IITR CERT GmbH
Eschenriederstraße 62c
82194 Gröbenzell

Tel. +49 (0)89 18917360
email@iitr.de
www.iitr-cert.de

Konformitätsbewertungsprogramm

IITR Standard CPS 300

(Stand 07. Januar 2022)

Inhaltsverzeichnis

Abkürzungen

AES	Advanced Encryption Standard
Art.	Artikel
Abs.	Absatz
bzw.	beziehungsweise
DS-GVO	EU-Datenschutz-Grundverordnung
etc.	et cetera
EU	Europäische Union
ggfs.	gegebenenfalls
IPS	Intrusion-Prevention-System
IDS	Intrusion Detection System
PFS	Perfect Forward Secrecy
PGP	Pretty Good Privacy
S/MIME	Secure / Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
usw.	und so weiter
vgl.	vergleiche
z.B.	zum Beispiel

Fachbegriffe / Erläuterungen

CPS	Certified Privacy Standard
CPS 300	Certified Privacy Standard 300 für Auftragsverarbeiter
Organisation	damit sind gemeint Behörden, Unternehmen, Vereine usw.

Redaktioneller Hinweis:
Zur besseren Lesbarkeit wird auf die zusätzliche Formulierung der weiblichen oder neutralen Form verzichtet. Die ausschließliche Verwendung der männlichen Form soll explizit als geschlechtsunabhängig verstanden werden.

1. 1. Rahmenbedingungen des Konformitätsbewertungsprogramms

1.1 Allgemeines

Die informationelle Selbstbestimmung und der damit einhergehende Umgang mit personenbezogenen Daten durch Organisationen haben in unserer Gesellschaft einen hohen Stellenwert. Um das Vertrauen der Mitarbeiter, der Kunden und der Geschäftspartner aufrechtzuerhalten bzw. zu verbessern müssen Organisationen einen datenschutzkonformen Umgang mit personenbezogenen Daten sicherstellen und diesen auch nachweisen.
Dies stellt Auftraggeber vor zusätzliche Herausforderungen, wenn diese einen Dienstleister mit der Verarbeitung personenbezogener Daten im Rahmen der Auftragsverarbeitung gemäß Art. 28 DS-GVO beauftragen.
Hier muss der Auftraggeber im Rahmen der Auftragsvergabe konkrete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten mit dem Dienstleister vereinbaren und deren Einhaltung durch den Dienstleister prüfen.
Die Prüfung und deren Ergebnis müssen vom Auftraggeber nachgewiesen werden, dies ist eine Folge der in Art. 5 Abs. 2 DS-GVO geforderten Rechenschaftspflicht.
Dieser Aufwand kann für die Beteiligten durch eine externe Überprüfung und Bestätigung der beim Auftragsverarbeiter eingerichteten technischen und organisatorischen Maßnahmen zum Schutz der im Auftrag verarbeiteten Daten minimiert werden.

1.2 Ziel

Ziel dieses CPS 300 ist die neutrale und objektive Überprüfung und Bestätigung der bei einem Dienstleister implementierten technischen und organisatorischen Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten für den Auftraggeber.

1.3 Nachweis

Der Nachweis zur Angemessenheit von technischen und organisatorischen Maßnahmen, die eine datenschutzkonforme Verarbeitung personenbezogener Daten im Rahmen der Auftragsverarbeitung ermöglichen, erfolgt durch eine Bewertung der von der Organisation bereitgestellten dokumentierten Informationen. Das vorliegende Konformitätsbewertungsprogramm ist die objektive Grundlage, an der sich die Zertifizierungsstelle bei ihrer Zertifizierungsentscheidung orientiert.

