

Entwurf

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 4.5.2016, S. 1, in der Fassung der Berichtigung ABl. Nr. L 127 vom 23.5.2018, 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 als eine Bedingung zur Feststellung oder Aufrechterhaltung der Zertifizierung zu erfüllen sind;
2. „Technischer Datenschutz“, sämtliche (physische) Maßnahmen, die eingesetzt werden, um zu gewährleisten, dass die Sicherheits- und Schutzanforderungen bei der Verarbeitung personenbezogener Daten erfüllt sind;
3. „Zertifizierungskriterien“, jene – von der akkreditierten Zertifizierungsstelle festgelegten und 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“, jener Verantwortliche 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“, jener Verantwortliche 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. Antragslegitimiert 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 Unterlagen anzuschließen. Die Akkreditierung als Zertifizierungsstelle setzt den Nachweis der Einhaltung 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 Unternehmensgesetzbuches – 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, auf deren Grundlage die Zertifizierung erteilt wird,

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: Darlegung der finanziellen, personellen und organisatorischen Ausstattung, und

8. den Nachweis der Abdeckung von finanziellen Verbindlichkeiten aus der Tätigkeit als Zertifizierungsstelle nach Maßgabe des Punktes 4.3 ISO/IEC 17065:2012.

(4) Die Angaben gemäß Abs. 3 sind durch Vorlage geeigneter Dokumente und Urkunden 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 und Urkunden in beglaubigter Übersetzung zu bescheinigen.

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

Unabhängigkeit

§ 5. (1) Die Zertifizierungsstelle hat die Unabhängigkeit der mit dem Zertifizierungsverfahren betrauten Personen sowie der für die Entscheidung über die Zertifizierung verantwortliche Person oder verantwortlichen Personen innerhalb der Zertifizierungsstelle nach Maßgabe der folgenden Bestimmungen durch Vorlage geeigneter Dokumente und Urkunden nachzuweisen.

(2) Unabhängigkeit liegt vor, wenn die Zertifizierungsstelle in keinem derart rechtlichen, wirtschaftlichen, finanziellen, organisatorischen, persönlichen oder fachlichen Abhängigkeits- oder Naheverhältnis zu dem Zertifizierungswerber steht, das ihr Urteil und ihre Unabhängigkeit und Integrität bei ihrer Tätigkeit als Zertifizierungsstelle in Frage stellen könnte.

(3) Der Unabhängigkeit steht entgegen, wenn die in Punkt 4.2 ISO/IEC 17065:2012 genannten Voraussetzungen nicht vollständig erfüllt sind und wenn zwischen der Zertifizierungsstelle und dem Zertifizierungswerber ein Vertragsverhältnis iSd Art. 26 Abs. 1 zweiter Satz oder Art. 28 Abs. 3 DSGVO besteht.

(4) Die Unabhängigkeit ist nachzuweisen durch:

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,
2. Angaben zu den entscheidungsbefugten Personen gemäß § 13 Abs. 1, aus welchen hervorgeht, dass keine personellen, organisatorischen oder finanziellen Verflechtungen zu den Zertifizierungswerbern bestehen und
3. Angaben zur fortlaufenden Finanzierung der Zertifizierungsstelle.

Fachwissen

§ 6. (1) Die Zertifizierungsstelle muss zusätzlich zu den Anforderungen des Punktes 6.1 ISO/IEC 17065:2012 über Ressourcen in den folgenden Bereichen verfügen und in der Lage sein, diese nachzuweisen:

1. Kenntnisse des Datenschutzrechts und hinreichende Erfahrung in seiner Anwendung, einschließlich technischer und organisatorischer Maßnahmen und Verfahren,
2. Kenntnisse des Telekommunikationsrechts sowie des Rechts der Dienste der Informationsgesellschaft und
3. Kenntnisse der für die Konformitätsbewertung 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 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, Naturwissenschaften, Technik oder Mathematik gekennzeichnet ist und das zur Führung des akademischen Grades Magister, Master oder Diplom-Ingenieur berechtigt, oder
2. den erfolgreichen Abschluss einer technischen Ausbildung, die zur Führung der Qualitätsbezeichnung Ingenieur im Sinne des Ingenieurgesetzes 2017 – InG 2017, BGBl. I Nr. 23/2017 berechtigt.

