Überwachungsschema Y07.3

Verhaltensregel gem. Art 40 DSGVO

für Bilanzbuchhaltungsberufe

Ausgabe 1.0: 2020-11-25

Medieninhaber und Hersteller
Austrian Standards plus GmbH Heinestraße 38, 1020 Wien
Akkreditierte Überwachungsstelle gemäß Art 41. EU DSGVO

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

Inhaltsverzeichnis

1 Anwendungsbereich

Dieses Überwachungsschema legt die Vorgangsweise zur Überwachung im Sinne des Art. 41 EU Datenschutz-Grundverordnung (DSGVO)[1] eines Unternehmens bzgl. der Einhaltung der folgenden Verhaltensregel fest:

- Datenschutz-Grundverordnung – Verhaltensregeln für Bilanzbuchhaltungsberufe (Bilanzbuchhalter, Buchhalter, Personalverrechner), Medieninhaber/Herausgeber: Fachverband Unternehmensberatung, Buchhaltung und Informationstechnologie, Wirtschaftskammer Österreich, Stand: 2020-11-04[2].

Die Austrian Standards plus GmbH führt Überwachungen als akkreditierte Überwachungsstelle im Sinne der Überwachungsstellenakkreditierungs-Verordnung[3] durch.

Die Überwachung von Unternehmen erfolgt im Rahmen der zwischen der Austrian Standards plus GmbH als Überwachungsstelle und dem Fachverband Unternehmensberatung, Buchhaltung und Informationstechnologie, Wirtschaftskammer Österreich geschlossen Bestellungsvereinbarung als Überwachungsstelle iSd Art. 40 (4) iVm Art 41 DSGVO.

Die Überwachungsstelle agiert unabhängig und weisungsfrei.

2 Begriffsbestimmungen

2.1
Antrag
Schriftliche Willenserklärung eines Unternehmens, dass sich das Unternehmen gemäß § 8 (2) der Verhaltensregeln verpflichtet, diese einzuhalten sowie sich einer Überwachung gemäß Art. 41 EU DSGVO unterwirft und bei der Überwachungsstelle beantragt, ein diesbezügliches Verfahren einzuleiten.

2.2
Überwachungszertifikat
Durch die Überwachungsstelle ausgestellte Bestätigung, dass ein Unternehmen die Verhaltensregeln einhält und eine Überwachung gemäß Art. 40 (4) und Art. 41 EU DSGVO zu einem gegebenen Zeitpunkt vorliegt.

3 Kriterien für die Überwachung

Für die Ausstellung eines Überwachungszertifikates gelten die Kriterien gemäß Anhang A.

4 Überwachungsprozess

4.1 Antragstellung

4.1.1 Der Antragsteller muss die Einleitung des Überwachungsverfahrens mittels eines von der Überwachungsstelle zur Verfügung gestellten Antragsformulars beantragen.

4.1.2 Der Antragsteller muss eine bevollmächtigte Kontaktperson für die Durchführung des Überwachungsverfahrens benennen.

4.1.3 Überwachungsverfahren von mehreren, miteinander verbundenen juristischen Personen können gebündelt werden. Es wird jedoch für jede juristische Person ein eigenes Zertifikat ausgestellt.

---

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments 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] Quelle: https://www.wko.at/branchen/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/buchhaltung/verhaltensregeln-fuer-bilanzbuchhaltungsberufe.pdf

[3] Verordnung der Datenschutzbehörde über die Anforderungen an eine Stelle für die Überwachung der Einhaltung von Verhaltensregeln (Überwachungsstellenakkreditierungs-Verordnung – ÜstAkk-V), BGBl. II Nr. 264/2019

4.1.4 Zusammen mit dem Antrag muss der Antragsteller folgende Informationen bereitstellen:

a. Nachweis der Berechtigung zur Ausübung eines Bilanzbuchhaltungsberufes gemäß BiBuG[4],
b. die allgemeinen Merkmale der antragstellenden Organisation, einschließlich deren Name sowie die Anschrift(en) ihres/ihrer physischen Standort(e)s,
c. Informationen bzgl. des/der Datenschutzbeauftragten bzw. der für den Datenschutz zuständigen Person(en),
d. Organigramm der Abteilungen (samt verantwortlichen Personen), die Verarbeitungstätigkeiten vornehmen, die in den Anwendungsbereich der Verhaltensregeln fallen,
e. Informationen bezüglich aller ausgegliederten datenverarbeitenden Prozesse, die von der Organisation genutzt werden und die Konformität mit den Anforderungen beeinflussen,
f. Verzeichnis der Verarbeitungstätigkeiten als Verantwortliche gem. Art 30 Abs. 1 DSGVO,
g. Verzeichnis der Verarbeitungstätigkeiten als Auftragsverarbeiter gem. Art 30 Abs. 2 DSGVO,
h. Muster einer Verpflichtungserklärung zum Datengeheimnis gem. § 6 DSG,
i. Dokumentation der technischen und organisatorischen Maßnahmen Sicherheitsmaßnahmen gem. Art 32 DSGVO.

