NORMENKONFORME ZERTIFIZIERUNG ZUM DATENSCHUTZBEAUFTRAGTEN

Galileo Fasching / Manfred Wöhrl / Norbert Palecek

Unternehmensberater und Geschäftsführer der creatinosbanoz KG
Kalvarienberggasse 17/1, 1170 Wien, AT
galileo.fasching@creatinos.com; www.creatinos.com

Allgemein gerichtlich beeideter Sachverständiger für Informationstechnik, Geschäftsführer des Digital-Society-Institute GmbH, Arbeitsgruppe IoT, Security und Datenschutz,
Graben 17/10, 1010 Wien, AT
Manfred.Woehrl@digisociety.institute

Unternehmensberater Digitale Transformation, Geschäftsführer der Digital Society Institute GmbH, Arbeitsgruppe Digitale Arbeitswelt, Datenschutz
Graben 17/10, 1010 Wien, AT
norbert.palecek@digisociety.institute; http://digisociety.institute

Schlagworte: ***Datenschutzbeauftragter, Datenschutz-Management-System, Informationssicherheit, Prozesskontrolle, Zertifizierung, Employer Branding, Normen***

Abstract: *Unter Zertifizierung versteht man die Überprüfung und Bestätigung der Richtigkeit eines Dokumentes oder einer Qualifikation durch eine unabhängige Instanz. Diese kann von staatlicher Stelle definiert, von Organisationen aber auch Firmen für interne Produkte oder Leistungen benannt werden. Als Basis für die Durchführung der Zertifizierung durch eine akkreditierte oder benannte Prüfstelle können allgemein anerkannte Dokumente oder Leistungsbeschreibungen dienen, aber auch Normen oder anerkannte Standards der Industrie. Besonders für die ab 25. Mai 2018 geltende EU-DSGVO ist es für internationale sowie nationale Gremien eine Herausforderung, die Basis für eine europaweit anerkannte Zertifizierung für Datenschutzbeauftragte zu schaffen.*

1. Einleitung

Zertifizierung von betrieblichen Datenschutzprozessen und auch Datenschutzbeauftragten wird in der EU-DSGVO eine wichtige Rolle spielen. Dies öffnet für die Wirtschaft neue Möglichkeiten für besseren Datenschutz, aber auch Gefahren, wie etwa durch unterschiedliche kommerzielle «Zertifizierungskurse» mit variabler Qualität. Der Aufsatz diskutiert die rechtlichen und organisatorischen Rahmenbedingungen für eine von der EU geforderten nationalen Reglementierung zukünftiger Zertifizierungen von Datenschutzbeauftragten. Wir zeigen, dass hier als Basis noch Bedarf für Normenkonkretisierung besteht, und zeigen Wege auf wie europaweit anerkannte Zertifizierungssysteme aussehen könnten.

2. Grundlagen der normenkonformen Zertifizierung

Mit dem Begriff Zertifikat wird in der heutigen Zeit sehr frei umgegangen. Von der Definition her ist ein Zertifikat nur eine Bestätigung einer unabhängigen Instanz, dass gewisse Regeln und Vorgaben eingehalten wurden. Demzufolge kann zum Beispiel jedes Trainingsinstitut gemeinsam mit unabhängigen Spezialisten (quasi als Prüfinstanz) ein Zertifikat definieren und ausstellen. Dabei handelt es sich aber keinesfalls um ein staatlich anerkanntes Zertifikat. Dieses darf nur von einer akkreditierten Stelle vergeben werden, wobei die Akkreditierung, zum Beispiel in Österreich, durch das Wirtschaftsministerium (Akkreditierung Austria) erfolgt. So entsteht eine dem Standard entsprechende «Vertrauenskette», die eine hohe Qualität garantiert.

2.1. Wie entstehen Normen?

Normen werden in Gremien definiert, bearbeitet und schlussendlich zur Standardisierung eingereicht. Diese Gremien sind in Arbeitsgruppen («Working Groups») organisiert, zusammengestellt aus Vertretern unterschiedlichster Interessensgruppen, sogenannter Stakeholder.

