BUNDESGESETZBLATT
FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2021 Ausgegeben am 17. Februar 2021 Teil II

79. Verordnung der Datenschutzbehörde über die Anforderungen an die Akkreditierung einer Zertifizierungsstelle (Zertifizierungsstellen-Akkreditierungs-Verordnung – ZeStAkk-V)

Auf Grund des § 21 Abs. 3 des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 14/2019, wird verordnet:

Allgemeine Bestimmungen

§ 1. Diese Verordnung regelt in Konkretisierung des Art. 43 Abs. 2 der Verordnung (EU) 2016/679 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), ABl. Nr. L 119 vom 04.05.2016 S. 1, in der Fassung der Berichtigung ABl. Nr. L 127 vom 23.05.2018 S. 2 und in Ergänzung der Vorgaben der Internationalen Norm ISO/IEC 17065:2012 Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren (im Folgenden: ISO/IEC 17065:2012), die Voraussetzungen für die Akkreditierung von Zertifizierungsstellen gemäß Art. 58 Abs. 3 lit. e DSGVO.

Begriffsbestimmungen

§ 2. Im Sinne dieser Verordnung bezeichnet der Begriff

1. „Zertifizierungsanforderungen“, Anforderungen – einschließlich den Zertifizierungskriterien –, die vom Zertifizierungswerber oder -inhaber als eine Bedingung zur Feststellung oder Aufrechterhaltung der Zertifizierung zu erfüllen sind;
2. „Technischer Datenschutz“, sämtliche Maßnahmen, die eingesetzt werden, um zu gewährleisten, dass die Sicherheits- und Schutzanforderungen bei der Verarbeitung personenbezogener Daten erfüllt sind;
3. „Zertifizierungskriterien“, jene gemäß Art. 42 Abs. 5 DSGVO genehmigten Kriterien, anhand derer eine Zertifizierung durchgeführt wird;
4. „Zertifizierungsstelle“, eine unabhängige Konformitätsbewertungsstelle, die gemäß dieser Verordnung akkreditiert wurde;
5. „Zertifizierungswerber“, jenen Verantwortlichen gemäß Art. 4 Z 7 DSGVO oder Auftragsverarbeiter gemäß Art. 4 Z 8 DSGVO, welcher eine Zertifizierung anstrebt und der dafür verantwortlich ist, sicherzustellen, dass die Zertifizierungsanforderungen erfüllt sind;
6. „Zertifizierungsinhaber“, jenen Verantwortlichen gemäß Art. 4 Z 7 DSGVO oder Auftragsverarbeiter gemäß Art. 4 Z 8 DSGVO, dem die Zertifizierungsstelle eine Zertifizierung erteilt hat und der dafür verantwortlich ist, sicherzustellen, dass die Zertifizierungsanforderungen laufend eingehalten werden.

Akkreditierung

§ 3. Mit der Akkreditierung als Zertifizierungsstelle wird diese ermächtigt, einem Zertifizierungswerber eine Zertifizierung zu erteilen.

Akkreditierungsverfahren

§ 4. (1) Die Akkreditierung als Zertifizierungsstelle erfolgt auf Grund eines schriftlichen Antrages an die Datenschutzbehörde mit Bescheid. Antragslegimitiert sind ausschließlich juristische Personen im Sinne des Punktes 4.1.1 ISO/IEC 17065:2012 (Antragsteller).

(2) Dem Antrag sind sämtliche für das Verfahren erforderlichen Dokumente anzuschließen. Die Akkreditierung als Zertifizierungsstelle setzt den Nachweis der Einhaltung der Anforderungen des Art. 43 Abs. 2 DSGVO, der Internationalen Norm ISO/IEC 17065:2012 samt Anhang und der in dieser Verordnung genannten zusätzlichen Anforderungen voraus.

(3) Der Antrag hat jedenfalls den Nachweis der Voraussetzungen nach §§ 5 bis 19 und folgende Angaben zu enthalten:

