weniger einschneidenden Prozess erreicht werden können (z. B. Menge der erhobenen Daten, Speicherfrist, Zweck der Verarbeitung, verfügbare Technologie).
- Abschnitt II-d-3 über das Recht auf Berichtigung in Bezug auf die Faktoren, auf die sich die Beurteilung der Unmöglichkeit oder Unverhältnismäßigkeit der Mitteilung an die Empfänger, denen personenbezogene Daten offengelegt wurden, stützen sollte.
- Abschnitt II-e-1 in Bezug auf die festgelegte Speicherfrist enthält keine Angaben zu den Faktoren, die zu berücksichtigen sind, wenn die Speicherfrist angesichts der geltenden rechtlichen Anforderungen (z. B. verfolgte(r) Zweck(e)) nicht festgelegt werden kann.

- Abschnitt II-e-3 über das Recht auf Löschung in Bezug auf die Faktoren, die bei der Beurteilung der Unmöglichkeit oder Unverhältnismäßigkeit der Mitteilung an die Empfänger, denen personenbezogene Daten offengelegt wurden, zu berücksichtigen sind.
- Abschnitt II-f-2 über die Risikoanalyse, siehe die spezifische Empfehlung in Nummer 52.
- Abschnitt II-f-9 über die Bewertung der Hinlänglichkeit, siehe die spezifische Aufforderung in Nummer 35.
- Abschnitt III-7 über das Risikomanagement, siehe die spezifische Empfehlung in Nummer 55.
- Abschnitt III-3 betreffend Übermittlungen an Drittländer, siehe die spezifische Empfehlung in Nummer 22.

Daher empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, die oben genannten Kriterien zu ändern, um die Faktoren anzugeben, die der Antragsteller bei der Durchführung der einschlägigen Bewertungen zu berücksichtigen hat, um gleichzeitig klarzustellen, was von der Zertifizierungsstelle geprüft wird.

2.5 Rechtmäßigkeit der Verarbeitung

11. Der Ausschuss stellt fest, dass die luxemburgische Aufsichtsbehörde in Abschnitt II-a-I auf eine „gültige Rechtsgrundlage“ verweist. Der Ausschuss ist jedoch der Auffassung, dass die luxemburgische Aufsichtsbehörde berücksichtigen sollte, wie die Anwendbarkeit der Rechtsgrundlage nachgewiesen wird und ob sie gegebenenfalls geeignet ist, wobei die Verarbeitungstätigkeiten je nach Art, Kontext, Umfang und Zweck der Verarbeitung zu berücksichtigen sind. Der Ausschuss empfiehlt der luxemburgischen Aufsichtsbehörde, dieses Kriterium entsprechend zu ändern[5].

12. In Abschnitt II-a-3 heißt es: „Die Einrichtung hat die Notwendigkeit der Einwilligung geprüft.“ Der Ausschuss empfiehlt der luxemburgischen Aufsichtsbehörde, aufzunehmen, dass die Einrichtung die Eignung der Einwilligung als Rechtsgrundlage für die Verarbeitung im Einzelfall nachweist anstatt der Notwendigkeit, damit dieses Kriterium im Einklang mit Erwägungsgrund 43 der DSGVO und den EDSA-Leitlinien zur Einwilligung gemäß der DSGVO steht[6].

13. In Bezug auf Abschnitt II-a-3 über die „freiwillig erteilte“ Einwilligung fordert der Ausschuss die luxemburgische Aufsichtsbehörde auf, zur Vollständigkeit einen Verweis auf Erwägungsgrund 32 aufzunehmen.

14. Der Ausschuss nimmt die Anforderung einer Einwilligung, die in informierter Weise und unmissverständlich abgegeben wird, in Abschnitt II-a-3 zur Kenntnis. Der Ausschuss ist jedoch

[5] Siehe Erwägungsgrund 43 der DSGVO sowie die EDSA-Leitlinien 05/2020 zur Einwilligung gemäß der DSGVO, abrufbar unter https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf.

[6] Siehe beispielsweise die Nummern 2, 3, 16, 17, 31 und 91 der EDSA-Leitlinien 05/2020 zur Einwilligung gemäß der DSGVO, abrufbar unter https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf.

der Auffassung, dass diesbezüglich weitere Informationen benötigt werden. Konkret empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, in ihren Entwurf der Zertifizierungskriterien die Mindestanforderungen aufzunehmen, die erfüllt sein müssen, damit die Einwilligung als in informierter Weise und unmissverständlich abgegeben angesehen werden kann und die Kriterien einen ausreichenden Mehrwert für die Einhaltung der DSGVO durch die zertifizierten Einrichtungen bieten.

15. In Abschnitt II-a-8 heißt es im Entwurf der Zertifizierungskriterien: „Der Gesetzgeber legt die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Behörden gesetzlich fest. Folglich sollte diese Rechtsgrundlage nicht für die Verarbeitung durch Behörden bei der Wahrnehmung ihrer Aufgaben gelten." In diesem Zusammenhang fordert der EDSA die luxemburgische Aufsichtsbehörde auf, das Wort „sollte" durch „gilt" zu ersetzen [und das Wort „gelten" am Ende zu streichen].

16. Der Ausschuss stellt fest, dass in Abschnitt II-a-9 in Bezug auf die Verarbeitung besonderer Kategorien personenbezogener Daten der Verweis auf geeignete Garantien fehlt, wenn Artikel 9 Absatz 2 der DSGVO dies vorsieht. Beispielsweise müssen für eine Verarbeitung, die aus Gründen des öffentlichen Interesses (Artikel 9 Absatz 2 Buchstabe i der DSGVO) im Bereich der öffentlichen Gesundheit erforderlich ist, die im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehenen angemessenen und spezifischen Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Personen, insbesondere des Berufsgeheimnisses, vorhanden sein. Der Ausschuss empfiehlt der luxemburgischen Aufsichtsbehörde, solche Garantien erforderlichenfalls in diesem Abschnitt zu berücksichtigen und diese Kriterien entsprechend zu ändern.