2.1.1. Nationale Normen

In jedem Land wird eine nationale Organisation mit der Definition von Normen beauftragt. Diese ist in Österreich «Austrian-Standards» oder in Deutschland «DIN». Diese organisieren Komitees, die ihrerseits Arbeitsgruppen bilden. In Österreich beschäftigt sich die Arbeitsgruppe 18 (AG 001.18) mit dem Thema Datenschutz und daher auch speziell mit der EU-DSGVO.

2.1.2. Internationale Normen

Auf internationaler Ebene funktioniert der Prozess der Normung ähnlich wie auf nationaler Ebene, es werden Working Groups gebildet, die auf nationaler Ebene quasi als «Spiegelkomitees» auftreten. Beschlüsse, die auf nationaler Ebene gefasst werden, können in internationalen Gremien durch den Komitee Manager eingebracht werden und müssen auf Länderebene einstimmig erfolgen. Der Prozess der Beschlussfassung ist durch entsprechende Geschäftsordnungen der Normungsorganisation definiert. Interessant ist in diesem Zusammenhang, dass auf ISO-Ebene jedes Land nur eine Stimme hat, unabhängig von der Größe des Landes. In diesem Prozess ist auch vorgesehen, dass jedes Land auch neue Normen initiieren kann.

2.2. Vorgaben der EU

Die EU-DSGVO[1] tritt europaweit am 25. Mai 2018 in Kraft. Zur allgemeinen Unterstützung der Mitgliedstaaten hat die EU begleitende Veröffentlichungen für die Umsetzung herausgegeben, angefangen bei einer einfachen Übersicht («Factsheet»[2]) bis hin zu konkreten Dokumenten seitens WP29 und ENISA.

2.2.1. Article-29 Working Party

Da die EU-DSGVO als Verordnung für alle Mitgliedsstaaten verpflichtend ist, gleichzeitig aber 71 «Öffnungsklauseln» als Freiheiten für die Umsetzung in nationale Rechtsprechung beinhaltet, wurden einige Interpretationen seitens der Arbeitsgruppe WP29[3] der EU bereits 2016 publiziert[4].

Darin wird auch speziell das Thema «Betrieblicher Datenschutzbeauftragter» konkret behandelt, seine Aufgabenpflichten und Rechte und somit kann dieses Dokument als Basis für Zertifizierungsvorgaben herangezogen werden.

2.2.2. Empfehlungen der ENISA

Die ENISA[5] als zuständige Stabsstelle der Europäischen Union hat im November 2017 konkrete Empfehlungen für Zertifizierungen[6] bezüglich der EU-DSGVO publiziert.

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection ofnatural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), ABl. L 119/1 of 4 May 2016.

2 http://ec.europa.eu/justice/data-protection/files/eujls08b-1002_-_protection_of_personnal_data_a4_en.pdf (alle Websites zuletzt besucht am 17. Januar 2018).

3 The Article 29 Working Party, composed of representatives from all EU Data Protection Authorities, the EDPS andthe European Commission, was set up under the Directive 95/46/EC. It has advisory status and acts independently.

4 Guidelines on Data Protection Officers («DPOs»), 16/EN WP 243 rev.01.

5 European Union Agency for Network and Information Security, Europäische Agentur für Netz- und Informationssicherheit, Details siehe http://www.enisa.europa.eu.

6 Details siehe https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification/at_download/fullReport.

2.3. Nationale Basisnormen für die EU-DSGVO in Österreich

Die Arbeitsgruppe AG 001.18 «Datenschutz» der Austrian-Standards beschäftigt sich u.a. mit der EU DSGVO und entsprechender normativer Umsetzung in Österreich. Zwei Themen haben sich herauskristallisiert: Normierung eines Datenschutzmanagementsystems (ÖNORM A 2017) und Vorgaben für die Zertifizierung eines Datenschutzbeauftragten (ÖNORM A 2018).