1. Zur Feststellung der Identität des Antragstellers:
   a) die Firma gemäß § 17 des Unternehmensgesetzesbuches – UGB, dRGBl. S. 219/1897, sowie die Firmenbuchnummer, bei Vereinen die ZVR-Zahl gemäß § 18 Abs. 2 des Vereinsgesetzes 2002 – VerG, BGBl. I Nr. 66, sowie im Falle der Ausübung einer Tätigkeit nach der Gewerbeordnung 1994 – GewO 1994, BGBl. Nr. 194, die GISA-Zahl gemäß § 365a Abs. 1 Z 11 bzw. § 365b Abs. 1 Z 8 GewO 1994,
   b) die Namen der für den technischen und rechtlichen Bereich gesamtverantwortlichen Leiter, gegebenenfalls deren Stellvertreter sowie jener Zeichnungsberechtigten, die für die fachliche Richtigkeit der Konformitätsbewertung verantwortlich sein sollen,
2. Angaben zum beantragten sachlichen Geltungsbereich der Konformitätsbescheinigung (Zertifizierungsgegenstand),
3. Angaben zu den Zertifizierungskriterien gemäß Art. 42 Abs. 5 DSGVO, auf deren Grundlage die Zertifizierung erteilt werden,
4. sofern Konformitätszeichen gemäß § 14 Abs. 1 verwendet werden: Eine Abbildung der Konformitätszeichen,
5. zum Nachweis der strafrechtlichen Unbescholtenheit: Sofern die Zuverlässigkeit und strafrechtliche Unbescholtenheit nicht Voraussetzung für die Ausübung der Tätigkeit ist, eine Registerauskunft für Verbände gemäß § 89m des Gerichtsorganisationsgesetzes – GOG, RGBl. Nr. 217/1896,
6. einen Sitz im Europäischen Wirtschaftsraum gemäß dem EWR-Abkommen, BGBl. Nr. 909/1993,
7. zur Gewährleistung einer fortdauernden Erfüllung der mit der Akkreditierung verbundenen Aufgaben und Befugnisse: eine Darlegung der finanziellen, personellen und organisatorischen Ausstattung, und
8. den Nachweis der Möglichkeit der Abdeckung finanzieller Verbindlichkeiten aus der Tätigkeit als Zertifizierungsstelle nach Maßgabe des Punktes 4.3 ISO/IEC 17065:2012, einschließlich des Abschlusses und des Nachweises einer Haftpflichtversicherung zur Deckung der aus der Tätigkeit als Zertifizierungsstelle entstehenden Schadenersatzansprüche, wobei die Versicherung während der gesamten Dauer der Tätigkeit aufrechtzuerhalten ist.

(4) Die Angaben gemäß Abs. 3 sind durch Vorlage geeigneter Dokumente zu bescheinigen, sofern sich deren Verfügbarkeit nicht aus allgemein zugänglichen öffentlichen Registern ergibt.

(5) Sofern der Antrag auf Akkreditierung nicht in deutscher Sprache erfolgt, sind die Angaben gemäß Abs. 3 durch Vorlage geeigneter Dokumente in beglaubigter Übersetzung zu bescheinigen.

(6) Die Akkreditierung wird für fünf Jahre – sofern sich der Zertifizierungsgegenstand auf die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO bezieht, für drei Jahre – erteilt und kann unter den in dieser Verordnung genannten Voraussetzungen verlängert werden.

(7) Zertifizierungsstellen müssen angemessene technische und organisatorische Maßnahmen treffen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung von personenbezogenen Daten gemäß der DSGVO erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Unparteilichkeit

§ 5. (1) Die Zertifizierungsstelle hat ihre Tätigkeit nach Maßgabe des Punktes 4.2 ISO/IEC 17065:2012 unparteiisch durchzuführen.

(2) Jede Art von wirtschaftlicher Beziehung zwischen Zertifizierungsstelle und Zertifizierungswerber oder -inhaber kann die Unparteilichkeit ihrer Tätigkeit beeinträchtigen. Der Unparteilichkeit gemäß Abs. 1 steht jedenfalls entgegen, wenn zwischen der Zertifizierungsstelle und dem Zertifizierungswerber oder -inhaber ein Vertragsverhältnis im Sinne des Art. 26 Abs. 1 zweiter Satz oder Art. 28 Abs. 3 DSGVO besteht.

Anforderungen an die Organisationsstruktur

§ 6. (1) Zur fortlaufenden Gewährleistung der Unparteilichkeit gemäß § 5 hat die Zertifizierungsstelle nachzuweisen, dass ihre Organisation nach Maßgabe des Punktes 5.1 ISO/IEC 17065:2012 strukturiert und ein Mechanismus nach Maßgabe des Punktes 5.2 ISO/IEC 17065:2012 implementiert ist.

(2) Die Zertifizierungsstelle hat gemäß Art. 43 Abs. 2 lit. a DSGVO die Unabhängigkeit ihres Personals in Bezug auf den Zertifizierungsgegenstand nachzuweisen.

(3) Zum Nachweis der Unabhängigkeit gemäß Abs. 2 ist jedenfalls Folgendes anzugeben:

1. eine Offenlegung der wirtschaftlichen Eigentümer, insbesondere durch die Vorlage eines Auszugs des bei der Registerbehörde geführten Registers für wirtschaftliche Eigentümer nach dem Wirtschaftliche Eigentümer Registergesetz – WiEReG, BGBl. I Nr. 136/2017, und
2. Angaben zur fortlaufenden Finanzierung der Zertifizierungsstelle.

(4) Die Zertifizierungsstelle hat gemäß Art. 43 Abs. 2 lit. e DSGVO nachzuweisen, dass die Aufgaben und Pflichten ihres Personals nicht zu einem Interessenkonflikt führen.

