IITR CERT GmbH
Eschenriederstraße 62c
82194 Gröbenzell

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

Konformitätsbewertungsprogramm

IITR Standard CPS 100

(Stand 29.03.2022)

Inhaltsverzeichnis

Abkürzungen

bzw. beziehungsweise

usw. und so weiter

vgl. vergleiche

z.B. zum Beispiel

Fachbegriffe / Erläuterungen

CPS	Certified Privacy Standard
CPS 100	Certified Privacy Standard 100 für KMUs
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. 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 nachweisen.

1.2 Ziel

Ziel dieses Konformitätsbewertungsprogramms ist die Überprüfung der von einer Organisation zur Verarbeitung von personenbezogenen Daten implementierten Maßnahmen und Prozesse hinsichtlich ihrer Fähigkeit, die Vorgaben dieses CPS 100 zu erfüllen.

1.3 Nachweis

Der Nachweis zur Umsetzung der Implementierung von Maßnahmen und Prozessen, die eine datenschutzkonforme Verarbeitung ermöglichen, erfolgt durch eine Bewertung der von der Organisation bereitgestellten dokumentierten Informationen. Das vorliegende Konformitätsbewertungsprogramm ist die Grundlage, an der sich die Zertifizierungsstelle bei ihrer Zertifizierungsentscheidung orientiert.

1.4 Grundsätze

Als Basis für die Zertifizierung sind die allgemeinen Grundsätze zur Verarbeitung personenbezogener Daten definiert. 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 Datenverarbeitungstätigkeiten
- der Anzahl der in die Datenverarbeitung involvierten Mitarbeiter
- der Anzahl der relevanten Datenverarbeitungsstandorte

- der Anzahl der eingesetzten Subunternehmer

1.5.2 Bewertung

Die Umsetzungsbewertung der in Ziffer 3 beschriebenen Vorgaben erfolgt im Rahmen einer Einsichtnahme in die von der zu zertifizierenden Organisation eingereichten dokumentierten Informationen. Diese können aus Richtlinien, Prozessanweisungen, Arbeitsanweisungen sowie Nachweisen zur Umsetzung bestehen. Bei nicht eindeutig zu bewertenden Sachverhalten oder widersprüchlichen Angaben werden im Einzelfall 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. Dabei wird bewertet, ob die von der zu zertifizierenden Organisation getroffenen Maßnahmen zum Schutz personenbezogener Daten als angemessen und ausreichend eingestuft werden können. Dabei werden die Art der verarbeiteten personenbezogenen Daten, die Standorte der Datenverarbeitungsanlagen, die eingesetzten Dienstleister und die damit einhergehenden Schutzrechte der von der Datenverarbeitung Betroffenen berücksichtigt.

1.5.3 Überwachung

Die Konformitätsüberwachung erfolgt im zweijährlichen Turnus. Hier muss die zu überwachende Organisation alle neuen, geänderten und aus der Verwendung genommenen dokumentierten Informationen zur Konformitätsbewertung einreichen. Zusätzlich muss die Anwendung und Aufrechterhaltung der in Ziffer 3 geforderten Vorgaben durch geeignete dokumentierte Informationen (Richtlinien, Prozessanweisungen, Arbeitsanweisungen, Nachweise zur Umsetzung) nachgewiesen werden. Dies können neben der Einsichtnahme in die eingereichten Informationen auch Gespräche mit den in der Organisation Beschäftigten sein.

1.5.4 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 festgestellt, muss die Organisation Korrekturmaßnahmen definieren und diese innerhalb von 90 Tagen nachweisbar umsetzen. Erst dann kann ein Zertifikat erteilt werden.

2. Gegenstand der Konformitätsbewertung

Gegenstand der Konformitätsbewertung sind die in Ziffer 3 beschriebenen Bewertungsvorgaben. Diese werden regelmäßig im Rahmen der Konformitätsbewertung vom Herausgeber des CPS 100 überprüft und mit den allgemeinen und besonderen Anforderungen an den Schutz personenbezogener Daten überprüft und aktualisiert.

