Allgemeiner Teil

Die 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), ABl. Nr. L 119 vom 04.05.2016 S. 1, (im Folgenden: DSGVO), in der Fassung der Berichtigung ABl. Nr. L 127 vom 23.05.2018 S. 2, gilt seit dem 25. Mai 2018.

Gemäß Art. 42 DSGVO können datenschutzspezifische Zertifizierungsverfahren sowie Datenschutzsiegel und –prüfzeichen eingeführt werden (Zertifizierung). Laut Erwägungsgrund 100 der DSGVO soll dadurch die Transparenz im Zusammenhang mit der Verarbeitung personenbezogener Daten erhöht und die Einhaltung der DSGVO verbessert werden. Darüber hinaus soll es Verbrauchern ermöglicht werden, sich einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen zu verschaffen.

Ein Zertifizierungsverfahren wird anhand der Zertifizierungsanforderungen und insbesondere anhand der gemäß Art. 42 Abs. 5 DSGVO genehmigten Zertifizierungskriterien durchgeführt. Das Ergebnis einer positiven Konformitätsbewertung ist die Erteilung einer schriftlichen Konformitätsbescheinigung (Zertifizierung), welche als Nachweis dafür dient, dass die DSGVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Bei der Möglichkeit der Zertifizierung handelt es sich – zusätzlich zur Möglichkeit der Teilnahme an branchenspezifischen Verhaltensregeln gemäß Art. 40 DSGVO – um ein Instrument der datenschutzrechtlichen Selbstregulierung für Rechtsunterworfene.

Datenschutzspezifische Zertifizierungsverfahren sowie Datenschutzsiegel und –prüfzeichen gemäß Art. 42 DSGVO können

- als Faktor herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen (Art. 24 Abs. 3 DSGVO),

- als Faktor herangezogen werden, um die Erfüllung der gemäß Art. 32 Abs. 1 DSGVO zu implementierenden technischen und organisatorischen Maßnahmen nachzuweisen (Art. 32 Abs. 3 DSGVO),

- unter den Voraussetzungen von Art. 46 Abs. 2 lit. f DSGVO „geeignete Garantien“ für die Übermittlung von personenbezogenen Daten an ein Drittland oder eine internationale Organisation sein (Art. 42 Abs. 2 DSGVO),

- bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag je nach Einzelfall gebührend berücksichtigt werden (Art. 83 Abs. 2 lit. j DSGVO).

Die Zertifizierung erfolgt unbeschadet der Aufgaben und Befugnisse der Datenschutzbehörde gemäß Art. 57 und Art. 58 DSGVO durch eine akkreditierte Zertifizierungsstelle gemäß Art. 43 Abs. 1 DSGVO. In Österreich fungiert die Datenschutzbehörde nach Maßgabe des § 24 Abs. 3 des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999 als einzige nationale Akkreditierungsstelle gemäß Art. 43 Abs. 1 lit. a DSGVO.

Art. 43 Abs. 2 DSGVO hat für die Akkreditierung einen allgemein gehaltenen Rahmen festgelegt, der in Grundsätzen vorgibt, welche Voraussetzungen die Zertifizierungsstellen erfüllen müssen, um akkreditiert werden zu können.

Demnach dürfen Zertifizierungsstellen nur dann akkreditiert werden, wenn sie:

(a) ihre Unabhängigkeit und ihr Fachwissen hinsichtlich des Gegenstands der Zertifizierung zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen haben,

(b) sich verpflichtet haben, die Kriterien nach Art. 42 Abs. 5, die von der gemäß Art. 55 oder Art. 56 zuständigen Aufsichtsbehörde oder – gemäß Art. 63 – von dem Europäischen Datenschutzausschuss (im Folgenden: Ausschuss) genehmigt wurden, einzuhalten,

(c) Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf der Datenschutzzertifizierung sowie der Datenschutzsiegel und -prüfzeichen festgelegt haben,

(d) Verfahren und Strukturen festgelegt haben, mit denen sie Beschwerden über Verletzungen der Zertifizierung oder die Art und Weise, in der die Zertifizierung von dem Verantwortlichen oder dem Auftragsverarbeiter umgesetzt wird oder wurde, nachgehen und diese Verfahren und Strukturen für betroffene Personen und die Öffentlichkeit transparent machen, und

(e) zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen haben, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

In Umsetzung der unionsrechtlichen Verpflichtung des Art. 57 Abs. 1 lit. p DSGVO und der innerstaatlichen Vorgaben des § 21 Abs. 3 DSG, werden im Verordnungsweg die Anforderungen an die Akkreditierung einer Zertifizierungsstelle festgelegt. Die Erteilung der Akkreditierung wird dabei an verschiedene Erfordernisse bzw. Bedingungen geknüpft, deren Vorliegen die Antragsteller erfüllen und gegenüber der Datenschutzbehörde als zuständige Akkreditierungsstelle in einem Verfahren nachweisen müssen. In diesem Zusammenhang treffen die Antragsteller umfassende Mitwirkungspflichten, um die Erfüllung der Voraussetzungen zu belegen.