1.4 Grundsätze

Für die Zertifizierung als Auftragsverarbeiter sind die allgemeinen Grundsätze zur Verarbeitung personenbezogener Daten einzuhalten. Dies sind im Einzelnen

- die Rechtmäßigkeit
- die Zweckbindung
- die Beschränkung
- die Richtigkeit
- die Speicherbegrenzung
- die Integrität und Vertraulichkeit

1.5. Zertifizierung

1.5.1 Grundlage

Die Anforderungen an das Zertifizierungsaudit basieren auf verschiedenen Kriterien. Diese sind immer auf die zu zertifizierende Organisation bezogen und im Einzelnen abhängig von

- der Tätigkeitsbranche
- der Anzahl und Art der im Rahmen der Auftragsverarbeitung erbrachten Datenverarbeitungstätigkeiten
- der Anzahl der in die Auftragsverarbeitung involvierten Mitarbeiter
- der Anzahl der für die Auftragsverarbeitung relevanten Standorte
- der Anzahl der eingesetzten Subunternehmer

1.5.2 Bewertung

Die Umsetzungsbewertung der in Ziffer 3 beschriebenen Vorgaben erfolgt im Rahmen einer Auswertung der von der zu zertifizierenden Organisation beantworteten Auditfragen sowie einer Einsichtnahme in die eingereichten dokumentierten Informationen. Die dokumentierten Informationen können z.B. aus Richtlinien, Prozessanweisungen, Arbeitsanweisungen sowie Nachweisen zur Umsetzung bestehen. Bei nicht eindeutig zu bewertenden Sachverhalten oder widersprüchlichen Angaben werden weitere zur Sachverhaltsklärung erforderliche dokumentierte Informationen bei der zu zertifizierenden Organisation angefordert.
Die Ermittlung der Konformität erfolgt immer auf Basis einer Stichprobenprüfung. Dabei werden die eingereichten dokumentierten Informationen (Richtlinien, Prozessanweisungen, Arbeitsanweisungen sowie Nachweise zur Umsetzung) hinsichtlich ihrer Plausibilität und Anwendbarkeit beurteilt. Im Einzelfall werden weitere öffentlich zugängliche Informationen und Angaben der obersten Leitung der zu zertifizierenden Organisation berücksichtigt und in die Konformitätsbewertung einbezogen.
Generell wird bewertet, ob die von der zu zertifizierenden Organisation implementierten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten als angemessen und für die Verarbeitungstätigkeit ausreichend eingestuft werden können. Dabei werden die mit der Auftragsverarbeitung Beschäftigten, die Art der verarbeiteten personenbezogenen Daten, die Standorte der Datenverarbeitungsanlagen und die damit einhergehenden Schutzrechte der von der Datenverarbeitung Betroffenen berücksichtigt.

1.5.3 Ergebnis

Im Rahmen des Audits werden die von der Organisation bereitgestellten dokumentierten Informationen auf ihre Konformität zu den in Ziffer 3 genannten Bewertungsvorgaben geprüft.
Werden dabei Nichtkonformitäten (Abweichungen) festgestellt muss die Organisation Korrekturmaßnahmen definieren und diese innerhalb von 90 Tagen nachweisbar umsetzen. Erst dann kann ein Zertifikat erteilt werden.

1.5.4 Überwachung

Die Konformitätsüberwachung erfolgt im zweijährlichen Turnus. Hier muss die zu überwachende Organisation wieder das gesamte Auditverfahren durchlaufen.
Sollte es innerhalb des zweijährlichen Turnus zu Änderungen der Verarbeitungstätigkeit oder zu einer Abschwächung/Herabsetzung der technischen und organisatorischen

Maßnahmen zum Schutz personenbezogener Daten kommen, muss die Organisation dies unverzüglich der Zertifizierungsstelle mitteilen. Die Zertifizierungsstelle wird dann über die weiteren Maßnahmen entscheiden und dies der Organisation mitteilen.

2. 2. Gegenstand der Konformitätsbewertung

Gegenstand der Konformitätsbewertung sind die in Ziffer 3 beschrieben Bewertungsvorgaben. Diese werden regelmäßig im Rahmen der Konformitätsbewertung vom Herausgeber des CPS 300 überprüft und aktualisiert.
Sollte im Rahmen der regelmäßigen Überprüfung festgestellt werden, dass der CPS 300 nicht mehr dazu geeignet ist, dem Anwender die Grundlage und Umsetzungsbegleitung für einen wirksamen Datenschutz in seiner Organisation zu ermöglichen, wird der CPS 300 umgehend von der für die Konformitätsbewertung verantwortlichen Stelle unter Berücksichtigung der neuen Anforderungen aktualisiert und die Anwender werden informiert. Ggfs. müssen die Anwender weiter Maßnahmen zur Gewährleistung der Anwendbarkeit ergreifen. Sollte eine Aktualisierung in der Folge von äußeren Einflüssen nicht möglich sein, so wird die für die Konformitätsbewertung verantwortliche Stelle entsprechende Maßnahmen zur Information der Anwender ergreifen.

