Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679

Version 3.0

vom 4. Juni 2019

angenommen

Versionsüberblick

Version 3.0	4. Juni 2019	Hinzufügung von Anhang 2 (Version 2.0 von Anhang 2 wurde im Anschluss an die öffentliche Konsultation am 4. Juni verabschiedet)
Version 2.1	9. April 2019	Annahme einer Berichtigung der Leitlinien (Ziffer 45)
Version 2.0	23. Januar 2019	Annahme der Leitlinien im Anschluss an die öffentliche Konsultation; am gleichen Tag wurde Anhang 2 (Version 1.0) für die öffentliche Konsultation verabschiedet
Version 1.0.	25. Mai 2018	Annahme der Leitlinien für die öffentliche Konsultation

Inhalt

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 70 Absatz 1 Buchstabe e 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 (Datenschutz-Grundverordnung, im Folgenden „DSGVO“),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum, insbesondere auf Anhang XI und Protokoll 37 in der durch den Beschluss Nr. 154/2018 des Gemeinsamen EWR-Ausschusses vom 6. Juli 2018 geänderten Fassung,

gestützt auf die Artikel 12 und 22 seiner Geschäftsordnung vom 25. Mai 2018,

nach Prüfung der Ergebnisse der öffentlichen Konsultation zu den Leitlinien und der öffentlichen Konsultation zu deren Anhang 2, die gemäß Artikel 70 Absatz 4 der DSGVO zwischen dem 30. Mai 2018 und dem 12. Juli 2018 bzw. zwischen dem 15. Februar 2019 und dem 29. März 2019 stattfand –

HAT FOLGENDE LEITLINIEN VERABSCHIEDET

1 EINFÜHRUNG

1. Die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, „DSGVO“ oder „Verordnung“) setzt einen modernisierten Rahmen für den Datenschutz in Europa, der auf die Einhaltung der Rechenschaftspflicht und der Grundrechte ausgerichtet ist. Den Kern dieses neuen Rahmens bilden eine Reihe von Maßnahmen, welche die Einhaltung der Bestimmungen der DSGVO erleichtern. Dazu gehören unter bestimmten Umständen verbindliche Anforderungen (u. a. bei der Ernennung von Datenschutzbeauftragten und der Durchführung von Datenschutz-Folgenabschätzungen) aber auch freiwillige Maßnahmen wie Verhaltensregeln und Zertifizierungsverfahren.
2. Schon vor dem Erlass der DSGVO stellte die Artikel 29-Arbeitsgruppe fest, dass der Zertifizierung eine wesentliche Rolle im Rahmen der Rechenschaftspflicht für den Datenschutzbereich zukommen könnte.[1] Damit eine Zertifizierung die Einhaltung der Datenschutzbestimmungen zuverlässig nachweisen kann, müssen klare Vorgaben für die Erbringung von Zertifizierungsdiensten festgelegt werden.[2] In Artikel 42 der DSGVO findet sich die Rechtsgrundlage für die Ausarbeitung solcher Vorgaben.
3. Artikel 42 Absatz 1 der DSGVO sieht Folgendes vor:

   „Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen,

[1] Artikel 29-Arbeitsgruppe, Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht, WP 173, 13. Juli 2010, Ziffern 69-71.
[2] Artikel 29-Arbeitsgruppe, Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht (WP 173), Ziffer 69.

nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen."

4. Zertifizierungsverfahren[3] können die Transparenz sowohl für die betroffenen Personen, als auch in den Beziehungen zwischen Unternehmen, etwa zwischen Verantwortlichen und Auftragsverarbeitern, verbessern. Laut Erwägungsgrund 100 der DSGVO kann die Einführung von Zertifizierungsverfahren die Transparenz und die Einhaltung der Verordnung fördern und dabei den betroffenen Personen ermöglichen, das Datenschutzniveau einschlägiger Produkte und Dienstleistungen zu bewerten. .[4]

5. Durch die DSGVO wird für Verantwortliche bzw. Auftragsverarbeiter weder ein Recht auf Zertifizierung noch eine Pflicht zur Zertifizierung eingeführt. Die Zertifizierung ist vielmehr nach Artikel 42 Absatz 3 ein freiwilliges Verfahren, das zum Nachweis der Einhaltung der DSGVO beiträgt. Sowohl die Mitgliedstaaten als auch die Aufsichtsbehörden sind aufgerufen, die Einführung von Zertifizierungsmechanismen zu fördern und die Beteiligung der Interessengruppen am Zertifizierungsprozess und dessen kontinuierlichen Aktualisierung sicherzustellen.

6. Darüber hinaus ist die Erfüllung der Anforderungen von genehmigten Zertifizierungsmechanismen ein Faktor, den die Aufsichtsbehörden im Rahmen der Entscheidung über die Verhängung einer Geldbuße und deren Höhe als erschwerenden oder mildernden Faktor berücksichtigen müssen. (Artikel 83 Absatz 2 Buchstabe j).[5]

1.1 Anwendungsbereich der Leitlinien

7. Der Anwendungsbereich dieser Leitlinien ist begrenzt; sie stellen kein Handbuch für die Zertifizierung gemäß der DSGVO dar. Das vorrangige Ziel dieser Leitlinien besteht darin, übergeordnete Anforderungen und Kriterien zu ermitteln, die für alle Arten von Zertifizierungsmechanismen nach den Artikeln 42 und 43 der DSGVO relevant sein können. Zu diesem Zweck wird in den vorliegenden Leitlinien

   - der Frage nachgegangen, inwieweit die Zertifizierung als Rechenschaftsinstrument dient,
   - eine Erläuterung der wichtigsten Begriffe der Zertifizierungsbestimmungen der Artikel 42 und 43 vorgenommen, und
   - der Anwendungsbereich der Zertifizierung nach den Artikeln 42 und 43 erläutert und der Zweck der Zertifizierung dargelegt,

[3] In diesen Leitlinien werden die Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen gemeinsam als „Zertifizierungsverfahren" bezeichnet, siehe Abschnitt 1.3.2.
[4] Laut Erwägungsgrund 100 sollte, um die Transparenz zu erhöhen und die Einhaltung der Verordnung zu verbessern, die Einführung von Zertifizierungsverfahren angeregt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.
[5] Vgl. Artikel 29-Arbeitsgruppe, Leitlinien für die Verhängung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679 (WP 253).

- Hilfestellung gegeben, damit das Ergebnis der Zertifizierung unabhängig von der jeweiligen Zertifizierungsstelle aussagekräftig, eindeutig, möglichst reproduzierbar und vergleichbar ist (Vergleichbarkeit).

8. Nach der DSGVO stehen den Mitgliedstaaten und den Aufsichtsbehörden eine Reihe von Möglichkeiten zur Umsetzung der Artikel 42 und 43 zur Verfügung. Die Leitlinien bieten Unterstützung bei der Auslegung und Umsetzung der Bestimmungen der Artikel 42 und 43 und sollen den Mitgliedstaaten, Aufsichtsbehörden und nationalen Akkreditierungsstellen bei der Einführung einer kohärenten und harmonisierten Vorgehensweise zur Umsetzung von Zertifizierungsmechanismen im Einklang mit der DSGVO behilflich sein.

9. Die in den vorliegenden Leitlinien enthaltenen Informationen sind maßgeblich für

   - die zuständigen Aufsichtsbehörden und den Europäischen Datenschutzausschuss (EDSA) bei der Genehmigung von Zertifizierungskriterien nach Artikel 42 Absatz 5, Artikel 58 Absatz 3 Buchstabe f und Artikel 70 Absatz 1 Buchstabe o,

   - die Zertifizierungsstellen bei der Abfassung und Überarbeitung von Zertifizierungskriterien, bevor diese den zuständigen Aufsichtsbehörden zur Genehmigung nach Artikel 42 Absatz 5 vorgelegt werden,

   - den Europäischen Datenschutzausschuss bei der Genehmigung eines Europäischen Datenschutzsiegels nach Artikel 42 Absatz 5 und Artikel 70 Absatz 1 Buchstabe o,

   - die Aufsichtsbehörden bei der Ausarbeitung eigener Zertifizierungskriterien,

   - die Europäische Kommission, die befugt ist, delegierte Rechtsakte zu erlassen, um die Anforderungen festzulegen, die bei den Zertifizierungsverfahren nach Artikel 43 Absatz 8 zu berücksichtigen sind,

   - den Europäischen Datenschutzausschuss bei der Abgabe einer Stellungnahme für die Kommission zu den Zertifizierungsanforderungen gemäß Artikel 70 Absatz 1 Buchstabe q und Artikel 43 Absatz 8,

   - die nationalen Akkreditierungsstellen, die den Zertifizierungskriterien für die Akkreditierung von Zertifizierungsstellen im Einklang mit EN-ISO/IEC 17065/2012 sowie mit den zusätzlichen, gemäß Artikel 43 festgelegten Anforderungen Rechnung tragen müssen, und

   - die Verantwortlichen und die Auftragsverarbeiter bei der Festlegung ihrer jeweiligen Strategie für die Gewährleistung der Konformität mit der DSGVO und bei der Erwägung, die Zertifizierung gegebenenfalls als Mittel zum Nachweis der Einhaltung dieser Vorschriften einzusetzen.

10. Der Europäische Datenschutzausschuss (EDSA) wird separate Leitlinien für die Ermittlung von Kriterien für die Genehmigung von Zertifizierungsmechanismen als Übermittlungsinstrumente an Drittländer oder internationale Organisationen gemäß Artikel 42 Absatz 2 veröffentlichen.

1.2 Zweck der Zertifizierung gemäß der DSGVO

11. Nach Artikel 42 Absatz 1 werden Zertifizierungsmechanismen eingeführt, um „nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird“.

12. In der DSGVO werden Beispiele für Rahmenbedingungen genannt, innerhalb derer genehmigte Zertifizierungsmechanismen als Faktor für den Nachweis der Pflichterfüllung von Verantwortlichen und Auftragsverarbeitern in Bezug auf folgende Punkte herangezogen werden können:

    - Umsetzung und Nachweis geeigneter technischer und organisatorischer Maßnahmen gemäß Artikel 24 Absätze 1 und 3, Artikel 25 und Artikel 32 Absätze 1 und 3,
    - hinreichende Garantien (vonseiten des Auftragsverarbeiters gegenüber dem Verantwortlichen bzw. vonseiten des Unterauftragsverarbeiters gegenüber dem Verantwortlichen) „im Sinne der Absätze 1 und 4“ (Artikel 28 Absatz 5).

13. Da die Zertifizierung als solche allein nicht für den Nachweis der Konformität ausreicht, sondern lediglich einen Faktor darstellt, der die Einhaltung der Vorschriften belegen kann, sollte der Zertifizierungsprozess transparent gestaltet werden. Zum Nachweis der Konformität sind Begleitunterlagen vorzulegen, insbesondere schriftliche Berichte, in denen die Einhaltung der Kriterien konkret beschrieben und diese nicht nur wiederholt werden. Für den Fall, dass die Kriterien zunächst nicht erfüllt wurden, sind Korrekturen und Abhilfemaßnahmen sowie deren Zweckmäßigkeit zu beschreiben und damit die Gründe für die Erteilung und Aufrechterhaltung der Zertifizierung darzulegen. Hierzu zählt auch eine kurze Darstellung der Rahmenbedingungen für die Entscheidung über die Erteilung, die Erneuerung oder den Widerruf eines Zertifikats. Dabei sollten die aus der Anwendung der Kriterien hergeleiteten Gründe, Argumente und Beweise ebenso aufgeführt werden wie die bei der Zertifizierung aufgrund von Fakten oder Voraussetzungen gezogenen Schlussfolgerungen, getroffenen Entscheidungen oder festgestellten Beeinträchtigungen.

