Zertifizierungsprogramm P43

Datenschutzbeauftragte:r

Version 2.3: 2024-02-01

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

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

Inhaltsverzeichnis

1 Geltungsbereich

Dieses Zertifizierungsprogramm 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 ISO/IEC 17024[2].

2 Anforderungen an die Kompetenz

2.1 Kompetenz- & Tätigkeitsprofil

Personen, die gemäß dem Zertifizierungsprogramm 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 Wissen und Fertigkeiten, Tätigkeitsprofil

Personen, die gemäß diesem Zertifizierungsschema zertifiziert sind, 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
- Pflichten von Verantwortlichen[3] und Auftragsverarbeitern[4] sowie Pflichten von gemeinsam für die Verarbeitung Verantwortlichen

---

[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.

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

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

- 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

2.2.4 Aufgaben & Verantwortung

- technische Anforderungen in Bezug auf Datenschutz steuern

---

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

- 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 Prüfung

Die Prüfung wird in Form eines Single-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.

Die Nutzung von Fachliteratur, Vortragsunterlagen, Mitschriften sowie die Nutzung des Internets (zu Recherchezwecken) ist in den Grenzen des vorgegebenen Zeitrahmens erlaubt.

4 Bewertungskriterien

Es können maximal 60 Punkte erreicht werden, wobei jede richtig beantwortete Frage mit einem Punkt bewertet wird.

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

5 Zertifizierungsvoraussetzungen Erst-Zertifizierung

Folgende Voraussetzung muss für die Ausstellung eines Zertifikates erfüllt sein:

- positives Prüfungsergebnis (gem. Abschnitt 4 Bewertungskriterien)

Die Zertifikate haben eine Gültigkeit von 3 Jahren.

6 Beschwerde, Einspruch, Prüfungseinsicht/-auskunft

6.1 Einspruch: Prüfungsteilnehmende haben das Recht, Einspruch gegen das Prüfungsergebnis einzulegen. Die Zertifizierungsstelle von Austrian Standards folgt der in der ISO/IEC 17024 vorgegebenen Definition eines Einspruchs: „Mit dem Einspruch bringt der Anbieter eines Gegenstandes der Konformitätsbewertung gegenüber der Konformitätsbewertungsstelle sein Verlangen zum Ausdruck, die Entscheidung bezüglich dieses Gegenstandes zu überprüfen".

6.2 Beschwerde: Prüfungsteilnehmende haben das Recht, Beschwerde bei der Zertifizierungsstelle einzulegen. Die Zertifizierungsstelle von Austrian Standards folgt der in der ISO/IEC 17024 vorgegebenen Definition einer Beschwerde: „Mit der Beschwerde bringt eine Person oder eine Organisation ihre Unzufriedenheit bezüglich der Tätigkeit der Konformitätsbewertungsstelle zum Ausdruck und erwartet eine Antwort".

Beschwerden und Einsprüche sind schriftlich bei der Zertifizierungsstelle einzureichen.

6.3 Prüfungseinsicht und -auskunft: Eine Prüfungseinsicht sowie eine Prüfungsauskunft (erreichte Punkteanzahl) kann ausschließlich bei Nicht-Bestehen der Prüfung und im Rahmen eines Einspruchsverfahrens vorgenommen/erteilt werden.

7 Rezertifizierung

7.1 Kriterien zur Verlängerung des Zertifikates

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

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

7.1.2 Der/Die Zertifikatsinhaber:in 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 3 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.

8 Autor:innen von Prüfungen

8.1 Anzahl der Autor:innen

Die Prüfungsfragen werden wird von zumindest einer/einem Autor:in erstellt.

8.2 Kompetenz der Autor:innen

Für die von AS+C eingesetzten Autor:innen gelten folgende Anforderungen (siehe ISO/IEC 17024).
Autor:innen müssen die Anforderungen von AS+C erfüllen, die auf den anzuwendenden Kompetenznormen und anderen relevanten Dokumenten basieren.
Der Auswahlvorgang stellt sicher, dass die einer Prüfung oder Teilen einer Prüfung zugeteilten Autor:innen mindestens

- mit diesem Zertifizierungsschema vertraut sind,
- umfassende Kenntnis über die relevanten Prüfungsmethoden und Prüfungsdokumente haben,
- über eine angemessene Kompetenz in dem zu prüfenden Gebiet verfügen,
- flüssig in der schriftlichen und mündlichen Prüfungssprache kommunizieren können und
- frei sind von allen Einflüssen, um unparteiische und nichtdiskriminierende Beurteilungen (Bewertungen) erstellen zu können.

Die Auswahl der Autor:innen obliegt AS+C, diese führt eine Liste der zugelassenen Autor:innen (Pool).