3. 3. Detaillierte Bewertungsvorgaben

Ein Zertifikat kann nur erteilt werden, wenn die nachfolgend beschriebenen Rahmenbedingungen von der antragstellenden Organisation eingehalten und nachgewiesen werden.

3.1 Allgemeine Informationen

Die Organisation muss den Geltungsbereich (Anwendungsbereich) ihrer Dienstleistung spezifizieren. Hierzu muss die Organisation spezifische Angaben machen zu

- der/den im Rahmen der Auftragsverarbeitung durchgeführten Verarbeitungstätigkeit(en)
- den im Rahmen der Auftragsverarbeitung verarbeiteten personenbezogenen Daten und Datenkategorien
- den im Rahmen der Auftragsverarbeitung betroffenen bzw. involvierten Standorten
- den in der Organisation vorhandenen Beschäftigten
- den im Rahmen der Auftragsverarbeitung eingesetzten Beschäftigten
- den im Rahmen der Auftragsverarbeitung eingesetzten Dienstleistern
- den aktuell vorhandenen Zertifikaten zur Informationssicherheit und zum Datenschutz

Die Organisation muss sicherstellen, dass für die als Auftragsverarbeiter durchzuführenden und zu zertifizierenden Verarbeitungstätigkeiten eine Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO vor Auftragsbeginn abgeschlossen ist. Dabei müssen in der Vereinbarung die nachfolgenden Vorgaben zwingend berücksichtigt werden:

- Beschreibung des Zwecks der Verarbeitung und. der vom Auftragsverarbeiter zu erbringenden Leistungen
- Dauer der Verarbeitung bzw. Laufzeit der Auftragsverarbeitung
- Arten der personenbezogenen Daten
- Kategorien der personenbezogenen Daten
- Besondere Kategorien der personenbezogenen Daten
- Pflichten und Rechte des Auftraggebers (u.a. zur Wahrung der Betroffenenrechte, zur Meldung von Datenschutzverletzungen, zur Durchführung von Datenschutz-Folgenabschätzungen)
- Weisungs- und Zweckgebundenheit des Auftragsverarbeiters
- Kontaktdaten des für die operative Auftragsverarbeitung verantwortlichen Beschäftigten beim Auftraggeber
- Kontaktdaten des für die operative Auftragsverarbeitung verantwortlichen Beschäftigten beim Auftragsverarbeiter
- Kontaktdaten des Datenschutzbeauftragten oder des für den Datenschutz Verantwortlichen
- Datenschutz-Verpflichtung der mit der Verarbeitung personenbezogener Daten Beschäftigten
- Einzuhaltende technische und organisatorische Maßnahmen
- Regelung zur Auftragsverarbeitung bei mobilem Arbeiten und bei Tätigkeiten im Home-Office
- Prüfrechte des Auftraggebers beim Auftragsverarbeiter
- Informationspflicht und Widerspruchsrecht des Auftraggebers hinsichtlich der Beauftragung von Subunternehmern
- Prüfrechte des Auftraggebers bei den Subunternehmern
- Unterstützung bei der Wahrung von Betroffenenrechten
- Unterstützung des Auftraggebers bei der Einhaltung der Vorgaben von Artt. 32 bis 36 D-GVO (TOMs, Meldung von Datenschutzverletzungen, Information der Betroffenen, Datenschutz-Folgenabschätzung, vorherige Konsultation)
- Pflicht des Auftragsverarbeiters zur Information des Auftraggebers, wenn eine Weisung gegen den Datenschutz verstößt
- Pflicht des Auftragsverarbeiters zur regelmäßigen Prüfung der Angemessenheit seiner technischen und organisatorischen Maßnahmen
- Pflicht des Auftragsverarbeiters zur Meldung von Datenschutzverletzungen
- Pflicht des Auftragsverarbeiters zur Löschung oder Rückgabe von Daten
- Pflicht zur regelmäßigen Sicherung der Daten des Auftraggebers, wenn eine Speicherung beim Auftragsverarbeiter erfolgt
- Pflicht des Auftragsverarbeiters zur separierten Speicherung der Daten des Auftraggebers, wenn eine Speicherung beim Auftragsverarbeiter erfolgt
- Pflicht zur regelmäßigen Prüfung der Verarbeitungsergebnisse durch den Auftragsverarbeiter
- Pflicht zur regelmäßigen Prüfung der Subunternehmer durch den Auftragsverarbeiter
- Bereitstellung der notwendigen Informationen, damit der Auftraggeber seiner Rechenschaftspflicht nachkommen kann