(5) Der Nachweis für Verhinderung von Interessenkonflikten gemäß Abs. 4 ist jedenfalls durch einen – gegenüber dem Personal der Zertifizierungsstelle für verbindlich zu erklärenden – Maßnahmenkatalog zu erbringen, der jedenfalls Folgendes vorzusehen hat:

1. Unvereinbarkeitsbestimmungen, welche festlegen, dass das Personal der Zertifizierungsstelle keiner weiteren, mit der Ausübung ihrer Tätigkeit unvereinbaren Geschäftstätigkeit nachgeht,

2. Implementierung von Stellvertreterregelungen im Falle identifizierter Interessenkonflikte,

3. Verschwiegenheitsklauseln, sowie

4. Weisungsfreiheit gegenüber den Zertifizierungswerbern oder -inhabern.

Fachwissen

§ 7. (1) Die Zertifizierungsstelle muss zusätzlich zu den Anforderungen des Punktes 6.1 ISO/IEC 17065:2012 über hinreichende personelle Ressourcen mit aktuellen Fachkenntnissen in den folgenden Bereichen verfügen und in der Lage sein, dies jederzeit nachzuweisen:

1. Kenntnisse des Datenschutzrechts und Erfahrung in seiner Anwendung, einschließlich technischer und organisatorischer Maßnahmen und Verfahren,
2. Kenntnisse in Bezug auf den Zertifizierungsgegenstand gemäß Art. 43 Abs. 2 lit. a DSGVO und
3. Kenntnisse der für Konformitätsbewertungen maßgeblichen gesetzlichen Bestimmungen sowie der national und international relevanten Normen (insbesondere EN, DIN, IEC und ISO).

(2) Die juristischen Fachkenntnisse sind nachzuweisen durch den erfolgreichen Abschluss eines mindestens acht Semester andauernden Studiums der Rechtswissenschaften oder des Wirtschaftsrechts an einer österreichischen oder einer als gleichwertig anerkannten ausländischen Universität oder einer Fachhochschule, das zur Führung des akademischen Grades Magister oder Master berechtigt.

(3) Die technischen Fachkenntnisse sind nachzuweisen durch:

1. den erfolgreichen Abschluss eines mindestens acht Semester andauernden Studiums an einer österreichischen oder einer als gleichwertig anerkannten ausländischen Universität oder einer Fachhochschule, das überwiegend durch die Fächer Informatik, Technik oder Mathematik gekennzeichnet ist und das zur Führung des akademischen Grades Magister, Diplom-Ingenieur oder Master berechtigt, oder
2. den erfolgreichen Abschluss einer Ausbildung, die zur Führung der Qualitätsbezeichnung Ingenieur im Sinne des Ingenieurgesetzes 2017 – IngG 2017, BGBl. I Nr 23/2017, berechtigt, oder
3. den erfolgreichen Abschluss einer gleichwertigen Berufsausbildung, für welchen in dem Mitgliedsstaat, in dem er erfolgte, ein anerkannter geschützter Titel oder eine solche Berufsbezeichnung verliehen wird.

(4) Die Fachkenntnisse gemäß Abs. 2 und Abs. 3 können auch in Form einer mindestens fünfjährigen Berufserfahrung nachgewiesen werden, die allgemein juristische und technische Fachkenntnisse vermittelt.

(5) Die mit dem Zertifizierungsverfahren betrauten Personen müssen zusätzlich zu den Anforderungen gemäß Abs. 2 bis Abs. 4 über ausreichende Kenntnisse und eine mindestens zweijährige Berufserfahrung mit Auditierungen im Sinne des § 16 Abs. 3 verfügen.

(6) Die für die Entscheidung über die Zertifizierung verantwortliche Person oder verantwortlichen Personen im Sinne des § 13 müssen zusätzlich zu den Anforderungen gemäß Abs. 2 bis Abs. 4 über eine mindestens fünfjährige spezifische Berufserfahrung im Datenschutzrecht und im Bereich des technischen Datenschutzes verfügen.

(7) Das Fachwissen der Zertifizierungsstelle muss nicht in einer Person alleine vorhanden sein.

(8) Das Personal, welches im Zertifizierungsverfahren und bei der Entscheidung über die Zertifizierung eingesetzt wird, muss sich im Sinne des Art. 43 Abs. 2 lit. b DSGVO verpflichten, die gemäß Art. 42 Abs. 5 DSGVO genehmigten Kriterien einzuhalten.

(9) Die Zertifizierungsstelle hat durch Verfahren zu gewährleisten, dass das Fachwissen des Personals, insbesondere unter Berücksichtigung von Änderungen der Gesetzeslage, des Risikos für die Verarbeitung und des Standes der Technik, auf aktuellem Stand gehalten wird.

(10) Die Zertifizierungsstelle muss zu dem Personal, welches im Zertifizierungsverfahren und bei der Entscheidung über die Zertifizierung eingesetzt ist, Aufzeichnungen im Sinne des Punktes 6.1.2.2 ISO/IEC 17065:2012 führen.

