Zertifizierungsschema P43

Datenschutzbeauftragter

Ausgabedatum: V1.0, 2017-08-22

Austrian Standards plus GmbH

Dr. Peter Jonas
Heinestraße 38
1020 Wien
E-Mail: p.jonas@austrian-standards.at

1 Anwendungsbereich

Dieses Zertifizierungsschema legt die Vorgangsweise zur Zertifizierung der Kompetenz einer Person als „Datenschutzbeauftragter“ im Sinne der Artikel 37-39 EU Datenschutz-Grundverordnung (DSGVO)[1] fest.

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

2 Anforderungen an die Kompetenz

2.1 Kompetenzprofil

Personen, die gemäß diesem Zertifizierungsschema zertifiziert sind, sind in der Lage die Aufgaben eines Datenschutzbeauftragten nach Art 39 DSGVO wahrzunehmen und kennen die Grundlagen der Informationssicherheit auf Basis der ISO/IEC 27001: 2013 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 das Wissen

Zertifizierte Personen müssen über folgendes Wissen in Bezug auf die Verarbeitung und Verwendung von personenbezogenen Daten verfügen:

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
- Hinzuziehung von Auftragsverarbeitern

---

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.

- Verzeichnis der Datenverarbeitungstätigkeiten
- Verletzung des Schutzes personenbezogener Daten
- Datenschutz-Folgenabschätzung aus rechtlicher Sicht
- Datenübermittlung an Drittländer
- Rechtsbehelfe, Strafen und Haftung

2.2.2 Österreichisches Datenschutzgesetz[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, die 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

2.3 Anforderungen an Fähigkeiten

Zertifizierte Personen müssen über folgende Fähigkeiten in Bezug auf die Verarbeitung und Verwendung von personenbezogenen Daten verfügen:

2.3.1 Aufgaben & Verantwortung

Zertifizierte Personen müssen über die Fähigkeiten verfügen, zu überprüfen, ob die folgenden Punkte im Unternehmen dokumentiert und umgesetzt werden:

[5] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), BGBl. I Nr. 165/1999 zuletzt geändert durch BGBL. I Nr. 83/2013

- 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

2.3.2 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 Weiterbildung

Der Datenschutzbeauftragte ist zur regelmäßigen und facheinschlägigen Weiterbildung verpflichtet (zumindest 8 Stunden pro Jahr), um sicherzustellen, dass seine Qualifikation dem jeweils aktuellen Stand der Technik entspricht.

4 Antragstellung

Der Antrag auf Zertifizierung erfolgt durch den Antragsteller mittels Antragsformular auf Grundlage der Geschäftsbedingungen der Zertifizierungsstelle AS+C.

5 Voraussetzungen für die Zulassung zur Prüfung

Voraussetzungen zur Zulassung zur Prüfung ist die Erfüllung einer der nachfolgenden Kriterien:

1.) Nachweis einer facheinschlägigen Ausbildung im Mindestausmaß von 24 Stunden oder

2.) Nachweis einer mindestens 2 jährigen Berufserfahrung mit Aufgaben im Bereich z.B. Datenverarbeitung, Datensicherheit, Datenschutzrecht etc.

Sämtliche Zeugnisse sowie Nachweise sind samt Antragsformular an die Zertifizierungsstelle zu übermitteln.

6 Prüfung

Die Prüfung wird schriftlich, in Form eines Multiple-Choice-Tests (Single Choice), abgehalten und umfasst 60 Fragen aus den 5 Themengebieten gemäß Abschnitt 2.2.1 bis 2.2.3 sowie 2.3.1 und 2.3.2. Pro Themengebiet werden 12 Fragen gestellt. Die maximale Dauer der schriftlichen Prüfung ist mit 1,5 Stunden festgelegt.

Bei den Fragen muss die Kandidatin bzw. der Kandidat nachweisen, dass die wesentlichen Zusammenhänge verstanden wurden, das Wissen zu den einzelnen Themenbereichen vorhanden ist und für die Praxis relevante Aufgabenstellungen korrekt mit dem Fokus auf das Wesentliche beantwortet werden können.