4.1.5 Mit der Übermittlung des Antrages erklärt der Antragsteller gemäß § 8 (2) der Verhaltensregeln verbindlich, dass er sich verpflichtet, die Verhaltensregeln bei der Verarbeitung personenbezogener Daten einzuhalten.

4.2 Prüfung des Antrags

4.2.1 Vor Durchführung des Überwachungsaudits prüft die Überwachungsstelle den Antrag, um sicherzustellen, dass

- die formalen Voraussetzungen seitens des Antragstellers zur Teilnahme an den Verhaltensregeln,
- die Informationen über die antragstellende Organisation ausreichend für die Durchführung des Audits sind,
- der Geltungsbereich der angestrebten Überwachung, der/die Standort(e) der Tätigkeiten der antragstellenden Organisation, die zur Ausführung der Audits erforderliche Zeit sowie andere Aspekte, die die Überwachungstätigkeiten beeinflussen, berücksichtigt werden.

4.2.2 Basierend auf dieser Prüfung wird die Überwachungsstelle ein Auditteam gemäß den Anforderungen nach Abschnitt 4.4 bestellen. Das Auditteam besteht zumindest aus einem Leitenden Auditor sowie aus Co-Auditoren nach Erfordernis.

4.3 Erstüberwachung

4.3.1 Vorprüfung

Die Vorprüfung wird durchgeführt, um das erstmalige Überwachungssaudit (Audit gemäß Abschnitt 4.3.2) vorzubereiten.

Die Vorprüfung wird durchgeführt, um

a. die datenschutzbezogene Managementsystem-Dokumentation der Organisation zu prüfen,
b. den Status der Organisation und deren Verständnis bezüglich der Anforderungen der Verhaltensregel zu bewerten,

[4] Bundesgesetz über die Bilanzbuchhaltungsberufe (Bilanzbuchhaltungsgesetz 2014 – BiBuG 2014)

c. die unternehmensspezifischen Bedingungen des Kunden zu beurteilen, um die Reife der Organisation für das erstmalige Überwachungsaudit gemäß 4.3.2 zu ermitteln,

d. notwendige Informationen bezüglich des Geltungsbereichs des Überwachungszertifikates zu erfassen, der Prozesse und des/der Standorts(e) des Kunden.

Feststellungen aus der Vorprüfung werden dokumentiert und dem Kunden mitgeteilt, einschließlich der Hinweise zu identifizierten Schwachstellen, die während des erstmaligen Überwachungsaudits als Nichtkonformität eingestuft werden könnten.

4.3.2 Erstmaliges Überwachungsaudit

Der Zweck des erstmaligen Überwachungsaudits ist es, die Umsetzung der Verhaltensrichtlinien einschließlich der Wirksamkeit der diesbezüglichen Maßnahmen der Organisation zu bewerten. Das erstmalige Überwachungsaudit kann in Form eines Fernaudits durchgeführt werden.

4.4 Anforderungen an Auditoren

4.4.1 Das Auditorenteam muss in seiner Gesamtheit folgende Qualifikationsanforderungen erfüllen:

- Kenntnisse des Datenschutzrechts und seiner Anwendung, im speziellen im Zusammenhang mit der Tätigkeit von Bilanzbuchhaltungsberufen,

  ANMERKUNG: Die datenschutzrechtlichen Kenntnisse können im Rahmen der universitären (einschließlich Fachhochschule) Ausbildung oder durch eine einschlägige berufliche Tätigkeit erworben worden sein, sie können beispielsweise auch durch einen Lehrgang (samt Zertifizierung) nachgewiesen werden.

- profunde Kenntnisse über die gegenständlichen Verhaltensregeln,

- profunde Kenntnisse über die Prozesse und Kriterien dieses Überwachungsschemas.