Die Organisation kann hierzu auf eine eigene Vereinbarung zur Auftragsverarbeitung zurückgreifen oder die Vereinbarung zur Auftragsverarbeitung eines Auftraggebers verwenden.
Die Organisation muss sicherstellen, dass alle eigenen Standorte und ggfs. auch die Standorte der Subunternehmen benannt sind, an denen eine Verarbeitung personenbezogener Daten des Auftraggebers erfolgt. Hierbei müssen auch Angaben zu etwaigen Standorten außerhalb der EU getätigt werden. Die Organisation muss sicherstellen, dass die technischen und organisatorischen Maßnahmen zum Schutz der im Rahmen der Auftragsverarbeitung verarbeiteten Daten für jeden Standort dokumentiert sind und diese die Anforderungen des Art. 32 DS-GVO erfüllen.
Die Organisation muss sicherstellen, dass eine Datenschutzrichtlinie oder eine Datenschutzhandbuch vorhanden ist. Die Datenschutzrichtlinie / das Datenschutzhandbuch muss mindestens Vorgaben

- zum datenschutzkonformen Umgang mit personenbezogenen Daten
- zu den einzuhaltenden technischen und organisatorischen Maßnahmen
- zur Wahrung der Betroffenenrechte
- zum Umgang mit Datenschutzverletzungen
- zur Beauftragung von Dienstleistern

beinhalten.

3.2 Verarbeitungstätigkeiten

Die Organisation muss sicherstellen, dass die als Auftragsverarbeiter durchgeführte Verarbeitungstätigkeiten gemäß den Vorgaben des Art. 30 Abs. 2 DS-GVO dokumentiert sind. Die Dokumentation muss folgendes beinhalten:

- Angaben zu den von der Datenverarbeitung betroffenen personenbezogenen Daten
- Angaben zu den von der Datenverarbeitung betroffenen Kategorien personenbezogener Daten
- Angaben zu den bei der Datenverarbeitung Beteiligten
- Angaben zu den bei der Datenverarbeitung eingesetzten Systemen
- Angaben zu den beteiligten externen Stellen oder Subunternehmen
- Angaben zu den Löschfristen der betroffenen personenbezogenen Daten
- Angaben zur Bewertung hinsichtlich besonderer Risiken für die von der Verarbeitung Betroffenen
- Angaben zu den technischen und organisatorischen Maßnahmen

Ebenso muss die Organisation sicherstellen, dass

- für die im Rahmen der Auftragsverarbeitung zu erbringenden Leistungen detaillierte Prozess- oder Verfahrensbeschreibungen vorhanden sind.
- ein Sicherheitskonzept für den sicheren und kontrollierten Umgang mit den Daten des Auftraggebers vorhanden ist.

3.3 Datenschutzbeauftragter

3.3.1 Bestellung

Die Organisation muss einen Datenschutzbeauftragten bestellen und an die zuständige Datenschutz-Aufsichtsbehörde melden, sofern mindestens 20 Personen mit der Verarbeitung personenbezogener Daten innerhalb des Unternehmens beschäftigt sind. Die Definition „mindestens 20 Personen“ bezieht sich nicht auf die spezifische Auftragsverarbeitung, sondern auf die übergeordnete Unternehmensorganisation.
Davon abweichend muss die Organisation einen Datenschutzbeauftragten bestellen und an die zuständige Datenschutz-Aufsichtsbehörde melden, wenn weniger wie 20 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind und die Verarbeitungsvorgänge eine umfangreiche, regelmäßige und systematische Überwachung von Personen zur Folge haben oder wenn die Kerntätigkeit der Organisation in der umfangreichen Verarbeitung von besonderen Arten personenbezogener Daten liegt.