Der Stellungnahme des Ausschusses „Stellungnahme 30/2020 für Zertifizierungsstellen gemäß Art. 43 Abs. 3 DSGVO“ wurde Rechnung getragen.

Der gegenständliche Verordnungswurf trägt darüber hinaus den Leitlinien des Ausschusses „Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43“ samt Anhang (siehe dazu: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en) sowie den bisherigen Stellungnahmen des Ausschusses zu den von Aufsichtsbehörden anderer Mitgliedstaaten verfassten Anforderungen im Sinne des Art. 43 Abs. 3 DSGVO Rechnung (siehe dazu: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en).

Besonderer Teil

Zu § 1:

Nach den Vorgaben der Leitlinien des Ausschusses hat ein Antragsteller die Voraussetzungen der Internationalen Norm ISO/IEC 17065:2012 Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren (im Folgenden: ISO/IEC 17065:2012) und darüber hinaus die zusätzlich gemäß Art. 43 Abs. 3 DSGVO festgelegten Voraussetzungen zu erfüllen, um als Zertifizierungsstelle akkreditiert zu werden.

Zu § 3:

Die akkreditierte Zertifizierungsstelle unterliegt der Aufsicht durch die Datenschutzbehörde, die die Akkreditierung gemäß Art. 43 Abs. 7 DSGVO zu widerrufen hat, wenn die Zertifizierungsstelle die Anforderungen an die Akkreditierung nicht oder nicht mehr erfüllt, oder wenn die Zertifizierungsstelle Maßnahmen ergreift, die nicht mit der DSGVO vereinbar sind. Weiters kommt der Datenschutzbehörde gemäß Art. 58 Abs. 2 lit. h DSGVO die Abhilfebefugnis zu, eine durch die Zertifizierungsstelle erteilte Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden (vgl. Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43, S 21).

Eine über diese Befugnisse hinausgehende Aufsicht gegenüber der Zertifizierungsstelle kommt der Datenschutzbehörde nach der DSGVO nicht zu, sodass im Setzen von Maßnahmen durch die Zertifizierungsstelle jedenfalls kein hoheitliches Tätigwerden eines „Beliehenen“ zu sehen ist. Allfällig gesetzte Maßnahmen sind ihrem Wesen nach zivilrechtlicher Natur. Gegen gesetzte Maßnahmen steht folglich auch kein Beschwerderecht eines Zertifizierungswerbers (etwa im Hinblick auf die Nichterteilung einer Zertifizierung durch die Zertifizierungsstelle) bzw. eines Zertifizierungsinhabers (etwa im Hinblick auf den Widerruf einer Zertifizierung durch die Zertifizierungsstelle) an die Datenschutzbehörde zu. Allfällige Streitigkeiten zwischen Zertifizierungsstelle und Zertifizierungswerber bzw. -inhaber sind jedenfalls und ausschließlich im Zivilrechtsweg auszutragen (vgl. *Kröpfl*, Datenschutzrechtliche Zertifizierungen in *Jahnel* [Hrsg.], Datenschutzrecht Jahrbuch 19 [2019] S 215 f).

Zu § 4:

Zu Abs. 1:

Um akkreditiert zu werden und die Funktion einer Zertifizierungsstelle ausüben zu können, bedarf es eines schriftlichen Antrages an die Datenschutzbehörde als zuständige Aufsichtsbehörde.

Nach Punkt 4.1.1 ISO/IEC 17065:2012 muss die Zertifizierungsstelle eine juristische Person sein. Zu berücksichtigen ist jedoch, dass der in der englischen Version des Punktes 4.1.1 ISO/IEC 17065:2012 verwendete Begriff „legal entity“ weiter zu verstehen ist als der in der deutschen Version verwendete Begriff „juristische Person“.

Demnach können auch Personengesellschaften als Zertifizierungsstelle akkreditiert werden.

Nicht als Zertifizierungsstelle akkreditiert werden können hingegen Einpersonenunternehmen, eingeschlossen auch solche, die unter einer Firma gemäß § 19 Abs. 1 Z 1 UGB gerichtlich protokolliert sind. Bei Einpersonenunternehmen ist ganz allgemein nicht davon auszugehen, dass diese in der Lage sein werden, die in der DSGVO und in dieser Verordnung geforderten Organisationsstrukturen zu etablieren.

Eine neuerliche Antragstellung auf Akkreditierung als Zertifizierungsstelle ist im Falle eines negativen Bescheids (Nicht-Akkreditierung) jederzeit möglich, unter der Voraussetzung, dass dieser negative Bescheid in Rechtskraft erwachsen ist.

Zu Abs. 3:

Der schriftliche Antrag hat neben den in den §§ 5 bis 19 normierten Voraussetzungen auch die in Z 1 bis Z 8 genannten Angaben zu enthalten.

Sofern alle Voraussetzungen erfüllt sind, besteht ein subjektiver Rechtsanspruch des Antragstellers auf Akkreditierung gemäß Art. 43 Abs. 3 erster Satz iVm Art. 58 Abs. 3 lit. e DSGVO.