4.4.2 Auditoren, die Überwachungsverfahren alleine durchführen, müssen alle Kriterien gemäß 4.4.1 erfüllen.

4.4.3 Sollten im Einzelfall Umstände vorliegen, die es nach Prüfung durch die Überwachungsstelle rechtfertigen, die Unbefangenheit in Zweifel zu ziehen, so teilt der Auditor diese Umstände und den Zweifel an der Unbefangenheit der Geschäftsstelle unverzüglich mit und ist vom jeweiligen Überwachungsverfahren auszuschließen.

4.4.4 Zu überwachende Organisationen haben das Recht, Auditoren ohne Angaben von Gründen abzulehnen.

4.5 Durchführung von Audits

4.5.1 Stichprobenprüfung an mehreren Standorten - Multi-site Audits

Für den Fall, dass eine Organisation mehr als einen Standort betreibt, an denen datenverarbeitende, für die Einhaltung der Verhaltensregeln relevante Prozesse stattfinden, kann eine Stichprobe aus den bestehenden Standorten für die Audits herangezogen werden.

Die Überwachungsstelle legt die Anzahl und die Örtlichkeiten der zu auditierenden Standorte fest.

4.5.2 Zu auditierende Funktionen

Es müssen alle für die Einhaltung der Verhaltensregeln relevanten Funktionen der Organisation durch das Audit abgedeckt werden können.

4.5.3 Unterlagenprüfung

Folgende Unterlagen, Dokumente und Aufzeichnungen sind im Rahmen des Audits zumindest zu prüfen und zu verifizieren:

- Dokumentation der datenverarbeitenden Prozesse inkl. einschlägiger Formvorlagen,

- das Verzeichnis der Verarbeitungstätigkeiten (gemäß Art. 30 DSGVO), als Verantwortlicher und/oder als Auftragsverarbeiter (sofern zutreffend),
- Handbuch bzgl. der technischen und organisatorischen Maßnahmen zur Sicherheit der Verarbeitung (gemäß Art. 32 DSGVO),
- Datenschutz-Folgenabschätzungen (sofern zutreffend),
- Personaldokumentation inkl. datenschutzrechtlicher Schulungen sowie Schulung in Bezug auf die zutreffende Verhaltensregel,
- stichprobenhafte Prüfung einschlägiger Geschäftsfälle in Bezug auf die Umsetzung der Anforderungen.

4.5.4 Auditschlussfolgerungen

Sollten im Rahmen eines Audits Nichtkonformitäten festgestellt werden, werden vom Auditteam entsprechende Auflagen zur Beseitigung der Abweichungen erteilt. Nichtkonformitäten werden wie folgt klassifiziert:

Untergeordnete Nichtkonformität: Geringfügige Nichtkonformität formaler Natur, die die Fähigkeit der Organisation zur Einhaltung der Verhaltensregel in ihren Zielsetzungen nicht beeinträchtigt.

Wesentliche Nichtkonformität: Nichtkonformität, die die Fähigkeit der Organisation zur Einhaltung der Verhaltensregel in ihrer Zielsetzung beeinträchtigt, und/oder ein evidenter Verstoß gegen die DSGVO.

Anmerkung: In folgenden Fällen könnten Nichtkonformitäten als wesentlich eingestuft werden:

- wenn erheblicher Zweifel daran besteht, dass eine wirksame Prozesslenkung besteht oder dass Datenschutz-Compliance Maßnahmen nicht umgesetzt werden;
- mehrere untergeordnete Nichtkonformitäten, die sich auf dieselbe Anforderung oder dasselbe Problem beziehen, könnten einen systembezogenen Fehler darstellen und somit eine wesentliche Nichtkonformität ergeben.

4.5.5 Korrekturmaßnahmen

Für alle untergeordneten Nichtkonformitäten muss die Organisation entsprechende Korrekturmaßnahmen implementieren. Die effektive Implementierung der Korrekturmaßnahmen zu untergeordneten Nichtkonformitäten wird durch eine Überprüfung von der Organisation bereitgestellter Unterlagen und Dokumentation verifiziert.

Für alle wesentlichen Nichtkonformitäten muss die Organisation entsprechende Korrekturmaßnahmen implementieren. Die effektive Implementierung der Korrekturmaßnahmen zu wesentlichen Nichtkonformitäten wird im Rahmen eines teilweisen oder vollständigen Nachaudits verifiziert. Sollte es nicht möglich sein, die Implementierung von Korrekturmaßnahmen zu einer oder mehrerer wesentlicher Nichtkonformitäten innerhalb von 6 Monaten nach dem letzten Tag des Audits zu verifizieren, muss in jedem Fall ein erneutes Audit durchgeführt werden.

