Zertifizierungssschema Y03.1

Anforderungen an die Compliance von Auftragsverarbeitern gem. Art. 28 DSGVO

Ausgabe 1.0:2020-11-10

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 Compliance eines Auftragsverarbeiters im Sinne des Art. 28 Datenschutz-Grundverordnung (DSGVO)[1] fest.

Zielsetzung des Zertifizierungsverfahrens ist es, zu verifizieren, ob ein Auftragsverarbeiter die in diesem Zertifizierungsschema festgelegten Maßnahmen implementiert hat, um sicherzustellen, dass die mit einem Verantwortlichen[2] getroffenen Vereinbarungen sowie die sich daraus ergebenden Pflichten als Auftragsverarbeiter im Sinne der DSGVO durch den Auftragsverarbeiter eingehalten werden können.

2 Kriterien für die Überwachung

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

3 Zertifizierungsprozess

3.1 Antragstellung

3.1.1 Der Antragsteller muss die Einleitung des Zertifizierungsverfahrens mittels eines von der Zertifizierungsstelle zur Verfügung gestellten Antragsformulars beantragen.

3.1.2 Der Antragsteller muss eine bevollmächtigte Kontaktperson für die Durchführung des Zertifizierungsverfahrens benennen.

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

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

a. die allgemeinen Merkmale der antragstellenden Organisation, einschließlich deren Name sowie die Anschrift(en) ihres/ihrer physischen Standort(e)s und Beziehungen in einer größeren Körperschaft (wenn zutreffend),

b. Art und Umfang der durchgeführten Auftragsverarbeitungen gem. Vereinbarung mit dem Verantwortlichen,

c. Informationen bzgl. aller Funktionen, die im Rahmen der einschlägigen Tätigkeit der Organisation zum Einsatz kommen,

d. Informationen bzgl. der datenverarbeitenden Prozesse und Tätigkeiten sowie die von der Organisation getroffene Datenschutz-Compliancemaßnahmen,

e. Dokumentation der technischen und organisatorischen Maßnahmen bzgl. Datenschutz.

3.2 Prüfung des Antrags

3.2.1 Vor Durchführung des Audits prüft die Zertifizierungsstelle den Antrag, um sicherzustellen, dass

- die Informationen über die Organisation ausreichend für die Durchführung des Audits sind,
- der Geltungsbereich der angestrebten Zertifizierung, der/die Standort(e) der Tätigkeiten der antragstellenden Organisation, die zur Ausführung der Audits erforderliche Zeit sowie andere Aspekte, die die Zertifizierungstätigkeiten beeinflussen, berücksichtigt werden.

---

[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] Im Sinne des Art. 4 Z. 7 DSGVO.

3.2.2 Basierend auf dieser Prüfung wird die Zertifizierungsstelle ein Auditteam bestellen. Das Auditteam besteht zumindest aus einem leitenden Auditor sowie aus Co-Auditoren nach Erfordernis.

3.3 Erstzertifizierung

3.3.1 Audit – Stufe 1

Das Audit der Stufe 1 wird durchgeführt um das eigentliche Zertifizierungsaudit (Audit der Stufe 2 gemäß Abschnitt 3.3.2) vorzubereiten.

Das Audit der Stufe 1 wird durchgeführt, um

a. die datenschutzbezogene Managementsystem-Dokumentation der Organisation zu prüfen,

b. den Status der Organisation und deren Verständnis bezüglich der mit dem Verantwortlichen vereinbarten Anforderungen zu erheben,

c. die unternehmensspezifischen Bedingungen zu beurteilen, um die Reife der Organisation für das Audit Stufe 2 gemäß 3.3.2 zu ermitteln,

d. notwendige Informationen bezüglich des Geltungsbereichs des Zertifikates, der Prozesse und der Standorte der Organisation zu erfassen.

Feststellungen aus der Vorprüfung werden dokumentiert und dem Kunden mitgeteilt, einschließlich der Hinweise zu identifizierten Schwachstellen, die während des Audits der Stufe 2 als Nichtkonformität eingestuft werden könnten.