17. Im Einzelnen wird in Abschnitt II-a-9, der sich auf Artikel 9 Absatz 2 Buchstabe b der DSGVO bezieht, erwähnt, dass „die Einrichtung die anwendbare Rechtsgrundlage ermittelt und ihre Anwendbarkeit auf diese Verarbeitungstätigkeit förmlich geprüft hat". Der EDSA erinnert daran, dass der Verantwortliche nach dem Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, worin geeignete Garantien für die Grundrechte und Interessen der betroffenen Person vorgesehen sind, für diese Verarbeitung befugt ist. Der EDSA ist der Auffassung, dass die Prüfungen und Kontrollen der Zertifizierungsstelle nicht konkret genug wären, wenn nicht alle in dieser Bestimmung vorgesehenen Elemente der Einhaltung berücksichtigt würden, wie etwa die vom Verantwortlichen eingehaltenen Garantien, da das Kriterium, auf das sich die Bewertung stützt, nicht detailliert genug ist. Daher empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, dieses Kriterium entsprechend zu ändern, damit die Bewertung durch die Zertifizierungsstelle erschöpfend sein kann.

18. Ebenso empfiehlt der Ausschuss in Bezug auf die „rechtmäßigen Tätigkeiten einer Stiftung, Vereinigung oder sonstigen Organisation ohne Gewinnerzielungsabsicht [...]", die geeigneten Garantien gemäß Artikel 9 Absatz 2 Buchstabe d der DSGVO zu berücksichtigen.

19. In gleicher Weise reicht in Bezug auf Artikel 9 Absatz 2 Buchstabe g der DSGVO betreffend das „erhebliche öffentliche Interesse" der bloße Verweis in den Kriterien auf das ermittelte Unionsrecht oder Recht der Mitgliedstaaten nicht aus. Die „spezifischen Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person" sollten in diesem Zusammenhang ebenfalls berücksichtigt und sichergestellt werden. Daher empfiehlt der Ausschuss, diese Elemente im Entwurf der Zertifizierungskriterien zu berücksichtigen, um den

zertifizierten Einrichtungen einen ausreichenden Mehrwert im Hinblick auf die Einhaltung der DSGVO zu bieten.

20. Ebenso stellt der Ausschuss in demselben Abschnitt fest, dass es keinen Verweis auf zusätzliche Bedingungen gibt, einschließlich Beschränkungen für die Verarbeitung von genetischen Daten, biometrischen Daten oder Gesundheitsdaten. Der Ausschuss empfiehlt, dass die luxemburgische Aufsichtsbehörde dieses Kriterium entsprechend ändert, um gegebenenfalls auf die Elemente der Einhaltung der DSGVO gemäß Artikel 9 Absatz 4 zu verweisen.

21. In Bezug auf Abschnitt II-a-18 betreffend die Übermittlung personenbezogener Daten an Drittländer empfiehlt der Ausschuss, dass die luxemburgische Aufsichtsbehörde in den Entwurf der Zertifizierungskriterien im Feld „Bezeichnung" einen Verweis auf die Artikel 44-45 der DSGVO sowie die entsprechenden Erwägungsgründe der DSGVO aufnimmt.

22. Zusätzlich zu der im Kriterium II-a-18 genannten Bewertung sollte die Einrichtung auch die Wahl des Datenübermittlungsmechanismus gemäß Kapitel V der DSGVO begründen.[7] Daher empfiehlt der Ausschuss, dass die luxemburgische Aufsichtsbehörde in den Entwurf der Kriterien die Notwendigkeit aufnimmt, die für den Datenübermittlungsmechanismus getroffene Wahl zu begründen.

2.6 Grundsätze des Artikels 5

23. In Bezug auf die Vereinbarkeit von Zwecken gemäß Abschnitt II-b-2 empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, weitere Einzelheiten zu den Elementen hinzuzufügen, auf denen die Prüfung der Vereinbarkeit weiterer Zwecke beruhen muss, und mindestens die in Artikel 6 Absatz 4 der DSGVO festgelegten Elemente aufzunehmen, da die darin aufgeführten Kriterien für die Vereinbarkeitsprüfung fehlen. In Bezug auf Abschnitt II-c-1 fordert der Ausschuss die luxemburgische Aufsichtsbehörde auf, die Menge, die Art und die Eigenschaften der erhobenen und verarbeiteten Daten bei den Faktoren zu berücksichtigen, die sich auf die Umsetzung des Grundsatzes der Datenminimierung auswirken könnten.

24. In Bezug auf Abschnitt II-c-2 fordert der Ausschuss die luxemburgische Aufsichtsbehörde auf, im Zusammenhang mit „weniger eingreifende Mittel" klarzustellen, was nachgewiesen werden muss.

25. In Bezug auf den Grundsatz der Datenrichtigkeit in Abschnitt II-d-2 heißt es im Entwurf der Zertifizierungskriterien: „Die Einrichtung hat ein Verfahren festgelegt und umgesetzt, mit dem die von ihr erhaltenen personenbezogenen Daten regelmäßig und mindestens einmal jährlich überprüft werden, indem sich die Einrichtung entweder direkt an die betroffene Person oder an die Quelle, von der sie die Daten erhalten hat, wendet. Die Einrichtung dokumentiert diese Überprüfung der Datenrichtigkeit und hat ein Verfahren zur Aktualisierung der Daten bei Bedarf eingerichtet." Der Ausschuss fordert die luxemburgische Aufsichtsbehörde auf, die in diesen Kriterien genannten personenbezogenen Daten nicht auf die Daten zu beschränken, die die Einrichtung „erhalten" hat, sondern auch auf die Daten zu verweisen, über die die Einrichtung allgemein verfügt (z. B. Daten, die aus den von der Einrichtung erhaltenen oder anderweitig erstellten Daten abgeleitet oder generiert wurden). Darüber hinaus fordert der Ausschuss die luxemburgische Aufsichtsbehörde aus Gründen der Vollständigkeit auf, im

[7] Im Rahmen dieser Bewertung sollten die einschlägigen Urteile des EuGH sowie die Leitlinien und Empfehlungen des EDSA berücksichtigt werden.

Passus „zur Aktualisierung der Daten bei Bedarf“ hinzuzufügen, dass Daten erforderlichenfalls auch berichtigt oder gelöscht werden.