3.3.2 Unabhängigkeit

Die Organisation muss sicherstellen, dass der Datenschutzbeauftragte seine Tätigkeit unabhängig und weisungsfrei erbringt. Miteinander in Konflikt stehende Aufgaben oder Funktionen dürfen die Unabhängigkeit des Datenschutzbeauftragten nicht gefährden oder in Frage stellen.

3.3.3 Qualifikation

Die Organisation muss sicherstellen, dass der Datenschutzbeauftragte für die von ihm zu erbringende Aufgabe qualifiziert ist. Hierzu muss die Organisation bei einem internen Datenschutzbeauftragten ausreichende Ressourcen für die Aus- und Weiterbildung bereitstellen. Bei einem extern bestellten Datenschutzbeauftragten muss die Organisation Nachweise zur Aus- und Weiterbildung einfordern.

3.4 Beschäftigte

3.4.1 Verpflichtung

Die Organisation muss sicherstellen, dass alle Beschäftigten in dokumentierter Form auf die Einhaltung des Datenschutzes bei der Verarbeitung personenbezogener Daten verpflichtet sind. Hierbei müssen auch Leiharbeitnehmer berücksichtigt werden. Die Verpflichtung muss über das Ende der Auftragsverarbeitung sichergestellt sein.
Die Organisation muss sicherstellen, dass allen Beschäftigten die wesentlichen Inhalte der Datenschutzrichtlinie / des Datenschutzhandbuchs vermittelt sind.

3.4.2 Schulung und Sensibilisierung

Die Organisation muss sicherstellen, dass alle mit der Auftragsverarbeitung Beschäftigten regelmäßig zu den Vorgaben des Datenschutzes geschult und unterwiesen sind. Dies muss auch eine laufende Sensibilisierung zu den Risiken und Gefahren im Zusammenhang mit der Auftragsverarbeitung beinhalten.

3.4.3 Weisungsgebundene Verarbeitung

Die Organisation muss sicherstellen, dass alle mit der Auftragsverarbeitung Beschäftigten zu den für den Auftraggeber vorzunehmenden Verarbeitungen unterwiesen sind.

3.5 Physischer Schutz Gebäude

Die Organisation muss sicherstellen, dass ein wirksamer Zutritts-Schutz zu den Räumlichkeiten, in denen eine Verarbeitung personenbezogener Daten des Auftraggebers erfolgt, implementiert ist. Dazu muss die Organisation Information bereitstellen zu den eingerichteten Schutzmaßnahmen zur

- Verhinderung von unbefugtem Zutritt
- Identifikation von Zutrittsberechtigten
- Überwachung von eingerichteten Schutzmechanismen
- Registrierung von Besuchern und fremden Personen
- Verpflichtung von Besuchern und fremden Personen zur Geheimhaltung

Hierzu können unter anderem die folgenden Kriterien Berücksichtigung finden.

- Verschlossene Räumlichkeiten, u.a. Büros der IT-Administration und Büros, in denen Daten eines Auftraggebers verarbeitetet werden, Server-Räume, etc.
- Server in verschlossenen Serverschränken
- Schließanlage mit Sicherheitsschlüssel
- Zutrittsberechtigungskonzept, Zutrittskontrollsysteme, dokumentierte Zutrittskontrollen
- Sicherheitszonenkonzept
- Zentraler Empfangsbereich
- Besucherregelung und Besucherregistrierung
- Videoüberwachung mit Aufzeichnung
- Einbruchmeldeanlagen, Werkschutz, Alarmverfolgung

3.6 Zugangsschutz / Netzwerk

Die Organisation muss sicherstellen, dass ein wirksamer Zugangsschutz zu dem Netzwerk, in dem eine Verarbeitung personenbezogener Daten des Auftraggebers erfolgt, implementiert ist. Dazu muss die Organisation Information bereitstellen zu den eingerichteten Schutzmaßnahmen

- zur eindeutigen Benutzeridentifikation
- zur Nutzung von Passwörtern, mit Vorgaben zu
- Passwortlänge
- Passwortkomplexität
- Passwortwechsel
- zur Sperrung von Zugängen
- zur Protokollierung von Zugängen und der Protokollauswertung
- zum Berechtigungskonzept
- zur Vergabe, zur Änderung und zum Entzug von Benutzerberechtigungen
- zur Vergabe von Berechtigungen nach dem „need to know Prinzip“
- zur Multi-Faktor Authentifizierung bei Zugängen auf cloudbasierte Anwendungen und bei risikobehafteten Daten

Hierzu können unter anderem die folgenden Kriterien Berücksichtigung finden.