3.3.2 Audit der Stufe 2

Der Zweck des Audits der Stufe 2 ist es, die Konformität der Leistungen der Organisation mit den Kriterien gemäß Anhang A und den Vereinbarungen mit dem Verantwortlichen festzustellen.

Das Audit der Stufe 2 muss zumindest das folgende umfassen:

a) Informationen und Nachweise über die Konformität mit allen Anforderungen;

b) Überwachung der Leistung, Messung, Berichterstattung und Überprüfung in Bezug auf Ziele und Vorgaben im Rahmen des Geltungsbereichs des Managementsystems;

c) Prüfung der operativen Lenkung der Prozesse der Organisation im Hinblick auf die Umsetzung der Vorgaben des Managementsystems und der Vereinbarungen mit dem Verantwortlichen.

3.4 Durchführung von Audits

3.4.1 Allgemeines

Zur Durchführung eines Audits wird von der Zertifizierungsstelle das Auditteam bestellt. Die Zertifizierungsstelle informiert den Kunden über die Namen und relevante Informationen des Auditteams. Der Kunde hat die Möglichkeit, bis spätestens 3 Wochen vor dem Audit, der Bestellung von Auditteammitgliedern schriftlich zu widersprechen.

Zur Planung eines Audits in Kooperation mit dem Kunden wird der Auditplan sowie die Daten zum Audit mit dem Kunden abgestimmt.

Audits müssen eine Eröffnungsbesprechung zu Beginn des Audits und eine Abschlussbesprechung nach Beendigung des Audits umfassen.

Das Audit kann entweder als Audit vorort oder mit elektronischen Mitteln (Remote-Audits) erfolgen. Der Einsatz von Remote-Audits wird von der Zertifizierungsstelle im Rahmen der Festlegung des Auditprogrammes festgelegt.

3.4.2 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 Vereinbarungen mit dem Verantwortlichen relevante Prozesse stattfinden, kann eine Stichprobe aus den bestehenden Standorten für die Audits herangezogen werden.

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

3.4.3 Zu auditierende Funktionen

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

3.4.4 Unterlagenprüfung

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

- Auftragsverarbeitungsvereinbarung(en) gem. Art 28 DSGVO mit Auftraggebern,
- Dokumentation der datenverarbeitenden Prozesse inkl. einschlägiger Formvorlagen,
- Dokumentation der technischen und organisatorischen Maßnahmen bzgl. Datenschutz (TOMs),
- Datenschutz-Folgenabschätzung (sofern zutreffend),
- Personaldokumentation inkl. einschlägiger datenschutzrechtlicher Schulungen,
- stichprobenhafte Prüfung einschlägiger Geschäftsfälle in Bezug auf die Umsetzung der Anforderungen.

3.4.5 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 Vereinbarungen in ihren Zielsetzungen nicht beeinträchtigt.

Wesentliche Nichtkonformität: Nichtkonformität, die die Fähigkeit der Organisation zur Einhaltung der Vereinbarungen in ihrer Zielsetzung beeinträchtigt, und/oder ein evidenter Verstoß gegen die Pflichten eines Auftragsverarbeiters im Sinne der 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.

3.4.6 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.

3.4.7 Empfehlungen

Über die Feststellung der Konformität hinaus können die Auditoren auch Empfehlungen in Bezug auf die Wirksamkeit und Verbesserungsmöglichkeiten in Bezug auf die erbrachten Dienstleistungen sowie das Managementsystem der Organisation abgeben. Diese werden im Auditbericht dokumentiert, haben aber keinen Einfluss auf die Ausstellung des Zertifikates gemäß Abschnitt 3.6.