26. In Bezug auf die Löschung oder Anonymisierung von Daten in Abschnitt II-e-2 werden im Entwurf der Zertifizierungskriterien bestimmte Anwendungsfälle aufgeführt, in denen der Antragsteller diese Vorgänge wirksam sicherstellen muss. Im zweiten und dritten Aufzählungspunkt wird insbesondere Folgendes erwähnt: „wenn personenbezogene Daten für die Zwecke der Verarbeitung nicht oder nicht mehr erforderlich sind; wenn sie die Daten nicht mehr benötigt; oder“. Der Ausschuss stellt fest, dass ein weiterer Anwendungsfall darin bestehen könnte, dass die Aufsichtsbehörde die Löschung personenbezogener Daten gemäß Artikel 58 Absatz 2 Buchstabe g der DSGVO anordnet. In jedem Fall fordert der Ausschuss die luxemburgische Aufsichtsbehörde auf, den Unterschied zwischen den beiden in diesen zwei Aufzählungspunkten beschriebenen Anwendungsfällen klarzustellen oder ansonsten einen davon zu streichen und im Entwurf der Zertifizierungskriterien andere mögliche Anwendungsfälle, wie etwa Artikel 58 Absatz 2 Buchstabe g, zu berücksichtigen.

2.7 Allgemeine Pflichten von Verantwortlichen und Auftragsverarbeitern

2.7.1. Pflicht von Verantwortlichen und Auftragsverarbeitern

27. In Abschnitt I-11 des Entwurfs der Zertifizierungskriterien, der die Kompetenzen des Datenschutzbeauftragten betrifft, stellt der Ausschuss fest, dass der Datenschutzbeauftragte, wenn er nicht über mindestens drei Jahre Berufserfahrung verfügt, entweder i) „über zwei Jahre juristische Erfahrung verfügen muss und umfassende Schulungen zum Datenschutz absolviert hat“ oder ii) „der Datenschutzbeauftragte entweder intern oder über einen nicht begrenzten Dienstleistungsvertrag mit einem externen Unternehmen Zugang zu Rechtsberatung hat, die alle DSGVO-Themen abdeckt“. Der Ausschuss ist der Auffassung, dass die Qualifikation des Datenschutzbeauftragten nicht ausschließlich anhand der zweiten Anforderung bewertet werden sollte. Dies bedeutet, dass der Datenschutzbeauftragte nicht nur deshalb als qualifiziert gelten sollte, weil er „intern oder über einen nicht begrenzten Dienstleistungsvertrag mit einem externen Unternehmen Zugang zu Rechtsberatung hat, die alle DSGVO-Themen abdeckt“. Dies könnte eine zusätzliche Anforderung für die Bewertung der Qualifikationen des Datenschutzbeauftragten sein, aber keine eigenständige Anforderung. Da das Verfahren in hohem Maße auf den Datenschutzbeauftragten angewiesen ist, muss dieser unbedingt über das entsprechende Fachwissen verfügen. Darüber hinaus sollten die erforderlichen Schulungen zum Datenschutz zeitnah und aktuell sein. Daher empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, diesen Abschnitt entsprechend zu ändern.

28. In Abschnitt I-12 des Entwurfs der Kriterien (letzter Punkt) bezieht sich die luxemburgische Aufsichtsbehörde auf Fälle, in denen Interessenkonflikte des Datenschutzbeauftragten festgestellt wurden. Der Ausschuss begrüßt diese Einbeziehung, ist jedoch der Auffassung, dass die Meldung an das höchste Management der Einrichtung und die Dokumentation der Interessenkonflikte nicht ausreichen. Es ist von wesentlicher Bedeutung, dass dieser Interessenkonflikt nach einem festgelegten Verfahren gelöst wird. Daher empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, dieses Element in diesen Abschnitt aufzunehmen.

29. Der Ausschuss stellt fest, dass die luxemburgische Aufsichtsbehörde in Abschnitt I-13 des Entwurfs der Kriterien auf die Pflicht des Datenschutzbeauftragten verweist, „die Einrichtung und ihre Beschäftigten, die Verarbeitungstätigkeiten durchführen, über ihre Pflichten gemäß der DSGVO und anderen Datenschutzbestimmungen der Union oder der Mitgliedstaaten zu informieren und zu beraten [...]“. Die luxemburgische Aufsichtsbehörde stellte klar, dass sich dies nicht auf Datenschutzbestimmungen anderer Mitgliedstaaten, sondern auf Bestimmungen nationaler Gesetze und Vorschriften bezieht. Daher fordert der Ausschuss die luxemburgische Aufsichtsbehörde auf, diesen Verweis in den Kriterien entsprechend zu ändern.

30. Der Ausschuss stellt fest, dass sich die Abschnitte I-14 und I-15 des Entwurfs der Zertifizierungskriterien auf Datenschutzverletzungen beziehen: Der erste Abschnitt soll Verantwortliche und der zweite Abschnitt für Auftragsverarbeiter gelten. Diese Abschnitte schreiben insbesondere vor, dass die Einrichtung, die eine Zertifizierung beantragt, „technische und organisatorische Maßnahmen zur Ermittlung, Bewältigung und Meldung von Verletzungen des Schutzes personenbezogener Daten“ ergreift. Diese Maßnahmen müssen verschiedene Aspekte abdecken, darunter den Grad der Einbeziehung des Datenschutzbeauftragten. In dieser Hinsicht scheinen beide Kriterien jedoch widersprüchlich zu sein, da sie einerseits vorsehen, dass „der Datenschutzbeauftragte stets über jede Datenschutzverletzung informiert werden sollte“, während sie sich andererseits auf ein „förmliches Verfahren“ beziehen, in dem festgelegt wird, „wann der Datenschutzbeauftragte unterrichtet werden muss und welche Informationen er dabei erhält“. Es ist nicht klar, ob sich diese beiden Anforderungen auf unterschiedliche faktische Zusammenhänge beziehen. Daher empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, zu erläutern, ob dies der Fall ist, und diesen Widerspruch zwischen beiden Abschnitten zu beseitigen.

31. In Abschnitt I-14 empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde in Bezug auf die Mitteilung an die Aufsichtsbehörde, im sechsten Aufzählungspunkt die Worte „falls zutreffend“ zu streichen.