(4) Die juristischen und technischen Fachkenntnisse gemäß Abs. 2 und Abs. 3 können auch in Form einer mindestens fünfjährigen einschlägigen Berufserfahrung nachgewiesen werden.

(5) Die mit dem Zertifizierungsverfahren betrauten Personen müssen über ausreichende Kenntnisse und Erfahrung mit Auditierungen im Sinne des § 16 Abs. 3 verfügen.

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

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

(8) 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.

(9) 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.

Anforderungen an die Organisationsstruktur und Maßnahmen zur Verhinderung von Interessenkonflikten und zur Sicherstellung der Vertraulichkeit

§ 7. (1) Eine Zertifizierungsstelle hat ihre Zertifizierungstätigkeit im Sinne des Punktes 5.1 ISO/IEC 17065:2012 zu strukturieren.

(2) Eine Zertifizierungsstelle hat durch geeignete Maßnahmen und Mechanismen im Sinne des Punktes 5.2 ISO/IEC 17065:2012 zu gewährleisten, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen und sie ihre Tätigkeit unparteiisch durchführt.

(3) Die Eignung ist durch einen – gegenüber dem gesamten Personal der Zertifizierungsstelle für verbindlich erklärten – Maßnahmenkatalog nachzuweisen, der jedenfalls folgendes zu beinhalten hat:

1. Unvereinbarkeitsbestimmungen, welche festlegen, dass das Personal der Zertifizierungsstelle keiner weiteren, mit der Ausübung ihrer Tätigkeit unvereinbaren Geschäftstätigkeit nachgeht,
2. Offenlegungspflichten hinsichtlich vergangener oder gegenwärtiger Verbindungen mit dem Zertifizierungswerber, welche die Unparteilichkeit in Frage stellen können,
3. Implementierung von Stellvertreterregelungen im Falle festgestellter Interessenkonflikte,
4. Verschwiegenheitsklauseln oder Geheimhaltungsvereinbarungen,
5. Verpflichtung zur Einhaltung des Datengeheimnisses iSd § 6 Abs. 1 DSGVO, sowie
6. Weisungsfreiheit gegenüber den Zertifizierungswerbern.

(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.

Zertifizierungsverfahren

§ 8. (1) Die Zertifizierung erfolgt auf Grundlage eines schriftlichen Antrags des Zertifizierungswerbers an die Zertifizierungsstelle, der sämtliche für den Zertifizierungsprozess 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 Zertifizierung, die beantragt wird,
3. Informationen bezüglich aller allfällig ausgegliederten Prozesse, die vom Zertifizierungswerber genutzt werden, einschließlich einer Kopie allfälliger Verträge gemäß Art. 26 Abs. 1 zweiter Satz oder Art. 28 Abs. 3 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 sämtliche für das Zertifizierungsverfahren erforderlichen Informationen im Sinne des Punktes 4.6 ISO/IEC 17065:2012 in allgemein zugänglicher Form zu veröffentlichen und auf Anfrage bereitzustellen.

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

(5) 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.

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

Zertifizierungsvereinbarung

§ 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,
2. die Dauer, für welche die Zertifizierung erteilt oder verlängert wird,
3. eine Berichtspflicht des Zertifizierungswerbers über wesentliche Änderungen, welche die Erfüllung der vereinbarten Verpflichtungen beeinträchtigen können,
4. Verpflichtungen des Zertifizierungswerbers im Zusammenhang mit der Beendigung, Einschränkung, Aussetzung oder Zurückziehung der Zertifizierung, insbesondere, dass
 - a) jeglicher Verweis oder jegliche Bezugnahme auf die erteilte Zertifizierung zu unterbleiben hat,