Sollte im Rahmen der regelmäßigen Überprüfung festgestellt werden, dass der CPS 100 nicht mehr dazu geeignet ist, dem Anwender die Grundlage und Umsetzungsbegleitung für einen wirksamen Datenschutz in seiner Organisation zu ermöglichen, wird der CPS 100 umgehend von der

für die Konformitätsbewertung verantwortlichen Stelle unter Berücksichtigung der neuen Anforderungen aktualisiert und die Anwender werden informiert. 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. Detaillierte Bewertungsvorgaben

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

3.1 Allgemeines

3.1.1 Datenschutz-Vorgaben

Die Organisation muss eine Datenschutz-Richtlinie oder ein Datenschutz-Handbuch wirksam implementieren, das die Anforderungen aus dem Datenschutz an die Organisation angemessen berücksichtigt.

3.1.2 Organisationsstruktur

Die Organisation muss ihre Organisationsstruktur abbilden. Dabei müssen alle datenverarbeitenden Stellen innerhalb der Organisation berücksichtigt und dargestellt werden. Alle Standorte, an denen eine Datenverarbeitung erfolgt, müssen dargestellt werden. Hierbei muss für jeden Standort die organisatorische Eingliederung in die Gesamtorganisation erkennbar sein.

3.1.3 Verarbeitungstätigkeiten

Die Organisation muss eine Übersicht über seine Datenverarbeitungstätigkeiten erstellen. Dabei muss jeder Verarbeitungstätigkeit ein Verantwortlicher zugewiesen sein. Jede Verarbeitungstätigkeit muss transparent dokumentiert sein und Angaben zu den folgenden Inhalten bereitstellen:

- 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 Software-Systemen
- Angaben zu den beteiligten externen Stellen
- Angaben zu den Löschfristen der betroffenen personenbezogenen Daten
- Angaben zur Bewertung hinsichtlich besonderer Risiken für die von der Verarbeitung Betroffenen
- Angaben zu den implementierten technischen und organisatorischen Maßnahmen

Hierbei müssen insbesondere mindestens die nachfolgend genannten Verarbeitungstätigkeiten erfasst werden, sofern diese für die Organisation anwendbar sind:

- Benutzeranlage DV-Systeme
- Beschaffung und Einkauf
- Bewerbermanagement
- Dienstleisterbetreuung
- Dienstplanerstellung
- Dokumentenmanagement-Archivierung
- Elektronischer Zahlungsverkehr
- Entgeltabrechnung
- E-Mail-Dienst
- Homepage-Kontaktformular
- Homepage-Tracking
- Internet-Dienst
- Kundenbetreuung
- Newsletter
- Personaldatenverarbeitung
- Reisekostenabrechnung
- TK-Anlage
- Videoüberwachung
- Zeiterfassung Anwesenheit
- Zutrittskontrolle

3.1.4 Grundsätze der Datenverarbeitung

Die Organisation muss Regelungen zu den Grundsätzen der Datenverarbeitung implementieren. Diese Regelungen müssen Maßnahmen beinhalten zur:

- Rechtmäßigkeit und Transparenz der Datenverarbeitung
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität, Vertraulichkeit und Verfügbarkeit

Die Regelungen zu den Grundsätzen der Datenverarbeitung müssen als dokumentierte Informationen zur Verfügung stehen und den mit der Datenverarbeitung beauftragten Personen bekannt gemacht sein.

3.2 Datenschutzbeauftragter (DSB)

3.2.1 Bestellung DSB

Die Organisation muss einen Datenschutzbeauftragten bestellen, sofern mehr als 19 Personen mit der Verarbeitung von personenbezogenen Daten beschäftigt sind.

3.2.2 Meldung des DSB bei der Aufsichtsbehörde

Die Organisation muss sicherstellen, dass der Datenschutzbeauftragte bei der zuständigen Datenschutz-Aufsichtsbehörde gemeldet ist, sofern eine gesetzliche Bestellpflicht besteht.

3.2.3 Unabhängigkeit des DSB

Die Organisation muss die organisatorische Unabhängigkeit des Datenschutzbeauftragten sicherstellen, damit es bei der Tätigkeit des Datenschutzbeauftragten nicht zu Interessenskonflikten kommen kann.