32. Abschnitt I-15 des Entwurfs der Zertifizierungskriterien, der für Auftragsverarbeiter gilt, fordert die Umsetzung „technischer und organisatorischer Maßnahmen zur Erkennung, Bewältigung und Meldung von Verletzungen des Schutzes personenbezogener Daten an Vertragspartner und/oder Verantwortliche innerhalb einer Frist, die es dem Verantwortlichen erlaubt, die Aufsichtsbehörde innerhalb von 72 Stunden zu benachrichtigen“. In Bezug auf den vorgesehenen Zeitrahmen stellt der Ausschuss fest, dass der Auftragsverarbeiter nach Artikel 33 Absatz 2 der DSGVO verpflichtet ist, dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten „unverzüglich“ zu melden, nachdem sie ihm bekannt wurde. Daher empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, den Begriff „unverzüglich“ in die Pflicht des Auftragsverarbeiters in diesem Abschnitt aufzunehmen.

2.7.2. Pflichten von Verantwortlichen

33. Der Ausschuss stellt fest, dass es in Abschnitt II-f-7 heißt: „Die Einrichtung überprüft die Datenschutzfolgenabschätzung regelmäßig und mindestens einmal jährlich oder wenn wesentliche Änderungen auftreten, die sich auf die Datenschutzfolgenabschätzung auswirken. Die Einrichtung berücksichtigt die förmliche Stellungnahme ihres Datenschutzbeauftragten.“ Der Ausschuss empfiehlt der luxemburgischen Aufsichtsbehörde, diesen Abschnitt mit Artikel 35 Absatz 9 der DSGVO in Einklang zu bringen, um die Möglichkeit zu berücksichtigen, den Standpunkt der betroffenen Personen oder ihrer Vertreter einzuholen

(unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge).

34. In Bezug auf die Überprüfung der Datenschutzfolgenabschätzung in Abschnitt II-f-7 wird darauf hingewiesen, dass diese unter anderem durchgeführt werden soll, „wenn wesentliche Änderungen auftreten, die sich auf die Datenschutzfolgenabschätzung auswirken". In diesem Zusammenhang verlangt das Kriterium, dass die Einrichtung „eine dokumentierte Methode anwendet, die sicherstellt, dass alle Faktoren berücksichtigt wurden, die sich auf die Datenschutzfolgenabschätzung auswirken könnten" und dass dies „externe oder interne Faktoren sein können, die unter anderem Änderungen des geltenden Rechtsrahmens umfassen [...]". In Bezug auf diese Änderungen empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, auch einen Verweis auf Änderungen des Risikos aufzunehmen, das von Verarbeitungsvorgängen im Sinne von Artikel 35 Absatz 11 der DSGVO ausgeht.

35. In Bezug auf Abschnitt II-f-9 des Entwurfs der Zertifizierungskriterien mit der Überschrift „Bewertung der Hinlänglichkeit", der den Einsatz von Auftragsverarbeitern durch den Antragsteller betrifft, fordert der Ausschuss die luxemburgische Aufsichtsbehörde auf, das Fachwissen, die Zuverlässigkeit und die Ressourcen zu berücksichtigen, über die der Auftragsverarbeiter vor der Beauftragung verfügen muss, im Einklang mit Erwägungsgrund 81 der DSGVO. In Bezug auf den letzten Aufzählungspunkt dieses Abschnitts empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde außerdem, klarzustellen, dass die Prüfungen, die der Verantwortliche gemäß den Abschnitten II-f-5 und II-f-6 des Entwurfs der Zertifizierungskriterien durchzuführen hat, gegenüber dem Auftragsverarbeiter durchgeführt werden können.

36. In Bezug auf Abschnitt II-f-10, der einen Vertrag/ein Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten betrifft, empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, die Elemente anzugeben, die in diesem Vertrag/Rechtsinstrument gemäß Artikel 28 Absatz 3 der DSGVO festgelegt werden müssen, wie Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sowie die Pflichten und Rechte des Verantwortlichen.

37. Wenn in dem Entwurf der Zertifizierungskriterien darauf hingewiesen wird, dass nach dem Unionsrecht oder dem Recht der Mitgliedstaaten ein Vertrag/Rechtsinstrument vorliegen muss, empfiehlt der Ausschuss darüber hinaus, festzulegen, dass dies gemäß Artikel 28 Absatz 9 der DSGVO schriftlich (auch in einem elektronischen Format) schriftlich abgefasst werden sollte, um von der Zertifizierungsstelle überprüft werden zu können.

38. Im sechsten Aufzählungspunkt desselben Kriteriums heißt es: „Der Auftragsverarbeiter unterstützt die Einrichtung unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen bei der Einhaltung ihrer Pflichten." Diesbezüglich empfiehlt der Ausschuss, zusätzlich auf die rechtlichen Pflichten der Einrichtung zu verweisen, die sich aus den Artikeln 32 bis 36 der DSGVO ergeben.

39. Die Kriterien in Abschnitt II-f-12 beziehen sich auf „Verfahren zur Erfüllung der Sorgfaltspflicht" zusätzlich zu der Prüfung und Überwachung durch den Antragsteller gegenüber den eingesetzten Auftragsverarbeitern. Der Ausschuss stellt fest, dass der Begriff „Sorgfaltspflicht" sehr weit gefasst sein und je nach Inhalt und Struktur des zugrunde liegenden Vertrags unterschiedliche Auslegungen haben kann, was wiederum besondere Datenschutzanforderungen für die jeweiligen Prüfungen bedeutet. Da das Risiko einer

nichtkonformen Umsetzung nicht unerheblich ist und die Verwendung dieses Begriffs zu Unklarheiten hinsichtlich des erforderlichen Umfangs von Prüfungen führen kann, fordert der Ausschuss die luxemburgische Aufsichtsbehörde auf, den Begriff „Verfahren zur Erfüllung der Sorgfaltspflicht“ im Entwurf der Kriterien zu präzisieren.

2.7.3. Pflichten von Auftragsverarbeitern

40. In Bezug auf Abschnitt III des Entwurfs der Zertifizierungskriterien, der die Grundsätze für die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter oder Unterauftragsverarbeiter betrifft, empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, in Abschnitt III-1 hinzuzufügen, dass der Vertrag oder das Rechtsinstrument zwischen dem Auftragsverarbeiter und dem Verantwortlichen oder zwischen dem Unterauftragsverarbeiter und dem Auftragsverarbeiter im Einklang mit Artikel 28 Absatz 9 der DSGVO schriftlich (auch in elektronischem Format) abgefasst werden sollte.