1.3 Wichtigste Begriffe

14. Im folgenden Abschnitt werden die wichtigsten Begriffe der Artikel 42 und 43 erläutert. Mit dieser Analyse wird ein Verständnis der Grundbegriffe und des Zertifizierungsbereichs nach der DSGVO entwickelt.

1.3.1 Auslegung des Begriffs „Zertifizierung“

15. Der Begriff „Zertifizierung“ wird in der DSGVO nicht definiert. Die Internationale Normungsorganisation (International Standards Organisation - ISO) versteht unter einer Zertifizierung allgemein die durch eine unabhängige Stelle erfolgende Vorlage einer schriftlichen Versicherung (eines Zertifikats), dass ein in Frage stehendes Produkt, eine Dienstleistung oder ein System bestimmte Anforderungen erfüllt. Als alternative Bezeichnung

für Zertifizierung ist auch der Begriff „Konformitätsbewertung durch eine unabhängige Stelle“ bekannt, und Zertifizierungsstellen können auch „Konformitätsbewertungsstellen“ genannt werden. In der Norm EN-ISO/IEC 17000:2004 – Konformitätsbewertung – Begriffe und allgemeine Grundlagen (auf die sich die Norm ISO17065 bezieht) – wird der Begriff Zertifizierung wie folgt definiert: „Bestätigung durch eine dritte Seite ... bezogen auf Produkte, Prozesse und Systeme oder Personen“.

16. Bestätigen bedeutet das „Erstellen einer Konformitätsaussage, auf der Grundlage einer Entscheidung, die der Bewertung folgt, dass die Erfüllung festgelegter Anforderungen dargelegt wurde“ (Abschnitt 5.2, ISO 17000:2004).

17. Im Rahmen der Zertifizierung nach den Artikeln 42 und 43 der DSGVO bezieht sich die Zertifizierung auf eine durch einem unabhängigen Dritten erfolgende Bescheinigung, die die Verarbeitungsvorgänge von Verantwortlichen und Auftragsverarbeitern betrifft.

1.3.2 Zertifizierungsverfahren, Siegel und Prüfzeichen

18. Die Begriffe „Zertifizierungsmechanismen“, „Siegel“ und „Prüfzeichen“ werden in der DSGVO nicht einzeln definiert, sondern gemeinsam verwendet. Ein Zertifikat ist eine Konformitätserklärung. Ein Siegel oder ein Prüfzeichen kann dazu verwendet werden, den erfolgreichen Abschluss des Zertifizierungsverfahrens kenntlich zu machen. Mit Siegel oder Prüfzeichen ist üblicherweise ein Logo oder Symbol gemeint, dessen Vorhandensein (neben einem Zertifikat) anzeigt, dass der Zertifizierungsgegenstand im Rahmen eines Zertifizierungsverfahrens von einer unabhängigen Stelle geprüft wurde und den festgelegten Anforderungen entspricht, die in normativen Dokumenten wie Rechtsvorschriften, Standards oder technischen Spezifikationen niedergelegt sind. Diese Anforderungen für die Zertifizierung nach der DSGVO sind in den zusätzlichen Anforderungen aufgeführt, die die Vorschriften für die Akkreditierung von Zertifizierungsstellen in der EN-ISO/IEC 17065/2012 sowie die von der zuständigen Aufsichtsbehörde oder dem Ausschuss genehmigten Zertifizierungskriterien ergänzen. Ein Zertifikat, Siegl oder Prüfzeichen darf gemäß der DSGVO nur nach einer unabhängigen Bewertung der Nachweise durch eine akkreditierte Zertifizierungsstelle oder zuständige Aufsichtsbehörde ausgestellt werden, aus der hervorgeht, dass die Zertifizierungskriterien erfüllt sind.

19. Die nachfolgende Tabelle zeigt ein allgemeines Beispiel für einen Zertifizierungsprozess:

Einreichung des Antrags durch den Verantwortlichen oder Auftragsverarbeiter	Formale Überprüfung durch die Zertifizierungsstelle	Bewertung Vorevaluierung	Bewertung Evaluierung des EVG	Bewertung Validierung der Ergebnisse	Information an die Aufsichtsbehörde für die Zertifizierung	Zertifizierung	Überwachung	Verlängerung der Zertifizierung
Ist die Beschreibung des Evaluationsgegenstands (EVG) eindeutig und vollständig, und schließt	Ist die Beschreibung des EVG akzeptabel?	Welche vorgesehenen Kriterien sind anwendbar?	Entspricht der EVG den Kriterien?	Sind alle relevanten Kriterien definiert, und spiegeln sie den EVG wider?	Wurden die Gründe für die Erteilung oder den Widerruf der Zertifizierung angegeben?	Kann das Zertifikat erteilt werden?	Entspricht der EVG weiterhin den Kriterien?	Entspricht die Verarbeitung noch den Zertifizierungskriterien?

sie die Schnittstellen ein?								
Kann der Zugang zu den Verarbeitungs-vorgängen des EVG zugesichert werden?	Sind die gesamten Unterlagen vollständig und auf dem neuesten Stand?	Welche anwend-baren Evaluie-rungsme-thoden gelten?	Ist die Dokumenta-tion des EVG zutreffend?	Wurde die Evaluierung ausreichend dokumen-tiert?		Können die Berichte veröffent-licht werden?	Wird das Zertifikat, Siegel oder Vertrau-enszeichen ordnungs-gemäß ver-wendet?	Wurden die Entwicklungs-bereiche ausreichend behandelt?
Art. 42 Abs. 6	Art. 43 Abs. 4	Art. 43 Abs. 4	Art. 42 Abs. 5, Art. 43 Abs. 4	Art. 43 Abs. 4	Art. 43 Abs. 1 und 5	Art. 43 Abs. 1, Art. 42 Abs. 7	Art. 42 Abs. 7	Art. 42 Abs. 7

2 DIE ROLLE DER AUFSICHTSBEHÖRDEN

20. Artikel 42 Absatz 5 sieht vor, dass die Zertifizierung von einer akkreditierten Zertifizierungsstelle oder einer zuständigen Aufsichtsbehörde erteilt wird. Damit wird durch die DSGVO allerdings für die Aufsichtsbehörden keine Pflichtaufgabe begründet, Zertifizierungen zu erteilen, vielmehr lässt die DSGVO hier eine Reihe verschiedener Modelle zu. Einer Aufsichtsbehörde stehen zum Beispiel folgende Entscheidungsmöglichkeiten offen:

    - Sie kann die Zertifizierung selbst für das eigene Zertifizierungsprogramm erteilen;
    - sie kann die Zertifizierung selbst für das eigene Zertifizierungsprogramm erteilen, dabei jedoch den gesamten Bewertungsprozess oder Teile davon an Dritte delegieren;
    - sie kann ihr eigenes Zertifizierungsprogramm erstellen und Zertifizierungsstellen, die dann die Zertifizierung erteilen, mit dem Zertifizierungsverfahren betrauen, und
    - sie kann Anreize für den Markt schaffen, Zertifizierungsmechanismen zu entwickeln.

21. Zudem muss sich die Aufsichtsbehörde im Lichte der auf nationaler Ebene getroffenen Entscheidungen zu den Akkreditierungsverfahren mit ihrer Rolle auseinandersetzen – insbesondere, wenn sie selbst befugt ist, Zertifizierungsstellen gemäß Artikel 43 Absatz 1 der DSGVO zu akkreditieren. Jede Aufsichtsbehörde hat somit für sich selbst zu entscheiden, wie sie vorgehen möchte, um den allgemeinen Zweck der Zertifizierung nach der DSGVO zu verfolgen. Diese Festlegung erfolgt nicht nur im Zusammenhang mit den Aufgaben und Befugnissen nach den Artikeln 57 und 58, sondern auch in Anbetracht der Zertifizierung als maßgeblichem Faktor im Rahmen der Festsetzung von Geldbußen bzw. allgemein als Mittel für den Konformitätsnachweis.

2.1 Die Aufsichtsbehörde als Zertifizierungsstelle

22. Entscheidet sich eine Aufsichtsbehörde dafür, Zertifizierungen durchzuführen, muss sie ihre Rolle sorgfältig im Hinblick auf die ihr nach der DSGVO zugewiesenen Aufgaben prüfen. Sie sollte bei der Ausübung ihrer Funktion eine hohe Transparenz anstreben. Um mögliche Interessenkonflikte zu vermeiden, sollte die Behörde darauf achten, dass eine Trennung zum Aufsichts- und Durchsetzungsbereich besteht.

23. Wenn eine Aufsichtsbehörde als Zertifizierungsstelle agiert, muss sie die ordnungsgemäße Einrichtung eines Verfahrens zur Durchführung von Zertifizierungen sicherstellen und eigene Zertifizierungskriterien ausarbeiten oder annehmen. Darüber hinaus fällt jeder Aufsichtsbehörde, die Zertifizierungen erteilt, die Aufgabe zu, diese regelmäßig zu überprüfen (Artikel 57 Absatz 1 Buchstabe o), und sie hat die Befugnis, diese zu widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden (Artikel 58 Absatz 2 Buchstabe h). Um diese Anforderungen zu erfüllen, empfiehlt sich die Einrichtung eines Verfahrens für die Durchführung von Zertifizierungen sowie verfahrenstechnische Anforderungen und – sofern nicht z. B. durch nationale Rechtsvorschriften anderweitig festgelegt – die Umsetzung rechtlich durchsetzbarer Vereinbarungen über die Erbringung von Zertifizierungsleistungen mit den einzelnen antragstellenden Organisationen. Hierbei sollte sichergestellt sein, dass der Antragsteller durch diese Zertifizierungsvereinbarung verpflichtet wird, zumindest die Zertifizierungskriterien einzuhalten, was die notwendigen Schritte für die Durchführung der Evaluierung und für die Überwachung der Einhaltung der Kriterien ebenso einschließt wie die regelmäßige Überprüfung einschließlich des Zugangs zu Informationen und/oder Räumlichkeiten, die Dokumentation, die Veröffentlichung von Berichten und Ergebnissen und die Bearbeitung etwaiger Beschwerden. Darüber hinaus wird von jeder Aufsichtsbehörde erwartet, dass sie neben den Anforderungen von Artikel 43 Absatz 2 auch die Anforderungen der Leitlinien zur Akkreditierung von Zertifizierungsstellen erfüllt.