3.2.4 Qualifikation des DSB

Die Organisation muss sicherstellen, dass der Datenschutzbeauftragte ausreichend für die ihm übertragenen Aufgaben qualifiziert ist. Bei einem internen Datenschutzbeauftragten muss die Organisation die regelmäßige Fortbildung zur Aufrechterhaltung der Qualifikation sicherstellen. Bei einem externen Datenschutzbeauftragten muss die Organisation regelmäßig Nachweise zur Aufrechterhaltung der Qualifikation einfordern.

3.3 Kontext und interessierte Parteien

3.3.1 Kontext

Die Organisation muss die externen und internen Themen bestimmen, die für die Zwecke der Datenverarbeitung relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse bei der Datenverarbeitung zu erreichen.

3.3.2 Interessierte Parteien

Die Organisation muss die interessierten Parteien, die für die Datenverarbeitung relevant sind, und deren Anforderungen mit Bezug zur Datenverarbeitung bestimmen.

3.3.3 Anwendungsbereich

Die Organisation muss die Grenzen und die Anwendbarkeit ihrer Vorgaben zum Datenschutz dokumentieren. Hierbei muss die Organisation auch die unter 3.3.1 geforderten externen und internen Themen, die unter 3.3.2 genannten Anforderungen der interessierten Parteien und die Schnittstellen und Abhängigkeiten zwischen den Verarbeitungstätigkeiten berücksichtigen. Dies muss unabhängig davon erfolgen, ob die Datenverarbeitung durch die Organisation selbst oder durch eine andere Organisation im Auftrag durchgeführt wird. Der Anwendungsbereich (zu zertifizierender Bereich) muss als dokumentierte Information verfügbar sein. Der Anwendungsbereich kann sich auch nur auf einzelne Bereiche oder einzelne Standorte beschränken. Funktionen einer Organisation, die zwingend für die Sicherstellung des Datenschutzes erforderlich sind, können nicht aus dem Anwendungsbereich ausgeschlossen werden.

3.3.4 Maßnahmen zum Schutz personenbezogener Daten

Die Organisation muss entsprechend den hier beschriebenen Anforderungen Maßnahmen zum Schutz personenbezogener Daten planen, verwirklichen, aufrechterhalten und fortlaufend verbessern. Dies muss dokumentierte Prüf- und Überwachungszyklen für die Datenverarbeitung und die Unternehmens-IT sowie die Bestätigung der obersten Leitung hinsichtlich der Einhaltung von IT-Mindeststandards (wie in Ziffer 3.7 definiert) beinhalten.

3.4 Führung und Verantwortung

3.4.1 Verpflichtung

Die oberste Leitung muss in Bezug auf den Datenschutz Führung und Verpflichtung übernehmen und hierbei sicherstellen, dass die Datenschutzpolitik und die Datenschutzziele festgelegt und mit der strategischen und operativen Ausrichtung der Organisation im Einklang sind. Die oberste Leitung muss sicherstellen,

- dass die Anforderungen des Datenschutzes in die Geschäfts- und Datenverarbeitungsprozesse der Organisation implementiert werden
- dass die für die Einführung und Aufrechterhaltung des Datenschutzes erforderlichen Ressourcen zur Verfügung stehen
- dass die Bedeutung eines wirksamen Datenschutzes vermittelt wird
- dass die Wichtigkeit der Erfüllung der Anforderungen des Datenschutzes vermittelt wird
- dass der Datenschutz sein beabsichtigtes Ergebnis bzw. seine beabsichtigten Ergebnisse erzielt
- dass die beteiligten Personen angeleitet und unterstützt werden, damit diese zur Wirksamkeit des Datenschutzes beitragen können
- dass die fortlaufende Verbesserung des Datenschutzes gefördert wird
- dass die Führungskräfte unterstützt werden, um die Wichtigkeit des Datenschutzes in ihrem jeweiligen Verantwortungsbereich deutlich zu machen

3.4.2 Politik / Leitlinie

Die oberste Leitung muss eine Datenschutzpolitik / Datenschutzleitlinie festlegen, und dabei sicherstellen,