4.6 Auditbericht zur erstmaligen Überwachung

Das Auditteam analysiert und bewertet alle während der Vorprüfung und des Audits gemäß 4.3.2 erfassten Informationen und Auditnachweise, trifft Auditfeststellungen und Auditschlussfolgerungen.

Die Informationen, die das Auditteam der Überwachungsstelle für die Ausstellung des Überwachungszertifikates bereitstellt, müssen mindestens enthalten:

a. die Auditberichte einschließlich Aufstellung der untergeordneten und wesentlichen Nichtkonformitäten sowie die Korrekturen und Korrekturmaßnahmen, die von der Organisation ergriffen wurden;
b. eine Dokumentation der Empfehlungen;
c. eine Empfehlung, ob das Überwachungszertifikat ausgestellt werden soll oder nicht, sowie –wenn zutreffend- die Bedingungen hierfür.

4.7 Entscheidung über die Ausstellung des Überwachungszertifikates

4.7.1 Bewertungsprozess

Vor der Entscheidung über die Ausstellung des Überwachungszertifikates, wird durch die Überwachungsstelle eine Bewertung wie folgt durchgeführt:

a) Prüfung der durch das Auditteam bereitgestellten Informationen im Hinblick auf die Anforderungen der Verhaltensregel und den Geltungsbereich;

b) Bewertung, Verifizierung und Freigabe der Korrekturmaßnahmen für alle Nichtkonformitäten.

4.7.2 Ausstellung des Überwachungszertifikates

Basierend auf den Ergebnissen der Bewertung gemäß Abschnitt 4.7.1 entscheidet die Überwachungsstelle formal über die Ausstellung des Überwachungszertifikates. Der Geltungsbereich eines Zertifikates wird durch die folgenden Angaben bestimmt:

- Identifikation der juristischen Person, die Inhaber des Überwachungszertifikates ist,
- Geltungsbereich in Bezug auf die Organisation bzw. fallweise Untereinheiten der Organisation,
- Standorte/Niederlassungen der überwachten Organisation.

Das Überwachungszertifikat enthält folgende Erklärung: „Dieses Zertifikat bestätigt eine aufrechte Überwachung im Sinne des Art. 41 der "Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutz-Grundverordnung, DSGVO)" der in diesem Zertifikat angeführten Verhaltensregeln gemäß Art 40 DSGVO.“

Das Zertifikat hat eine Gültigkeit von 3 Jahren vorausgesetzt, dass die Bedingungen zur Aufrechterhaltung des Überwachungszertifikates gegeben sind.

4.8 Beschwerdeverfahren

4.8.1 Begriffsbestimmung

Beschwerden im Sinne der DSGVO Art 41 (2) (c) sind Einsprüche von betroffenen Personen in Bezug auf die Verletzung der Verhaltensregel durch das überwachte Unternehmen.

4.8.2 Einbringung einer Beschwerde

Natürliche Personen, die behaupten, von der Datenverarbeitung eines überwachten Unternehmens betroffen zu sein, können bei der Überwachungsstelle, sofern sich die Beschwerde auf einen Verstoß gegen die Verhaltensregel gemäß diesem Überwachungsschema bezieht, eine Beschwerde einbringen.

Die Einbringung einer Beschwerde an die Überwachungsstelle ist für die betroffene Person kostenfrei.

Erhält die Überwachungsstelle Kenntnis davon, dass die betroffene Person in derselben Sache auch die Datenschutzbehörde befasst hat, ist das Überprüfungsverfahren mit dieser Begründung einzustellen.

Die Beschwerde muss zumindest Folgendes beinhalten:

- Name und Anschrift des Beschwerdeführers,
- Bezeichnung des überwachten Unternehmens auf welches sich die Beschwerde bezieht,
- Bezeichnung der anwendbaren Verhaltensregeln und die Bestimmung der Verhaltensregeln, welche nach Auffassung des Beschwerdeführers verletzt wurde bzw. die Bezeichnung des als verletzt erachteten Rechts,

- Sachverhaltsbeschreibung, aus der die Verletzung der Verhaltensregeln abgeleitet wird unter Angabe, ob der behauptete Verstoß andauert oder in welchem Zeitraum er begangen wurde,
- Darlegung der Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt mit entsprechender Belegung der Behauptung,
- Darlegung der individuellen Betroffenheit durch die beanstandete Verletzung der Verhaltensregeln.