3.4.8 Abschlussbesprechung

Am Ende des Audits wird eine Abschlussbesprechung gemeinsam mit dem zuständigen Management des Kunden und gegebenenfalls mit den Personen, die die Verantwortung für die zu auditierenden Funktionen oder Prozesse tragen, durchgeführt werden. Die Anwesenheit bei dieser Abschlussbesprechung wird aufgezeichnet.

Der Zweck der Abschlussbesprechung besteht darin, die aus dem Audit gezogenen Schlussfolgerungen einschließlich der Empfehlung hinsichtlich der Zertifizierung vorzustellen. Alle Nichtkonformitäten werden vom Auditteam erläutert sodass sie verstanden werden. Weiters wird folgendes erläutert bzw. vereinbart:

- weitere Vorgehensweise der Zertifizierungsstelle inkl. Behandlung von Nichtkonformitäten einschließlich aller Konsequenzen, die den Status der Zertifizierung des Kunden betreffen;
- Zeitrahmen, innerhalb dessen der Kunde einen Plan für Korrekturen und Korrekturmaßnahmen in Bezug auf die im Verlauf des Audits ermittelten Nichtkonformitäten vorlegen muss;
- Informationen zu den Prozessen für die Behandlung von Beschwerden und Einsprüchen.

Der Kunde erhält die Möglichkeit, Fragen zu stellen. Alle Meinungsverschiedenheiten zwischen dem Auditteam und dem Kunden in Bezug auf die Auditfeststellungen oder die aus dem Audit gezogenen Schlüsse werden erörtert und wenn möglich ausgeräumt. Alle nicht gelösten Meinungsverschiedenheiten werden dokumentiert und an die Zertifizierungsstelle weitergeleitet.

3.5 Auditbericht zur Erstzertifizierung

Das Auditteam analysiert und bewertet alle während der Audits der Stufe 1 und der Stufe 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 zu Korrekturen und Korrekturmaßnahmen, die von der Organisation ergriffen wurden;

b. Dokumentation der Empfehlungen;

c. eine Empfehlung, ob das Überwachungszertifikat ausgestellt werden soll oder nicht, sowie –wenn zutreffend- die Bedingungen hierfür.

3.6 Entscheidung über die Ausstellung des Zertifikates

3.6.1 Bewertungsprozess

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

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

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

3.6.2 Ausstellung des Zertifikates

Basierend auf den Ergebnissen der Bewertung gemäß Abschnitt 3.6.1 entscheidet die Zertifizierungsstelle formal über die Ausstellung des Zertifikates. Der Geltungsbereich eines Zertifikates wird durch die folgenden Angaben bestimmt:

- Identifikation der Organisation, die Inhaberin des Zertifikates ist,
- Geltungsbereich in Bezug auf die Organisation bzw. fallweise Untereinheiten der Organisation,
- Geltungsbereich in Bezug auf die Art und Umfang der Auftragsverarbeitung,
- Standorte/Niederlassungen der überwachten Organisation.

Das Zertifikat hat eine Gültigkeit von 6 Jahren vorausgesetzt, dass die Bedingungen zur Aufrechterhaltung des Überwachungszertifikates gegeben sind.

3.7 Überwachungsaktivitäten

3.7.1 Überwachungsaudits

Zur Aufrechterhaltung des Zertifikates sind Überwachungsaudits und andere Überwachungsaktivitäten im Abstand von 2 Jahren durchzuführen.

Änderungen bzgl. der zertifizierten Organisation (Struktur, Rechtspersonen, Standorte u.dgl.) sind im Rahmen von Überwachungsaktivitäten zu berücksichtigen und sind entsprechend zu planen. In Abhängigkeit der Art und des Umfanges der Änderungen wird die Zertifizierungsstelle die erforderlichen Überwachungsmaßnahmen festlegen.

Das Überwachungsauditprogramm muss mindestens umfassen:

a. eine Bewertung der ergriffenen Maßnahmen zu Nichtkonformitäten, die im Rahmen des vorhergehenden Audits festgestellt wurden;
b. Stichproben aus geschäftlichen Transaktionen und datenverarbeitenden Prozessen;
c. Wirksamkeit der Datenschutz-Compliancemaßnahmen;
d. Bewertung von Änderungen und
e. Nutzung von Zeichen und/oder andere Verweise auf die Zertifizierung.