Zu Z 2:

Eine Akkreditierung darf in jedem Fall nur dann erfolgen, wenn die geplante Zertifizierungstätigkeit und der Zertifizierungsgegenstand vorgelegt werden. Es muss klar ersichtlich sein, welche Verarbeitungsvorgänge Gegenstand der Zertifizierung sind und welche Komponenten bewertet werden.

Gegenstand einer Zertifizierung ist immer eine Datenverarbeitung im Zusammenhang mit personenbezogenen Daten. Vor dem Hintergrund, dass eine Prüfung der Datenverarbeitung auch die eingesetzten technischen Systeme sowie die Verarbeitungsorganisation umfasst, werden Hard- und Software sowie getroffene technische und organisatorische Maßnahmen (wie ein Datenschutzmanagementsystem) mittelbar geprüft und zertifiziert (vgl. *Kröpfl*, Datenschutzrechtliche Zertifizierungen in *Jahnel*, Datenschutzrecht Jahrbuch 19 S 170 mwN).

Die Leitlinien des Ausschusses 1/2018 über Zertifizierungen und Zertifizierungskriterien nach Artikel 42 und 43 DSGVO (siehe dazu: https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-12018-certification-and-identifying-certification_en) gehen auf S 15 ff von einem weiten Begriffsverständnis des Zertifizierungsgegenstandes aus. Als Beispiele für Zertifizierungsgegenstände werden etwa genannt:

- Sicheres Log-in

- Teile von Online-Banking-Systemen.

Eine Zertifizierung der Organisation des Verantwortlichen oder Auftragsverarbeiters in ihrer Gesamtheit ist jedoch nicht möglich (vgl. Leitlinien des Ausschusses 1/2018 über Zertifizierungen und Zertifizierungskriterien nach Artikel 42 und 43 DSGVO, S 15 ff; *Strohmaier* in *Knyrim* (Hrsg), DatKomm [2019] Art. 42 DSGVO Rz 17 f).

Zu Z 3:

Gemäß Art. 43 Abs. 2 lit. b DSGVO erteilt die Zertifizierungsstelle Zertifizierungen auf Grundlage der gemäß Art. 42 Abs. 5 DSGVO genehmigten Zertifizierungskriterien. Im Rahmen des Akkreditierungsverfahrens sind daher die Zertifizierungskriterien, die von der Zertifizierungsstelle verwendet werden, anzugeben. Eine Zertifizierung kann auf Grundlage von Zertifizierungskriterien erfolgen, die von der Datenschutzbehörde oder dem Europäischen Datenschutzausschuss genehmigt wurden. Sofern die Erteilung von Zertifizierungen auf Grundlage von weiteren Zertifizierungskriterien erfolgen soll, die zum Zeitpunkt der Akkreditierung der Zertifizierungsstelle noch nicht existiert haben oder aus anderen Gründen nicht im Akkreditierungsverfahren angegeben wurden, kann die akkreditierte Zertifizierungsstelle einen Änderungsantrag an die Datenschutzbehörde stellen.

Eine Liste aller Zertifizierungskriterien, auf deren Grundlage eine Zertifizierung erfolgen kann, findet sich auf der Webseite der Österreichischen Datenschutzbehörde (siehe dazu: https://www.dsb.gv.at/aufgaben-taetigkeiten/Zertifizierungen).

Die Genehmigung von Zertifizierungskriterien erfolgt durch schriftlichen Antrag an die Datenschutzbehörde. Ein Antrag auf Genehmigung von Zertifizierungskriterien kann jederzeit und unabhängig vom Antrag auf Akkreditierung als Zertifizierungsstelle eingebracht werden. Dies bedeutet, dass auch Stellen, wie beispielsweise unabhängige Normungsgremien, die nicht als Zertifizierungsstelle tätig werden, Zertifizierungskriterien ausarbeiten und deren Genehmigung beantragen können.

Sofern die Datenschutzbehörde den Antrag als genehmigungsfähig erachtet, werden, zum Zwecke der Rechtsharmonisierung, alle Zertifizierungskriterien gemäß Art. 64 Abs. 1 lit. c DSGVO dem Ausschuss vorgelegt. Im Falle einer positiven Stellungnahme des Ausschusses erfolgt die Genehmigung der Zertifizierungskriterien mit Bescheid durch die Datenschutzbehörde.

Im Rahmen des Antrags ist anzugeben, ob die Genehmigung zu einem Europäischen Datenschutzsiegel gemäß Art. 42 Abs. 5 letzter Satz DSGVO führen soll.

Bei der Ausarbeitung von Zertifizierungskriterien sind Methoden festzulegen, die – abhängig von Art und Umfang des Zertifizierungsgegenstandes – eine Bewertung beispielsweise folgender Aspekte ermöglichen:

- die Verarbeitung personenbezogener Daten erfolgt nach den Grundsätzen des Kapitels II der DSGVO;

- die Verarbeitung personenbezogener Daten erfolgt unter Beachtung der Rechte der betroffenen Personen nach den Bestimmungen der Art. 12 bis 23 DSGVO;

- die Verarbeitung personenbezogener Daten erfolgt unter Berücksichtigung der Vorgaben des Art. 25 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen);

- die Implementierung geeigneter technischer und organisatorischer Maßnahmen, die dafür ausgelegt sind, ein angemessenes Schutzniveau nach den Vorgaben des Art. 32 Abs. 1 DSGVO herzustellen (Sicherheit der Verarbeitung);

- die Implementierung von Abhilfemaßnahmen gemäß Art. 35 Abs. 7 lit. d DSGVO im Rahmen der Durchführung einer Datenschutz-Folgenabschätzung.