- dass diese für den Zweck der Organisation angemessen ist
- dass die Datenschutzziele beinhaltet sind
- dass die Datenschutzpolitik / Datenschutzleitlinie den Rahmen zur Definition von Datenschutzzielen bietet
- dass eine Verpflichtung zur Erfüllung der Anforderungen mit Bezug zum Datenschutz vorhanden ist
- dass eine Verpflichtung zur fortlaufenden Verbesserung des Datenschutzes vorhanden ist

Die Datenschutzpolitik / Datenschutzleitlinie muss als dokumentierte Information verfügbar sein und in der Organisation bekannt gemacht sein. Für interessierte Parteien muss die

Datenschutzpolitik / Datenschutzleitlinie verfügbar sein, soweit diese ein berechtigtes Interesse daran begründen können.

3.4.3. Verantwortlichkeiten

Die Rollen und Verantwortlichkeiten für die datenverarbeitenden Bereiche müssen zugewiesen und im Unternehmen bekannt gemacht sein. Ebenso müssen die Befugnisse, die zur Sicherstellung des Datenschutzes erforderlich sind, eindeutig zugewiesen sein. Hierbei müssen auch Regelungen zu Berichten über etwaige Anforderungen, Änderungen, Risiken und Abweichungen beim Datenschutz und den Datenverarbeitungsverfahren definiert und bekannt gemacht sein.

Im Einzelnen müssen die

- Verantwortlichkeiten für Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DS-GVO
- Verantwortlichkeiten für die Sicherstellung der Wahrung der Betroffenenrechte gemäß Art. 13 bis 21 DS-GVO (vgl. Ziffer 3.9)
- Verantwortlichkeit für die Bearbeitung von Datenschutzverletzungen gemäß Art. 33 und 34 DS-GVO (vgl. Ziffer 3.10)

definiert und zugewiesen werden.

3.5 Planung

3.5.1 Allgemeines

Bei der Planung des Datenschutzes muss die Organisation den Kontext (vgl. Ziffer 3.3.1) und die Anforderungen der interessierten Parteien (vgl. Ziffer 3.3.2) berücksichtigen.

3.5.2 Risiken

Die Organisation muss die Risiken ermitteln und bewerten, die den Datenschutz gefährden oder negative Auswirkungen für den Datenschutz haben können. Die identifizierten Risiken müssen bearbeitet werden mit dem Ziel einer nachhaltigen Risikominimierung. Die Wirksamkeit der Maßnahmen muss bewertet und überwacht sein.

3.5.3 Ziele

Die Organisation muss die Datenschutzziele für alle relevanten Funktionen und Bereiche festlegen. Bei der Definition der Datenschutzziele muss sichergestellt werden,

- dass die Ziele mit der Datenschutzpolitik im Einklang stehen
- dass die Ziele messbar sind
- dass die Ziele und deren Ergebnisse die Risiken berücksichtigen
- dass die Ziele in der Organisation vermittelt werden
- dass die Ziele aktualisiert werden, sofern dies in Folge geänderter Rahmenbedingungen erforderlich ist

Die Organisation muss dokumentierte Informationen zu den Datenschutzzielen aufbewahren. Zur Erreichung der Datenschutzziele muss die Organisation die hierfür notwendigen Maßnahmen und Ressourcen definieren. Ebenso muss für jedes Ziel die Verantwortung zugewiesen werden. Im Rahmen der Überwachung muss die Organisation die Ergebnismessung sicherstellen.

3.6 Unterstützung

3.6.1 Ressourcen

Die Organisation muss die erforderlichen Ressourcen für den Aufbau, die Umsetzung und die fortlaufende Verbesserung des Datenschutzes bestimmen und bereitstellen.

3.6.2 Kompetenzen

Die Organisation muss die Kompetenzen bestimmen, die für die Sicherstellung des Datenschutzes erforderlich sind. Sie muss die mit der Datenverarbeitung beauftragten Personen auf die Einhaltung des Datenschutzes verpflichten. Die Organisation muss dokumentierte Informationen zum Nachweis der Kompetenzen führen.