Wird die Beschwerde von einem Bevollmächtigten des Beschwerdeführers eingebracht, ist eine schriftliche Vollmacht beizulegen. Bei Rechtsanwälten genügt die Berufung auf die erteilte Vollmacht, die Anführung des Rechtsanwalts-Codes ersetzt den Identitätsnachweis.

4.8.3 Prüfung der Einbringung

Die Überwachungsstelle prüft jede eingelangte Beschwerde auf Vollständigkeit gemäß 4.8.2. Unvollständige Beschwerden werden zurückgewiesen bzw. erst nach Komplettierung durch die einbringende Person weiterbearbeitet.

Die Überwachungsstelle leitet aufgrund eingelangter Beschwerden ein Beschwerdeverfahren ein, wenn:

- die Beschwerde die formalen Voraussetzungen erfüllt und
- sich das in der Beschwerde genannte Unternehmen, auf welches sich die Beschwerde bezieht, den Verhaltensregeln unterworfen hat und damit der Überwachung durch die Überwachungsstelle unterliegt; und
- die Beschwerde sich auf einen nach Angaben der betroffenen Person andauernden oder nicht länger als sechs Monate zurückliegenden Verstoß gegen die Verhaltensregel bezieht; und
- über den Verstoß keine Entscheidung der Datenschutzbehörde vorliegt.

Werden die Voraussetzungen nicht erfüllt, wird die Beschwerde von der Überwachungsstelle zurückgewiesen. Der Beschwerdeführer ist diesbezüglich zu informieren.

4.8.4 Sachliche Prüfung der Beschwerde

Erfüllt die Beschwerde die inhaltlichen und formalen Voraussetzungen, wird das Beschwerdeverfahren eingeleitet. Die Überwachungsstelle ist berechtigt und befugt, Befragungen durchzuführen, Dokumentvorlagen zu fordern und sonstige Beweisaufnahmen durchzuführen, die zur Aufklärung des Sachverhalts erforderlich sind.

Die Überwachungsstelle leitet die Beschwerde an das überwachte Unternehmen weiter und holt eine diesbezügliche Stellungnahme durch das Unternehmen ein. Die Frist zur Stellungnahme durch das Unternehmen beträgt längstens zwei Wochen.

Die Überwachungsstelle bestellt zum Zwecke einer sachlichen Prüfung der Beschwerde einen Auditor gemäß 4.4. Die Beschwerde sowie die diesbezügliche Stellungnahme des überwachten Unternehmens werden dem Auditor zur fachlichen Beurteilung übermittelt.

Wenn kein Verstoß gegen die Verhaltensregeln festgestellt wird oder wenn das untersuchte Verhalten durch das unterzeichnende Unternehmen nachweislich abgestellt wurde, kann die Überwachungsstelle die Einstellung des Verfahrens beschließen.

Die Überwachungsstelle informiert den Beschwerdeführer über das Ergebnis bzw. den Stand des Verfahrens spätestens 3 Monate nach Beginn des Verfahrens zur sachlichen Prüfung der Beschwerde. Über das endgültige Ergebnis des Verfahrens ist der Beschwerdeführer in jedem Fall zu informieren.

4.8.5 Korrekturmaßnahmen

Sollten im Rahmen des Beschwerdeverfahrens Nichtkonformitäten (d.h. Abweichungen von den Verhaltensregeln) festgestellt werden, werden von der Überwachungsstelle entsprechende Auflagen zur Beseitigung der Abweichungen erteilt.

Für alle untergeordneten Nichtkonformitäten (gemäß Abschnitt 4.5.4) muss das Unternehmen entsprechende Korrekturmaßnahmen implementieren. Die effektive Implementierung der Korrekturmaßnahmen zu untergeordneten Nichtkonformitäten wird durch eine Überprüfung von der Organisation bereitgestellter Unterlagen und Dokumentation verifiziert.

Für alle wesentlichen Nichtkonformitäten (gemäß Abschnitt 4.5.4) muss die Organisation entsprechende Korrekturmaßnahmen implementieren. Die effektive Implementierung der Korrekturmaßnahmen zu wesentlichen Nichtkonformitäten wird im Rahmen eines teilweisen oder vollständigen Nachaudits verifiziert.