Bevor die Zertifizierungsstelle Zertifizierungen anhand von Zertifizierungskriterien gemäß Art. 42 Abs. 5 zweiter Satz DSGVO (Europäisches Datenschutzsiegel) in einer möglichen Niederlassung eines anderen Mitgliedstaates durchführt, hat die Zertifizierungsstelle die zuständige Aufsichtsbehörde des jeweiligen Mitgliedstaates zu benachrichtigen (vgl. Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43, S 19).

Zu Z 5:

Die Akkreditierung soll dem Antragsteller nur erteilt werden, wenn gegen ihn keine strafrechtlichen Verurteilungen vorliegen. Die Tätigkeit als Zertifizierungsstelle ist mit einem Vertrauensverhältnis verbunden. Dazu ist es erforderlich, dass ein Antragsteller nachweist, dass er sich gesetzestreu verhalten hat (vgl. dazu die Rechtsprechung des Verwaltungsgerichtshofes in Bezug auf die Frage der Vertrauenswürdigkeit eines Sachverständigen, VwGH 23.03.1999, Zl. 96/19/1229, 03.07 2000, Zl. 98/10/0368, und 26.06.2008,

Zl. 2008/06/0033). Die Regelung ist an die Gewerbeordnung 1994 – GewO 1994, BGBl. Nr. 194, angelehnt, die an verschiedenen Stellen vorsieht, dass die Erteilung der Gewerbeberechtigung der Überprüfung der Zuverlässigkeit bedarf. Sofern die Zuverlässigkeit und strafrechtliche Unbescholtenheit nicht Voraussetzung für die Ausübung der beruflichen Tätigkeit ist, ist daher die Vorlage einer Registerauskunft für Verbände gemäß § 89m Gerichtsorganisationsgesetz – GOG, RGBl. Nr. 217/1896, erforderlich.

Zu Abs. 4:

Eine Akkreditierung setzt die Erfüllung der mit dem vorliegenden Entwurf normierten Akkreditierungsvoraussetzungen im Zeitpunkt der Antragstellung voraus. In diesem Zusammenhang treffen den Antragsteller Mitwirkungspflichten. Sofern die Angaben des Antragstellers nicht aus allgemein zugänglichen öffentlichen Registern überprüfbar sind, hat der Antragsteller dem Antrag sämtliche Dokumente beizufügen, welche die Erfüllung der Akkreditierungsvoraussetzungen bescheinigen. Die Bescheinigung kann durch Vorlage eines Dokuments erfolgen. Allgemein zugänglich in diesem Sinn sind Register, wenn der Zugang kostenlos ist, ohne dass das Erfordernis einer besonderen (materien-)gesetzlichen Berechtigung für Behörden besteht.

Zu Abs. 5:

Die Akkreditierung ist nicht von einem Sitz bzw. Aufenthalt in Österreich abhängig; somit sind auch im Europäischen Wirtschaftsraum gemäß EWR-Abkommen, BGBl. Nr. 909/1993, ansässige Personen antragslegitimiert. Die in Abs. 3 normierten Akkreditierungsvoraussetzungen sind in diesem Fall durch Vorlage geeigneter Dokumente allenfalls in beglaubigter Übersetzung nachzuweisen (vgl. in diesem Zusammenhang Art. 8 Abs. 1 Bundes-Verfassungsgesetz – B-VG, BGBl. Nr. 1/1930, demgemäß die deutsche Sprache, unbeschadet der den sprachlichen Minderheiten bundesgesetzlich eingeräumten Rechte, die Staatssprache der Republik ist).

Zu Abs. 7:

Es gilt zu beachten, dass Zertifizierungsstellen als datenschutzrechtliche Verantwortliche gemäß Art. 4 Z 7 DSGVO personenbezogene Daten verarbeiten. Hierzu zählt etwa die Verarbeitung von Daten, die von Zertifizierungswerbern oder –inhabern zum Zwecke der Abwicklung des Zertifizierungsverfahrens zur Verfügung gestellt werden, oder die sie im Rahmen von Beschwerdeverfahren gemäß § 18 erhalten.

Es ist davon auszugehen, dass eine Stelle, die ihrer Eigenschaft als datenschutzrechtlicher Verantwortlicher gegen die DSGVO verstößt, nicht den für die Ausübung der Tätigkeit als Zertifizierungsstelle erforderlichen Sorgfaltsmaßstab erfüllt.

Ein Verstoß gegen die DSGVO kann daher dazu führen, dass ein Antrag auf Akkreditierung abgewiesen bzw. dass eine bereits erteilte Akkreditierung gemäß Art. 43 Abs. 7 DSGVO widerrufen wird.