3.6.3 Bewusstsein

Die Organisation muss sicherstellen, dass den mit der Datenverarbeitung beauftragten Personen die Datenschutzpolitik vermittelt ist und diese sich ihres Beitrags zur Sicherstellung des Datenschutzes bewusst sind. Die Organisation muss die mit der Datenverarbeitung beauftragten Personen regelmäßig schulen und sensibilisieren. Etwaige Dienstleister mit Zugang zu personenbezogenen Daten müssen angemessen berücksichtigt werden. Weiter muss die Organisation die Folgen der Nichteinhaltung des Datenschutzes vermitteln. Die Organisation muss dokumentierte Informationen zum Nachweis der Bewusstseinsvermittlung aufbewahren.

3.6.4 Kommunikation

Die Organisation muss die datenschutzrelevante interne und externe Kommunikation festlegen. Hierbei muss die Organisation definieren, wer mit wem wann und worüber kommuniziert. Die Organisation muss dokumentierte Informationen über die Kommunikation führen.

3.6.5 Dokumentierte Informationen

Die Organisation muss dokumentierte Informationen erstellen, aufrechterhalten und weiterentwickeln, die sie für die Wirksamkeit und die Nachweisfähigkeit des Datenschutzes bestimmt hat. Hierbei muss die Organisation ihre Größe und Struktur, die Art ihrer Tätigkeiten, die Prozesse, die Produkte und Dienstleistungen sowie deren Komplexität berücksichtigen. Die Organisation kann die dokumentierten Informationen in Papierform oder in elektronischer Form mit der Möglichkeit alle elektronischen Informationen auszudrucken aufrechterhalten. Die benötigten

dokumentierten Informationen müssen gelenkt sein. Die Organisation muss dokumentierte Informationen über die Methodik zur Lenkung der dokumentierten Informationen aufbewahren.

3.7 Technische und organisatorischen Maßnahmen

Die Organisation muss geeignete technische und organisatorische Maßnahmen zum Schutz aller personenbezogenen Daten implementieren, die unter die Verantwortung der Organisation fallen. Hierbei muss die Organisation neben dem Stand der Technik (dieser sollte 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 in der Anlage beschriebenen Kriterien herangezogen werden. Dabei ist zu beachten, dass die in der Anlage beschriebenen Kriterien nicht abschließend sind und immer einzelfallbezogen betrachtet werden müssen. Vor dem Einsatz neuer Datenverarbeitungen muss die Organisation immer im Rahmen der Planung die in Ziffer 3.1.4 genannten Grundsätze angemessen berücksichtigten. Hierzu muss die Organisation ein Verfahren implementieren, welches die Berücksichtigung des Datenschutzes und den Umgang mit personenbezogenen Daten vollständig gewährleistet.

3.8 Spezifische Maßnahmen zum Datenschutz

Die Organisation muss Aussagen treffen zu den organisationsspezifischen Maßnahmen zum Schutz der personenbezogenen Daten. Hierbei muss die Organisation die nachfolgenden Themen in allen Bereichen angemessen berücksichtigten:

- die Organisationsstruktur
- die Orte der Datenverarbeitung
- die Mitarbeiter
- die Art der verarbeiteten personenbezogenen Daten
- die zur Datenverarbeitung eingesetzten Systeme
- die zur Datenverarbeitung eingesetzten Dienstleister
- die Schnittstellen zwischen den verschiedenen an einer Datenverarbeitung beteiligten Bereichen und Systemen.

Die Organisation muss ein Verfahren planen, verwirklichen und aufrechterhalten, damit besondere Risiken für die Rechte und Freiheiten der Betroffenen berücksichtigt werden, die durch eine Datenverarbeitung entstehen können. Hierbei muss die Organisation sicherstellen, dass die notwendige Fachkompetenz zur Beurteilung des Sachverhalts intern oder extern bereitgestellt ist.

3.9 Wahrung der Betroffenenrechte

3.9.1 Information der von der Datenverarbeitung Betroffenen

Die Organisation muss sicherstellen, dass die von der Verarbeitung personenbezogener Daten Betroffenen gemäß Art. 13 und 14 DS-GVO informiert werden.

3.9.2 Anfragen und Eingaben der von der Datenverarbeitung Betroffenen

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 und vollständig bearbeitet wird.