Zertifizierungsverfahren

§ 8. (1) Die Zertifizierung erfolgt auf Grundlage eines schriftlichen Antrags des Zertifizierungswerbers an die Zertifizierungsstelle. Die Zertifizierungsstelle hat nach Maßgabe von Punkt 7.2 ISO/IEC 17065:2012 Vorgaben für den Antrag festzulegen, der sämtliche für das Zertifizierungsverfahren erforderlichen Informationen und jedenfalls folgende Angaben zu enthalten hat:

1. Angaben zur Feststellung der Identität des Zertifizierungswerbers, einschließlich der Generalien der vertretungsbefugten Personen des Zertifizierungswerbers,
2. Angaben zur beantragten Zertifizierung einschließlich der Information, ob es sich bei der Zertifizierung um ein Europäisches Datenschutzsiegel gemäß Art. 40 Abs. 5 zweiter Satz DSGVO handelt,
3. Informationen bezüglich aller allfällig ausgegliederten Prozesse, die vom Zertifizierungswerber genutzt werden, einschließlich Informationen zu einem Verhältnis gemäß Art. 26 oder Art. 28 DSGVO.

(2) Die Zertifizierungsstelle hat zur Abwicklung des Zertifizierungsverfahrens ein Zertifizierungsprogramm nach Maßgabe des Punktes 7.1 ISO/IEC 17065:2012 zu betreiben.

(3) Die Zertifizierungsstelle hat den schriftlichen Antrag des Zertifizierungswerbers nach Maßgabe des Punktes 7.3 ISO/IEC 17065:2012 zu bewerten, den Zertifizierungswerber innerhalb angemessener Frist sowie auf Anfrage über den Stand des Zertifizierungsverfahrens zu informieren.

(4) Sofern das Zertifizierungsverfahren ergibt, dass die Zertifizierung aller Voraussicht nach nicht erteilt werden kann, ist dem Zertifizierungswerber auf dessen Antrag und unter angemessener Fristsetzung die Möglichkeit zu geben, die dafür maßgebenden Umstände oder Gründe zu beseitigen.

(5) Die Zertifizierungsstelle hat eine Zertifizierungsentscheidung gemäß § 13 innerhalb einer angemessenen Frist zu treffen. Die Frist ist im Zertifizierungsprogramm festzulegen.

(6) Die Zertifizierungsstelle hat im Rahmen ihrer Tätigkeit die nicht diskriminierenden Bedingungen im Sinne des Punktes 4.4 ISO/IEC 17065:2012 zu erfüllen.

(7) Die Zertifizierungsstelle hat sämtliche Informationen zum Zertifizierungsprogramm im Sinne des Punktes 4.6 ISO/IEC 17065:2012 in allgemein zugänglicher Form zu veröffentlichen und auf Anfrage bereitzustellen.

Zertifizierungsvereinbarung und Maßnahmen zur Sicherstellung der Kommunikation und der Vertraulichkeit

§ 9. (1) Zwischen Zertifizierungsstelle und Zertifizierungswerber ist eine Zertifizierungsvereinbarung abzuschließen.

(2) In der Zertifizierungsvereinbarung ist zusätzlich zu den Anforderungen im Sinne des Punktes 4.1.2 ISO/IEC 17065:2012 jedenfalls Folgendes festzulegen:

1. Die Verpflichtung des Zertifizierungswerbers zur fortlaufenden Einhaltung der Zertifizierungsanforderungen und der darin vorgesehenen Fristen, einschließlich der Zertifizierungskriterien gemäß Art. 42 Abs. 5 DSGVO,
2. die Verpflichtung des Zertifizierungswerbers, Änderungen von Zertifizierungsanforderungen gemäß § 10 nach Gewährung einer angemessenen Frist umzusetzen,