Über die Durchführung des Überwachungsaudits wird vom Leitenden Auditor ein Bericht erstellt.

3.7.2 Bewertung durch die Zertifizierungsstelle

Dieser Bericht bildet die Basis für die Entscheidung der Zertifizierungsstelle, das Zertifikat aufrechtzuerhalten. In Abhängigkeit der Ergebnisse der Überwachung kann der Geltungsbereich eines Zertifikates erweitert oder eingeschränkt werden.

3.8 Rezertifizierung

3.8.1 Rezertifizierungsprozess

Zur Verlängerung des Zertifikates sind die folgenden Aktivitäten durchzuführen:

1. Prüfung der Überwachungsberichte des vorangegangenen Zertifizierungszyklus und einer Bewertung der Dienstleistungen der Organisation und des Managementsystems,
2. die Durchführung eines Rezertifizierungsaudits gemäß 3.8.2.

Für den Fall signifikanter Änderungen der Organisation, der Dienstleistungen der Organisation, des Managementsystems oder des Umfeldes der Organisation, kann die Zertifizierungsstelle auch die Durchführung eines weiteren Audits der Stufe 1 anordnen.

3.8.2 Rezertifizierungsaudit

Das Rezertifizierungsaudit muss Folgendes beinhalten:

a. Die Prüfung der Konformität der erbrachten Leistungen mit den Vereinbarungen mit dem Verantwortlichen sowie mit den Kriterien gemäß Anhang A;

b. die Wirksamkeit der Datenschutz-Compliancemaßnahmen in seiner Gesamtheit angesichts interner oder externer Änderungen und deren fortgesetzte Bedeutung und Anwendbarkeit im Geltungsbereich der Zertifizierung.

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

3.8.3 Auditbericht zum Rezertifizierungsaudit

Die Zertifizierungsstelle trifft die Entscheidungen über die Erneuerung der Zertifizierung auf der Grundlage der Ergebnisse des Rezertifizierungsaudits sowie der Ergebnisse aus der Bewertung der Dienstleistungen der Organisation über den Zeitraum der Zertifizierung.

3.8.4 Zertifikatsausstellung

In Abhängigkeit der Ergebnisse der Rezertifizierung kann der Geltungsbereich eines Zertifikates erweitert oder eingeschränkt werden.

Wenn alle Rezertifizierungsaktivitäten vor Ablauf der bestehenden Zertifizierung erfolgreich abgeschlossen werden, dann kann das Ablaufdatum der neuen Zertifizierung auf dem Ablaufdatum der bestehenden Zertifizierung beruhen. Das Ausgabedatum des neuen Zertifikats entspricht dem Tag der Rezertifizierungsentscheidung.

Für den Fall, dass vor Ablauf des Zertifizierungsdatums das Rezertifizierungsaudit nicht abgeschlossen wurde oder es nicht möglich ist, die Umsetzung von Korrekturmaßnahmen für eine wesentliche Nichtkonformität zu verifizieren, dann wird keine Empfehlung für die Rezertifizierung ausgesprochen und die Gültigkeit der Zertifizierung nicht verlängert.

Unter der Voraussetzung, dass die ausstehenden Rezertifizierungstätigkeiten abgeschlossen worden sind, kann innerhalb von 6 Monaten nach Ablauf der Zertifizierung, das Zertifikat wieder ausgestellt werden; andernfalls ist mindestens ein Audit der Stufe 2 durchzuführen. Das Gültigkeitsdatum des Zertifikats muss dem Tag der Re-Zertifizierungsentscheidung oder einem späteren entsprechen und das Ablaufdatum muss auf dem vorangegangenen Zertifizierungszyklus basieren.