2.2 Weitere Aufgaben der Aufsichtsbehörde im Zusammenhang mit der Zertifizierung

24. In Mitgliedstaaten, in denen Zertifizierungsstellen ihre Tätigkeit aufnehmen, ist die Aufsichtsbehörde unbeschadet ihrer eigenen Tätigkeiten befugt und dafür zuständig,

- die Kriterien für die Zertifizierungsprogramme zu bewerten und einen Beschlussentwurf zu erstellen (Artikel 42 Absatz 5),
- den Beschlussentwurf dem Ausschuss zu übermitteln, falls sie beabsichtigt, die Zertifizierungskriterien zu billigen (Artikel 64 Absatz 1 Buchstabe c, Artikel 64 Absatz 7), und der Stellungnahme des Ausschusses Rechnung zu tragen (Artikel 64 Absatz 1 Buchstabe c, Artikel 70 Absatz 1 Buchstabe t),
- die Zertifizierungskriterien zu billigen (Artikel 58 Absatz 3 Buchstabe f), bevor die Akkreditierung und die Zertifizierung erfolgen können (Artikel 42 Absatz 5 und Artikel 43 Absatz 2 Buchstabe b),
- die Zertifizierungskriterien zu veröffentlichen (Artikel 43 Absatz 6),
- als die zuständige Behörde für EU-weite Zertifizierungsprogramme zu fungieren, was zu dem vom Europäischen Datenschutzausschuss genehmigten Europäischen Datenschutzsiegel führen kann (Artikel 42 Absatz 5 und Artikel 70 Absatz 1 Buchstabe o), und
- eine Zertifizierungsstelle anzuweisen, a) keine Zertifizierung zu erteilen, oder b) eine Zertifizierung zu widerrufen, wenn die Voraussetzungen für die Zertifizierung

(Zertifizierungsverfahren oder -kriterien) nicht oder nicht mehr erfüllt werden (Artikel 58 Absatz 2 Buchstabe h).

25. Die Aufsichtsbehörde hat nach der DSGVO die Aufgabe, Zertifizierungskriterien zu billigen, wird aber nicht dazu verpflichtet, solche zu entwickeln. Jede Aufsichtsbehörde sollte im Hinblick auf die Billigung der Zertifizierungskriterien gemäß Artikel 42 Absatz 5 klare Erwartungen haben. Dies gilt insbesondere für den Anwendungsbereich und den Inhalt des Nachweises der Einhaltung der DSGVO sowie für ihre Aufgabe, die Anwendung der Verordnung zu überwachen und durchzusetzen. Im Anhang finden sich Leitlinien für die Sicherstellung eines harmonisierten Vorgehens bei der Bewertung von Kriterien im Hinblick auf deren etwaige Billigung.

26. Nach Artikel 43 Absatz 1 sind die Zertifizierungsstellen vor der Erteilung oder Verlängerung von Zertifizierungen zur Unterrichtung ihrer zuständigen Aufsichtsbehörde verpflichtet, damit diese ihre Abhilfebefugnisse gemäß Artikel 58 Absatz 2 Buchstabe h ausüben kann. Darüber hinaus müssen die Zertifizierungsstellen nach Artikel 43 Absatz 5 der zuständigen Aufsichtsbehörde die Gründe für die Erteilung oder den Widerruf der beantragten Zertifizierung mitteilen. Die Aufsichtsbehörden können die Modalitäten des Eingangs, der Bestätigung, der Prüfung und des operativen Umgangs mit diesen Informationen nach der DSGVO festlegen (zum Beispiel unter Einbeziehung technischer Lösungen für die Berichterstattung durch die Zertifizierungsstellen), möglich ist aber auch die Einrichtung eines Prozesses mit Kriterien für die Verarbeitung der Informationen und Berichte, die zu jedem erfolgreichen Zertifizierungsprojekt von der Zertifizierungsstelle gemäß Artikel 43 Absatz 1 übermittelt werden. Auf der Grundlage dieser Informationen kann die Aufsichtsbehörde ihre Befugnis ausüben, die Zertifizierungsstelle anzuweisen, eine Zertifizierung zu widerrufen oder keine Zertifizierung zu erteilen (Artikel 58 Absatz 2 Buchstabe h), sowie die Anwendung der Zertifizierungsanforderungen und -kriterien im Sinne der DSGVO zu überwachen und durchzusetzen (Artikel 57 Absatz 1 Buchstabe a und Artikel 58 Absatz 2 Buchstabe h). Dies fördert zum einen harmonisierten Ansatz und zum anderen die Vergleichbarkeit von durch unterschiedliche Zertifizierungsstellen vorgenommenen Zertifizierungen und bewirkt zudem, dass die Aufsichtsbehörden über den Zertifizierungsstatus einer Organisation auf dem Laufenden gehalten werden.

3 DIE ROLLE DER ZERTIFIZIERUNGSSTELLE

27. Die Rolle der Zertifizierungsstelle besteht darin, auf der Grundlage eines Zertifizierungssystems und genehmigter Kriterien (Artikel 43 Absatz 1) Zertifizierungen zu erteilen, zu überprüfen, zu verlängern und zu widerrufen (Artikel 42 Absätze 5 und 7). Jede Zertifizierungsstelle und jeder (Zertifizierungs-) Programmeigner ist demnach verpflichtet, Zertifizierungskriterien und Verfahren für eine Zertifizierung festzulegen und einzurichten, was Verfahren zur Kontrolle der Vorschrifteneinhaltung, zur Überprüfung, zur Bearbeitung von Beschwerden und für den Widerruf einschließt. Die Zertifizierungskriterien werden im Rahmen des Akkreditierungsprozesses nach Maßgabe der Vorschriften und Verfahren überprüft, die

für die Erteilung von Zertifizierungen, Siegeln oder Prüfzeichen gelten (Artikel 43 Absatz 2 Buchstabe c).

28. Das Vorhandensein eines Verfahrens für die Zertifizierung und von Zertifizierungskriterien ist eine notwendige Voraussetzung für die erfolgreiche Akkreditierung einer Zertifizierungsstelle gemäß Artikel 43. Der Anwendungsbereich und die Art der Zertifizierungskriterien, einschließlich ihrer Interdependenz mit den Zertifizierungsverfahren, haben wesentliche Auswirkungen auf die Tätigkeit einer Zertifizierungsstelle. Beispielsweise können bestimmte Kriterien bestimmte Evaluierungsmethoden wie etwa Inspektionen vor Ort oder Kodexüberprüfungen erforderlich machen. Diese Verfahren sind für die Akkreditierung zwingend vorgeschrieben und werden in den Leitlinien für die Akkreditierung näher erläutert.

29. Gemäß der DSGVO muss die Zertifizierungsstelle den Aufsichtsbehörden Informationen übermitteln, insbesondere zu Einzelzertifizierungen. Dies ergibt sich aus der Notwendigkeit, die Anwendung des Zertifizierungsmechanismus zu überwachen (Artikel 42 Absatz 7, Artikel 43 Absatz 5, Artikel 58 Absatz 2 Buchstabe h).

4 GENEHMIGUNG VON ZERTIFIZIERUNGSKRITERIEN

30. Die Zertifizierungskriterien sind ein fester Bestandteil eines jeden Zertifizierungsmechanismus. Dementsprechend sieht die DSGVO vor, dass die Zertifizierungskriterien der Genehmigung durch die zuständige Aufsichtsbehörde unterliegen (Artikel 42 Absatz 5 und Artikel 43 Absatz 2 Buchstabe b). Im Falle des Europäischen Datenschutzsiegels unterliegen die Zertifizierungskriterien der Genehmigung durch den Europäischen Datenschutzausschuss (Artikel 42 Absatz 5 und Artikel 70 Absatz 1 Buchstabe o). Beide Möglichkeiten für die Genehmigung der Zertifizierungskriterien werden nachstehend erläutert.

31. Der Europäische Datenschutzausschuss (EDSA) erkennt folgende Zwecke für die Genehmigung von Zertifizierungskriterien an:

    - die ordnungsgemäße Widerspiegelung der in der Verordnung (EU) 2016/679 niedergelegten Anforderungen und Grundsätze betreffend den Schutz natürlicher Personen im Hinblick auf die Verarbeitung personenbezogener Daten und
    - die Leistung eines Beitrags zur einheitlichen Anwendung der DSGVO.

32. In Bezug auf den Zertifizierungsmechanismus sieht die DSGVO als Voraussetzung für die Genehmigung vor, dass die Verantwortlichen und die Auftragsverarbeiter dadurch in die Lage versetzt werden, die Einhaltung der DSGVO nachzuweisen. Damit die Genehmigung erteilt werden kann, muss dies in den Zertifizierungskriterien vollständig widergespiegelt werden.

4.1 Genehmigung der Kriterien durch die zuständige Aufsichtsbehörde

33. Die Zertifizierungskriterien müssen vor oder während des Akkreditierungsprozesses für eine Zertifizierungsstelle von der zuständigen Aufsichtsbehörde genehmigt werden. Auch für aktualisierte oder zusätzliche Programme oder Kriterienkataloge nach ISO 17065 derselben Zertifizierungsstelle ist vor der Verwendung dieser geänderten Zertifizierungsangebote eine Genehmigung erforderlich (Artikel 42 Absatz 5 und Artikel 43 Absatz 2 Buchstabe b). Die

Aufsichtsbehörden müssen Anträge auf Genehmigung von Zertifizierungskriterien fair und unterschiedslos nach Maßgabe eines öffentlich zugänglichen Verfahrens behandeln, das die zu erfüllenden allgemeinen Bedingungen präzisiert und eine Beschreibung des Genehmigungsprozesses enthält.

34. Jede Zertifizierungsstelle darf Zertifizierungen gemäß den durch die Aufsichtsbehörde im jeweiligen Mitgliedstaat gebilligten Kriterien nur in diesem bestimmten Mitgliedstaat erteilen. Anders ausgedrückt: Die Zertifizierungskriterien müssen von der zuständigen Aufsichtsbehörde des Mitgliedstaats gebilligt worden sein, in dem die Zertifizierungsstelle Zertifizierungen anbieten möchte und ihre Akkreditierung erhält. Siehe auch den nachfolgenden Abschnitt zu den europaweiten Zertifizierungsprogrammen.

4.2 Genehmigung der Kriterien für das Europäische Datenschutzsiegel durch den Europäischen Datenschutzausschuss

35. Eine Zertifizierungsstelle kann auch Zertifizierungen nach Maßgabe der vom EDSA für ein Europäisches Datenschutzsiegel genehmigten Kriterien erteilen. Die vom EDSA gemäß Artikel 63 genehmigten Zertifizierungskriterien können zu einem Europäischen Datenschutzsiegel führen (Artikel 42 Absatz 5). Angesichts der bestehenden Zertifizierungs- und Akkreditierungsvereinbarungen erkennt der EDSA an, dass es wünschenswert ist, eine Fragmentierung des Marktes für Datenschutzzertifizierungen zu vermeiden. Er weist darauf hin, dass die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission gemäß Artikel 42 Absatz 1 insbesondere auf Unionsebene die Einführung von Zertifizierungsverfahren fördern sollen.

4.2.1 Der Antrag auf Genehmigung

36. Der Antrag auf Genehmigung der Kriterien nach Artikel 42 Absatz 5 und Artikel 70 Absatz 1 Buchstabe o durch den EDSA muss über eine zuständige Aufsichtsbehörde eingereicht werden und die Absicht des Programmeigners, des Kandidaten oder der akkreditierten Zertifizierungsstelle widerspiegeln, die Kriterien im Rahmen eines Zertifizierungsverfahrens anzubieten, das sich an die Verantwortlichen und die Auftragsverarbeiter in allen Mitgliedstaaten richtet. Wenn die zuständige Aufsichtsbehörde der Ansicht ist, dass eine Genehmigung der Kriterien durch den EDSA möglich ist, übermittelt sie dem EDSA einen Entwurf.