3.9.3 Webseite

Sofern die Organisation eine oder mehrere Webseiten/online-Auftritte als Verantwortlicher gemäß Art. 4 Nr. 7 DS-GVO bereitstellt muss sie sicherstellen, dass

- die Besucher über die Verarbeitung Ihrer personenbezogenen Daten umfassend informiert werden
- die Verarbeitung personenbezogener Daten der Besucher im Einklang mit den Vorgaben der DS-GVO erfolgt (vor allem auch zur Besucherverfolgung / zum Tracking)
- Dritt-Dienstleister datenschutzkonform eingesetzt werden

3.10 Verletzung des Datenschutzes

Die Organisation muss ein Verfahren zur Identifikation und Bearbeitung von Datenschutzverletzungen implementieren. Hierzu muss die Organisation die Verantwortlichkeiten für die Bearbeitung von Datenschutzverletzungen und die dazu notwendigen Prozesse implementieren und bekannt machen. Dabei müssen auch etwaige Datenschutzverletzungen außerhalb der Organisation berücksichtigt werden, sofern diese im Zusammenhang mit der Datenverarbeitung bzw. in der Verantwortung der Organisation stehen.

3.11 Bewertung

3.11.1 Überwachung, Messung, Analyse und Bewertung

Die Organisation muss die Wirksamkeit des Datenschutzes bewerten. Hierzu muss die Organisation folgendes festlegen:

- Definition, was im Datenschutz überwacht und gemessen werden soll, einschließlich der hierzu notwendigen Prozesse und Maßnahmen
- Definition der Methoden zur Überwachung, Messung, Analyse und Bewertung (sofern zutreffend)
- Zeitpunkt, an dem die Überwachung und Messung durchzuführen ist
- Zuweisung der Verantwortung für die Überwachung und Messung

- Definition, wie die Ergebnisse der Überwachung und Messung zu analysieren und zu bewerten sind
- Zuweisung der Verantwortung für die Analyse und Bewertung der Ergebnisse

Die Organisation muss als Nachweis der Überwachung, Messung, Analyse und Bewertung dokumentierte Informationen aufbewahren.

3.11.2 Internes Audit

Die Organisation muss regelmäßig interne Audits durchführen, um Informationen über den Stand des Datenschutzes zu erhalten. Hierzu muss die Organisation Audits planen und durchführen. Dabei sind für jedes Audit der Auditumfang und die Auditkriterien festzulegen. Bei der Durchführung des Audits muss die Unparteilichkeit des Auditors und eine objektive Beurteilung sichergestellt werden. Über die durchgeführten Audits müssen dokumentierte Informationen aufbewahrt werden. Das Ergebnis eines Audits muss den für die Organisation und den auditierten Bereich verantwortlichen Personen zugänglich gemacht werden.

3.11.3 Review

Die oberste Leitung muss den Datenschutz in der Organisation regelmäßig (mindestens einmal p.a.) bewerten, damit die fortdauernde Eignung, die Angemessenheit und die Wirksamkeit sichergestellt werden. Hierbei müssen die folgenden Themen berücksichtigt werden:

- Veränderungen bei internen Themen die den Datenschutz betreffen (Bereiche, Prozesse, Verantwortlichkeiten, Mitarbeiter)
- Veränderungen bei externen Themen die den Datenschutz betreffen (Dienstleister, Prozesse, Verantwortlichkeiten)
- Rückmeldung zu Nichtkonformitäten und Korrekturmaßnahmen
- Ergebnisse der Überwachungen und Messungen
- Ergebnisse der durchgeführten Audits
- Ergebnis der Zielerreichung
- Rückmeldungen der interessierten Parteien
- Ergebnisse zur Beurteilung und Behandlung der Risiken
- Maßnahmen und Möglichkeiten zur fortlaufenden Verbesserung des Datenschutzes

Die Ergebnisse des Reviews müssen Möglichkeiten der fortlaufenden Verbesserung sowie den notwendigen Änderungsbedarf im Datenschutz beinhalten und müssen der obersten Leitung zur weiteren Entscheidung vorgelegt werden.