3. die Dauer, für welche die Zertifizierung erteilt oder verlängert wird, wobei gemäß Art. 42 Abs. 7 DSGVO die Höchstdauer von drei Jahren zu berücksichtigen ist,
4. die Bedingungen, unter welchen gemäß Art. 42 Abs. 7 und Art. 43 Abs. 4 DSGVO die Zertifizierung verlängert oder widerrufen werden kann, einschließlich angemessener Zeitabstände für die Neubewertung der Erfüllung der Zertifizierungsanforderungen und der Zertifizierungskriterien gemäß Art. 42 Abs. 5 DSGVO,
5. eine Berichtspflicht des Zertifizierungswerbers über wesentliche Änderungen, welche die Erfüllung der vereinbarten Verpflichtungen beeinträchtigen können,
6. Verpflichtungen des Zertifizierungswerbers im Zusammenhang mit der Beendigung, Einschränkung, Aussetzung oder Zurückziehung der Zertifizierung gemäß § 17, insbesondere, dass
   a) jeglicher Verweis oder jegliche Bezugnahme auf die erteilte Zertifizierung zu unterbleiben hat,
   b) etwaige Konformitätszeichen nach § 15 Abs. 1 zurückzustellen und nicht mehr zu verwenden sind,
7. die Verpflichtung des Zertifizierungswerbers, den mit Durchführung der Zertifizierung betrauten Personen der Zertifizierungsstelle, soweit zur Überprüfung der fortlaufenden Einhaltung der in der Zertifizierungsvereinbarung festgelegten Verpflichtungen erforderlich, nach vorheriger Ankündigung Zugang zu den Betriebs- oder Produktionsstätten sowie Einsicht in die erforderlichen Dokumente zu gewähren,
8. die Verpflichtung des Zertifizierungswerbers, vollständige Transparenz des Zertifizierungsverfahrens gegenüber der Datenschutzbehörde zu gewährleisten, einschließlich vertraulicher Vertragsangelegenheiten in Zusammenhang mit der Einhaltung der Bestimmungen gemäß Art. 42 Abs. 7 und Art. 58 Abs. 1 lit. c DSGVO,
9. die Möglichkeit der Zertifizierungsstelle, sämtliche Information offenzulegen, die gemäß Art. 42 Abs. 8 und Art. 43 Abs. 5 DSGVO zur Erteilung der Zertifizierung erforderlich sind,
10. der Hinweis darauf, dass die Zertifizierung unbeschadet der aus der DSGVO resultierenden Verpflichtungen, denen der Zertifizierungswerber unterliegt und unbeschadet der Aufgaben und Befugnisse der Datenschutzbehörde erfolgt,
11. die Konsequenzen für den Zertifizierungswerber, wenn die Akkreditierung der Zertifizierungsstelle gemäß Art. 43 Abs. 7 DSGVO widerrufen wird,
12. Verpflichtungen der Zertifizierungsstelle im Zusammenhang mit Beschwerden in Bezug auf die Einhaltung der Zertifizierungsanforderungen, wie insbesondere
    a) Erstellung eines internen Maßnahmenkatalogs für die Behandlung der einlangenden Beschwerden, und
    b) Dokumentations- und Aufbewahrungspflichten über die Beschwerdefälle und die ergriffenen Maßnahmen sowie über die Dauer der Aufbewahrung unter Berücksichtigung der Grundsätze für die Verarbeitung personenbezogener Daten im Sinne der DSGVO, sowie
13. die gemäß § 11 festgelegten Evaluierungsmethoden in Bezug auf den Zertifizierungsgegenstand.

(3) Es sind geeignete Maßnahmen zu treffen, damit eine effektive Kommunikation zwischen Zertifizierungsstelle und berechtigten Dritten gewährleistet wird. Dazu zählt jedenfalls die laufende Dokumentation über:

1. über die Tätigkeit der Zertifizierungsstelle zum Zwecke der Behandlung von Informationsanfragen oder zur Kontaktaufnahme im Falle einer Beschwerde im Zusammenhang mit einer Zertifizierung, sowie
2. über das Antragsverfahren, insbesondere um Informationen über den aktuellen Stand von Anträgen gemäß § 8 Abs. 1 erteilen zu können.

(4) Die Zertifizierungsstelle verpflichtet sich vertraglich gegenüber dem Zertifizierungswerber, die auf Grund ihrer Tätigkeit erhaltenen Informationen im Sinne des Punktes 4.5.1 ISO/IEC 17065:2012 vertraulich zu behandeln.

Änderung von Zertifizierungsanforderungen

§ 10. (1) Im Falle einer Änderung der Zertifizierungsanforderungen hat die Zertifizierungsstelle den Zertifizierungsinhaber unverzüglich schriftlich zu verständigen und nach Gewährung einer angemessenen Frist für die Umsetzung der erforderlichen Änderungen diese auch zu überprüfen.

(2) Zusätzlich zu den Vorgaben des Punktes 7.10 ISO/IEC 17065:2012 umfassen Änderungen, die die Zertifizierungsanforderungen betreffen und von der Zertifizierungsstelle zu berücksichtigen sind, insbesondere die Änderung der Rechtslage, höchstgerichtliche Entscheidungen im Zusammenhang mit

dem Datenschutz, den Erlass delegierter Rechtsakte der Kommission gemäß Art. 43 Abs. 8 und Abs. 9 DSGVO, sowie angenommene Dokumente des Europäischen Datenschutzausschusses.

Evaluierung

§ 11. (1) Die Zertifizierungsstelle hat unter Einhaltung der Vorgaben des Punktes 7.4 ISO/IEC 17065:2012 standardisierte Bewertungsmethoden festzulegen, welche ihr die Beurteilung der Übereinstimmung der Verarbeitungsvorgänge mit den Zertifizierungskriterien ermöglicht. Zusätzlich zu den Vorgaben des Punktes 7.4.6 ISO/IEC 17065:2012 hat die Zertifizierungsstelle Modalitäten festzulegen, wie der Zertifizierungswerber über allfällige Abweichungen von Zerfizierungskriterien informiert wird. In diesem Rahmen sind jedenfalls Art und Zeitpunkt der Informationsmitteilung zu regeln.