3.9 Außerordentliche Audits

Auf Basis der Ergebnisse eines Erst- oder Rezertifizierungsaudits, eines Überwachungsaudits und/oder auf Basis einer sonstigen Information der Zertifizierungsstelle, kann es erforderlich sein, kurzfristig, anlassbezogen ein Audit zur Überprüfung der Konformität der Dienstleistungen durchzuführen. Solche außerordentlichen Audits sind unter den folgenden Voraussetzungen durchzuführen.

- es gibt eine Vereinbarung mit dem Kunden;
- der Geltungsbereich und Zweck des Audits sind klar definiert und dem Kunden kommuniziert;
- das Auditteam ist bestimmt und dem Kunden kommuniziert.

Darüber hinaus gelten für die Durchführung dieser Audits und die Festlegung von Ergebnissen analog die Bestimmungen gemäß 3.4, sofern anwendbar.

4 Änderungen im Geltungsbereich

Sollte der Zertifikatsinhaber die Erweiterung des Geltungsbereichs in Bezug auf weitere Organisationseinheiten und/oder der Art und des Umfangs der Auftragsverarbeitung wünschen, muss er dies bei der Zertifizierungsstelle schriftlich beantragen. Die Zertifizierungsstelle 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 und/oder der Art und des Umfangs der Auftragsverarbeitung wünschen, muss er dies der Zertifizierungsstelle schriftlich mitteilen. Die Zertifizierungsstelle reduziert den Anwendungsbereich des Zertifikates entsprechend. Ab diesem Zeitpunkt darf die Organisation keinerlei Aussagen in Bezug auf die Zertifizierung gemäß dieses Zertifizierungsschemas mehr tätigen.

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

Jegliche Änderungen in Bezug auf die juristische Person der Organisation, bedingen einen neuen Antrag auf Zertifizierung und die Durchführung eines neuen Zertifizierungsverfahrens.

5 Zurückziehung von Zertifikaten

Es gelten die Allgemeinen Geschäftsbedingungen der Zertifizierungsstelle in der jeweils gültigen Fassung.

Anhang A Kriterien zur Zertifizierung

1 Auftragsverarbeitungsvereinbarung

1.1 Der Auftragsverarbeiter schließt (eine) schriftliche Auftragsverarbeitungsvereinbarung(en) mit Verantwortlichen ab. Die Vereinbarung(en) enthält/enthalten die folgenden Bestimmungen:

- Gegenstand und Dauer des Auftrags
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten
- Kategorien der betroffenen Personen
- Rechte und Pflichten des Verantwortlichen

1.2 Die Auftragsverarbeitungsvereinbarung stellt sicher, dass die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter nur auf dokumentierte Weisung des Verantwortlichen erfolgt.

Anmerkung: Über Ausnahmen von dieser Weisungspflicht oder falls der Auftragsverarbeiter der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen verstößt, hat der Auftragsverarbeiter den Verantwortlichen zu informieren.

1.3 Die Auftragsverarbeitungsvereinbarung stellt sicher, dass die im Rahmen der Auftragsverarbeitung verarbeiteten Daten ausschließlich zur Erfüllung der vertraglich vereinbarten Leistung verwendet werden.

1.4 Die Auftragsverarbeitungsvereinbarung stellt sicher, dass alle im Rahmen der Auftragsverarbeitung erworbenen Kenntnisse und Informationen über den Verantwortlichen und die in seinem Auftrag verarbeiteten Daten auch nach Abschluss der Erbringung der Verarbeitungsleistungen vertraulich behandelt werden.

1.5 Die Auftragsverarbeitungsvereinbarung regelt die Bedingungen zur Inanspruchnahme weiterer Auftragsverarbeiter (Subauftragsverarbeiter bzw. Subauftragnehmer). Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne Genehmigung durch den Verantwortlichen in Anspruch. Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind.