41. Wenn im selben Entwurf der Zertifizierungskriterien erwähnt wird, dass die Einrichtung „den Vertragspartner und den Verantwortlichen bei der Sicherstellung der Einhaltung seiner Pflichten unterstützt, wobei die Art der Verarbeitung und die der Einrichtung zur Verfügung stehenden Informationen berücksichtigt werden“, fordert der Ausschuss die luxemburgische Aufsichtsbehörde auf, einen ausdrücklichen Verweis auf die Pflichten des Unterauftragsverarbeiters zur Unterstützung des Auftragsverarbeiters und die vergleichbare Pflicht des Auftragsverarbeiters zur Unterstützung des Verantwortlichen in Bezug auf dessen Pflichten gemäß den Artikeln 32 bis 36 der DSGVO aufzunehmen.

42. In Bezug auf Abschnitt III-3 des Entwurfs der Kriterien betreffend die Beschränkung der Verarbeitung auf die dokumentierten Anweisungen, die der Verantwortliche oder der Vertragspartner erhalten hat, empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, einen Verweis auf internationale Übermittlungen im Einklang mit Artikel 28 Absatz 3 Buchstabe a der DSGVO aufzunehmen.

43. In Abschnitt III-11 des Entwurfs der Zertifizierungskriterien in Bezug auf die Bewertung der Hinlänglichkeit stellt der Ausschuss fest, dass es einen Verweis auf die Pflicht des Auftragsverarbeiters geben sollte, die Unterauftragsverarbeiter zu bewerten, deren Einsatz er beabsichtigt[8]. Der Ausschuss fordert die luxemburgische Aufsichtsbehörde auf, dieses Kriterium entsprechend zu ändern.

44. In Bezug auf Abschnitt III-3 des Entwurfs der Zertifizierungskriterien betreffend die Übermittlung personenbezogener Daten an Drittländer empfiehlt der Ausschuss, dieses Kriterium an die oben genannte Empfehlung für Abschnitt II-a-18 anzupassen.

2.8 Rechte betroffener Personen

45. In Abschnitt I-9 des Entwurfs der Zertifizierungskriterien über die „Ermöglichung der Ausübung der Rechte betroffener Personen“ nimmt der Ausschuss zwei verschiedene

[8] Ähnliche Pflichten finden sich in der Stellungnahme des EDSA zu den Standardvertragsklauseln gemäß Artikel 28 der DSGVO, Klausel 7.6 über die Genehmigung zum Einsatz eines Unterauftragsverarbeiters: „Um die Bewertung und die Entscheidung über die Genehmigung der Vergabe von Unteraufträgen vorzunehmen, stellt der Auftragsverarbeiter dem Verantwortlichen alle erforderlichen Informationen über den vorgesehenen Unterauftragsverarbeiter zur Verfügung, einschließlich seiner Standorte, der von ihm durchzuführenden Verarbeitungstätigkeiten und etwaiger zu treffender Garantien und Maßnahmen.“

Szenarien zur Kenntnis, in denen die Einrichtung einem Antrag des Verantwortlichen nicht nachkommen kann. Der Ausschuss geht davon aus, dass sich das erste Szenario auf Situationen bezieht, in denen die Einrichtung die vom Verantwortlichen gesetzte Frist nicht einhalten kann, während sich das zweite Szenario auf eine absolute Unmöglichkeit der Einhaltung bezieht. Die Unterscheidung zwischen den beiden Szenarien ist jedoch in den Kriterien nicht klar, weshalb der Ausschuss die luxemburgische Aufsichtsbehörde dazu anhält, dies zu präzisieren.

46. In Bezug auf die Ausübung der Rechte betroffener Personen begrüßt der Ausschuss betreffend die Gebühren, die der Verantwortliche im Falle offenkundig unbegründeter oder exzessiver Anträge der betroffenen Person erheben kann, die Pflicht der Einrichtung, zu dokumentieren, „wie sie die Höhe der erhobenen Gebühren rechtfertigt". Diese Pflicht findet sich in Abschnitt II-a-10 (Widerspruchsrecht), Abschnitt II-a-11 (Recht auf Einschränkung der Verarbeitung), Abschnitt II-a-12 (Recht, nicht einer automatisierten Entscheidungsfindung im Einzelfall unterworfen zu werden), Abschnitt II-a-16 (Auskunftsrecht) und Abschnitt II-a-17 (Recht auf Datenübertragbarkeit). In diesem Zusammenhang stellt der Ausschuss fest, dass die zu berücksichtigenden Faktoren, um die Höhe der erhobenen Gebühren als angemessen zu betrachten, in Artikel 12 Absatz 5 Buchstabe a der DSGVO festgelegt sind und nicht dem Ermessen der Einrichtung, die eine Zertifizierung beantragt, oder der Zertifizierungsstelle überlassen werden sollten. Daher empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, einen Verweis auf diese Faktoren in diesen Abschnitt aufzunehmen (d. h. die Verwaltungskosten für die Mitteilung oder die Durchführung der von der betroffenen Person beantragten Maßnahmen).

47. In Bezug auf das Recht der betroffenen Person, nicht einer automatisierten Entscheidungsfindung, einschließlich Profiling, unterworfen zu werden, stellt der Ausschuss fest, dass „Profiling" in der Überschrift des entsprechenden Abschnitts II-a-12 enthalten ist. Es fehlt jedoch im Haupttext des Kriteriums (erster Absatz). Der Ausschuss fordert diese Ergänzung.

48. Darüber hinaus ist das Auskunftsrecht der betroffenen Personen in Abschnitt II-a-16 des Entwurfs der Zertifizierungskriterien geregelt. Der Entwurf enthält jedoch keine Liste der Informationen, die der betroffenen Person gemäß Artikel 15 Absatz 1 zur Verfügung zu stellen sind. Aus Gründen der Kohärenz mit dem Entwurf der übrigen Zertifizierungskriterien, die sich auf die Rechte betroffener Personen beziehen, empfiehlt der Ausschuss daher, an dieser Stelle auch auf alle in Artikel 15 Absatz 1 der DSGVO genannten Pflichten zu verweisen (d. h. auf die Informationen, die der Verantwortliche den betroffenen Personen bei der Ausübung ihres Auskunftsrechts zur Verfügung stellen sollte).