37. Die Entscheidung, in welchem Mitgliedstaat die Genehmigung der Kriterien zu beantragen ist, richtet sich nach dem Sitz der (Zertifizierungs-) Programmeigner bzw. Zertifizierungsstellen.

38. Die antragstellende Zertifizierungsstelle befindet sich im Regelfall in der Phase der Akkreditierungsbeantragung oder hat die Akkreditierung bereits von der zuständigen Aufsichtsbehörde oder von der nationalen Akkreditierungsstelle ihres Mitgliedstaats erhalten. Ist eine Zertifizierungsstelle bereits für ein datenschutzrechtliches Zertifizierungsverfahren akkreditiert, kann dies dazu beitragen, den Genehmigungsprozess zu straffen.

4.2.2 Die Kriterien für das Europäische Datenschutzsiegel

39. Der EDSA koordiniert den Bewertungsprozess und genehmigt gegebenenfalls die Kriterien für das Europäische Datenschutzsiegel. Im Rahmen der Bewertung werden u. a. der Anwendungsbereich der Kriterien und die Eignung für die allgemeine Zertifizierung behandelt. Falls der EDSA die Kriterien genehmigt, wird von der zuständigen Aufsichtsbehörde für die Hauptniederlassung der Zertifizierungsstelle in der EU die Bearbeitung etwaiger Beschwerden über das Verfahren selbst und die Benachrichtigung der anderen Aufsichtsbehörden erwartet. Die Aufsichtsbehörde ist auch dafür zuständig, etwaige Maßnahmen gegen die Zertifizierungsstelle zu ergreifen. Die anderen Aufsichtsbehörden und der EDSA sind von der zuständigen Aufsichtsbehörde gegebenenfalls zu benachrichtigen.

40. Zertifizierungskriterien für eine gemeinsame Zertifizierung müssen EU-weiten Anforderungen genügen und sollten daher ein spezifisches Verfahren für die Erfüllung dieser Anforderungen vorsehen. Die Verfahren für europäische Zertifizierungsmechanismen müssen für den Einsatz in sämtlichen Mitgliedstaaten ausgelegt sein. Nach Artikel 42 Absatz 5 müssen die Verfahren und Kriterien für ein Europäisches Datenschutzsiegel angepasst werden können, so dass gegebenenfalls sektorspezifische nationale Rechtsvorschriften (beispielsweise für die Datenverarbeitung in Schulen) berücksichtigt werden, und sie müssen eine EU-weite Anwendung vorsehen.

41. Beispiel: Eine internationale Schule, die betroffenen Personen in der Union eine schulische Ausbildung anbietet, hat ihren Sitz im Mitgliedstaat A. Um das Europäische Datenschutzsiegel verliehen zu bekommen, möchte die Schule ihr Online-Bewerbungsverfahren im Rahmen eines EU-weiten Zertifizierungsprogramms zertifizieren lassen. Die Schule strebt die Beantragung einer Zertifizierung der Verarbeitungsvorgänge auf Grundlage des Europäischen Datenschutzsiegels an, die von einer Zertifizierungsstelle mit Sitz im Mitgliedstaat B angeboten wird. Die in dem entsprechenden Verfahren vorgesehenen und dokumentierten Kriterien für das Siegel müssen den im Mitgliedstaat A geltenden Vorschriften für Schulen gerecht werden. Laut den Kriterien sollen im Rahmen des Online-Bewerbungsverfahrens der Schule unbedingt auch Informationen über die geltenden Datenschutzanforderungen des Mitgliedstaats, die sich eventuell von den Regelungen in anderen Mitgliedstaaten unterscheiden, bereitgestellt und berücksichtigt werden. Als Beispiel seien hier die personenbezogenen Daten, die im Rahmen von Bewerbungen zu übermitteln sind (z. B. Vorschulnoten oder Prüfungsergebnisse), die unterschiedlichen Speicherfristen, die Erhebung und Verarbeitung finanzieller oder biometrischer Daten sowie die Einschränkungen bei der weiteren Verarbeitung genannt.

- Die Kriterien, die für die Genehmigung von Zertifizierungsprogrammen zum Europäischen Datenschutzsiegel festgelegt werden, sollen folgendes beinhalten
  - vom Ausschuss genehmigte Kriterien,
  - eine rechtsordnungsübergreifende Anwendung im Einklang mit etwaigen einschlägigen nationalen rechtlichen Anforderungen und sektorspezifischen Vorschriften,

- harmonisierte Kriterien, die an die nationalen Anforderungen angepasst werden können,

- eine Beschreibung der Spezifizierung der Zertifizierungsverfahren,
- die Zertifizierungsvereinbarungen mit der Anerkennung paneuropäischer Anforderungen,
- Verfahren, die landesspezifische Abweichungen zulassen, entsprechende Lösungen bereitstellen und sicherstellen, dass das Siegel zum Nachweis der Konformität mit der Datenschutz-Grundverordnung beiträgt, und
- die Sprache der Berichte, die sich an alle betroffenen Aufsichtsbehörden richten.

42. Im Anhang finden sich ebenfalls Empfehlungen zu den Kriterien für das Europäische Datenschutzsiegel.

4.2.3 Die Funktion der Akkreditierung

43. Wie in Abschnitt 4.2.1 festgestellt, können – sofern die Kriterien für die gemeinsame Zertifizierung für angemessen befunden und entsprechend vom Ausschuss nach Artikel 42 Absatz 5 genehmigt wurden – die Zertifizierungsstellen per Akkreditierung dazu befugt werden, Zertifizierungen nach Maßgabe dieser Kriterien auf Unionsebene durchzuführen.

44. Systeme, die nur in bestimmten Mitgliedstaaten angeboten werden sollen, stehen für die EU-Siegel nicht zur Auswahl. Um für den Anwendungsbereich des Europäischen Datenschutzsiegels akkreditiert zu werden, ist eine Akkreditierung in dem Mitgliedstaat erforderlich, in dem die Zertifizierungsstelle, die dieses System verwenden möchte, d. h. die für die Erteilung von Zertifizierungen und für die Verwaltung der Zertifizierungstätigkeiten ihrer Einrichtungen und Nebenstellen in anderen Mitgliedstaaten verantwortlich ist, ihre Hauptniederlassung hat. Falls andere Niederlassungen Zertifizierungen autonom steuern und durchführen, ist für jede dieser Niederlassungen oder Stellen eine eigene Akkreditierung in dem Mitgliedstaat erforderlich, in dem sich ihr Sitz befindet. Anders ausgedrückt: Falls ausschließlich die Hauptniederlassung Zertifikate erteilt, ist eine Akkreditierung ausschließlich in dem Mitgliedstaat erforderlich, in dem die Zertifizierungsstelle ihren Hauptsitz hat. Erteilen andere Niederlassungen der Zertifizierungsstelle ebenfalls Zertifikate, müssen diese jedoch ebenfalls akkreditiert werden.

45. Wenn eine Zertifizierungsstelle nicht im Wege der Akkreditierung dazu befugt wurde, Zertifizierungen gemäß dem Europäischen Datenschutzsiegel durchzuführen, können die vom EDSA genehmigten Kriterien folglich nicht zum Einsatz kommen, und das Siegel darf nicht verliehen werden.

5 AUSARBEITUNG VON ZERTIFIZIERUNGSKRITERIEN

46. Die DSGVO bestimmt den Rahmen für die Ausarbeitung von Zertifizierungskriterien. Während in den Artikeln 42 und 43 die grundlegenden Anforderungen in Bezug die Durchführung der Zertifizierung behandelt und auch wesentliche Kriterien für die Zertifizierungsverfahren

vorgelegt werden, muss die Grundlage für die Zertifizierungskriterien aus den Grundsätzen und Vorschriften der DSGVO abgeleitet werden und zur sicheren Erfüllung dieser Kriterien beitragen.

47. Bei der Ausarbeitung von Zertifizierungskriterien sollte der Schwerpunkt auf ihre Überprüfbarkeit, Tragweite und Eignung im Hinblick auf den Nachweis der Einhaltung der Verordnung gelegt werden. Die Zertifizierungskriterien sollten klar und verständlich formuliert sein und die praktische Anwendung zulassen.

48. Bei der Abfassung von Zertifizierungskriterien sind insbesondere zur Unterstützung der Bewertung der Verarbeitungsvorgänge gegebenenfalls folgende Konformitätsaspekte zu berücksichtigen:

- die Rechtmäßigkeit der Verarbeitung nach Artikel 6,
- die Grundsätze der Datenverarbeitung nach Artikel 5,
- die Rechte der betroffenen Personen nach den Artikeln 12 bis 23,
- die Meldepflicht bei Datenschutzverletzungen nach Artikel 33,
- die Pflicht zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen nach Artikel 25,
- eine etwaige erfolgte Datenschutz-Folgenabschätzung nach Artikel 35 Absatz 7 Buchstabe d und
- die gemäß Artikel 32 eingeführten technischen und organisatorischen Maßnahmen.

49. Das Ausmaß, in dem sich diese Erwägungen in den Kriterien widerspiegeln, kann je nach Anwendungsbereich der Zertifizierung, zu dem etwa die Art der Verarbeitungsvorgänge und der betreffende Bereich (z. B. der Gesundheitsbereich) der Zertifizierung gehören können, variieren.

5.1 Was kann nach der DSGVO zertifiziert werden?

50. Solange der Schwerpunkt auf der Unterstützung des Nachweises liegt, dass diese Verordnung von den Verantwortlichen und Auftragsverarbeitern bei Verarbeitungsvorgängen eingehalten wird (Artikel 42 Absatz 1), ist nach Ansicht des EDSA das Spektrum dessen, was nach der DSGVO zertifiziert werden kann, breit gefächert.

51. Bei der Bewertung eines Verarbeitungsvorgangs sind gegebenenfalls folgende drei Kernelemente zu berücksichtigen:

1. die personenbezogenen Daten (sachlicher Anwendungsbereich der DSGVO),
2. die technischen Systeme – die zur Verarbeitung der personenbezogenen Daten verwendete Infrastruktur, wie etwa Hardware und Software, und
3. die mit den Verarbeitungsvorgängen verbundenen Prozesse und Verfahren.

52. Jedes in den Verarbeitungsvorgängen verwendete Element ist einer Bewertung im Hinblick auf festgelegte Kriterien zu unterziehen. Hier können mindestens vier verschiedene Faktoren einen nennenswerten Einfluss ausüben: 1) die Organisation und Rechtsform des Verantwortlichen oder Auftragsverarbeiters, 2) die an den Verarbeitungsvorgängen beteiligte(n) Abteilung, Umgebung und Personen, 3) die technische Beschreibung der zu bewertenden Elemente und 4) die IT-Infrastruktur zur Unterstützung des Verarbeitungsvorgangs einschließlich der Betriebssysteme, virtuellen Systeme, Datenbanken, Authentifizierungs- und Autorisierungssysteme, Router und Firewalls, Speichersysteme und Kommunikationsinfrastruktur bzw. des Internetzugangs und der damit verbundenen technischen Maßnahmen.