(2) Die Zertifizierungsstelle hat in den standardisierten Bewertungsmethoden gemäß Abs. 1 festzulegen, inwiefern Instrumente wie Verhaltensregeln gemäß Art. 40 DSGVO, an denen der Zertifizierungswerber teilnimmt, Zertifizierungen gemäß Art. 42 DSGVO, die ein Zertifizierungswerber bereits besitzt, oder anderweitige etablierte Standards, die eingehalten werden, zum Nachweis der Übereinstimmung der Verarbeitungsvorgänge mit den Zertifizierungskriterien herangezogen werden können. Die Zertifizierungsstelle ist jedenfalls verpflichtet, die Konformität der Verarbeitungsvorgänge des Zertifizierungswerbers mit den Zertifizierungskriterien zu überprüfen. Der vollständige Ersatz dieser Überprüfung durch Verweis auf derartige Instrumente ist nicht möglich.

(3) Die Zertifizierungsstelle hat die Vorgaben des Punktes 6.2 ISO/IEC 17065:2012 für die Ressourcen der Evaluierung zu erfüllen.

(4) Die Betrauung von externen Sachverständigen zur Durchführung der erforderlichen Evaluierungstätigkeiten ist nach Maßgabe der folgenden Bestimmungen zulässig:

1. Die extern Betrauten verfügen gemeinsam über das Fachwissen und die Erfahrung gemäß § 7 Abs. 2 bis Abs. 5,
2. die Tätigkeit erfolgt nach den Anforderungen der relevanten internationalen (insbesondere ISO/IEC) Normen,
3. Unvereinbarkeitsbestimmungen und Maßnahmen zur Sicherstellung der Vertraulichkeit unter sinngemäßer Anwendung von § 5 und § 6 wurden vertraglich vereinbart,
4. der Zertifizierungswerber wurde vorab informiert und ihm wurde die Möglichkeit zur Erhebung einer Ablehnung eingeräumt, und
5. die Verantwortung für die übertragenen Tätigkeiten verbleibt bei der Zertifizierungsstelle.

(5) Die Zertifizierungsstelle hat, insbesondere unter Berücksichtigung von Änderungen der Rechtslage, des Risikos für die Verarbeitung, des Standes der Technik und der Kosten für die Durchführung technischer und organisatorischer Maßnahmen, Verfahren festzulegen, nach denen die Bewertungsmethoden gemäß Abs. 1 fortentwickelt werden.

(6) Die Zertifizierungsstelle hat gemäß Punkt 7.4.9 ISO/IEC 17065:2012 die Ergebnisse aller Evaluierungstätigkeiten in einem Verzeichnis zu dokumentieren und der Datenschutzbehörde jederzeit Zugang zu diesem zu gewähren.

Bewertung

§ 12. (1) Die Zertifizierungsstelle hat alle Informationen und Ergebnisse, die mit der Evaluierung im Zusammenhang stehen, im Sinne des Punktes 7.5 ISO/IEC 17065:2012 zu bewerten.

(2) Die Zertifizierungsstelle hat gemäß Art. 43 Abs. 2 lit. c DSGVO Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf von Zertifizierungen zu implementieren.

Zertifizierungsentscheidung

§ 13. (1) Die Zertifizierungsstelle hat die Entscheidung in Bezug auf die Erteilung oder Nichterteilung einer Zertifizierung anhand der Evaluierungsergebnisse gemäß § 11 und anhand der Bewertung gemäß § 12 und unter Einhaltung der Vorgaben des Punktes 7.6 ISO/IEC 17065:2012 zu treffen.

(2) Die Zertifizierungsstelle hat Verfahren festzulegen, wie die Unabhängigkeit und Verantwortung der entscheidungsbefugten Personen in Bezug auf jede Zertifizierungsentscheidung gewährleistet wird.

(3) Die Betrauung von externen Sachverständigen zur Durchführung der Zertifizierungsentscheidung ist nicht zulässig.

(4) Die Zertifizierungsstelle hat dem Zertifizierungswerber im Falle der Erteilung einer Zertifizierung eine schriftliche Bescheinigung auszustellen, die folgende Angaben enthält:

1. Name und Anschrift der Zertifizierungsstelle,
2. die Generalien des Zertifizierungsinhabers,
3. das Datum, an welchem die Zertifizierung erteilt oder verlängert wurde,
4. den Geltungsbereich der Zertifizierung und eine Beschreibung des Zertifizierungsgegenstandes, sowie
5. den Zeitraum im Sinne des § 9 Abs. 2 Z 3, für welchen die Zertifizierung erteilt wird.

(5) Im Fall der Nichterteilung einer Zertifizierung hat die Zertifizierungsstelle den Zertifizierungswerber schriftlich darüber zu informieren und die maßgeblichen Gründe für diese Entscheidung darzulegen.

(6) Die schriftliche Bescheinigung gemäß Abs. 4 und die schriftliche Entscheidung gemäß Abs. 5 ist von der gemäß § 4 Abs. 3 Z 1 lit. b dazu bevollmächtigten Person der Zertifizierungsstelle zu unterfertigen.

(7) Die Zertifizierungsstelle hat der Datenschutzbehörde die Gründe über Anfrage für die Erteilung oder Nichterteilung einer Zertifizierung mitzuteilen.