Sollte es nicht möglich sein, die Implementierung von Korrekturmaßnahmen zu einer oder mehrerer Nichtkonformitäten innerhalb von 6 Monaten nach Erteilung der Auflagen umzusetzen, wird das Überwachungszertifikat zurückgezogen.

Fristsetzungen haben sich nach den Umständen im Einzelfall zu richten und einen angemessenen Zeitraum zur Behebung allfälliger Verstöße und regelwidriger Zustände einzuräumen. Auf Anfrage des Unternehmens können Fristverlängerungen (in begründeten Fällen auch mehrfach) gewährt werden.

4.9 Verlängerung des Überwachungszertifikates

4.9.1 Prozess

Zur Verlängerung des Zertifikates nach Ablauf der regulären Laufzeit muss ein Audit gemäß Abschnitt 4.3.2 und 4.5 durchgeführt werden. Das Verlängerungsaudit muss spätestens 2 Monate vor Ablauf des Überwachungszertifikates durchgeführt werden.

Das Verlängerungsaudit muss die Prüfung aller Kriterien gemäß Anhang A umfassen.

Für jede festgestellte wesentliche Nichtkonformität wird die Überwachungsstelle Fristen für umzusetzende Korrekturen und Korrekturmaßnahmen noch vor Ablauf des Überwachungszertifikates festlegen. Solche Korrekturmaßnahmen müssen noch vor dem Ablauf des Überwachungszertifikates von der Organisation implementiert und von der Überwachungsstelle verifiziert werden.

4.9.2 Verlängerung des Überwachungszertifikates

Die Zertifizierungsstelle trifft die formale Entscheidung über die Verlängerung des Überwachungszertifikates auf der Grundlage der Ergebnisse des Verlängerungsaudits sowie der Ergebnisse aus der Bewertung des Systems über den Zeitraum der Zertifizierung.

Wenn alle Überwachungsaktivitäten vor Ablauf des bestehenden Überwachungszertifikates erfolgreich abgeschlossen werden, dann kann das Ablaufdatum der neuausgestellten Überwachungszertifikates auf dem Ablaufdatum des bestehenden Überwachungszertifikates beruhen. Das Ausgabedatum des neuen Zertifikats entspricht dem Tag der Entscheidung zur Verlängerung.

Für den Fall, dass vor Ablauf des Überwachungszertifikates das Verlängerungsaudit nicht abgeschlossen wurde oder es nicht möglich ist, die Umsetzung von Korrekturmaßnahmen für eine wesentliche Nichtkonformität zu verifizieren, wird die Gültigkeit des Überwachungszertifikates nicht verlängert.

Unter der Voraussetzung, dass die ausstehenden Rezertifizierungstätigkeiten abgeschlossen worden sind, kann innerhalb von 6 Monaten nach Ablauf des Überwachungszertifikates das Zertifikat wieder ausgestellt werden; andernfalls ist mindestens ein vollständiges Audit durchzuführen. Das Gültigkeitsdatum des Zertifikats muss dem Tag der Entscheidung zur Verlängerung oder einem späteren entsprechen und das Ablaufdatum muss auf dem vorangegangenen Zertifizierungszyklus basieren.

5 Änderungen der Verhaltensregeln

Änderungen der dem Überwachungszertifikat zu Grunde liegenden Verhaltensregeln werden dem Inhaber eines Überwachungszertifikates von der Überwachungsstelle umgehend mitgeteilt.

Dem Inhaber eines Überwachungszertifikates wird bei veränderten Anforderungen der Verhaltensregeln eine Frist von 12 Monaten zur Anpassung an die geänderten Anforderungen eingeräumt.

Der Nachweis der Erfüllung der Anforderungen ist im Rahmen eines außerordentlichen Überwachungsaudits zu erbringen. Nach Erbringung des Nachweises wird das Überwachungszertifikat mit einer neuen Referenz auf die geänderte Verhaltensregel ausgestellt.

6 Änderungen im Geltungsbereich

Sollte der Zertifikatsinhaber die Erweiterung des Geltungsbereichs in Bezug auf weitere Organisationseinheiten wünschen, muss er dies bei der Überwachungsstelle schriftlich beantragen. Die Überwachungsstelle wird nach Prüfung der Sachlage die für die Erweiterung des Geltungsbereiches des Zertifikates erforderlichen Prüfungen von Unterlagen und/oder Audits festlegen.

