

Zertifizierungsprogramm P43

Datenschutzbeauftragte:r gem. DSGVO Art.39

Version 4.0: 2025-05-12

Programmeigner, Medieninhaber und Hersteller

Austrian Standards plus GmbH

Heinestraße 38, 1020 Wien

Copyright© Austrian Standards plus GmbH 2025 All rights reserved.

E-Mail: certification@austrian-standards.at

Internet: www.austrian-standards.at

Inhalt

1	Geltungsbereich	3
2	Anforderungen an die Kompetenz	3
2.1	Kompetenz- & Tätigkeitsprofil.....	3
2.2	Anforderungen an Wissen und Fertigkeiten.....	3
2.2.1	Datenschutz-Grundverordnung (DSGVO).....	3
2.2.2	EU-Datenschutzrecht, Verhältnis zum nationalen Recht, grenzüberschreitende Datenverarbeitungen innerhalb der EU.....	4
2.2.3	Informationssicherheit.....	4
2.2.4	Aufgaben & Verantwortung.....	5
2.2.5	Datenverarbeitung.....	5
3	Prüfung	5
4	Bewertungskriterien	6
4.1	Allgemeines.....	6
4.2	Prüfung.....	6
5	Zertifizierungsvoraussetzungen Erst-Zertifizierung	6
6	Beschwerde, Einspruch, Prüfungseinsicht/-auskunft	6
7	Rezertifizierung	7
7.1	Kriterien zur Verlängerung des Zertifikates.....	7
7.2	Ausstellung des Zertifikates.....	7
7.3	Fristen.....	7

1 Geltungsbereich

Das vorliegende Zertifizierungsprogramm legt die Vorgangsweise zur Zertifizierung der Kompetenz von Personen als „Datenschutzbeauftragte:r“ im Sinne der Artikel 37-39 EU Datenschutz-Grundverordnung (DSGVO) ¹durch 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 17024².

2 Anforderungen an die Kompetenz

2.1 Kompetenz- & Tätigkeitsprofil

Personen, die gemäß dem Zertifizierungsprogramm zertifiziert sind, können die Aufgaben einer/eines Datenschutzbeauftragten gem. DSGVO Art. 39 wahrnehmen und kennen die Grundlagen der Informationssicherheit gem. Art 32 DSGVO.

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

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

Sie sind kompetent, mit Aufsichtsbehörden im Bereich des Datenschutzes 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

Personen, die gemäß diesem Zertifizierungsschema zertifiziert sind, müssen Wissen und Fertigkeiten gemäß der Abschnitte 2.2.1 bis 2.2.5 aufweisen.

2.2.1 Datenschutz-Grundverordnung (DSGVO)

- Grundprinzipien des Datenschutzrechtes
- Sachlicher und räumlicher Anwendungsbereich der DSGVO (z.B. Datenverarbeitungen im Ausland mit Unionsbezug)
- Rechtmäßigkeit der Datenverarbeitung
- besondere Kategorien von Daten
- Informationspflichten

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.

- Betroffenenrechte
- Pflichten von Verantwortlichen³ und Auftragsverarbeitern⁴ 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, Haftung und Sanktionen

2.2.2 EU-Datenschutzrecht, Verhältnis zum nationalen Recht, grenzüberschreitende Datenverarbeitungen innerhalb der EU

- Ausnahmen und Ausgestaltungsvorbehalte zugunsten der Mitgliedstaaten
- Aufgabe und Funktion des Europäischen Datenschutzausschusses
- Rolle der Rechtsprechung des Gerichtshofs der Europäischen Union für die Auslegung der DSGVO
- Aufgaben, Zuständigkeiten und Befugnisse der nationalen Aufsichtsbehörden
- Rechtsschutz gegenüber Entscheidungen der nationalen Aufsichtsbehörden
- Grenzüberschreitende Datenverarbeitungen innerhalb der Union

2.2.3 Informationssicherheit

- Grundlagen der Informationssicherheit gem. ISO/IEC 27001⁵
- 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 ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

2.2.4 Aufgaben & Verantwortung

- technische Anforderungen in Bezug auf Datenschutz steuern
- Benennung eines Datenschutzbeauftragten
- Aufgaben und Stellung des Datenschutzbeauftragten samt der diesbezüglichen Verantwortung, insbesondere hinsichtlich seiner Weisungsfreiheit, Geheimhaltungsverpflichtung und möglicher Interessenskonflikten.
- Datenschutz-Folgenabschätzung und Konsultationsverfahren
- Zusammenarbeit mit der nationalen Aufsichtsbehörde einschließlich der Ermittlung der federführenden Aufsichtsbehörde bei grenzüberschreitenden Verarbeitungsvorgängen
- 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 70 Minuten festgelegt.

Anmerkung: die Verwendung sämtlicher Hilfsmittel ist untersagt. Ausgenommen hiervon ist das nachstehend genannte Dokument, das während der Prüfung bereitgestellt wird:

- 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).

4 Bewertungskriterien

4.1 Allgemeines

4.1.1 Die Erbringung der Prüfungsleistung hat eigenständig und ohne Verwendung unlauterer Hilfsmittel/Hilfestellungen zu erfolgen. Sollte der Verdacht bestehen, dass während der Prüfung unlautere Hilfsmittel/Hilfestellungen genutzt/verwendet wurden oder andere Täuschungshandlungen vorgenommen wurden, wird die Prüfung negativ bewertet. Die Verwendung von Systemen der Künstlichen Intelligenz, wie zum Beispiel ChatGPT, verunmöglicht eine nachvollziehbare Beurteilung der Eigenleistung des Kandidaten/der Kandidatin und wird daher in jedem Fall als unlauteres Hilfsmittel eingestuft.

4.1.2 Täuschungsversuche führen zu einer negativen Gesamtbewertung der Prüfungsleistung, weil damit eine eigenständige Prüfungsleistung des/der Kandidaten nicht festgestellt werden kann.

4.2 Prüfung

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

Die Prüfung ist in jedem Falle zur Gänze zu wiederholen, wenn diese negativ bewertet wird.

5 Zertifizierungsvoraussetzungen Erst-Zertifizierung

Folgende Voraussetzung muss für die Ausstellung eines Zertifikates erfüllt sein:

1. Nachweis einer Ausbildung bezogen auf die Inhalte gem. Abschnitt 2 im Ausmaß von mind. 24 Wochenstunden **ODER** Nachweis einer zweijährigen Berufserfahrung im Bereich Datenschutz, Datenverarbeitung, Datensicherheit, Datenschutzrecht etc.
2. positives Prüfungsergebnis (gem. Abschnitt 4 Bewertungskriterien), welches eindeutig die Kompetenz (gem. Pkt. 2.1), aufgrund einer erbrachten Eigenleistung des Kandidaten/der Kandidatin nachweist

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 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 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.