- Ausschließlich personifizierte Benutzer
- Automatisierte Passwort-Kontrolle

- Dokumentierte Vergabe, Änderung und Entzug von Zugangsberechtigungen
- Sperrung von Benutzern bei fehlerhaften Anmeldeversuchen
- Benutzerbezogene 2-Faktor-Authentifizierung
- Dokumentiertes rollen- oder gruppenbasiertes Benutzerberechtigungskonzept
- Firewall auf Servern und auf Endgeräten
- Protokollierung und Auswertung der Zugänge zum Netzwerk bzw. zu den Datenverarbeitungssystemen
- Dokumentierte Freigabe von Zugriffsberechtigungen durch den Dateneigner
- Eingeschränkte und streng limitierte Zugriffsberechtigungen auf die Daten des Auftraggebers
- Protokollierung und Auswertung über die Eingabe, Änderung und Löschung von Daten des Auftraggebers

3.7 Weitergabe

Die Organisation muss sicherstellen, dass ein Verfahren implementiert ist, mit dem die Weitergabe von personenbezogenen Daten des Auftraggebers dokumentiert wird, damit die Wahrung der Betroffenenrechte sichergestellt wird.
Dies beinhaltet auch den Schutz der personenbezogenen Daten, insbesondere vor einer unbefugten Kenntnisnahme. Dazu muss die Organisation Informationen bereitstellen zu den eingerichteten Schutzmaßnahmen

- zur sicheren Leitungsverbindungen
- zur E-Mail-Verschlüsselung
- zur eindeutigen Identifikation von Endgeräten
- zur Verwendung von sicheren Endgeräten
- zu verschlüsselten Datenträgern (z.B. Notebook-Festplattenverschlüsselung und mobilen Devices)
- zur Verschlüsselung von Übertragungen (Ende zu Ende Verschlüsselung)
- zur Verhinderung von unbefugten Datenübermittlungen

Hierzu können unter anderem die folgenden Kriterien Berücksichtigung finden.

- HTTPS-Verschlüsselung mit mindestens TLS 1.2 und PFS
- VPN-Verbindungen
- TLS-Mail-Verschlüsselung
- Zertifikate und Mac-Adressfilterung
- Geräte- und Verzeichnisverschlüsselung (z.B. Bitlocker, VeraCrypt, etc.)
- Ende zu Ende Verschlüsselung durch S/MIME, PGP oder alternativ durch sichere Datenaustauschplattform
- Sperrung von Endgeräte-Schnittstellen
- Sperrung oder Einschränkung von Web-Schnittstellen
- Einschränkung der Nutzung von privaten Endgeräten
- Verhinderung von Datenübertragungen auf ein Endgerät
- Protokollierung und Auswertung von Datenströmen
- Versandprotokolle

3.8 Subunternehmer Datenschutz

Die Organisation muss sicherstellen, dass

- mit allen Subunternehmern Vereinbarungen zur Auftragsverarbeitung gemäß Art. 28 DS-GVO abgeschlossen sind
- alle eingesetzten Subunternehmen für Auftragsvergabe hinsichtlich der Einhaltung der Datenschutzvorgaben überprüft werden
- alle eingesetzten Subunternehmen während der Auftragsdurchführung hinsichtlich der Einhaltung der Datenschutzvorgaben regelmäßig mindestens alle 2 Jahre überprüft werden
- alle Eingesetzten Subunternehmer dokumentierte Weisungen zur Auftragsverarbeitung erhalten