Sollte der Zertifikatsinhaber die Einschränkung des Geltungsbereichs in Bezug auf die zertifizierten Organisationseinheiten wünschen, muss er dies der Überwachungsstelle schriftlich mitteilen. Die Überwachungsstelle reduziert den Anwendungsbereich des Überwachungszertifikates entsprechend. Ab diesem Zeitpunkt darf die Organisation keinerlei Aussagen in Bezug auf die Überwachung gemäß der Verhaltensregel mehr tätigen.

Änderungen von Überwachungszertifikaten in Bezug auf formale Angaben des Zertifikatsinhabers (wie z.B. Änderungen im Firmennamen oder der Adresse) sind der Überwachungsstelle schriftlich mitzuteilen. Die Überwachungsstelle stellt ohne fachliche Prüfung ein geändertes Überwachungszertifikat aus.

Jegliche Änderungen in Bezug auf die juristische Person des Zertifikatsinhabers bedingen einen neuen Antrag auf Zertifizierung und die Durchführung eines neuen Zertifizierungsverfahrens.

7 Zurückziehung von Überwachungszertifikaten

Das Zertifikat verliert seine Gültigkeit sofort nach Kündigung des Vertrages durch den Zertifikatsinhaber oder nach Zurückziehung durch Austrian Standards plus GmbH

Das Zertifikat wird durch Austrian Standards plus GmbH zurückgezogen, wenn

- die Voraussetzungen für die Ausstellung des Zertifikats nicht mehr gegeben sind,
- der Kunde die erforderlichen Verlängerungsmaßnahmen nicht fristgerecht durchführen lässt,
- der Kunde Auflagen bzw. vereinbarte Korrekturmaßnahmen, nicht oder nicht vollständig erfüllt,
- der Kunde Nachaudits verweigert.

Wird das Zertifikat zurückgezogen, so setzt die Überwachungsstelle den Zertifikatinhaber davon schriftlich in Kenntnis.

Anhang A Kriterien zur Überwachung

§ 2 Datenverarbeitungen der Bilanzbuchhalterberufe

A.2.1 Berufsberechtigte führen ein Verarbeitungsverzeichnis für Verantwortliche gem. Art 30 (1) DSGVO.

A.2.2 Berufsberechtigte führen ein Verarbeitungsverzeichnis für Auftragsverarbeiter gem. Art 30 (2) DSGVO, sofern sie Datenverarbeitungen im Rahmen eines Auftragsverarbeitungsverhältnisses gem. Art 28 DSGVO vornehmen.

A.2.3 Datenverarbeitungen gemäß BiBuG werden ausschließlich als Verantwortlicher gem. Art 4 Ziffer 7 DSGVO vorgenommen und nicht als Auftragsverarbeiter gem. Art 4 Ziffer 8 DSGVO.

A.2.4 Datenverarbeitungen gemäß BiBuG werden vollständig im Verarbeitungsverzeichnis für Verantwortliche gem. Art 30 (1) DSGVO dokumentiert.

A.2.5 Datenverarbeitungen gemäß BiBuG werden nicht als gemeinsame Verantwortliche gem. Art 26 DSGVO vorgenommen.

§ 3 Rechtsgrundlage für Datenverarbeitungen gem. Art. 4 Z 1 DSGVO

A.3.1 Datenverarbeitungen werden jeweils auf eine rechtmäßige Rechtsgrundlage gestützt, die insbesondere entsprechend den Erwägungen des § 3 der Verhaltensregeln festgelegt wird. Die jeweils anwendbare Rechtsgrundlage wird dokumentiert.

A.3.2 Die Anwendung der Rechtsgrundlage berücksichtigt die Unterscheidung in allgemeine personenbezogene Daten gem. Art 6 DSGVO.

§ 4 Besondere Kategorien von Daten gem. Art 9 DSGVO

A.4.1 Datenverarbeitungen werden jeweils auf eine rechtmäßige Rechtsgrundlage gestützt, die insbesondere entsprechend den Erwägungen des § 4 der Verhaltensregeln festgelegt wird. Die jeweils anwendbare Rechtsgrundlage wird dokumentiert.

A 4.2 Die Anwendung der Rechtsgrundlage berücksichtigt die Unterscheidung in besondere Kategorien personenbezogener Daten gem. Art 9 DSGVO.