- b) etwaige Konformitätszeichen nach § 14 Abs. 1 zurückzustellen und nicht mehr zu verwenden sind.
- 5. die Verpflichtung des Zertifizierungswerbers, den mit der Durchführung der Zertifizierung betrauten Personen der Zertifizierungsstelle zur Überprüfung der fortlaufenden Einhaltung der in der Zertifizierungsvereinbarung festgelegten Verpflichtungen Zugang zu den Betriebs- oder Produktionsstätten sowie Einsicht in die erforderlichen Unterlagen zu gewähren,
- 6. der Hinweis darauf, dass die Zertifizierung unbeschadet der aus der DSGVO resultierenden Verpflichtungen erfolgt, denen der Zertifizierungswerber unterliegt,
- 7. die Konsequenzen für den Zertifizierungswerber, wenn die Akkreditierung der Zertifizierungsstelle gemäß Art. 43 Abs. 7 DSGVO widerrufen wird,
- 8. Verpflichtungen der Zertifizierungsstelle im Zusammenhang mit Beschwerden in Bezug auf die Einhaltung der Zertifizierungsanforderungen, wie insbesondere
 - a) einen internen Maßnahmenkatalog für die Behandlung der einlangenden Beschwerden zu erstellen, 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 iSd DSGVO.
- 9. die gemäß § 11 festgelegten Evaluierungsmethoden in Bezug auf den Zertifizierungsgegenstand, sowie
- 10. die Festlegung geeigneter Kommunikationsstrukturen zwischen Zertifizierungsstelle und Zertifizierungswerber.

Änderung von Zertifizierungsanforderungen

§ 10. (1) Im Falle einer Änderung der Zertifizierungsanforderungen hat die Zertifizierungsstelle den Zertifizierungsinhaber unverzüglich zu verständigen und die Umsetzung der erforderlichen Änderungen zu überprüfen.

(2) Zusätzlich zu den Punkten 7.10.1 und 7.10.2 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 Entscheidungen 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.

(2) Die Zertifizierungsstelle hat in den standardisierten Bewertungsmethoden gemäß Abs. 1 festzulegen, inwiefern Verhaltensregeln gemäß Art. 40 DSGVO, an denen der Zertifizierungswerber teilnimmt, sowie Zertifizierungen gemäß Art. 42 DSGVO, die ein Zertifizierungswerber bereits besitzt, zum Nachweis der Übereinstimmung der Verarbeitungsvorgänge mit den Zertifizierungskriterien herangezogen werden können.

(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 im Rahmen des Zertifizierungsverfahrens ist nach Maßgabe der folgenden Bestimmungen zulässig:

- 1. die extern Betrauten verfügen über das Fachwissen und die Erfahrung gemäß § 6 Abs. 2 bis Abs. 4,
- 2. die Tätigkeit erfolgt nach den Anforderungen der relevanten internationalen (insbesondere ISO/IEC) Normen,
- 3. vertraglich vereinbarte Unvereinbarkeitsbestimmungen und Maßnahmen zur Sicherstellung der Vertraulichkeit unter sinngemäßer Anwendung des § 7 Abs. 2 bis Abs. 4,
- 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. 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.

Zertifizierungsentscheidung

§ 13. (1) Die Zertifizierungsstelle hat die Entscheidung in Bezug auf die Zertifizierung des Zertifizierungswerbers 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 Zertifizierungsstelle hat dem Zertifizierungswerber im Falle der 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 aussagekräftige Beschreibung des Zertifizierungsgegenstandes, sowie
5. den Zeitraum im Sinne des § 9 Abs. 2 Z 2, für welchen die Zertifizierung erteilt wird.

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

Konformitätszeichen

§ 14. (1) Zusätzlich zur schriftlichen Bescheinigung gemäß § 13 Abs. 3 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 im Sinne des Punktes 4.1.3 ISO/IEC 17065:2012 zu überprüfen.

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 eine Zusammenfassung der Bewertungsberichte in geeigneter Form zu veröffentlichen und auf Anfrage bereitzustellen.

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).

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

(3) Im Verfahren sind 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.

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

(4) 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. 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.

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 Unterlagen 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 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. Verfahrensrichtlinien, 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. 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.

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.