3.12 Verbesserung

3.12.1 Nichtkonformitäten und Verbesserung

Bei aufgetretenen Datenschutzverletzungen oder sonstigen Nichtkonformitäten muss die Organisation die möglichen negativen Auswirkungen identifizieren und Maßnahmen zur Verringerung

oder Abstellung ergreifen. Hierbei muss die Organisation immer mit dem Ziel der zukünftigen und nachhaltigen Risikovermeidung agieren.

3.12.2 Fortlaufende Verbesserung

Die Organisation muss die Eignung, die Angemessenheit und die Wirksamkeit des Datenschutzes fortlaufend verbessern. Hierzu müssen neben den Nichtkonformitäten und den daraus resultierenden Verbesserungen auch die Eingaben der Mitarbeiter und der interessierten Parteien einbezogen werden.

Anlage zu Ziffer 3.7

A 1 Räumliche Anforderungen und Zutrittsschutz

A 1.1

Die Organisation muss sicherstellen, dass Gebäude und Büroräume mit Datenverarbeitungsgeräten über einen wirksamen Zutrittsschutz verfügen.

A 1.2

Die Organisation muss sicherstellen, dass Serverräume bzw. Server über eine wirksamen Zutrittsschutz verfügen, bei dem nur die IT-Administratoren Zutritt zu den Servern haben.

A 1.3

Die Organisation muss sicherstellen, dass wirksame Sicherungsmaßnahmen für den Schutz der Server vorhanden sind (z.B. Schutz gegen Einbruch oder Sabotage, Schutz die Einwirkung von Umwelteinflüssen (z.B. Feuer, Wasser, Temperatur, Stromversorgung, usw.).

A 1.4

Die Organisation muss sicherstellen, dass Sie jederzeit Kenntnis darüber hat, welche organisationsfremden Personen sich in den Räumlichkeiten aufhalten.

A 2 Zugangsschutz

A 2.1

Die Organisation muss sicherstellen, dass eine dokumentierte und personifizierte Benutzerregistrierung, Benutzeränderung und Benutzerlöschung im Netzwerk vorhanden ist. Das Benutzerberechtigungskonzept muss hierbei rollen- oder gruppenbasiert aufgebaut sein. Dabei muss sichergestellt sein, dass auch cloudbasierte Anwendungen berücksichtigt werden und dass der jeweilige Dateneigner den Zugang zu personenbezogenen Daten autorisiert. Das „need to know Prinzip“ muss ebenfalls eingehalten werden.

A 2.2

Die Organisation muss sicherstellen, dass bei Zugang zum Netzwerk der Organisation von außerhalb der Organisation ein ausreichender Schutz der Verbindung mittels VPN oder dergleichen vorhanden ist. Hierbei muss die Organisation auch sicherstellen, dass eine Zugangsprotokollierung vorhanden ist.

A 2.3

Die Organisation muss sicherstellen, dass eine Multi-Faktor-Authentifizierung bei Zugängen von außerhalb der Geschäftsräume zu Netzwerk oder Daten der Organisation durch Beschäftigte vorhanden ist.

A 2.4

Die Organisation muss sicherstellen, dass eine Multi-Faktor-Authentifizierung bei Zugang auf cloudbasierte Anwendungen mit risikobehafteten Daten vorhanden ist. Risikobehaftete Daten sind z.B. besondere Arten personenbezogener Daten (z.B. Gesundheitsdaten), Zahlungsdaten (z.B. Kontodaten) oder Daten, die für den Betrieb der eigenen Organisation essenziell erforderlich sind (z.B. Kundenkartei).

A 2.5

Die Organisation muss sicherstellen, dass eine Mobile-Device-Management-Software (MDM) bei Nutzung von privaten Endgeräten durch Beschäftigte vorhanden ist.

A 2.6

Die Organisation muss sicherstellen, dass komplexe Passwörter mit mindestens 8 Zeichen für den Zugang zum Netzwerk verwendet werden. Dabei müssen mindestens 3 der folgenden Zeichen (Großbuchstabe, Kleinbuchstabe, Ziffer, Sonderzeichen) verwendet werden.