3.9 Datenverarbeitungsanlagen

Die Organisation muss geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten implementieren, die im Rahmen der Auftragsverarbeitung verarbeitet werden. Hierbei muss die Organisation neben dem Stand der Technik (dieser kann sich z.B. an ISO 27001, ISIS 12 o.ä. orientieren) auch die Art der verarbeiteten Daten und den damit einhergehenden Schutzbedarf berücksichtigen.
Als geeignete Maßnahmen können je nach Art der Verarbeitungstätigkeit insbesondere die nachfolgenden Kriterien herangezogen werden:

- Keine Server im Live-Einsatz, bei denen keine Sicherheits-Updates verfügbar sind (z.B. Windows Server 2003, Windows Server 2008)
- Keine Betriebssysteme im Live-Einsatz, bei denen keine Sicherheits-Updates verfügbar sind (z.B. Windows XP, Windows 7)
- Bauliche Sicherung von Servern (Einbruch, Sabotage, Umwelteinwirkungen, Temperatur, Stromversorgung, usw.)
- Technische Sicherung von Servern (Redundante Systeme, aktueller Virenscanner, aktuelle Firewall, Next Generation Firewall, Malware-Schutz mit Sandboxing und IPS/IDS)
- Technische Sicherung von Endgeräten (Virenscanner, Firewall)
- Verschlüsselung von Notebook (Festplattenverschlüsselung) und mobilen Devices
- TLS-Mail-Verschlüsselung
- HTTPS-Verschlüsselung mit mindestens TLS und PFS
- Durchgängiges und dokumentiertes Patch-Management für Server
- Durchgängiges und dokumentiertes Patch-Management für Endgeräte
- Regelmäßiges mehrstufiges und dokumentiertes Backup-Verfahren
- Datensicherungskonzept
- Verschlüsselte Datensicherungen (mit AES-256 Verschlüsselung)
- Komplexe Passwörter mit mind. 10 Zeichen
- Zwei Faktor Authentifizierung bei Zugängen auf cloudbasierte Anwendungen bei risikobehafteten Daten.
- Redundante Internetanbindung
- System-und Anwendungs-Monitoring
- Notfall-Management

- Wiederherstellungs-Management

Diese Aufzählung ist nicht abschließend um muss immer einzelfallbezogen betrachtet werden. Vor dem Einsatz neuer Datenverarbeitungen muss die Organisation immer im Rahmen der Planung die Grundsätze zur Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 DS-GVO angemessen berücksichtigten. Hierzu muss die Organisation ein Verfahren implementieren, welches die Berücksichtigung des Datenschutzes und den Umgang mit personenbezogenen Daten bei der Auftragsverarbeitung vollständig gewährleistet.

Die Organisation muss ein Verfahren planen, verwirklichen und aufrechterhalten, damit besondere Risiken für die Rechte und Freiheiten der im Rahmen der Auftragsverarbeitung Betroffenen berücksichtigt werden, die durch die Auftragsverarbeitung bei der Organisation oder bei eingesetzten Subunternehmern entstehen können. Hierbei muss die Organisation sicherstellen, dass die notwendige Fachkompetenz zur Beurteilung des Sachverhalts intern oder extern bereitgestellt ist. Die Organisation muss den Auftraggeber über besondere Risiken informieren, die sie in Ihrem Verantwortungsbereich identifiziert hat.

3.10 Vertraulichkeit

Die Organisation muss sicherstellen, dass ein Verfahren implementiert ist,

- mit dem der Zugriff auf die personenbezogenen Daten des Auftraggebers durch Unbefugte wirksam verhindert wird.

Hierzu können unter anderem die folgenden Kriterien Berücksichtigung finden.