Zu § 5:

Aufgrund der Organisationsstruktur der Zertifizierungsstelle muss jedenfalls Folgendes gewährleistet werden:

- Unparteilichkeit gemäß § 5;

- Unabhängigkeit gemäß § 6 Abs. 2;

- Maßnahmen zur Identifizierung und Verhinderung von Interessenkonflikten gemäß § 6 Abs. 4.

Diese Maßnahmen sollen sicherstellen, dass eine Zertifizierungsstelle ihre Tätigkeit ohne ungebührliche Beeinflussung von außen ausübt und Zertifizierungen nur deshalb erteilt, weil ein Abhängigkeits- oder Naheverhältnis besteht, das eine objektiven Beurteilung nicht ermöglicht.

Unparteilichkeit bedeutet insbesondere, dass keine Befangenheit oder der Anschein einer Befangenheit gegenüber einem Zertifizierungswerber vorliegt. Befangenheit ist beispielsweise anzunehmen, wenn eine Zertifizierung in eigener Sache vorgenommen werden soll oder der Zertifizierungswerber ein Angehöriger (vgl. dazu § 36a AVG) jener Personen ist, die die Evaluierung (§ 11) oder die Zertifizierungsentscheidung (§ 13) vornehmen.

Unabhängigkeit bedeutet insbesondere, dass kein finanzielles oder wirtschaftliches Abhängigkeitsverhältnis besteht, das eine objektiv durchgeführte Zertifizierung verhindert.

Zu § 6:

Zu Abs. 1:

Im Zeitpunkt der Antragstellung sind der Zertifizierungsstelle die konkreten Zertifizierungswerber noch nicht bekannt. Deshalb soll durch die Umsetzung dieser Anforderungen sichergestellt werden, dass die Unparteilichkeit der Zertifizierungsstelle bei ihren Tätigkeiten laufend gegeben ist.

Zu Abs. 2:

Unabhängigkeit im Sinne des Art. 43 Abs. 2 lit. a DSGVO bedeutet insbesondere, dass die Zertifizierungsstelle frei von Weisungen und Druck handeln kann und deren finanzielle Stabilität sichergestellt ist (vgl. Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43, S 16).

Zu § 7:

Zu Abs. 1:

Die Ressourcen im Zusammenhang mit dem geforderten Fachwissen müssen bei der Zertifizierungsstelle vorhanden sein, aber nicht notwendigerweise in einer Person (siehe Abs. 7). Sofern Personen aus der Zertifizierungsstelle ausscheiden, die ein bestimmtes Fachwissen besitzen (Schlüsselpersonal), hat die Zertifizierungsstelle diese Personen unverzüglich nachzubesetzen. Im Managementsystem nach § 19 ist ein Prozess zur Sicherstellung der unverzüglichen Nachbesetzung von Schlüsselpersonal vorzusehen.

Zu Z 2:

Hierzu zählen insbesondere Kenntnisse über alle nationalen und internationalen materienspezifischen Bestimmungen, die für den Zertifizierungsgegenstand von Relevanz sind.

Zu Abs. 4:

Die durch eine Berufserfahrung erworbenen Fachkenntnisse sollen jenen Kenntnissen, die im Rahmen eines Studiums erworben werden, weitgehend entsprechen. Spezifische Fachkenntnisse sind dabei nicht gefordert.

Zu Abs. 5:

Zur Durchführung der Evaluierung (§ 11) und der Bewertung der Evaluierungsergebnisse (§ 12) ist es erforderlich, dass das eingesetzte Personal über ausreichende Kenntnisse und Erfahrung mit Auditierungen im Sinne des § 16 Abs. 3 verfügt.

Zu Abs. 6:

Die für die Entscheidung über die Zertifizierung verantwortliche Person oder verantwortlichen Personen im Sinne des § 13 tragen die Letztverantwortung darüber, ob eine Zertifizierung erteilt wird. Vor diesem Hintergrund ist im Hinblick auf deren Fachwissen und deren Erfahrung ein hoher Maßstab zu setzen.

Im Gegensatz zur erforderlichen Berufserfahrung gemäß Abs. 4, die allgemein juristische und technische Fachkenntnisse vermittelt, muss es sich bei der erforderlichen Berufserfahrung gemäß Abs. 6 um eine spezifische Berufserfahrung im Bereich Datenschutzrecht und im Bereich des technischen Datenschutzes handeln. In diesem Zusammenhang wird insbesondere auf die Implementierung von Datenschutzmaßnahmen innerhalb einer Organisation abgestellt.

Die Berufserfahrung gemäß Abs. 6 ist zusätzlich zu den Anforderungen gemäß Abs. 2 bis Abs. 4 zu erbringen. Dies bedeutet, dass für jene für die Entscheidung über die Zertifizierung verantwortliche Person oder verantwortlichen Personen, die den Nachweis für die juristischen und technischen Fachkenntnisse nach Maßgabe des Abs. 4 erbringen, insgesamt zehn Jahre Berufserfahrung erforderlich sind, wovon mindestens fünf Jahre spezifisch auf den Bereich Datenschutzrecht oder technischer Datenschutz entfallen.