1.6 Die Auftragsverarbeitungsvereinbarung regelt die Verpflichtung des Auftragsverarbeiters den Verantwortlichen bei der Einhaltung dessen in den Art. 32 bis 36 DSGVO genannten Pflichten (Sicherheit der Verarbeitung, Meldung von Verletzungen an die Aufsichtsbehörde, Benachrichtigung der betroffenen Personen bei Verletzungen, Durchführung einer Datenschutz-Folgenabschätzung, Vorherige Konsultation) zu unterstützen.

1.7 Die Auftragsverarbeitungsvereinbarung stellt sicher, dass die Pflicht zur Löschung bzw. Rückgabe der Daten nach Beendigung des Auftrags, besteht.

1.9 Die Auftragsverarbeitungsvereinbarung regelt die Pflicht des Auftragsverarbeiters, dem Verantwortlichen die Einhaltung der datenschutzrechtlichen Anforderungen nachzuweisen bzw. alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten zur Verfügung zu stellen und Überprüfungen vom Verantwortlichen oder einem von diesem beauftragten Prüfer zu ermöglichen.

1.10 Die Auftragsverarbeitungsvereinbarung regelt die Pflicht alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung zu treffen.

1.11 Die Auftragsverarbeitungsvereinbarung stellt sicher, dass die Örtlichkeit der Datenhaltung beim Auftragsverarbeiter eindeutig bestimmt und schriftlich festgehalten ist. Eine Änderung bedarf der Zustimmung des Verantwortlichen.

1.12 Die Auftragsverarbeitungsvereinbarung regelt welches Gericht in Streitfällen anzurufen ist und welches Recht dabei zur Anwendung kommt.

2 Technische und organisatorische Maßnahmen

2.1 Um Unbefugten den Zutritt zu relevanten Gebäuden oder Räumen, in denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren, sind Maßnahmen zur Zutrittskontrolle implementiert.

2.2 Um zu verhindern, dass Unbefugte Zugang zu IT-Systemen oder Datenverarbeitungsanlagen erhalten, sind Maßnahmen zur Zugangskontrolle implementiert.

2.3 Um sicherzustellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, sind Maßnahmen zur Zugriffskontrolle implementiert.

2.4 Um sicherzustellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, sind Maßnahmen zur Weitergabekontrolle implementiert.

2.5 Um sicherzustellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, sind Maßnahmen zur Eingabekontrolle implementiert.

2.7 Um sicherzustellen, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind, sind Maßnahmen zur Verfügbarkeitskontrolle implementiert.

2.8 Um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können, sind Maßnahmen zum Trennungskontrolle implementiert.

3 Vorfälle und Meldewege

3.1 Der Auftragsverarbeiter hat die Vorgehensweise bei Verletzungen des Schutzes von Daten als auch das Eskalationsverfahren festgelegt. Der Auftragsverarbeiter stellt sicher, dass der Verantwortliche von solchen Vorkommnissen umgehend informiert wird.

3.2 Der Auftragsverarbeiter führt Aufzeichnungen über alle Verletzungen des Schutzes von Daten .

3.3 Der Auftragsverarbeiter stellt sicher, dass der Verantwortliche schriftlich über Änderungen in den Prozessen und der Art und Weise der Verarbeitung im Rahmen der Auftragsverarbeitung informiert wird.

4 Personal

4.1 Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben.

4.2 Die Mitarbeiter des Auftragsverarbeiters werden bezüglich der Einhaltung des Datenschutzes und der Datensicherheit informiert und geschult. Sie sind fachlich qualifiziert.

4.3 Beim Auftragsverarbeiter wurde eine verantwortliche Person für die Aufgaben des Datenschutzes (z.B. Datenschutzbeauftragter, Datenschutzkoordinator) benannt. Diese Person ist in die notwendigen Prozesse eingebunden.

4.4 Befindet sich der Auftragsverarbeiter außerhalb der EU/EWR wurde ein Vertreter innerhalb der EU gem. Art 27 DSGVO genannt. Dieser ist innerhalb eines Mitgliedstaats der EU niedergelassen.