(8) Die Zertifizierungsstelle hat Anweisungen der Datenschutzbehörde, eine Zertifizierung nicht zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht erfüllt werden, zu befolgen. Der Zertifizierungswerber, der von dieser Anweisung betroffen ist, hat im Rahmen des Widerrufverfahrens Parteistellung.

Konformitätszeichen

§ 14. (1) Zusätzlich zur schriftlichen Bescheinigung gemäß § 13 Abs. 4 kann die Zertifizierungsstelle dem Zertifizierungswerber Konformitätszeichen in Form von Datenschutzsiegel und -prüfzeichen ausstellen, sofern dies in den anzuwendenden Zertifizierungskriterien gemäß Art. 42 Abs. 5 DSGVO vorgesehen ist.

(2) Die Zertifizierungsstelle hat die Verwendung von Konformitätszeichen gemäß Abs. 1 im Sinne des Punktes 4.1.3 ISO/IEC 17065:2012 zu überprüfen. Konformitätszeichen dürfen jedenfalls nur in Einklang mit Art. 42 und Art. 43 DSGVO verwendet werden.

Zertifizierungsverzeichnis

§ 15. (1) Die Zertifizierungsstelle hat ein Verzeichnis über erteilte Zertifizierungen zu führen, welches zusätzlich zu den Vorgaben des Punktes 7.8 ISO/IEC 17065:2012 zumindest folgende Angaben enthält:

1. Den Geltungsbereich der Zertifizierung und eine aussagekräftige Beschreibung des Zertifizierungsgegenstandes,
2. die jeweiligen Zertifizierungskriterien,
3. die durchgeführten Evaluierungsmethoden und Tests und
4. die Ergebnisse der Zertifizierungsentscheidungen.

(2) Die Zertifizierungsstelle hat Informationen zu zertifizierten Verarbeitungsvorgängen und eine Zusammenfassung der Zertifizierungsverfahren einschließlich der Bewertungsberichte zu dokumentieren, in geeigneter Form zu veröffentlichen und bereitzustellen.

(3) Die Zertifizierungsstelle stellt der Datenschutzbehörde auf Anfrage das vollständige Verzeichnis gemäß Abs. 1 zur Verfügung.

Überwachungsverfahren und Aufzeichnungen

§ 16. (1) Die Zertifizierungsstelle hat nach Maßgabe des Punktes 7.9 ISO/IEC 17065:2012 geeignete Verfahren vorzusehen, die es ihr ermöglichen, die fortlaufende Einhaltung der Zertifizierungsanforderungen durch die Zertifizierungsinhaber zu überwachen (Überwachungsverfahren). Sämtliche mit den Überwachungsverfahren im Zusammenhang stehende Maßnahmen, einschließlich der Zeitraum der beabsichtigten Überwachung, sind zu dokumentieren.

(2) Ein Überwachungsverfahren ist geeignet, wenn festgelegt wird, wie die Überwachungstätigkeit in der Praxis durchgeführt und nach welchen Kriterien das Überwachungsverfahren evaluiert wird.

(3) Im Überwachungsverfahren sind in Einklang mit Art. 43 Abs. 2 lit. c DSGVO systematische, nach festgelegten Regeln durchgeführte Überprüfungen vorzusehen (Auditierungen). Es sind jedenfalls Festlegungen zu folgenden Kriterien zu treffen:

1. Terminpläne, die in bestimmten, im Voraus festgelegten, Zeitabständen eine Überprüfung vorsehen. Die Häufigkeit der Überprüfungen hat sich dabei insbesondere am

Zertifizierungsgegenstand, dem Ergebnis der Risikoanalyse und an der Anzahl an Beschwerdefällen zu orientieren.

2. Festlegung der anzuwendenden Methoden und der zu bewertenden Kriterien nach einem Bewertungsraster.

(4) Die Eignung des Verfahrens gemäß Abs. 2 ist durch eine konzeptionelle Darstellung des Überwachungsverfahrens nachzuweisen.

(5) Die Zertifizierungsstelle hat Aufzeichnungen gemäß Punkt 7.12 ISO/IEC 17065:2012 zu führen, um nachzuweisen, dass der Zertifizierungsinhaber die Anforderungen an die Zertifizierung erfüllt. Der Datenschutzbehörde ist jederzeit Zugang zu diesen Aufzeichnungen zu gewähren.

Beendigung, Einschränkung, Aussetzung oder Widerruf der Zertifizierung

§ 17. (1) Die Zertifizierungsstelle hat für den Fall der Beendigung, Einschränkung, Aussetzung oder des Widerrufs einer Zertifizierung die Voraussetzungen des Punktes 7.11 ISO/IEC 17065:2012 zu erfüllen.

(2) Die Zertifizierungsstelle hat der Datenschutzbehörde die Gründe für die Beendigung, Einschränkung, Aussetzung oder den Widerruf einer Zertifizierung mitzuteilen.