49. In demselben Abschnitt stellt der Ausschuss fest, dass der Entwurf der Zertifizierungskriterien nicht vorsieht, dass die erste Kopie, die die Einrichtung der betroffenen Person zur Verfügung stellt, kostenlos sein sollte und dass die Einrichtung für alle weiteren beantragten Kopien ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen kann. Der Ausschuss empfiehlt der luxemburgischen Aufsichtsbehörde, diesen Aspekt in die Kriterien aufzunehmen.

50. Ebenso fehlt der Verweis auf die Modalitäten für die Bereitstellung der von der betroffenen Person angeforderten Informationen. Der Ausschuss empfiehlt, klarzustellen, dass im Falle eines Antrags der betroffenen Person auf elektronischem Wege und sofern nichts anderes

verlangt wird, die Informationen in einem gängigen elektronischen Format zur Verfügung gestellt werden müssen.

51. Im Abschnitt II-a-17 zum Recht auf Datenübertragbarkeit fehlt ein wichtiges zu bewertendes Element. Insbesondere ist nach Artikel 20 Absatz 4 der DSGVO zu prüfen, ob das Recht der betroffenen Personen auf Datenübertragbarkeit die Rechte und Freiheiten anderer Personen beeinträchtigt. Der Ausschuss empfiehlt diese Ergänzung, da dieses Element ebenfalls von der Zertifizierungsstelle im Zusammenhang mit dem Recht auf Datenübertragbarkeit bewertet werden muss.

2.9 Risiken für die Rechte und Freiheiten natürlicher Personen sowie technische und organisatorische Schutzmaßnahmen

52. In den Abschnitten II-f-2 und III-6 über die Risikoanalyse wird nicht hinreichend klargestellt, welche Risiken, insbesondere die der betroffenen Personen, angegangen werden. Der Ausschuss empfiehlt der luxemburgischen Aufsichtsbehörde, unter den in dieser Anforderung genannten Risiken auch die Risiken für die Rechte und Freiheiten der betroffenen Personen aufzunehmen. Darüber hinaus empfiehlt der Ausschuss, dass die luxemburgische Aufsichtsbehörde weitere Informationen über die verschiedenen Arten von Risiken für die betroffenen Personen hinzufügt.

53. Im Einklang mit den früheren Empfehlungen zur Risikoanalyse empfiehlt der Ausschuss der luxemburgischen Aufsichtsbehörde, in den Abschnitten II-f-3 und III-7 außerdem hinzuzufügen, dass beim Risikomanagement die verschiedenen Arten von Risiken für die Rechte und Freiheiten der betroffenen Personen berücksichtigt werden.

54. Darüber hinaus wird darauf hingewiesen, dass die Einrichtung zumindest die technischen und organisatorischen Maßnahmen für die Zugangskontrolle ergreifen sollte. Der Ausschuss empfiehlt der luxemburgischen Aufsichtsbehörde, dies mit Artikel 32 Absatz 4 der DSGVO in Einklang zu bringen, indem die Pflicht der Einrichtung hinzugefügt wird, Schritte zu unternehmen, mit denen sichergestellt wird, dass ihr unterstellte natürliche oder juristische Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung der Einrichtung verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

55. Im Entwurf der Zertifizierungskriterien heißt es ferner in den Abschnitten II-f-3 und III-7, dass die Einrichtung die Wirksamkeit des Risikomanagementplans mindestens einmal jährlich oder wenn Änderungen auftreten, die sich auf die Risikobewertung auswirken, überprüft und den Risikomanagementplan erforderlichenfalls anpasst. Der Ausschuss fordert die luxemburgische Aufsichtsbehörde auf, deutlich zu machen, dass es Verfahren zur Messung und Gewährleistung der Wirksamkeit des genannten Plans gibt, um sicherzustellen, dass die Zertifizierungskriterien selbsterklärend sind und dass die Zertifizierungsstelle allein anhand der Formulierung der Kriterien wissen kann, was sie überprüfen muss.

56. In Bezug auf die Umsetzung organisatorischer und technischer Maßnahmen heißt es im Entwurf der Zertifizierungskriterien in den Abschnitten II-f-4 und III-8, dass tägliche Berichte über durchgeführte Kontrollen und Sicherheitsvorfälle, die mit den in den Anwendungsbereich fallenden Verarbeitungstätigkeiten im Zusammenhang stehen, mindestens dem Datenschutzbeauftragten und dem Management der Einrichtung vorzulegen

sind. Der Ausschuss fordert die luxemburgische Aufsichtsbehörde auf, hinzuzufügen, dass diese Berichte auch den beteiligten relevanten Personen innerhalb der Organisation – also nicht nur dem Datenschutzbeauftragten und dem Management der Einrichtung – zur Verfügung gestellt werden sollten.

3 SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

57. Abschließend ist der EDSA der Auffassung, dass die Zertifizierungskriterien für GDPR-CARPA 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:

58. In Bezug auf den „Anwendungsbereich des Zertifizierungsverfahrens und Evaluationsgegenstand (EVG)“ empfiehlt der Ausschuss, dass die luxemburgische Aufsichtsbehörde

    1. spezifische Kriterien für Verarbeitungstätigkeiten gemäß den Artikeln 85 bis 89 der DSGVO aufnimmt;

    2. eine von der Einrichtung durchzuführende Analyse der einschlägigen Rechtsvorschriften aufnimmt, aus der hervorgeht, dass spezifische und geeignete Maßnahmen ergriffen wurden, um die Grundrechte und Interessen der betroffenen Personen gemäß Artikel 89 der DSGVO zu wahren.

59. In Bezug auf das „Verfahren zur Festlegung eines Evaluationsgegenstands (EVG)“ empfiehlt der Ausschuss, dass die luxemburgische Aufsichtsbehörde

    1. am Anfang des Entwurfs der Zertifizierungskriterien in einem eigenen Abschnitt ausreichende Informationen zu den Kriterien für die Festlegung des EVG aufführt.