Die spezifische Berufserfahrung umfasst beispielsweise:

- Mitarbeit in der Rechts- oder Technikabteilung eines Unternehmens mit Schwerpunkt auf Datenschutzrecht oder Datensicherheit;

- Mitarbeit bei Projekten im Bereich Datenschutzrecht oder technischer Datenschutz;

- Tätigkeit als fachkundiger Laienrichter nach § 27 Abs. 2 DSG;

- Tätigkeit als fachkundiger Laienrichter in der Schiedsgerichtsbarkeit in den genannten Bereichen;

- Tätigkeit als gerichtlich beeideter und zertifizierter Sachverständiger in den genannten Bereichen;

- Tätigkeit als Unternehmensberater oder im Rahmen einer freiberuflichen Tätigkeit mit Schwerpunkt in den genannten Bereichen;

- Tätigkeit als Datenschutzbeauftragter.

Zu Abs. 7:

Das juristische und technische Fachwissen kann durch die Beschäftigung mehrerer Personen (juristisches und technisches Personal) nachgewiesen werden.

Zu Abs. 9:

Zu diesen Verfahren zählen etwa Fortbildungs- und Schulungsmaßnahmen, die in angemessenen Abständen abgehalten werden.

Zu § 8:

Zu Abs. 1:

Der zeitliche Ablauf eines Zertifizierungsverfahrens gestaltet sich wie folgt:

a) Antrag des Zertifizierungswerbers an die Zertifizierungsstelle (§ 8 Abs. 1);

b) Bewertung des Antrags durch die Zertifizierungsstelle (§ 8 Abs. 3);

c) Evaluierung durch die Zertifizierungsstelle, ob die Zertifizierungsanforderungen erfüllt sind, insbesondere, ob die Verarbeitungsvorgänge des Zertifizierungswerbers in Übereinstimmung mit den Zertifizierungskriterien erfolgen (§ 11);

d) Bewertung der Evaluierungserbnisse (§ 12);

e) Zertifizierungsentscheidung (§ 13).

Zu Abs. 2:

Im Rahmen des Zertifizierungsprogrammes ist insbesondere der genaue Ablauf des Zertifizierungsverfahrens festzulegen.

Zu Abs. 5:

Es wird davon Abstand genommen, im Verordnungstext eine konkrete Entscheidungsfrist zu normieren. Dies soll es der Zertifizierungsstelle ermöglichen, eine angemessene Frist unter Berücksichtigung von Art und Umfang des Zertifizierungsgegenstandes festzulegen.

Zu Abs. 6:

Nach Art. 42 Abs. 1 letzter Satz DSGVO ist den besonderen Bedürfnissen von Klein- und Mittelunternehmen Rechnung zu tragen. Bei der Festlegung der Kosten für das Zertifizierungsverfahren

sind daher – abhängig von Art und Umfang des Zertifizierungsgegenstandes – die finanziellen Ressourcen von Klein- und Mittelunternehmen größtmöglich zu berücksichtigen.

Zu Abs. 7:

Dies umfasst auch allfällige ältere Informationsversionen zum Zertifizierungsprogramm.

Zu § 9:

Zu Abs. 1:

Die Aufgaben und Befugnisse der Datenschutzbehörde bleiben von der Zertifizierungsvereinbarung unberührt.

Zu Abs. 2:

Zu Z 3:

Es gilt zu beachten, dass eine Zertifizierung gemäß Art. 42 Abs. 7 DSGVO für eine Höchstdauer von drei Jahren erteilt werden kann. Die Festlegung einer kürzeren Zertifizierungsdauer ist zulässig, muss jedoch begründet werden.

Zu Abs. 4:

Dies umfasst die Tätigkeit der Zertifizierungsstelle im Rahmen des Zertifizierungsverfahrens, als auch die Tätigkeit nach erteilter Zertifizierung.

Unter Tätigkeit der Zertifizierungsstelle ist sowohl die Tätigkeit im Rahmen des Zertifizierungsverfahrens als auch jede Tätigkeit nach erteilter Zertifizierung zu verstehen.

Zu § 10:

Zu Abs. 1:

Der Zertifizierungsinhaber hat sich im Vorfeld in der Zertifizierungsvereinbarung gemäß § 9 Abs. 2 Z 2 verpflichtet, die von der Zertifizierungsstelle gemäß § 10 festgestellten erforderlichen Änderungen von Zertifizierungsanforderungen nach Gewährung einer angemessenen Frist umzusetzen.

Es kann der Fall auftreten, dass eine Änderung von Zertifizierungsanforderungen mit einer Änderung von Zertifizierungskriterien einhergeht. Allerdings ist darauf hinzuweisen, dass eine einseitige Änderung der durch die Datenschutzbehörde oder dem Europäischen Datenschutzausschuss gemäß Art. 42 Abs. 5 DSGVO genehmigten Zertifizierungskriterien durch die Zertifizierungsstelle nicht möglich ist. Diesfalls ist ein Änderungsantrag an die zuständige Aufsichtsbehörde – in dem Fall, dass die Zertifizierungskriterien durch die Datenschutzbehörde genehmigt wurden, an die Datenschutzbehörde – durch jene Stelle notwendig, die die Zertifizierungskriterien ausgearbeitet hat.