(3) Die Zertifizierungsstelle hat Anweisungen der Datenschutzbehörde, eine bereits erteilte Zertifizierung zu widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht mehr erfüllt werden, zu befolgen. Der Zertifizierungsinhaber, der von dieser Anweisung betroffen ist, hat im Rahmen des Widerrufverfahrens Parteistellung.

Beschwerdeverfahren

§ 18. (1) Die Zertifizierungsstelle hat nach Maßgabe des Punktes 7.13 ISO/IEC 17065:2012 geeignete Verfahrensrichtlinien über die Behandlung der bei ihr einlangenden Beschwerden über Verstöße gegen oder die Umsetzung von Zertifizierungsanforderungen durch Zertifizierungsinhaber festzulegen und das diesbezügliche Verfahren und die Strukturen durch Vorlage geeigneter Dokumente nachzuweisen.

(2) Verfahrensrichtlinien sind geeignet, wenn jedenfalls Folgendes festgelegt wird:

1. Angaben zu den beschwerdebefugten Personen (Beschwerdelegitimation),
2. Angaben zu den Personen, die für die Behandlung von Beschwerden zuständig sind, einschließlich Angaben über deren Ernennung, allfällige Unvereinbarkeitsregelungen und die vorgesehene Funktionszeit,
3. im Falle der Einrichtung eines kollegialen Entscheidungsgremiums, das Recht der Parteien, eine von ihnen ernannte natürliche Person in das Gremium zu entsenden,
4. Richtlinien über die Streitbeilegung, die vorsehen, dass Streitigkeiten innerhalb angemessener Frist, einfach, transparent und auf der Grundlage einer objektiven Bewertung der Umstände der Beschwerde und unter gebührender Berücksichtigung der Rechte der Parteien beurteilt werden,
5. das Recht der Parteien, innerhalb angemessener, von der Zertifizierungsstelle festzulegender Frist, zu Vorbringen der Gegenparteien Stellung zu nehmen,
6. eine Informationspflicht dahingehend, dass der Beschwerdeführer innerhalb von drei Monaten über den Stand des Verfahrens zu informieren ist, sowie
7. Gründe, die der Behandlung einer Beschwerde entgegenstehen.

(3) Die Verfahrensrichtlinien sind nach erfolgter Akkreditierung der Zertifizierungsstelle in allgemein zugänglicher Weise zu veröffentlichen.

(4) Die Zertifizierungsstelle hat ein Verzeichnis über die bei ihr eingegangenen Beschwerden und die ergriffenen Maßnahmen zu führen und der Datenschutzbehörde jederzeit Zugang zu diesem zu gewähren.

Anforderungen an ein Managementsystem

§ 19. (1) Die Zertifizierungsstelle hat nach Maßgabe der Punkte 8.1 bis 8.8 ISO/IEC 17065:2012 ein Managementsystem zu implementieren, welches ihr ermöglicht, den Nachweis dafür zu erbringen, dass sie die an sie gestellten Anforderungen und die ihr übertragenen Aufgaben und Befugnisse nach dieser Verordnung und nach der DSGVO erfüllen kann.

(2) Im Managementsystem sind zusätzlich zu den Vorgaben der Punkte 8.1 bis 8.8 ISO/IEC 17065:2012 vorzusehen:

1. Verfahren gemäß § 17 für den Fall der Beendigung, Einschränkung, Aussetzung oder des Widerrufs der Zertifizierung, einschließlich der Festlegung von Fristen, innerhalb derer die Mitteilung an die Datenschutzbehörde gemäß § 17 Abs. 2 zu erfolgen hat,
2. Verfahren für den Fall, dass die Akkreditierung der Zertifizierungsstelle gemäß Art. 43 Abs. 7 DSGVO widerrufen wird, einschließlich der Pflicht zur Benachrichtigung der Zertifizierungswerber oder –inhaber, sowie
3. Verfahren für den Fall von Beschwerden gemäß § 18, mit denen insbesondere die Vorgaben der Punkte 4.1.2.2 lit. c und lit. j, 4.6 lit. d und 7.13 ISO/IEC 17065:2012 umgesetzt werden.

(3) Die Zertifizierungsstelle hat der Datenschutzbehörde jederzeit Zugang zu den Dokumenten des implementierten Managementsystems zu gewähren.

Personenbezogene Bezeichnungen

§ 20. Bei den in dieser Verordnung verwendeten personenbezogenen Bezeichnungen gilt die gewählte Form für alle Geschlechter.

Verweisungen

§ 21. Verweisungen in dieser Verordnung auf andere Bundesgesetze sind als Verweisungen auf die jeweils geltende Fassung zu verstehen.

Inkrafttreten

§ 22. Diese Verordnung tritt mit Ablauf des Tages der Kundmachung im Bundesgesetzblatt in Kraft.

Jelinek

Unterzeichner	serialNumber=932783133,CN=Bundeskanzleramt,C=AT
Datum/Zeit	2021-02-17T15:46:26+01:00
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bundeskanzleramt.gv.at/verifizierung
Hinweis	Dieses Dokument wurde amtssigniert.