53. Für die Gestaltung der Zertifizierungsverfahren und -kriterien sind alle drei Kernelemente relevant. Sie können je nach Zertifizierungsgegenstand in unterschiedlichem Umfang berücksichtigt werden. Beispielsweise können einige Elemente in bestimmten Fällen vernachlässigt werden, wenn sie als nicht relevant für den Zertifizierungsgegenstand gelten.

54. Zur weiteren Festlegung dessen, was nach der DSGVO zertifiziert werden kann, finden sich in der Verordnung zusätzliche Orientierungshilfen. Aus Artikel 42 Absatz 7 folgt, dass Zertifizierungen nach der DSGVO ausschließlich den Verantwortlichen und Auftragsverarbeitern erteilt werden dürfen, was etwa die Zertifizierung von Datenschutzbeauftragten ausschließt. In Artikel 43 Absatz 1 Buchstabe b wird auf die Norm ISO 17065 verwiesen, die die Akkreditierung von Zertifizierungsstellen vorsieht, welche die Konformität von Produkten, Dienstleistungen und Prozessen bewerten. In der Terminologie der ISO 17065 können ein oder mehrere Verarbeitungsvorgänge ein Produkt oder eine Dienstleistung ergeben, das bzw. die einer Zertifizierung unterliegen kann. Die Verarbeitung von Beschäftigtendaten zum Zwecke der Gehaltszahlung oder der Urlaubsverwaltung entspricht zum Beispiel Verarbeitungsvorgängen im Sinne der DSGVO und kann in der Terminologie der ISO zu einem Produkt, einem Prozess oder einer Dienstleistung führen.

55. Auf der Grundlage dieser Erwägungen vertritt der EDSA die Auffassung, dass der Zertifizierungsbereich nach der DSGVO auf Verarbeitungsvorgänge bzw. Vorgangsreihen ausgerichtet ist. Diese können Steuerungsprozesse im Sinne von organisatorischen Maßnahmen beinhalten, die dementsprechend fester Bestandteil eines Verarbeitungsvorgangs sind (z. B. der zur Bearbeitung etwaiger Beschwerden eingerichtete Steuerungsprozess als Teilprozess der Verarbeitung von Beschäftigtendaten zum Zwecke der Gehaltszahlung).

56. Damit die Konformität des Verarbeitungsvorgangs mit den Zertifizierungskriterien bewertet werden kann, muss ein Anwendungsfall vorgelegt werden. Inwieweit die eingesetzte technische Infrastruktur, die im Rahmen eines Verarbeitungsvorgangs genutzt wird, eine solche Konformität gewährleistet, hängt zum Beispiel von den Kategorien der Daten ab, die dabei verarbeitet werden sollen. Die organisatorischen Maßnahmen richten sich nach den Kategorien und Datenmengen sowie nach der für die Verarbeitung genutzten technischen Infrastruktur, wobei die Art, der Anwendungsbereich, der Inhalt und die Zwecke der Verarbeitung sowie die Risiken für die Rechte und Freiheiten der betroffenen Personen berücksichtigt werden müssen.

57. Darüber hinaus darf nicht vergessen werden, dass große Unterschiede zwischen den IT-Anwendungen bestehen können, auch wenn sie dem gleichen Verarbeitungszweck dienen. Entsprechend muss dies bei der Festlegung des Anwendungsbereichs der

Zertifizierungsmechanismen und Abfassung der Zertifizierungskriterien berücksichtigt werden, d. h. der Anwendungsbereich einer Zertifizierung und die betreffenden Kriterien dürfen nicht so eng gefasst werden, dass anders ausgelegte IT-Anwendungen ausgeschlossen werden.

5.2 Festlegung des Zertifizierungsgegenstands

58. Bei den einzelnen Zertifizierungsprojekten im Rahmen eines Zertifizierungsmechanismus ist der Anwendungsbereich des Letzteren von dessen Gegenstand – auch Evaluierungsgegenstand (EVG) genannt – zu unterscheiden. Der Anwendungsbereich eines Zertifizierungsmechanismus kann entweder allgemein oder auf eine bestimmte Art bzw. einen bestimmten Bereich von Verarbeitungsvorgängen festgelegt sein und so bereits die Zertifizierungsgegenstände bestimmen, die in den Anwendungsbereich des Zertifizierungsmechanismus fallen (z. B. die sichere Speicherung und der Schutz personenbezogener Daten in einem digitalen Safe). Eine zuverlässige, aussagekräftige Bewertung der Konformität kann immer nur dann stattfinden, wenn der jeweilige Gegenstand eines Zertifizierungsprojekts genau beschrieben ist. Aus der Beschreibung muss neben den Kernelementen (d. h. den bewerteten bzw. von einer Bewertung ausgeschlossenen Daten, Vorgängen und technischen Infrastrukturen) klar ersichtlich sein, welche Verarbeitungsvorgänge der Zertifizierungsgegenstand beinhaltet. Dabei müssen auch stets die Schnittstellen zu anderen Prozessen berücksichtigt und beschrieben werden. Ist etwas nicht bekannt, kann es natürlich nicht Teil der Bewertung und demzufolge auch nicht Gegenstand der Zertifizierung sein. In jedem Fall muss das einzelne Zertifizierungsobjekt Aussagekraft für die durch die Zertifizierung getroffene Feststellung und den dabei erhobenen Anspruch besitzen und darf Nutzer, Kunden und Verbraucher nicht in die Irre führen.

59. [Beispiel 1]

    Eine Bank stellt ihren Kunden eine Website zum Zwecke des Online-Bankings bereit. Im Rahmen dieser Dienstleistung können Überweisungen getätigt, Aktien erworben, Daueraufträge eingerichtet und das Konto verwaltet werden. Die Bank strebt eine Zertifizierung gemäß einem Datenschutz-Zertifizierungsverfahren mit einem allgemeinen Anwendungsbereich auf Grundlage generischer Kriterien an, die für Folgendes gelten soll:

    a) Sichere Anmeldung

       Bei der sicheren Anmeldung handelt es sich um einen für den Nutzer nachvollziehbaren Datenverarbeitungsvorgang, der datenschutzrechtlich insofern relevant ist, als er entscheidend zur Sicherheit der betreffenden personenbezogenen Daten beiträgt. Der Verarbeitungsvorgang ist mithin für die sichere Anmeldung erforderlich und kann somit einen aussagekräftigen EVG darstellen, wenn aus dem Zertifikat klar hervorgeht, dass sich die Zertifizierung ausschließlich auf den Verarbeitungsvorgang für die Anmeldung bezieht.

    b) Web-Benutzeroberfläche

       Die Web-Benutzeroberfläche ist zwar datenschutzrechtlich relevant, kann aber, weil hier keine Nachvollziehbarkeit für den Endnutzer gegeben ist, keinen aussagekräftigen EVG darstellen. Auch ist für den Nutzer nicht ersichtlich, welche auf der Website

angebotenen Dienstleistungen (und somit welche Verarbeitungsvorgänge) von der Zertifizierung abgedeckt sind.

c) Online-Banking

Die Web-Benutzeroberfläche steht im Zusammenspiel mit dem Back-End für Verarbeitungsvorgänge, die im Rahmen der Online-Banking-Dienstleistungen bereitgestellt werden und für den Nutzer Aussagekraft haben können. Vor diesem Hintergrund müssen beide Teil des EVG sein. Nicht direkt mit der Bereitstellung der Online-Banking-Dienstleistungen verbundene Verarbeitungsvorgänge, wie etwa solche zur Verhinderung von Geldwäsche, müssen hingegen nicht zum EVG gehören.

Die von der Bank über ihre Website angebotenen Online-Banking-Dienstleistungen können indessen auch andere Dienstleistungen beinhalten, die ihrerseits eigene Verarbeitungsvorgänge erforderlich machen. Das Anbieten eines Versicherungsprodukts beispielsweise kann in diesem Zusammenhang zu solchen anderen Dienstleistungen gehören. Da diese zusätzliche Dienstleistung (Versicherung) nicht direkt mit dem Zweck der Bereitstellung von Online-Banking-Dienstleistungen verknüpft ist, ist es möglich, sie nicht zum EVG zu zählen. In diesem Fall gelten dann jedoch die auf der Website integrierten diesbezüglichen Benutzerschnittstellen als Teil des EVG und müssen folglich beschrieben werden, um eine saubere Trennung zwischen den Dienstleistungen zu vollziehen. Diese Beschreibung ist notwendig, um mögliche Datenströme zwischen den beiden Dienstleistungen ermitteln und evaluieren zu können.

60. [Beispiel 2]

Eine Bank bietet ihren Kunden eine Dienstleistung an, die es diesen ermöglicht, Informationen zu verschiedenen Konten und Kreditkarten bei mehreren Banken zusammenzufassen (Kontenzusammenfassung). Die Bank strebt eine Zertifizierung ihrer Dienstleistung nach der DSGVO an. Die zuständige Aufsichtsbehörde hat einen spezifischen Kriterienkatalog genehmigt, der sich auf diese Tätigkeit bezieht. Der Anwendungsbereich des Zertifizierungsmechanismus bezieht sich in diesem Fall nur auf folgende Konformitätsaspekte:

- Authentisierung des Benutzers und
- die zulässigen Lösungen zur Einholung der zusammenzufassenden Daten bei anderen Banken bzw. Diensten.

Da der EVG als solcher durch den Anwendungsbereich dieses Zertifizierungsmechanismus festgelegt ist, ist es nicht möglich, eine aussagekräftige Eingrenzung des EVG im Rahmen des vorgeschlagenen Anwendungsbereichs vorzunehmen und lediglich bestimmte Funktionen oder einen einzigen bestimmten Verarbeitungsvorgang zu zertifizieren. In diesem Szenario muss der EVG einem bestimmten Anwendungsbereich entsprechen.

5.3 Evaluierungsmethoden und Vorgehensweise bei der Bewertung

61. Für eine Konformitätsbewertung zur Unterstützung des Nachweises, dass die Verarbeitungsvorgänge die Anforderungen erfüllen, müssen die Evaluierungsmethoden und

die Vorgehensweise bei der Bewertung ermittelt und festgelegt werden. Maßgeblich ist hierbei, ob die für die Bewertung herangezogenen Informationen nur aus der Dokumentation stammen (was an sich nicht ausreichen würde), oder ob sie aktiv vor Ort durch unmittelbaren bzw. mittelbaren Zugang erhoben wurden. Die Art und Weise, in der Informationen erhoben werden, wirkt sich auf die Tragweite der Zertifizierung aus und sollte daher festgelegt und beschrieben werden.

Die Verfahren für die Erteilung und regelmäßige Überprüfung von Zertifizierungen sollten Spezifikationen beinhalten, anhand derer der angemessene Bewertungsgrad (Tiefe und Granularität) für die Erfüllung der Zertifizierungskriterien bestimmt werden kann, und Folgendes umfassen:

- Informationen über die bzw. Spezifikationen der angewandten Bewertungsmethoden und -ergebnisse, die z. B. im Rahmen von Audits vor Ort oder aus der Dokumentation erhoben wurden,
- Evaluierungsmethoden mit Schwerpunkt auf den Verarbeitungsvorgängen (Daten, Systeme, Prozesse) und dem Verarbeitungszweck,
- Angabe der Datenkategorien, des Schutzbedarfs und ob Auftragsverarbeiter oder Dritte beteiligt sind,
- Angabe der Rollen und des etwaigen Bestehens eines Verfahrens zur Zugangssteuerung auf der Grundlage von Rollen und Zuständigkeiten.

