Zertifizierungsschema P43

Datenschutzbeauftragte/ Datenschutz-beauftragter

Ausgabe 2.1: 2022-05-17

Medieninhaber und Hersteller
Austrian Standards plus GmbH Heinestraße 38, 1020 Wien

E-Mail: certification@austrian-standards.at
Internet: www.austrian-standards.at

Inhaltsverzeichnis

1 Anwendungsbereich

Dieses Zertifizierungsschema legt die Vorgangsweise zur Zertifizierung der Kompetenz von Personen als „Datenschutzbeauftragter“ im Sinne der Artikel 37-39 EU Datenschutz-Grundverordnung (DSGVO)[1] durch Austrian Standards plus Certification (AS+C), dem Geschäftsbereich Zertifizierung der Austrian Standards plus GmbH, fest.

Gegenstand der Zertifizierung ist ausschließlich die Kompetenz natürlicher Personen.

Die Zertifizierung erfolgt nach den Grundsätzen der Internationalen Norm ISO/IEC 17024[2].

Die Zertifizierungsstelle von Austrian Standards ist ein eigenständiger Unternehmensbereich innerhalb der Austrian Standards plus GmbH. Die Austrian Standards plus GmbH ist ein 100 % Tochterunternehmen von Austrian Standards International.

2 Anforderungen an die Kompetenz

2.1 Kompetenzprofil

Personen, die gemäß dem Zertifizierungsschema zertifiziert sind, sind befähigt, die Aufgaben eines Datenschutzbeauftragten nach Art 39 DSGVO wahrzunehmen und kennen die Grundlagen der Informationssicherheit gem. Art 32 DSGVO.

Sie sind in der Lage, Personen oder Organisationen hinsichtlich ihrer Pflichten nach der DSGVO und den österreichischen Datenschutzvorschriften zu beraten.

Sie sind kompetent, die Einhaltung der geltenden Datenschutzvorschriften zum Schutz personenbezogener Daten zu überwachen und zu koordinieren. Weiters sind sie in der Lage, bei Datenschutz-Folgenabschätzungen gem. Art 35 DSGVO zu beraten und ihre Durchführung zu überwachen.

Sie sind kompetent, mit Aufsichtsbehörden im Bereich Datenschutz zusammenzuarbeiten und als Anlaufstelle für die Aufsichtsbehörde zu fungieren sowie Beratung zu allen sonstigen Fragen in Bezug auf Datenschutz an betroffene Personen zu leisten.

2.2 Anforderungen an Wissen und Fertigkeiten

Zertifizierte Personen müssen Kompetenzen und Wissen gemäß der Abschnitte 2.2.1 bis 2.2.5 aufweisen.

2.2.1 Datenschutz-Grundverordnung (DSGVO)

- Grundprinzipien des Datenschutzrechtes
- Rechtmäßigkeit der Datenverarbeitung
- besondere Kategorien von Daten
- Informationspflichten
- Betroffenenrechte

[1] Verordnung (EU) 2016/679 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

[2] ISO/IEC 17024:2012-07 Konformitätsbewertung - Allgemeine Anforderungen an Stellen, die Personen zertifizieren

- Pflichten von Verantwortlichen[3] und Auftragsverarbeitern[4] sowie Pflichten von gemeinsam für die Verarbeitung Verantwortlichen
- Hinzuziehung von Auftragsverarbeitern
- Verzeichnis der Datenverarbeitungstätigkeiten
- Verletzung des Schutzes personenbezogener Daten
- Datenschutz-Folgenabschätzung aus rechtlicher Sicht
- Datenübermittlung an Drittländer
- Rechtsbehelfe, Strafen und Haftung

2.2.2 Datenschutzgesetz (DSG)[5]

- Geltungsbereich
- Datenverarbeitung zu spezifischen Zwecken
- Beispiel: wissenschaftliche Forschungszwecke, Bildverarbeitung
- Aufgaben und Befugnisse der Datenschutzbehörde
- Rechtsbehelfe
- Haftung und Sanktionen mit Ausnahme der Bestimmungen über die Verarbeitung personenbezogener Daten in Umsetzung der Richtlinie 2016/680 und im Zusammenhang mit der Verarbeitung von personenbezogenen Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs
- Regelungen des Datenschutzes in der elektronischen Kommunikation
- Beispiel: Spamming, Cold Calling, Einsatz von Cookies

2.2.3 Informationssicherheit

- Grundlagen der Informationssicherheit gem. ISO 27001
- Informationssicherheitsmanagementsysteme: Aufbau & Struktur, Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen in der Praxis
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Sicherheit der Datenverarbeitung
- Datenschutz-Folgenabschätzung aus Sicht der Informationssicherheit
- Zertifizierung und Verhaltensregeln

---

[3] Definition gemäß DSGVO Art. 4, Begriffsbestimmung 7.

[4] Definition gemäß DSGVO Art. 4, Begriffsbestimmung 8.

[5] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz - DSG), BGBl. I Nr. 165/1999 idgF.