Zu § 11:

Zu Abs. 1:

In den standardisierten Bewertungsmethoden ist zu präzisieren, auf welche Weise die Zertifizierungsstelle den Zertifizierungswerber über die Nichtkonformität mit den Zertifizierungskriterien informiert. In diesem Zusammenhang sollte jedenfalls die Art und der Zeitpunkt der Informationserteilung festgelegt werden. Die standardisierten Bewertungsmethoden sind aktuell zu halten.

Zu § 12:

Zu Abs. 1:

Es hat eine Bewertung der Evaluierungsergebnisse in Form der Erstellung eines Gutachtens zu erfolgen. Das Gutachten dient als Grundlage für die Zertifizierungsentscheidung gemäß § 13 sowie für eine allfällige Verlängerung oder einen allfälligen Widerruf der Zertifizierung.

Zu § 13:

Zu Abs. 1:

Die für die Entscheidung über die Zertifizierung verantwortliche Person oder verantwortlichen Personen sind inhaltlich nicht an die Bewertung gemäß § 12 gebunden.

Zu Abs. 3:

Bei der Zertifizierungsentscheidung handelt es sich um die Kerntätigkeit einer Zertifizierungsstelle, die bei dieser verbleiben soll. Eine Auslagerung dieser Kerntätigkeit an externe Sachverständige ist daher nicht möglich. Sofern im Einzelfall eine Zertifizierungsentscheidung nicht möglich ist (beispielweise aufgrund identifizierter Interessenkonflikte aller entscheidungsbefugten Personen) hat eine solche zu unterbleiben.

Zu Abs. 4:

Zu Z 4:

Bei der Beschreibung des Zertifizierungsgegenstands sind insbesondere die konkreten Verarbeitungsvorgänge, die Gegenstand der Zertifizierung sind, sowie die konkreten Komponenten, die bewertet wurden, anzugeben.

Zu Abs. 5:

Dem Zertifizierungswerber steht im Falle der Nichterteilung einer Zertifizierung kein Beschwerderecht an die Datenschutzbehörde zu. Allfällige Streitigkeiten zwischen Zertifizierungsstelle und Zertifizierungswerber sind ausschließlich im Zivilrechtsweg auszutragen (siehe dazu bereits die Erläuterungen zu § 3).

Zu Abs. 8:

Die Datenschutzbehörde hat gemäß Art. 58 Abs. 2 lit. h dritter Fall DSGVO die Befugnis, die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht erfüllt werden. Die Ausübung dieser Befugnis kommt beispielsweise dann in Betracht, wenn der Datenschutzbehörde im Rahmen einer Datenschutzüberprüfung gemäß Art. 58 Abs. 1 lit. a DSGVO (amtswegiges Prüfverfahren) zur Kenntnis gelangt, dass das zu überprüfende Unternehmen eine Zertifizierung beantragt hat, obwohl die Datenschutzbehörde im Rahmen der Datenschutzüberprüfung Verstöße gegen die DSGVO festgestellt hat, die einer Zertifizierung entgegenstehen.

Die Anweisung erfolgt mit Bescheid an die Zertifizierungsstelle. Um dem Zertifizierungswerber einen größtmöglichen Rechtsschutz zu bieten, ist dieser neben der Zertifizierungsstelle in das Verfahren als Partei einzubeziehen.

Zu § 14:

Zu Abs. 2:

Konformitätszeichen dürfen nicht in einer Art verwendet werden, die geeignet ist, einen falschen Eindruck über den Zertifizierungsgegenstand zu vermitteln und Verbraucher in die Irre zu führen. Sofern Zertifizierungsgegenstand ein einzelner Aspekt der DSGVO ist (etwa die Übereinstimmung mit den Grundsätzen nach Art. 5), so darf beispielsweise nicht der Eindruck vermittelt werden, dass der Verarbeitungsprozess in seiner Gesamtheit zertifiziert wurde.

Die einschlägigen Leitlinien des Ausschusses zu den Art. 42 f DSGVO sind zur Auslegung der Frage, auf welche Art und Weise Konformitätszeichen zu verwenden sind, heranzuziehen (siehe dazu bereits die Erläuterungen im allgemeinen Teil, S. 2).

Zu § 15

Zu Abs. 1:

Das Zertifizierungsverzeichnis dient dazu, sich einen raschen Überblick über erteilten Zertifizierungen zu verschaffen.

Zu Abs. 2:

Die Bewertungsberichte haben jedenfalls die Dauer der Gültigkeit einer bestimmten Zertifizierung zu enthalten.

Bei der Festlegung des Inhalts der Bewertungsberichte, die veröffentlicht und auf Anfrage zur Verfügung gestellt werden, ist der Schutz allfälliger Geschäfts- und Betriebsgeheimnisse gemäß §26b Bundesgesetz gegen den unlauteren Wettbewerb 1984 (UWG), BGBl. Nr. 448/1984, von Zertifizierungsinhabern zu berücksichtigen.