7 Kriterien für die Bewertung der Kandidaten

Für die insgesamt positive Bewertung und somit für den Nachweis der Kompetenz über die oben angeführten Inhalte müssen je Abschnitt (2.2.1 bis 2.2.3 sowie 2.3.1 und 2.3.2) mindestens 50 % der Fragen richtig beantwortet werden. Insgesamt müssen über alle Themengebiete (2.2.1 bis 2.2.3 sowie 2.3.1 und 2.3.2) mindestens 60 % richtig beantwortet werden.

Wird ein Abschnitt negativ beurteilt, so ist die Prüfung insgesamt negativ zu beurteilen. Eine negative Prüfung muss in jedem Fall zur Gänze wiederholt werden.

8 Ausstellung der Zertifikate, Gültigkeit

Die erfolgreiche Bewertung der Erstzertifizierungsprüfung gemäß Abschnitt 7 ist Voraussetzung für die Ausstellung eines Zertifikates.

Die Zertifikate haben eine Gültigkeit von 3 Jahren.

Für die Ausstellung der Zertifikate gelten die Regelungen der Geschäftsbedingungen der Zertifizierungsstelle von Austrian Standards.

9 Konformitätszeichen und Aussagen zur Zertifizierung

Mit der Ausstellung des Zertifikates erhält der Inhaber das Recht das Konformitätszeichen „Certified by Austrian Standards“ gemäß Bild 1 in Bezug auf die zertifizierte Kompetenz zu verwenden.

Bild 1 – Konformitätszeichen

Die Kennzeichnung darf auf Visitenkarten, Verkaufsunterlagen, Werbematerialien u. Ä. angebracht werden. Der Zertifikatsinhaber ist verpflichtet, das Konformitätszeichen nur im Zusammenhang mit der zertifizierten Kompetenz gemäß den Angaben auf dem Zertifikat sowie nur in der in Bild 1 angegebenen graphischen Darstellung zu verwenden.

Der Zertifikatsinhaber ist verpflichtet, Aussagen in Bezug auf die erfolgte Zertifizierung nur im Zusammenhang mit der zertifizierten Kompetenz gemäß den Angaben auf dem Zertifikat zu treffen.

Kompetenzen für die von AS+C kein Zertifikat ausgestellt wurde, dürfen weder auf die oben beschriebene Art noch in anderer, zur Verwechslung Anlass gebender Weise gekennzeichnet oder bezeichnet werden.

10 Re-Zertifizierung

Zur Verlängerung des Zertifikates ist

- der Nachweis von facheinschlägigen Weiterbildungen von mindestens 8 Stunden pro Jahr (insgesamt mind. 24 Stunden) sowie
- die positive Absolvierung eines Rezertifizierungsworkshops erforderlich.

Der Kandidat weist im Rahmen der Rezertifizierung nach, dass er die folgenden Kriterien erfüllt:

- der Kandidat/die Kandidatin ist im Bereich des Datenschutzes aktiv tätig,
- der Kandidat/die Kandidatin ist fähig zu überprüfen, ob die DSGVO in einer Organisation korrekt umgesetzt wurde,
- der Kandidat/die Kandidatin hat in den vergangenen 3 Jahren im ausreichenden Maß Fort- und Weiterbildungsmaßnahmen absolviert.

11 Prüfer

11.1 Prüfer

Die schriftliche Prüfung gemäß Abschnitt 6 wird von einem Prüfer bewertet.

Der Rezertifizierungsworkshop gemäß Abschnitt 9 wird durch einen Prüfer abgehalten und bewertet.

11.2 Kompetenz der Prüfer

Für die von AS+C eingesetzten Prüfer gelten folgende Anforderungen.

Prüfer 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 Prüfer 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 nicht diskriminierende Beurteilungen (Bewertungen) erstellen zu können.

Über die oben angeführten allgemeinen Anforderungen hinaus gelten die folgenden Anforderungen bzgl. der fachspezifischen Qualifikation eines Prüfers:

- mindestens fünfjährige Tätigkeit und Erfahrungen im Bereich Datenschutz.

Die Auswahl der Prüfer obliegt AS+C, diese führt eine Liste der zugelassenen Prüfer (Prüferpool).