62. Die Evaluierungstiefe wirkt sich auf die Tragweite und den Wert einer Zertifizierung aus. Eine aus pragmatischen Gründen oder zwecks Kosteneinsparung gewählte geringere Evaluierungstiefe schmälert die Tragweite der Datenschutzzertifizierung. Andererseits können Entscheidungen hinsichtlich der Granularität der Evaluierung nicht nur die finanziellen Möglichkeiten des Antragstellers, sondern oft auch die Kapazitäten der Gutachter und Prüfer übersteigen. Für den Nachweis der Konformität ist es, um die Aussagekraft zu wahren, unter Umständen nicht in allen Fällen erforderlich, eine äußerst genaue Analyse der eingesetzten IT-Systeme durchzuführen.

5.4 Dokumentation der Bewertung

63. Die Dokumentation zur Zertifizierung sollte gründlich und vollständig sein. Ohne diese Dokumentation ist eine ordnungsgemäße Bewertung nicht möglich. Die wesentliche Funktion der Dokumentation zur Zertifizierung besteht darin, für die Transparenz des Evaluierungsprozesses im Rahmen des Zertifizierungsverfahrens zu sorgen. Die Dokumentation liefert Antworten auf Fragen im Zusammenhang mit den rechtlich vorgegebenen Anforderungen. In den Zertifizierungsmechanismen sollte eine einheitliche Methodik für die Erstellung der Dokumentation vorgesehen werden. Bei der Evaluierung kann sodann die Dokumentation zur Zertifizierung im Lichte der Zertifizierungskriterien mit dem Ist-Zustand vor Ort verglichen werden.

64. Eine umfassende Dokumentation dessen, was zertifiziert wurde (einschließlich der dabei zugrunde gelegten Methodik), fördert die Transparenz. Gemäß Artikel 43 Absatz 2 Buchstabe c sollten durch die Zertifizierungsmechanismen Maßnahmen festgelegt werden, die eine Überprüfung der Zertifizierungen ermöglichen. Für die von der Aufsichtsbehörde vorzunehmende Prüfung, ob und in welchem Umfang die Zertifizierung im Rahmen amtlicher Untersuchungen anerkannt werden kann, ist eine ausführliche Dokumentation das vielleicht zweckmäßigste Kommunikationsmittel. Die im Rahmen der Evaluierung erstellte Dokumentation sollte sich daher auf drei wesentliche Aspekte konzentrieren:

- Konsistenz und Kohärenz der angewandten Evaluierungsmethoden,
- Evaluierungsmethoden zum Nachweis der Übereinstimmung des Zertifizierungsobjekts mit den Zertifizierungskriterien (und somit mit der Verordnung) und
- erfolgte Validierung der Evaluierungsergebnisse durch eine unabhängige und unparteiische Zertifizierungsstelle.

5.5 Dokumentation der Ergebnisse

65. In Erwägungsgrund 100 finden sich Informationen zu den Zielen, die mit der Einführung der Zertifizierung verfolgt werden:

„Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsmechanismen sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen."

66. Bei der Erhöhung der Transparenz spielen die Dokumentation und die Vermittlung von Ergebnissen eine wichtige Rolle. Zertifizierungsstellen mit Zertifizierungsmechanismen, Siegeln oder Prüfzeichen, die auf die betroffenen Personen (als Verbraucher oder Kunden) ausgerichtet sind, sollten leicht zugängliche, verständliche und aussagekräftige Informationen über die zertifizierten Verarbeitungsvorgänge bereitstellen. Diese öffentlichen Informationen sollten mindestens Folgendes umfassen:

- eine Beschreibung des EVG,
- Verweise auf die genehmigten Kriterien, die auf den spezifischen EVG angewandt wurden,
- die Methodik für die Evaluierung der Kriterien (Evaluierung vor Ort, Dokumentation, usw.) und
- die Gültigkeitsdauer des Zertifikats, und
- außerdem sollten sie die Ergebnisse für die Aufsichtsbehörden und die Öffentlichkeit vergleichbar machen.

6 LEITLINIEN FÜR DIE FESTLEGUNG VON ZERTIFIZIERUNGSKRITERIEN

67. Zertifizierungskriterien sind ein fester Bestandteil des Zertifizierungsverfahrens. Wie, durch wen, in welchem Umfang und mit welcher Granularität die Bewertung eines bestimmten Gegenstands oder Evaluationsgegenstands (EVG) in den einzelnen Zertifizierungsprojekten erfolgen soll, wird durch die Anforderungen des jeweiligen Zertifizierungsverfahrens geregelt. Die nominalen Anforderungen, nach denen der im EVG festgelegte konkrete Verarbeitungsvorgang bewertet wird, finden sich in den Zertifizierungskriterien. Die vorliegenden Leitlinien für die Festlegung von Zertifizierungskriterien enthalten allgemeine Empfehlungen, die eine wirksamere Bewertung von Zertifizierungskriterien im Hinblick auf deren Genehmigung ermöglichen sollen.

Bei der Genehmigung oder Festlegung von Zertifizierungskriterien empfiehlt es sich, folgende allgemeine Erwägungen zu berücksichtigen. Zertifizierungskriterien sollten

- einheitlich und nachprüfbar sein,
- insbesondere Ziele festlegen und praktische Leitlinien für die Erreichung dieser Ziele geben, um im Hinblick auf eine systematische Evaluierung der Verarbeitungsvorgänge nach der DSGVO überprüfbar zu sein,
- für die Zielgruppe (z. B. B2B und Business-to-Customer (B2C)) relevant sein,
- andere Standards (etwa ISO-Normen oder nationale Standards) berücksichtigen oder gegebenenfalls mit diesen interoperabel sein und
- im Hinblick auf die Anwendung auf Organisationen unterschiedlicher Art und Größe einschließlich Kleinstunternehmen, kleiner und mittlerer Unternehmen gemäß Artikel 42 Absatz 1 sowie des risikobasierten Ansatzes gemäß Erwägungsgrund 77 flexibel und skalierbar sein.

68. Ein kleines heimisches Unternehmen, wie etwa ein Einzelhändler, führt üblicherweise weniger komplexe Verarbeitungsvorgänge durch als ein großes multinationales Handelsunternehmen. Es gelten zwar die gleichen Anforderungen in Bezug auf die Rechtmäßigkeit der Verarbeitungsvorgänge, doch sind außerdem der Umfang der Datenverarbeitung und ihre Komplexität zu berücksichtigen. Daraus ergibt sich die Notwendigkeit von Zertifizierungsverfahren mit je nach Verarbeitungsvorgang skalierbaren Kriterien.

6.1 Bestehende Standards

69. Die Zertifizierungsstellen müssen sich mit der Frage befassen, wie die bestehenden einschlägigen Instrumente (beispielsweise Verhaltensregeln, technische Standards oder

nationale Rechtsetzungsinitiativen bzw. Legislativmaßnahmen) in den spezifischen Kriterien Berücksichtigung finden. Idealerweise sind die Kriterien mit den bestehenden Standards interoperabel, was den Verantwortlichen bzw. den Auftragsverarbeitern die Erfüllung ihrer Pflichten nach der DSGVO erleichtern kann. Während bei den Industriestandards der Schwerpunkt zumeist auf dem Schutz und der Sicherheit der Organisation vor Bedrohungen liegt, zielt die DSGVO auf den Schutz der Grundrechte natürlicher Personen ab. Diesen unterschiedlichen Blickwinkel gilt es bei der Gestaltung von Kriterien bzw. der Genehmigung von Kriterien oder Zertifizierungsverfahren auf der Grundlage von Industriestandards zu berücksichtigen.

6.2 Festlegung der Kriterien

70. Die Zertifizierungskriterien müssen im Einklang mit der Zertifizierungsaussage des Zertifizierungsmechanismus oder -programms stehen und den geweckten Erwartungen entsprechen. Schon durch die Bezeichnung eines Zertifizierungsmechanismus kann der Anwendungsbereich ermittelt und die Bestimmung der Kriterien beeinflusst werden.

71. [Beispiel 3]

    Der Anwendungsbereich eines Prüfzeichens für Datenschutz im Gesundheitswesen sollte auf eben diesen Bereich begrenzt werden. Die Bezeichnung des Siegels lässt erwarten, dass die Datenschutzanforderungen im Zusammenhang mit Gesundheitsdaten untersucht wurden. Dementsprechend müssen die Kriterien im Rahmen dieses Verfahrens dem Zweck der Bewertung von Datenschutzanforderungen in diesem Bereich entsprechen.

72. [Beispiel 4]

    Für ein Verfahren, das sich auf die Zertifizierung von Verarbeitungsvorgängen mit Steuerungssystemen (Governance) bei der Datenverarbeitung bezieht, sollten Kriterien ermittelt werden, welche die Erkennung und Bewertung von Governance-Prozessen und flankierender technischer und organisatorischer Maßnahmen ermöglichen.

73. [Beispiel 5]

    Bei den Kriterien für ein Verfahren, dass sich auf Cloud-Computing bezieht, müssen die spezifischen technischen Anforderungen berücksichtigt werden, die für die Nutzung Cloud-gestützter Dienste erforderlich sind. Erfolgt die Nutzung der Server zum Beispiel außerhalb der EU, müssen die Kriterien den in Kapitel V der DSGVO festgelegten Bedingungen für die Übermittlung von Daten an Drittländer Rechnung tragen.

74. Kriterien, die so gestaltet sind, dass sie sich auf unterschiedliche EVG in verschiedenen Bereichen und/oder Mitgliedstaaten anwenden lassen, sollten eine Anwendung im Rahmen unterschiedlicher Szenarien zulassen, die Festlegung angemessener Maßnahmen für Verarbeitungsvorgänge sowohl kleineren, mittleren als auch größeren Umfangs ermöglichen und im Einklang mit der DSGVO den mit unterschiedlichen Eintrittswahrscheinlichkeiten einhergehenden bzw. unterschiedlich gravierenden Risiken für die Rechte und Freiheiten natürlicher Personen Rechnung tragen. Dementsprechend müssen die Zertifizierungsverfahren (z. B. für die Dokumentation, Prüfung oder Evaluierungsmethode und -tiefe) zur Ergänzung der Kriterien diesen Anforderungen genügen und Vorschriften zulassen

bzw. für das Vorhandensein von Vorschriften sorgen, die beispielsweise die Anwendung der einschlägigen Kriterien im Rahmen einzelner Zertifizierungsprojekte regeln. Die Kriterien müssen die Bewertung erleichtern, ob hinreichende Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen gegeben wurden.