60. In Bezug auf die „Zertifizierungskriterien“ empfiehlt der Ausschuss, dass die luxemburgische Aufsichtsbehörde

    1. die in Nummer 10 dieser Stellungnahme aufgeführten Kriterien ändert, indem die Faktoren angegeben werden, die der Antragsteller bei der Durchführung der einschlägigen Bewertungen zu berücksichtigen hat, um damit auch klarzustellen, was von der Zertifizierungsstelle überprüft wird.

61. In Bezug auf die „Rechtmäßigkeit der Verarbeitung“ empfiehlt der Ausschuss, dass die luxemburgische Aufsichtsbehörde

    1. den Abschnitt II-a-I über eine „gültige Rechtsgrundlage“ ändert, um zu berücksichtigen, wie die Anwendbarkeit der Rechtsgrundlage und gegebenenfalls ihre Eignung unter Berücksichtigung der Verarbeitungstätigkeiten je nach Art, Kontext, Umfang und Zweck der Verarbeitung nachgewiesen wird;

    2. in Bezug auf Abschnitt II-a-3 berücksichtigt, dass die Einrichtung die „Eignung“ der Einwilligung als Rechtsgrundlage für die Verarbeitung im Einzelfall nachweist, damit dieses Kriterium im Einklang mit Erwägungsgrund 43 der DSGVO und den EDSA-Leitlinien 05/2020 zur Einwilligung gemäß der DSGVO steht;

3. in Abschnitt II-a-3 die Mindestanforderungen hinzufügt, die notwendigerweise erfüllt sein müssen, damit die Einwilligung als in informierter Weise und unmissverständlich abgegeben angesehen werden kann und die Zertifizierungskriterien einen ausreichenden Mehrwert für die Einhaltung der DSGVO durch die zertifizierten Einrichtungen bieten;

4. im gesamten Abschnitt II-a-9 erforderlichenfalls die geeigneten Garantien gemäß Artikel 9 Absatz 2 der DSGVO in Bezug auf die Verarbeitung besonderer Kategorien von Daten berücksichtigt und die betreffenden Kriterien entsprechend ändert;

5. das Kriterium in Abschnitt II-a-9, in dem auf Artikel 9 Absatz 2 Buchstabe b der DSGVO verwiesen wird, so ändert, dass der Verantwortliche nach dem Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, worin geeignete Garantien für die Grundrechte und Interessen der betroffenen Person vorgesehen sind, für diese Verarbeitung befugt sein muss, damit die Bewertung durch die Zertifizierungsstelle erschöpfend sein kann;

6. in Abschnitt II-a-9 die geeigneten Garantien gemäß Artikel 9 Absatz 2 Buchstabe d der DSGVO in Bezug auf die „rechtmäßigen Tätigkeiten einer Stiftung, Vereinigung oder sonstigen Organisation ohne Gewinnerzielungsabsicht [...]“ berücksichtigt;

7. in Abschnitt II-a-9 die spezifischen Maßnahmen berücksichtigt, die zur Wahrung der Grundrechte und Interessen der betroffenen Person in Bezug auf das „erhebliche öffentliche Interesse“ im Zusammenhang mit Artikel 9 Absatz 2 Buchstabe g der DSGVO ergriffen werden;

8. in Abschnitt II-a-9 das Kriterium so ändert, dass erforderlichenfalls auf zusätzliche Bedingungen, einschließlich Beschränkungen für die Verarbeitung von genetischen Daten, biometrischen Daten oder Gesundheitsdaten, die im nationalen Recht gemäß Artikel 9 Absatz 4 der DSGVO festgelegt sind, verwiesen wird;

9. einen Verweis auf die Artikel 44-45 der DSGVO im Feld „Bezeichnung“ in Abschnitt II-a-18 des Entwurfs der Zertifizierungskriterien aufnimmt, zusammen mit den entsprechenden Erwägungsgründen der DSGVO;

11. in Abschnitt II-a-18 verlangt, dass die Einrichtung die für den Datenübermittlungsmechanismus getroffene Wahl gemäß Kapitel V der DSGVO begründet.

62. In Bezug auf die „Grundsätze des Artikels 5“ empfiehlt der Ausschuss, dass die luxemburgische Aufsichtsbehörde

1. in Abschnitt II-b-2 weitere Einzelheiten zu den Elementen hinzufügt, auf denen die Prüfung der Vereinbarkeit weiterer Zwecke beruhen muss, und mindestens die in Artikel 6 Absatz 4 der DSGVO festgelegten Elemente aufnimmt;

63. In Bezug auf die „allgemeinen Pflichten von Verantwortlichen und Auftragsverarbeitern“ empfiehlt der Ausschuss, dass die luxemburgische Aufsichtsbehörde

1. das Kriterium in Abschnitt I-11 für die Kompetenzen des Datenschutzbeauftragten ändert, um sicherzustellen, dass die Anforderung (ii) nicht allein steht, sondern eine zusätzliche Anforderung für die Bewertung der Qualifikation des Datenschutzbeauftragten darstellt, und dass die erforderlichen Schulungen zum Datenschutz zeitnah und aktuell sind;

2. in Abschnitt I-12 hinzufügt, dass ein festgestellter Interessenkonflikt nach einem festgelegten Verfahren gelöst wird;

3. in den Abschnitten I-14 und I-15 den Grad der Einbeziehung des Datenschutzbeauftragten präzisiert, da die Entwurfskriterien einerseits vorsehen, dass „der Datenschutzbeauftragte stets über jede Datenschutzverletzung informiert werden sollte“, während sie sich andererseits auf ein „förmliches Verfahren“ beziehen, in dem festgelegt wird, „wann der Datenschutzbeauftragte unterrichtet werden muss und welche Informationen er dabei erhält“;

4. die Worte „falls zutreffend“ im sechsten Aufzählungspunkt von Abschnitt I-14 über die Meldung von Datenschutzverletzungen an die Aufsichtsbehörde streicht;

5. in Abschnitt I-15 den Begriff „unverzüglich“ in Bezug auf die Pflicht des Auftragsverarbeiters hinzufügt, dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten gemäß Artikel 33 Absatz 2 der DSGVO zu melden, nachdem sie ihm bekannt wurde;