Als gesetzliche Grundlage wurde in Österreich das Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000), BGBl. I Nr. 165/1999, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 83/2013 und die Kundmachung BGBl. I Nr. 132/2015, am 31. Juli 2017 mit dem Kurztitel «Datenschutz-Anpassungsgesetz-2018»[7] adaptiert. Einige wesentliche Änderungen konnten mangels einer möglichen Zweidrittelmehrheit im Parlament (Verfassungsparagraphen) nicht umgesetzt werden, daher ist in absehbarer Zeit mit einer Novellierung dieses Gesetzes zu rechnen.

3. Begriffsdefinitionen: Zertifizierung und Datenschutzbeauftragter

3.1. Zertifizierung

Die EU-DSGVO verweist an mehreren Stellen – beispielsweise in Erwägungsgrund 81, Artikel 24 und 25 (Pflichten des Verantwortlichen), Artikel 28 (Pflichten des Auftragsverarbeiters) und Artikel 32 (Sicherheit der Verarbeitung) – auf Artikel 42, in welchem die Zertifizierung näher geregelt ist. Die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen durch die nationale Aufsichtsbehörde soll demnach dazu dienen, dass die Einhaltung der Vorschriften der EU-DSGVO vom Verantwortlichen bzw. Auftragsverarbeiter nachgewiesen werden kann.

Die Zertifizierung wird künftig auf die Dauer von drei Jahren von einer beliebigen Akkreditierungsstelle erteilt, muss jedoch freiwillig und über ein transparentes Verfahren zugänglich sein. Diese Zertifizierung ist verlängerbar, sofern die Voraussetzungen weiterhin erfüllt werden oder kann auch widerrufen werden, wenn die geforderten Standards nicht mehr eingehalten werden. Die Erteilung der Zertifizierung mindert jedoch nicht die Verantwortung des Verantwortlichen bzw. des Auftragsverarbeiters.

3.2. Datenschutzbeauftragter

In den Artikeln 37-39 EU-DSGVO sind die Grundlagen zum Datenschutzbeauftragten normiert. Dieser kann in Form einer Stabstelle beim Verantwortlichen bzw. Auftragsverarbeiters beschäftigt sein oder extern seine Aufgaben über einen Dienstleistungsvertrag erfüllen. Seine Arbeit wird durch einen umfassenden Zugang zu personenbezogenen Daten, Weisungsungebundenheit und Vertraulichkeit charakterisiert. Es stellt sich hierbei jedoch die Frage, wie ein Verantwortlicher bzw. Auftragsverarbeiter nun sicherstellen kann, dass der ins Auge gefasste Datenschutzbeauftragte die vorgeschriebenen Anforderungen – in der Verordnung wird nur abstrakt von besonderer beruflicher Qualifikation und Fachwissen gesprochen – erfüllt.

Es werden bereits zahlreiche Lehrgänge zum Datenschutzbeauftragten angeboten. Diese folgen zumeist einem Vorgehens-/Verfahrensmodell mit einer strukturierten Ausbildung und etwaiger individueller Schwerpunktsetzung. Möglich ist jedoch auch die Evaluierung des Datenschutzbeauftragten anhand bestimmter Kriterien, die zu erfüllen sind (etwa einschlägiges Studium, mehrjährige einschlägige Praxiserfahrung). Bislang gibt es keine zertifizierte Ausbildung zum Datenschutzbeauftragten, somit gibt es auch kein einheitliches Mindestniveau an die Lehrenden bzw. Absolventen eines solchen Lehrgangs. Eine derartige Zertifizierung wäre jedoch im Sinne der Qualitätssicherung der Arbeit beim Verantwortlichen bzw. Auftragsverarbeiters wünschenswert.

[7] NR: GP XXV RV 1664 AB 1761 S. 190. BR: 9824 AB 9856 S. 871.[CELEX-Nr.: 32016L0680].

4. Bedeutung der Zertifizierung des Datenschutzbeauftragten für die Arbeitswelt

4.1. Notwendigkeit eines Datenschutzbeauftragten

Im Artikel 37 EU-DSGVO wird bestimmt, ob Unternehmen / Behörden einen Datenschutzbeauftragten benötigen. Ebenso welche Kriterien maßgeblich sind, um einen Datenschutzbeauftragten für eine ganze Unternehmensgruppe oder mehrere Behörden einzusetzen. Hinsichtlich der Qualifizierung kann es vorteilhaft sein, wenn diese Person einschlägige Erfahrung mit der Einführung bzw. Verwendung von Managementsystemen wie etwa ISO 9000 hat, da laut Artikel 24 entsprechende Nachweise zu erbringen sind («Rechenschaftspflicht»). Dies vor allem um Geldbußen laut Artikel 83 durch entsprechende Prozesse zu vermeiden.