6.3 Gültigkeitsdauer der Zertifizierungskriterien

75. Obwohl die Zertifizierungskriterien im Zeitablauf verlässlich sein müssen, sollten sie dennoch nicht unumstößlich sein. Ihre Überprüfung ist beispielsweise angezeigt,

- wenn der Rechtsrahmen geändert wird,
- wenn Begriffe oder Bestimmungen durch Urteile des Europäischen Gerichtshofs ausgelegt werden, oder
- wenn sich der Stand der Technik weiterentwickelt hat.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)

ANHANG 1: AUFGABEN UND BEFUGNISSE DER AUFSICHTSBEHÖRDEN IM ZUSAMMENHANG MIT DER ZERTIFIZIERUNG GEMÄß DER DSGVO

	Bestimmungen	Anforderungen
Aufgaben	Artikel 43 Absatz 6	Hierdurch wird die Aufsichtsbehörde verpflichtet, die Kriterien nach Artikel 42 Absatz 5 in leicht zugänglicher Form zu veröffentlichen und dem Ausschuss zu übermitteln.
	Artikel 57 Absatz 1 Buchstabe n	Hierdurch wird die Aufsichtsbehörde verpflichtet, Zertifizierungskriterien nach Artikel 42 Absatz 5 zu billigen.
	Artikel 57 Absatz 1 Buchstabe o	Hierdurch wird die Aufsichtsbehörde verpflichtet, gegebenenfalls (d. h. falls sie Zertifizierungen erteilt) regelmäßig die nach Artikel 42 Absatz 7 erteilten Zertifizierungen zu überprüfen.
	Artikel 64 Absatz 1 Buchstabe c	Hierdurch wird die Aufsichtsbehörde verpflichtet, dem Ausschuss den Entwurf des Beschlusses zu übermitteln, wenn dieser der Billigung der Zertifizierungskriterien nach Artikel 42 Absatz 5 dient.
Befugnisse	Artikel 58 Absatz 1 Buchstabe c	Hierdurch wird der Aufsichtsbehörde die Befugnis übertragen, nach Artikel 42 Absatz 7 Überprüfungen der Zertifizierungen durchzuführen.
	Artikel 58 Absatz 2 Buchstabe h	Hierdurch wird der Aufsichtsbehörde die Befugnis übertragen, eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen.
	Artikel 58 Absatz 3 Buchstabe e	Hierdurch wird der Aufsichtsbehörde die Befugnis übertragen, Zertifizierungsstellen zu akkreditieren.
	Artikel 58 Absatz 3 Buchstabe f	Hierdurch wird der Aufsichtsbehörde die Befugnis übertragen, Zertifizierungen zu erteilen und Kriterien für die Zertifizierung zu billigen.
	Artikel 58 Absatz 3 Buchstabe e	Hierdurch wird der Aufsichtsbehörde die Befugnis übertragen, Zertifizierungsstellen zu akkreditieren.
	Artikel 58 Absatz 3 Buchstabe f	Hierdurch wird der Aufsichtsbehörde die Befugnis übertragen, Zertifizierungen zu erteilen und Kriterien für die Zertifizierung zu billigen.

ANHANG 2

1 EINLEITUNG

In Anhang 2 werden Leitlinien für die Überprüfung und Bewertung von Zertifizierungskriterien nach Artikel 42 Absatz 5 vorgegeben und Aspekte aufgeführt, die die zuständige Datenschutzaufsichtsbehörde und der EDSA bei ihrer Prüfung im Hinblick auf die etwaige Genehmigung von Zertifizierungskriterien für Zertifizierungsmechanismen berücksichtigen. Zertifizierungsstellen und -programmeigner, die Zertifizierungskriterien ausarbeiten und zur Genehmigung einreichen möchten, sollten diesen Aspekten Rechnung tragen. Die Liste ist nicht erschöpfend, sondern enthält nur jene Punkte, die es mindestens zu berücksichtigen gilt. Obschon nicht alle Aspekte in allen Fällen maßgeblich sind, sollten sie dennoch bei der Ausarbeitung von Kriterien berücksichtigt werden, und gegebenenfalls sollte bei Kriterien, die bestimmten Aspekten nicht Rechnung tragen, eine entsprechende Begründung hinzugefügt werden. Einige Fragen werden mehrfach aufgeführt, weil sie verschiedene Blickwinkel betreffen. Diese Leitlinien sind im Lichte der rechtlichen Anforderungen der DSGVO und etwaiger einschlägiger nationaler Rechtsvorschriften zu betrachten.

2 ANWENDUNGSBEREICH DES ZERTIFIZIERUNGSVERFAHRENS UND EVALUIERUNGSGEGENSTAND (EVG)

a. Ist der Anwendungsbereich des Zertifizierungsmechanismus, bei dem Datenschutzkriterien angewendet werden sollen, eindeutig beschrieben?

b. Ist der Anwendungsbereich des Zertifizierungsmechanismus für die Adressaten relevant und nicht irreführend formuliert?

- *Beispiel: Ein einem Unternehmen ausgestelltes „Vertrauenssiegel" suggeriert, dass sämtliche Verarbeitungsvorgänge des betreffenden Unternehmens geprüft worden sind, selbst wenn in Wirklichkeit nur bestimmte Verarbeitungsvorgänge (z.B. Online-Zahlungsvorgänge) Gegenstand des Zertifizierungsverfahrens waren. Eine solche Bezeichnung des Anwendungsbereichs des Zertifizierungsverfahrens ist folglich irreführend.*

c. Trägt der Anwendungsbereich des Zertifizierungsmechanismus allen maßgeblichen Aspekten der Verarbeitungsvorgänge Rechnung?

- *Beispiel: Ein Prüfzeichen für Datenschutz im Gesundheitswesen muss sämtliche sich auf die Gesundheit beziehenden Evaluierungsdaten einschließen, um den Anforderungen von Artikel 9 DSGVO gerecht zu werden.*

d. Ermöglicht der Anwendungsbereich des Zertifizierungsmechanismus eine sinnvolle Datenschutzzertifizierung unter Berücksichtigung von Art und Inhalt der betreffenden Datenverarbeitungsvorgänge und der mit ihnen verbundenen Risiken?

- *Beispiel: Wenn sich der Anwendungsbereich des Zertifikats lediglich auf bestimmte Aspekte der Verarbeitungsvorgänge (z.B. die Datenerhebung), aber nicht auf die Weiterverarbeitung (beispielsweise für die Erstellung von Werbeprofilen oder für die Verwaltung der Rechte der betroffenen Person) bezieht, ist dies für die betroffenen Personen nicht sinnvoll.*

e. Erstreckt sich der Anwendungsbereich des Zertifizierungsmechanismus auch auf die Verarbeitung von personenbezogenen Daten im Land der Anwendung, oder gilt er lediglich für die grenzüberschreitende Verarbeitung und/oder Übermittlung solcher Daten?

f. Ist in den Zertifizierungskriterien hinreichend genau beschrieben, wie der EVG zu definieren ist?

- *Beispiel: Bei einem Datenschutzsiegel mit allgemeinem Anwendungsbereich, für das lediglich „eine Spezifizierung des zu zertifizierenden Verarbeitungsvorgangs" erforderlich ist, ist nicht präzise genug vorgegeben, wie der betreffende EVG festzulegen und zu beschreiben ist.*
- *Beispiel: Der (spezifische) Anwendungsbereich eines Siegels für die sichere Speicherung personenbezogener Daten in einem digitalen Safe sollte eine ausführliche Beschreibung der hierfür zu erfüllenden Kriterien enthalten (Definition eines digitalen Safes, Systemanforderungen, obligatorische technische und organisatorische Vorkehrungen usw.). In diesem Fall lässt sich der EVG eindeutig durch den Anwendungsbereich festlegen.*

  (1) Machen es die Kriterien erforderlich, bei der Festlegung des EVG alle relevanten Verarbeitungsvorgänge aufzuführen, die betreffenden Datenströme aufzuzeigen und den Anwendungsbereich des EVG zu bestimmen?

  - *Beispiel: Bei einem Zertifizierungsmechanismus für nach Maßgabe der DSGVO durchzuführende Verarbeitungsvorgänge von Verantwortlichen ist der (allgemeine) Anwendungsbereich nicht näher spezifiziert. Die Kriterien, nach denen das Verfahren durchgeführt wird, schreiben vor, dass der antragstellende Auftragsverarbeiter den EVG unter Angabe der verwendeten Datenarten, Systeme und Verarbeitungsvorgänge festzulegen hat.*

  (2) Schreiben die Kriterien vor, dass der Antragsteller eindeutig anzugeben hat, wo der Verarbeitungsvorgang, der Gegenstand der Evaluierung ist, anfängt und endet? Machen es die Kriterien erforderlich, bei der Festlegung des EVG auch jene Schnittstellen anzugeben, an denen voneinander abhängige Datenverarbeitungsvorgänge erfolgen, die nicht im EVG eingeschlossen sind? Ist dies hinreichend gerechtfertigt?

  - *Beispiel: ein EVG, bei dem der durch einen internetbasierten Dienst erfolgende Datenverarbeitungsvorgang hinreichend detailliert beschrieben ist (beispielsweise in Bezug auf die Nutzerregistrierung, Diensterbringung, Rechnungslegung, Protokollierung von IP-Adressen und Schnittstellen für Nutzer und Dritte) und bei dem nicht auf das Serverhosting eingegangen wird (aber die betreffenden Vereinbarungen über Datenverarbeitungen und technische und organisatorische Vorkehrungen aufgeführt werden)*

g. Wird durch die Kriterien sichergestellt, dass jeder einzelne EVG für die jeweiligen Adressaten sowie gegebenenfalls für die betroffenen Personen verständlich ist?

3 ALLGEMEINE ANFORDERUNGEN

a. Sind alle relevanten Begriffe, die im Kriterienkatalog verwendet werden (d.h. sämtliche Zertifizierungskriterien), angegeben, erklärt und beschrieben?

b. Sind alle Normenverweise angegeben?

c. Schließen die Kriterien auch die Definition aller in den Anwendungsbereich des Zertifizierungsverfahrens fallenden datenschutzspezifischen Verantwortlichkeiten, Verfahren und Verarbeitungsvorgänge ein?

4 VERARBEITUNGSVORGÄNGE NACH ARTIKEL 42 ABSATZ 1 DSGVO

Werden, was den (allgemeinen oder spezifischen) Anwendungsbereich des Zertifizierungsmechanismus anbelangt, von den Kriterien alle relevanten Bestandteile der Verarbeitungsvorgänge (Daten, Systeme und Verarbeitungsvorgänge) erfasst?

a. Schreiben die Kriterien bezüglich der Festlegung des EVG die Angabe der geltenden Rechtsgrundlagen für die Verarbeitung vor?

b. Tragen die Kriterien in Bezug auf den EVG den relevanten Verarbeitungsphasen und dem gesamten Lebenszyklus der Daten einschließlich ihrer Anonymisierung und/oder Löschung Rechnung?

c. Schreiben die Kriterien für den EVG die Portabilität der betreffenden Daten vor?

d. Lassen die Kriterien in Bezug auf den EVG die Möglichkeit zu, besondere Arten der Datenverarbeitung (beispielsweise für automatisierte Entscheidungen oder die Profilerstellung) anzugeben oder zu berücksichtigen?

e. Lassen die Kriterien in Bezug auf den EVG die Möglichkeit zu, besondere Datenkategorien anzugeben?

f. Sehen die Kriterien vor, dass die Risiken der einzelnen Verarbeitungsvorgänge bewertet werden können oder müssen und der Schutzbedarf für die Rechte und Freiheiten der betroffenen Personen ermittelt werden kann oder muss?

g. Sehen die Kriterien die Möglichkeit und die Pflicht vor, den bestehenden Risiken für die Rechte und Freiheiten natürlicher Personen angemessen Rechnung zu tragen?