6. in Bezug auf die Überprüfung der Datenschutzfolgenabschätzung den Abschnitt II-f-7 ändert, um ihn mit Artikel 35 Absatz 9 der DSGVO in Einklang zu bringen und der Möglichkeit Rechnung zu tragen, den Standpunkt der betroffenen Personen oder ihrer Vertreter einzuholen (unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge);

7. in Bezug auf Faktoren, die sich auf die Datenschutzfolgenabschätzung auswirken könnten, den Abschnitt II-f-7 ändert, um einen Verweis auf Änderungen des Risikos aufzunehmen, das von Verarbeitungsvorgängen im Sinne von Artikel 35 Absatz 11 der DSGVO ausgeht;

8. den letzten Aufzählungspunkt in Abschnitt II-f-9 ändert, um klarzustellen, dass die Prüfungen, die der Verantwortliche gemäß den Abschnitten II-f-5 und II-f-6 des Entwurfs der Zertifizierungskriterien durchzuführen hat, gegenüber einem Auftragsverarbeiter durchgeführt werden können;

9. in Abschnitt II-f-10 einen Verweis auf die Elemente hinzufügt, die in dem Vertrag/Rechtsinstrument gemäß Artikel 28 Absatz 3 der DSGVO festgelegt werden müssen, wie Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sowie die Pflichten und Rechte des Verantwortlichen;

10. in den Abschnitten II-f-10 und III-1 festlegt, dass, wenn nach dem Unionsrecht oder dem Recht der Mitgliedstaaten ein Vertrag/Rechtsinstrument vorliegen muss, dies gemäß Artikel 28 Absatz 9 der DSGVO schriftlich erfolgen sollte, um von der Zertifizierungsstelle überprüft werden zu können;

11. in Abschnitt III-3 über die Beschränkung der Verarbeitung auf die dokumentierten Anweisungen, die der Verantwortliche oder der Vertragspartner erhalten hat, einen Verweis auf internationale Übermittlungen im Einklang mit Artikel 28 Absatz 3 Buchstabe a der DSGVO aufnimmt;

12. Abschnitt III-3 des Entwurfs der Zertifizierungskriterien an die Empfehlung für Abschnitt II-a-18 anpasst.

64. In Bezug auf die „Rechte der betroffenen Personen“ empfiehlt der Ausschuss, dass die luxemburgische Aufsichtsbehörde

1. einen Verweis auf die Elemente aufnimmt, die bei der Prüfung der angemessenen Höhe der erhobenen Gebühren gemäß Artikel 12 Absatz 5 Buchstabe a der DSGVO im Falle offenkundig unbegründeter oder exzessiver Anträge der betroffenen Person zu berücksichtigen sind (d. h. die Verwaltungskosten für die Mitteilung oder die Durchführung der von der betroffenen Person beantragten Maßnahmen);

2. in Abschnitt II-a-16 aufnimmt, dass die erste Kopie, die die Einrichtung der betroffenen Person zur Verfügung stellt, kostenlos sein sollte und dass die Einrichtung für alle weiteren Kopien ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen kann;

3. in demselben Abschnitt klarstellt, dass im Falle eines Antrags der betroffenen Person auf elektronischem Wege und sofern nichts anderes verlangt wird, die Informationen in einem gängigen elektronischen Format zur Verfügung gestellt werden müssen;

4. in Abschnitt II-a-17 darauf hinweist, dass geprüft werden muss, ob das Recht der betroffenen Personen auf Datenübertragbarkeit die Rechte und Freiheiten anderer Personen beeinträchtigt;

65. In Bezug auf die „Risiken für die Rechte und Freiheiten natürlicher Personen“ und die „technischen und organisatorischen Schutzmaßnahmen“ empfiehlt der Ausschuss, dass die luxemburgische Aufsichtsbehörde

1. unter den in den Abschnitten II-f-2 und III-6 genannten Risiken die Risiken für die Rechte und Freiheiten der betroffenen Personen angibt und Informationen über die verschiedenen Arten von Risiken in Bezug auf die betroffenen Personen hinzufügt;

2. in den Abschnitten II-f-3 und III-7 hinzufügt, dass beim Risikomanagement die verschiedenen Arten von Risiken für die Rechte und Freiheiten der betroffenen Personen berücksichtigt werden;

3. die Anforderung an die Einrichtung, zumindest die technischen und organisatorischen Maßnahmen für die Zugangskontrolle zu berücksichtigen, mit Artikel 32 Absatz 4 der DSGVO in Einklang bringt, indem die entsprechende Pflicht hinzugefügt wird.

66. Schließlich erinnert der EDSA im Einklang mit den Leitlinien auch daran, dass die luxemburgische Aufsichtsbehörde im Falle von wesentlichen Änderungen[9] der Zertifizierungskriterien für GDPR-CARPA dem EDSA die geänderte Fassung gemäß Artikel 42 Absatz 5 und Artikel 43 Absatz 2 Buchstabe b der DSGVO vorlegen muss.

4 ABSCHLIEßENDE BEMERKUNGEN

67. Diese Stellungnahme ist an die luxemburgische Aufsichtsbehörde gerichtet und wird gemäß Artikel 64 Absatz 5 Buchstabe b der DSGVO veröffentlicht.

68. Gemäß Artikel 64 Absätze 7 und 8 der DSGVO hat die luxemburgische Aufsichtsbehörde dem Vorsitz binnen zwei Wochen nach Eingang der Stellungnahme auf elektronischem Wege

[9] 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“ mit „Leitlinien zur Bewertung der Zertifizierungskriterien“, für die der Zeitraum der öffentlichen Konsultation am 26. Mai 2021 abgelaufen ist.

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.

69. Die luxemburgische Aufsichtsbehörde muss dem EDSA ihren endgültigen Beschluss mitteilen, damit dieser ihn gemäß Artikel 70 Absatz 1 Buchstabe y der DSGVO im Register der Beschlüsse in Bezug auf Fragen, die im Rahmen des Kohärenzverfahrens behandelt wurden, erfassen kann.

70. Der EDSA weist darauf hin, dass die luxemburgische Aufsichtsbehörde gemäß Artikel 43 Absatz 6 der DSGVO die Zertifizierungskriterien für GDPR-CARPA 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)