4.2. Qualitätssteigerung durch interne oder externe Beratung

Sowohl interne als auch externe Datenschutzbeauftragte können gemäß Artikel 37 ernannt und mit der Tätigkeit beauftragt werden. Interne haben den Vorteil, dass sie das Unternehmen, deren Prozesse und IT Systeme sowie die handelnden Personen bereits kennen und dadurch entsprechende Vorgänge rasch mit Verantwortlichen adaptieren können. Externe beauftragte Dienstleister wiederum geraten weniger in die Gefahr weisungsgebunden zu sein oder aufgrund anderer Tätigkeiten zu wenig Zeit und Ressourcen dem Thema zu widmen. In beiden Fällen bewirkt eine entsprechende Zertifizierung zu dieser Position eine Qualitätssteigerung bei der Durchführung und einen nach Außen sichtbaren Qualitätsnachweis.

4.3. Datenschutzmanagementsysteme zum Abbilden von Prozessen

Um effektiv personenbezogene Daten zu schützen, brauchen Unternehmen im Bezug zu Artikel 24, 5 EU-DSGVO, ein Datenschutz-Management-System (DSMS). Speziell zwei existierende Systeme können durch geeignete Erweiterung oder Adaptierung im Sinne der EU-DSGVO beispielhaft genannt werden. Erstens die Qualitätsmanagementnorm ISO 9000 ff., in der definiert ist, welche Anforderungen ein Managementsystem zu erfüllen hat, damit die Maßnahmen zur Umsetzung eines Qualitätsmanagements entsprechend dokumentiert sind. Nachweis gegenüber Dritten erfolgt durch Zertifizierungsprozess und ein zeitlich limitiertes Zertifikat. Und zweitens die Normenreihe ISO/IEC 27000, die einen Überblick und Begriffe für Informationssicherheitsmanagementsysteme (ISMS) abbildet und die Auswahl angemessener Sicherheitsmaßnahmen zum Schutz des Informationsbestands von Organisationen gewährleistet. Unternehmen die gemäß diesen Normen agieren, haben daher entsprechendes Wissen, um durch Anpassung, den EU-DSGVO Anforderungen gerecht zu werden.

4.4. Vorteile für Organisationen

Ein nach definierten Kriterien (Normen) zertifizierter Datenschutzbeauftragter gibt Organisationen und deren Partnern und Kunden den Nachweis, dass gesetzlich erforderliche Maßnahmen eingehalten werden. Dies bezieht sich nicht nur auf externe Dienstleistungen, sondern auch auf Personal und Image des Unternehmens in Form der Arbeitgebermarke (engl. Employer Branding). Dadurch ergibt sich ein klarer Wettbewerbsvorteil.

5. Fazit

Normen dienen der Standardisierung von Vorgängen und Prozessen als Resultat von bekannten «Best Practises». Eine normenkonforme Zertifizierung zum Datenschutzbeauftragten bringt daher Organisationen, die solche zertifizierten Mitarbeiter beschäftigen oder beauftragen, ein hohes Maß an (Rechts)Sicherheit und vielfältige ökonomische Vorteile. Derzeit wird eine Vielzahl von unterschiedlichen Zertifizierungen zum Datenschutzbeauftragten am Markt angeboten, denen eine gegenseitige Abstimmung, Anerkennung und Offenlegung der Curricula sowie der Fragenkataloge fehlt. Damit ist auch nicht gewährleistet, dass ein Katalog von Mindestanforderungen erfüllt ist. Ziel sollte sein: Ein erfolgreicher Absolvent eines Zertifizierlehrgangs der Institution A sollte (auf europäischer Ebene) auch die Zertifizierung bei Institution B erlangen.