…

5 RECHTMÄßIGKEIT DER VERARBEITUNG

a. Schreiben die Kriterien vor, dass für jeden einzelnen Verarbeitungsvorgang die Rechtmäßigkeit der Verarbeitung in Bezug auf deren Zweck und Notwendigkeit zu prüfen ist?

b. Sehen die Kriterien vor, dass sämtliche Anforderungen einer Rechtsgrundlage für einzelne Verarbeitungsvorgänge zu prüfen sind?

6 GRUNDSÄTZE DES ARTIKELS 5 DSGVO

a. Tragen die Kriterien allen in Artikel 5 aufgeführten Datenschutzgrundsätzen gebührend Rechnung?

b. Schreiben die Kriterien vor, dass für jeden einzelnen EVG darzulegen ist, wie die betreffenden Daten minimiert werden sollen?

…

7 ALLGEMEINE PFLICHTEN VON VERANTWORTLICHEN UND AUFTRAGSVERARBEITERN

a. Schreiben die Kriterien den Nachweis vertraglicher Beziehungen zwischen Auftragsverarbeitern und Verantwortlichen vor?

b. Sind die Vereinbarungen zwischen dem Verantwortlichen und dem Auftragsverarbeitern Gegenstand einer Evaluierung?

c. Tragen die Kriterien den in Kapitel IV niedergelegten Pflichten des Verantwortlichen Rechnung?

d. Schreiben die Kriterien den Nachweis der Prüfung und Aktualisierung technischer und organisatorischer Vorkehrungen des Verantwortlichen nach Artikel 24 Absatz 1 vor?

e. Erfolgt durch die Kriterien eine Kontrolle, ob die betreffende Organisation geprüft hat, ob ein Datenschutzbeauftragter gemäß Artikel 37 zu benennen ist? Erfüllt der Datenschutzbeauftragte gegebenenfalls die Anforderungen der Artikel 37 bis 39?

f. Sehen die Kriterien vor, dass ein Verzeichnis der Verarbeitungstätigkeiten gemäß Artikel 30 Absatz 5 zu führen ist und die Anforderungen des Artikels 30 in geeigneter Weise erfüllt werden müssen?

8 RECHTE DER BETROFFENEN PERSON

a. Gehen die Kriterien hinreichend auf das Informationsrecht der betroffenen Person ein, und schreiben sie diesbezügliche Maßnahmen vor?

b. Sehen die Kriterien vor, dass allen betroffenen Personen hinreichender oder sogar weiter reichender Zugang und größere Kontrolle über ihre Daten (einschließlich Datenportabilität) zu gewähren ist?

c. Schreiben die Kriterien die Einführung von Maßnahmen vor, mit welchen in die Verarbeitung eingegriffen werden kann, um die Rechte der betroffenen Personen zu wahren und Berichtigungen, Löschungen oder Einschränkungen vorzunehmen?

…

9 RISIKEN FÜR DIE RECHTE UND FREIHEITEN NATÜRLICHER PERSONEN

a. Sehen die Kriterien die Möglichkeit und die Pflicht vor, eine Bewertung der für die Rechte und Freiheiten natürlicher Personen bestehenden Risiken vorzunehmen?

b. Sehen die Kriterien die Möglichkeit und die Pflicht vor, nach einer anerkannten Risikobewertungsmethode vorzugehen? Ist diese sowohl geeignet als auch angemessen?

c. Sehen die Kriterien die Möglichkeit und die Pflicht vor, eine Abschätzung der Folgen der geplanten Verarbeitungsvorgänge für die Rechte und Freiheiten natürlicher Personen vorzunehmen?

d. Schreiben die Kriterien eine vorherige, auf den Ergebnissen der Datenschutz-Folgenabschätzung basierende Konsultation zu den verbleibenden, nicht verringerbaren Risiken vor?

10 TECHNISCHE UND ORGANISATORISCHE SCHUTZVORKEHRUNGEN

a. Schreiben die Kriterien die Anwendung technischer und organisatorischer Vorkehrungen zur Wahrung der Vertraulichkeit der Verarbeitungsvorgänge vor?

b. Schreiben die Kriterien die Anwendung technischer und organisatorischer Vorkehrungen zur Wahrung der Integrität der Verarbeitungsvorgänge vor?

c. Schreiben die Kriterien die Anwendung technischer und organisatorischer Vorkehrungen zur Sicherstellung der Verfügbarkeit der Verarbeitungsvorgänge vor?

d. Schreiben die Kriterien die Anwendung von Maßnahmen vor, durch welche Transparenz geschaffen wird in Bezug auf die

e. Rechenschaftspflicht?

f. Rechte der betroffenen Personen?

g. Bewertung einzelner Verarbeitungsvorgänge (u.a. algorithmische Transparenz)?

h. Schreiben die Kriterien die Anwendung technischer und organisatorischer Vorkehrungen zur Wahrung der Rechte der betroffenen Personen vor (z.B. in Bezug auf die Fähigkeit, ihnen Informationen bereitzustellen oder in Bezug auf die Datenportabilität)?

i. Schreiben die Kriterien die Anwendung technischer und organisatorischer Vorkehrungen vor, durch die die Möglichkeit geschaffen wird, in Verarbeitungsvorgänge einzugreifen, um die Rechte der betroffenen Personen zu wahren und Berichtigungen, Löschungen oder Einschränkungen vorzunehmen?

j. Schreiben die Kriterien die Anwendung von Maßnahmen vor, durch die die Möglichkeit geschaffen wird, in Verarbeitungsvorgänge einzugreifen, um das betreffende System oder den betreffenden Vorgang zu korrigieren oder zu überprüfen?

k. Schreiben die Kriterien die Anwendung technischer und organisatorischer Vorkehrungen zur Datenminimierung vor (beispielsweise durch Trennung der Daten von der betroffenen Person oder durch Aufhebung einer entsprechenden Verknüpfung, durch Anonymisierung oder Pseudonymisierung oder durch Isolation der Datensysteme)?

l. Schreiben die Kriterien technische Maßnahmen zur Umsetzung des Datenschutzes durch datenschutzfreundliche Voreinstellungen vor?

m. Schreiben die Kriterien technische und organisatorische Vorkehrungen zur Umsetzung des Datenschutzes durch Technikgestaltung vor (beispielsweise ein Datenschutzmanagementsystem, das datenschutzspezifische Anforderungen aufzeigt und über diese informiert sowie für ihre Umsetzung sorgt und diese kontrolliert)?

n. Schreiben die Kriterien technische und organisatorische Vorkehrungen zur Umsetzung geeigneter regelmäßiger Datenschutzschulungen für Personal mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten vor?

o. Sehen die Kriterien Überprüfungsmaßnahmen vor?

p. Sehen die Kriterien eine Selbstbewertung (self-assessment) oder eine interne Prüfung (Audit) vor?

q. Schreiben die Kriterien Maßnahmen vor, durch die sichergestellt werden soll, dass der Pflicht zur Meldung etwaiger Verletzungen des Schutzes personenbezogener Daten zeitnah und in gebührendem Umfang nachgekommen wird?

r. Schreiben die Kriterien die Einführung und Überprüfung von Verfahren für den Umgang mit Vorfällen vor?

s. Sehen die Kriterien die Überwachung entstehender datenschutzrechtlicher und technologischer Fragestellungen und die entsprechende Anpassung der Regelung vor?

…

11 SONSTIGE BESONDERE DATENSCHUTZFREUNDLICHE ASPEKTE

a. Sehen die Kriterien die Anwendung von technischen Maßnahmen vor, die den Datenschutz fördern? Hierbei könnten auch Kriterien berücksichtigt werden, die auf einen verbesserten Datenschutz durch die Eliminierung oder Verringerung von personenbezogenen Daten und/oder Datenschutzrisiken abzielen.

- *Beispiel: Kriterien, die eine verbesserte Unverknüpfbarkeit durch Rückgriff auf eine nutzerorientierte Identitätsverwaltung (beispielsweise mittels attributbasiertem Identitätsnachweis) anstelle einer organisationsorientierten Identitätsverwaltung vorschreiben, würden eine Technik zur Verbesserung des Datenschutzes widerspiegeln.*

b. Schreiben die Kriterien die Anwendung verbesserter Kontrollen der betroffenen Personen vor, durch die deren Selbstbestimmungs- und Entscheidungsmöglichkeiten verbessert werden sollen?

…

12 KRITERIEN FÜR DEN NACHWEIS, DASS IM RAHMEN DER ÜBERMITTLUNG PERSONENBEZOGENER DATEN GEEIGNETE GARANTIEN GEBOTEN WERDEN

Diese Kriterien werden in den in Kürze erscheinenden Leitlinien zu Artikel 42 Absatz 2 behandelt werden.

13 ZUSÄTZLICHE KRITERIEN FÜR DAS EUROPÄISCHE DATENSCHUTZSIEGEL

a. Sind die Kriterien für alle Mitgliedstaaten gedacht?

b. Sind die Kriterien dazu geeignet, auch den Datenschutzvorschriften oder -szenarien der Mitgliedstaaten Rechnung zu tragen?

c. Schreiben die Kriterien die Evaluierung jedes einzelnen EVG in Bezug auf die sektorspezifischen Datenschutzvorschriften der Mitgliedstaaten vor?

d. Sehen die Kriterien vor, dass den betroffenen Personen und interessierten Parteien vom Verantwortlichen oder vom Auftragsverarbeiter folgende Informationen in den Landessprachen der Mitgliedstaaten zur Verfügung gestellt werden:

e. Informationen über die Verarbeitung bzw. den EVG?

f. die Dokumentation der Verarbeitung bzw. des EVG?

g. die Evaluierungsergebnisse?

…

14 ALLGEMEINE BEWERTUNG DER KRITERIEN

a. Decken die Kriterien den gesamten Anwendungsbereich des Zertifizierungsmechanismus ab (d.h. sind die Kriterien umfassend), sodass hinreichende Garantien dafür gegeben werden, dass die Zertifizierung vertrauenswürdig ist?

- *Beispiel: Falls sich der Anwendungsbereich des Zertifizierungsmechanismus auf Verarbeitungsvorgänge bei Gesundheitsdaten konzentriert, sollten, um einen hohen Datenschutz zu garantieren, beispielsweise Kriterien festgelegt werden, die eine tief greifende Bewertung und die Anwendung der Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sicherstellen.*

b. Sind die Kriterien dem Umfang des in den Anwendungsbereich des Zertifizierungsmechanismus fallenden Verarbeitungsvorgangs, dem sensiblen Charakter der betreffenden Informationen und den mit der Verarbeitung einhergehenden Risiken angemessen?

c. Werden die Kriterien voraussichtlich zu einer Verbesserung der Einhaltung der Datenschutzvorschriften durch die Verantwortlichen und die Auftragsverarbeiter beitragen?

d. Wird dem Informationsrecht der betroffenen Personen Genüge getan werden, indem ihnen beispielsweise die erhofften Ergebnisse erläutert werden?