2.2.4 Aufgaben & Verantwortung

- technische Anforderungen in Bezug auf Datenschutz steuern
- Benennung eines Datenschutzbeauftragten
- Aufgaben und Stellung des Datenschutzbeauftragten samt der diesbezüglichen Verantwortung
- Anmerkung: Insbesondere hinsichtlich seiner Weisungsfreiheit, Geheimhaltungsverpflichtung und möglicher Interessenskonflikten.
- Datenschutz-Folgenabschätzung und Konsultationsverfahren
- Zusammenarbeit mit der Aufsichtsbehörde
- Aufbau einer Datenschutzorganisation
- Einführung eines Datenschutz-Managements
- Haftungen und Strafrisiken

2.2.5 Datenverarbeitung

- Einhaltung der Grundprinzipien und Rechtmäßigkeit
- Einhaltung der Informationspflichten und Betroffenenrechte
- Führung des Verzeichnisses der Verarbeitungstätigkeiten
- Beachtung der Regeln zum internationalen Datenverkehr
- Einhaltung der Datensicherheitsmaßnahmen
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- Durchführung von Datenschutz-Folgenabschätzungen sowie Privacy Impact Analysen
- Umsetzung des Datengeheimnisses

3 Voraussetzungen für die Zulassung zur Prüfung

Voraussetzung für die Zulassung zur Prüfung ist die Erfüllung einer der nachfolgend angeführten Kriterien

- Nachweis einer facheinschlägigen Ausbildung basierend auf den Inhalten gemäß Abschnitt 2.2 im Ausmaß von mindestens 24 Wochenstunden.

Oder

- Nachweis einer mindestens zweijährigen Praxiserfahrung im Bereich Datenschutz, Datenverarbeitung, Datensicherheit, Datenschutzrecht etc.

Die Nachweise sind vor Prüfungsantritt von der Kandidatin/vom Kandidaten an die Zertifizierungsstelle zu übermitteln.

4 Prüfung

Die Prüfung wird in Form eines Sincle-Choice-Tests abgehalten und umfasst 60 Fragen aus den 5 Themengebieten gemäß Abschnitt 2.2.1 bis 2.2.5.

Die maximale Dauer der schriftlichen Prüfung ist mit 90 Minuten festgelegt.

Anmerkung: Die Verwendung folgender Unterlagen ist erlaubt:

- Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) idgF
- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) idgF

5 Bewertungskriterien

5.1 Single-Choice Prüfung

Je Abschnitt (2.2.1 bis 2.2.5) muss mindestens 50% der Gesamtpunktzahl erreicht werden.

5.2 Gesamtbewertung und Prüfungswiederholung

Zur positiven Absolvierung der Gesamtprüfung müssen mindestens 60% der Gesamtpunktzahl (=36 von insgesamt 60 Punkten) erreicht werden.

Wird ein Abschnitt negativ beurteilt, so ist die Prüfung insgesamt negativ zu beurteilen.

Die Prüfung ist in jedem Falle zur Gänze zu wiederholen.

6 Ausstellung und Gültigkeit der Zertifikate

Die erfolgreiche Bewertung der Erstzertifizierungsprüfung gemäß Abschnitt 5 ist Voraussetzung für die Ausstellung eines Zertifikates.

Die Zertifikate haben eine Gültigkeit von 3 Jahren.

7 Rezertifizierung

7.1 Kriterien zur Verlängerung des Zertifikates

Zur Verlängerung des Zertifikates muss die Zertifikatsinhaberin/der Zertifikatsinhaber die folgenden Kriterien erfüllen:

7.1.1 Die Zertifikatsinhaberin/der Zertifikatsinhaber muss Nachweise über facheinschlägige Weiterbildungen im Ausmaß von mindestens 24 Stunden für den gesamten Zertifizierungszyklus erbringen.

7.1.2 Die Zertifikatsinhaberin/der Zertifikatsinhaber muss Nachweise über die aufrechte, einschlägige Tätigkeit erbringen. Dies hat in Form von Tätigkeits- bzw. Projektbeschreibung zu erfolgen.

7.2 Ausstellung des Zertifikates

Nach Erfüllung aller Kriterien gemäß 7.1.1 und 7.1.2 wird das Zertifikat für drei Jahre verlängert.

7.3 Fristen

Die Rezertifizierung muss vor dem Ablauf des Zertifikates erfolgen. In Ausnahmefällen kann die Rezertifizierung auch nach Ablauf des Zertifikates erfolgen. Hierbei gelten folgende Bedingungen:

7.3.1 Erfolgt die Rezertifizierung nach Ablauf der Gültigkeit eines Zertifikats innerhalb eines Zeitraums von maximal sechs Monaten, wird die Rezertifizierung gemäß den Kriterien und dem Prozess gemäß Abschnitt 7.1 durchgeführt. Andernfalls ist eine Prüfung im Umfang der Erstzertifizierung gemäß Abschnitt 4 durchzuführen.

7.3.2 Die Gültigkeit des Zertifikats richtet sich immer nach dem Datum der Erstzertifizierung. Das heißt, es wird immer vom Datum der Erstzertifizierung ausgegangen, unabhängig von dem Datum der tatsächlich erfolgten Rezertifizierung.