Zu § 17:

Zu Abs. 2:

Im Managementsystem gemäß § 19 sind Fristen festzulegen, innerhalb derer die Mitteilung an die Datenschutzbehörde über die Gründe für die Beendigung, Einschränkung, Aussetzung oder den Widerruf einer Zertifizierung zu erfolgen hat.

Zu Abs. 3:

Die Datenschutzbehörde hat gemäß Art. 58 Abs. 2 lit. h zweiter Fall DSGVO die Befugnis, die Zertifizierungsstelle anzuweisen, eine bereits erteilte Zertifizierung zu widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht mehr erfüllt werden

Die Anweisung erfolgt mit Bescheid an die Zertifizierungsstelle. Um dem Zertifizierungsinhaber einen größtmöglichen Rechtsschutz zu bieten, ist dieser neben der Zertifizierungsstelle als Partei in das Verfahren einzubeziehen.

Zu § 18:

Zu Abs. 1:

Die Bestimmung dient der Präzisierung von Art. 43 Abs. 2 lit. d DSGVO.

Bei dem Beschwerdeverfahren handelt es sich nicht um ein hoheitliches Verfahren. Dies ergibt sich schon aus

Art. 43 Abs. 1 DSGVO, wonach die Tätigkeit von Zertifizierungsstellen unbeschadet der Aufgaben und Befugnisse der Aufsichtsbehörde erfolgt. Folglich kann auch eine Entscheidung der Zertifizierungsstelle keine Wirkung entfalten, die gegebenenfalls mit staatlichem Zwang durchgesetzt werden kann. Dem Wesen der freiwilligen Selbstbindung durch die Einhaltung der Zertifizierungsanforderungen folgend, setzt die Führung solcher Verfahren sowie deren Umsetzung die freiwillige Mitwirkung sowie die Akzeptanz des Zertifizierungsinhabers (also des Verantwortlichen oder Auftragsverarbeiters) voraus. Dies bedeutet, dass eine betroffene Person bei Vorliegen der erforderlichen Voraussetzungen statt Inanspruchnahme des Beschwerdeverfahrens bei der Zertifizierungsstelle jederzeit Beschwerde an die Datenschutzbehörde erheben kann.

Zu Abs. 2:

Zu Z 2:

Durch Aufnahme von Unvereinbarkeitsregelungen in die Verfahrensrichtlinien über die Behandlung von Beschwerden, die das Personal der Zertifizierungsstelle zu befolgen hat, soll eine ausreichende Trennung zwischen Zertifizierungstätigkeiten und Beschwerdeverfahren gewährleistet werden (vgl. Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43, S 22).

Zu § 19:

Zu Abs. 1:

Eine Anforderung an das Managementsystem nach Punkt 8 ISO/IEC 17065:2012 ist, dass die Umsetzung aller nach dieser Verordnung vorgesehenen Voraussetzungen durch die Zertifizierungsstelle dokumentiert, bewertet, gesteuert und überwacht wird. Insbesondere muss die Zertifizierungsstelle sicherstellen, dass eine vollständige Dokumentation über die erteilten Zertifizierungen besteht und dass die jeweilige Zertifizierungsentscheidung samt Begründung nachvollzogen werden kann. Damit wird gewährleistet, dass die dauerhafte Einhaltung der Akkreditierungsvoraussetzungen durch die Zertifizierungsstelle überprüfbar ist. In diesem Zusammenhang ist darauf hinzuweisen, dass die Datenschutzbehörde die Einhaltung der Akkreditierungsvoraussetzungen auch nach erteilter Akkreditierung im Rahmen eines anlassunabhängigen amtswegigen Prüfverfahrens gemäß Art. 58 Abs. 1 lit. b DSGVO überprüfen kann (vgl. Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43, S 21).

Der Nachweis für den Aufbau eines Managementsystems kann entweder in Übereinstimmung mit Option A (Punkt 8.1.2) oder Option B (Punkt 8.1.3) erbracht werden.

Konkret sind jedenfalls folgende Voraussetzungen an ein Managementsystem zu erfüllen:

- Allgemeine Voraussetzungen (Punkt 8.1)
- Dokumentation (Punkt 8.2)
- Lenkung von Dokumenten (Punkt 8.3)
- Kontrolle von Dokumenten (Punkt 8.4)
- Managementbewertung (Punkt 8.5)
- Interne Audits (Punkt 8.6)
- Korrekturmaßnahmen (Punkt 8.7)
- Vorbeugende Maßnahmen (Punkt 8.8).

Zu Abs. 2:

Dies bedeutet, dass auch sämtliche Informationen dokumentiert, bewertet, gesteuert und überwacht werden müssen, die im Zusammenhang mit den in § 19 Abs. 2 Z 1 bis Z 3 genannten Fällen stehen (vgl. Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43, S 24).

Zu Z 2:

In den Verfahren ist jedenfalls festzulegen, innerhalb welcher Frist:

- Maßnahmen zu treffen sind, um die Gründe für den Widerruf der Akkreditierung zu beseitigen, sowie
- innerhalb welcher Frist Zertifizierungswerber oder – inhaber über den Widerruf der Akkreditierung in Kenntnis zu setzen sind.