- Ausschließlich personifizierte Benutzer
- Rollenbasierte Berechtigungskonzept
- Rechtevergabe nach dem „need to know“ Prinzip
- Protokollierung von Zugriffen
- Anonymisierung
- Pseudonymisierung
- Verschlüsselung der Daten
- Durchgängige 2- Faktor-Authentifizierung bei Cloud-Systemen
- Separierung der Daten
- Trennung von Datenbeständen oder Datenbanken unterschiedlicher Auftraggeber
- Trennung von Testdaten und Echtdaten
- Richtlinie zur Speicherung von Datenbeständen oder Datenbanken unterschiedlicher Auftraggeber
- Richtlinie zur Verarbeitung von Daten des Auftraggebers außerhalb der Geschäftsräume
- Protokollierung von Zugriffen, Eingaben, Änderungen und Löschungen
- Patch-Management für Server
- Patch-Management für Endgeräte
- Penetrationstest (intern und extern)

3.11 Datenschutzüberprüfung

Die Organisation muss die Wirksamkeit des Datenschutzes bei der Auftragsverarbeitung regelmäßig bewerten. Hierzu muss die Organisation festlegen, was im Datenschutz überwacht und gemessen werden soll, einschließlich der hierzu notwendigen Prozesse und Maßnahmen. Dies muss sowohl die internen Prozesse und Verarbeitungen als auch die Subunternehmer beinhalten. Die Organisation muss als Nachweis der Überwachung dokumentierte Informationen aufbewahren. Diese müssen mindestens die nachfolgenden Themen beinhalten:

- Eingerichtete technische und organisatorische Maßnahmen zum Schutz der Daten
- Eingerichtete Maßnahmen zur Verpflichtung der Beschäftigten
- Eingerichtete Maßnahmen zur Überwachung der Auftragsverarbeiter / Subunternehmer
- Eingerichtete Maßnahmen zur Wahrung der Betroffenenrechte
- Eingerichtete Maßnahmen zur Sicherstellung der Bearbeitung und Meldung von Datenschutzverletzungen

Die Organisation muss sicherstellen, dass die Datenschutzüberprüfungen von einer sachkundigen Person oder Stelle durchgeführt wird, die unabhängig vom auditierten Bereich ist.

3.12 Datenschutzverletzung

3.12.1 Allgemein

Die Organisation muss ein Verfahren zur Identifikation und Bearbeitung von Datenschutz-Verletzungen im Zusammenhang mit der Auftragsverarbeitung implementieren. Hierzu muss die Organisation die Verantwortlichkeiten für die Bearbeitung von Datenschutz-Verletzungen und die dazu notwendigen Prozesse implementieren und bekannt machen.
Dabei müssen auch etwaige Datenschutz-Verletzungen außerhalb der Organisation (z.B. bei Subunternehmern) berücksichtigt werden, sofern diese im Zusammenhang mit der Auftragsverarbeitung der Organisation stehen.

3.12.2 Interne Meldepflicht

Die Organisation muss sicherstellen, dass die mit der Auftragsverarbeitung Beschäftigten darüber informiert sind,

- was unter einer möglichen Datenschutz-Verletzung zu verstehen ist und
- welche Maßnahmen bei Kenntnisnahme einer möglichen Datenschutz-Verletzungen erforderlich sind.

3.12.3 Externe Meldepflicht

Die Organisation muss sicherstellen, dass eine mit der Auftragsverarbeitung in Zusammenhang stehende Datenschutz-Verletzung unverzüglich (innerhalb von 36 Stunden) an den Auftraggeber gemeldet wird. Dies muss auch die Meldung von Datenschutz-Verletzungen beinhalten, die bei einem Subunternehmer aufgetreten sind.

3.13 Betroffenenrechte

Sofern ein Betroffener bei der Organisation das Recht auf

- Auskunft
- Berichtigung
- Löschung
- Einschränkung
- Mitteilungspflicht
- Datenübertragung
- Widerspruch

geltend macht, muss die Organisation sicherstellen, dass das Ersuchen eines Betroffenen unverzüglich an den Auftraggeber weitergeleitet wird.
Die Organisation muss auch sicherstellen, dass ein bei einem Subunternehmer eingehendes Ersuchen unverzüglich an den Auftraggeber weitergeleitet wird.
Ebenso muss die Organisation sicherstellen, dass das Ersuchen eines Betroffenen unverzüglich bearbeitet wird, wenn das Ersuchen die Organisation als Verantwortlicher der Datenverarbeitung selbst betrifft.

3.14 Löschung / Rückgabe der Daten

Die Organisation muss sicherstellen, dass alle Daten, die im Rahmen der Auftragsverarbeitung verarbeitet werden, nach Beendigung des Auftrags vollständig gelöscht oder an den Auftraggeber übertragen werden.