§ 5 Zeitliche Begrenzung der Datenverarbeitungen

Speicherfristen

A.5.1 Gemäß dem Grundsatz der „Datenminimierung“ (Art 5 Abs. 1 lit c DSGVO) werden Datenverarbeitungen auf jenes Maß eingeschränkt, das für die Erfüllung des jeweiligen Zwecks erforderlich ist. Diese Einschränkung wird sowohl im Umfang („Zweckbindungsgrundsatz“) als auch hinsichtlich der Dauer (Grundsatz der „Speicherbegrenzung eingehalten.

A.5.2 Daten gem. § 5 (2) der Verhaltensregeln werden jeweils für die dort angeführte Dauer gespeichert.

A.5.3 Daten werden jedenfalls so lange gespeichert, wie sie für ein drohendes oder anhängiges gerichtliches oder behördliches Verfahren, in dem der Unternehmer oder der Berufsberechtigte Parteistellung hat, von Bedeutung sind.

A.5.4 Pauschale, nicht näher begründete Aufbewahrungsdauern sind unzulässig.

A.5.5 Berufsberechtige legen die Speicherdauer für den jeweils konkreten Fall fest, etwa durch Erstellung eines Löschkonzepts. Ein Löschkonzept hat eine Kategorisierung von Daten nach Rechtsgrundlage und Frist der Löschung, eine konkrete Ausweisung der Fristen zur Löschung sowie eine Beschreibung der Löschprozesse für automationsunterschützte Datenverarbeitung und manuell geführte Akte zu umfassen.

Datensicherung

A.5.6 Berufsberechtigte führen regelmäßig Datensicherungen durch.

A.5.7 Berufsberechtigte definieren ein Wiederherstellungskonzept, um die Verfügbarkeit von Systemen, Diensten und personenbezogenen Daten auch bei physischen oder technischen Zwischenfällen zu gewährleisten.

A.5.8 Löschungen von automationsunterstützt verarbeiteten personenbezogenen Daten müssen gem. § 4 Abs. 2 DSG nicht unverzüglich vorgenommen werden, wenn sie aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden können. Die Verarbeitung der so über die eigentliche zulässige Speicherdauer hinaus erfassten Daten muss dabei jedoch mit der Wirkung nach Art 18 Abs. 2 DSGVO eingeschränkt werden.

Anonymisierung

A.5.9 Mit Ablauf der zulässigen Speicherdauer werden betroffene Datenverarbeitungen eingestellt und gespeicherte Daten zum technisch nächstmöglichen Zeitpunkt gelöscht.

A.5.10 Personenbezogene Daten gelten nur dann als anonymisiert, wenn der Personenbezug tatsächlich nicht mehr wiederhergestellt werden kann. Da selten gänzlich ausschließbar ist, dass Daten denkunmöglich jemals wieder der entsprechenden Person zugeordnet werden können, reicht es für eine Anonymisierung (und damit für die Einhaltung einer Speicherbegrenzung) aus, wenn die Rekonstruktion des Personenbezugs nur mit unverhältnismäßigem Aufwand möglich wäre.

§ 6. Technische und organisatorische Sicherheitsmaßnahmen

A.6.1 Berufsberechtigte treffen gemäß Art 32 DSGVO und § 6 DSG unter Berücksichtigung der konkreten Umstände einer Datenverarbeitung die geeigneten technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

§ 7 Informationspflichten

A.7.1 Die Berufsberechtigten erfüllen ihre Informationspflichten gem. Art 13 und Art 14 DSGVO in ihrer Rolle als Verantwortliche gem. Art 4 Z 7 DSGVO.

A.7.2 Berufsberechtigte können sich im Rahmen ihrer Berufsausübung auf die Ausnahmebestimmung des Art 14 Abs. 5 lit b DSGVO stützen, wenn diese Informationen jeweils allen Arbeitnehmern, Lieferanten und Geschäftspartnern sämtlicher Kunden erteilt werden müssten und dies für den Berufsberechtigten mit einem unverhältnismäßigen Aufwand verbunden wäre.

A.7.3 Berufsberechtigte sind im Einzelfall gem. Art 14 Abs. 5 lit d DSGVO von ihrer Informationspflicht gem. Art 14 Abs. 1 bis 4 befreit, wenn sie gem. § 39 BiBuG zur berufsmäßigen Verschwiegenheit über die ihnen anvertrauten Angelegenheiten verpflichtet sind. Diese Verschwiegenheitspflicht gilt über das Ende des Auftragsverhältnisses hinaus.