A 3 Weitergabeschutz

A 3.1

Die Organisation muss sicherstellen, dass eine TLS-Mail-Verschlüsselung und zusätzlich die Möglichkeit einer „Ende zu Ende Verschlüsselung“ beim E-Mail Versand vorhanden ist. Die Organisation muss sicherstellen, dass eine HTTPS-Verschlüsselung mit mindestens TLS 1.2 und Perfect Forward Secrecy (PFS) vorhanden ist.

A 3.2

Die Organisation muss sicherstellen, dass Datenströme im Unternehmensnetzwerk überwacht und ausgewertet werden.

A 4 Technische Maßnahmen

A 4.1

Die Organisation muss sicherstellen, dass keine Server im Live-Einsatz sind, bei denen keine Sicherheits-Updates verfügbar sind (z.B. Windows Server 2003).

A 4.2

Die Organisation muss sicherstellen, dass keine Betriebssysteme im Live-Einsatz sind, bei denen keine Sicherheits-Updates verfügbar sind (z.B. Windows XP, Windows 7).

A 4.3

Die Organisation muss sicherstellen, dass ein durchgängiges und dokumentiertes Patch-Management für die IT-Hardware (Server, Switches, Router, etc.) vorhanden ist.

A 4.4

Die Organisation muss sicherstellen, dass ein durchgängiges und dokumentiertes Patch-Management für Endgeräte vorhanden ist.

A 4.5

Die Organisation muss sicherstellen, dass ein regelmäßiges, mehrstufiges und dokumentiertes Backup-Verfahren vorhanden ist.

A 4.6

Die Organisation muss sicherstellen, dass das Backup-System vom Hauptserver räumlich getrennt ist.

A 4.7

Die Organisation muss sicherstellen, dass verschlüsselte Backups (mit AES-256 Verschlüsselung) erstellt werden.

A 4.8

Die Organisation muss sicherstellen, dass eine technische Sicherung von Servern vorhanden ist. Dies sind unter anderem redundante Systeme, aktueller Virenscanner, aktuelle Firewall, Next Generation Firewall, Malewarschutz mit Sandboxing und Intrusion-Prefention-System Intrusion-Detection-System IPS/IDS.

A 4.9

Die Organisation muss sicherstellen, dass eine technische Sicherung von Endgeräten vorhanden ist. Dies sind unter anderem ein lokaler Virenscanner und eine lokale Firewall.

A 4.10

Die Organisation muss sicherstellen, dass ein IT-Betriebshandbuch zur Sicherstellung eines dokumentierten und geordneten IT-Betrieb vorhanden ist.

A 4.11

Die Organisation muss sicherstellen, dass ein Notfallhandbuch vorhanden ist.

A 4.12

Die Organisation muss sicherstellen, dass Rücksicherungs-/Wiederherstellungstests regelmäßig durchgeführt werden.

A 4.13

Die Organisation muss sicherstellen, dass alle Notebooks über eine Festplattenverschlüsselung verfügen, sofern nicht ausgeschlossen werden kann, dass personenbezogene Daten auf dem Notebook gespeichert werden.

A 4.14

Die Organisation muss sicherstellen, dass der Einsatz von mobilen Speichermedien

Verboten ist oder beim Einsatz von mobilen Speichermedien ausschließlich verschlüsselte und im Eigentum der Organisation stehende Speichermedien verwendet werden.

A 4.15

Die Organisation muss sicherstellen, dass Beschäftigte im Standard keine lokalen Admin-Rechte auf den Endgeräten haben. Für die Vergabe von lokalen Admin-Rechten muss die Organisation einen dokumentierten Freigabeprozess implementiert haben.

A 4.16

Die Organisation sollte sicherstellen, dass innerhalb der Organisation redundante und räumlich getrennte Datenverarbeitungssysteme vorhanden sind.

A 4.17

Die Organisation sollte sicherstellen, dass regelmäßige und dokumentierte Penetrationstests auf die internen IT-Systeme durchgeführt werden.

A 4.18

Die Organisation sollte sicherstellen, dass regelmäßige und dokumentierte Penetrationstests auf online-shops durchgeführt werden.

A 5 Testdaten

A 5.1

Die Organisation muss sicherstellen, dass auf Testumgebungen keine personenbezogenen Echtdaten genutzt werden. Sollte eine Test mit personenbezogenen Daten zwingend erforderlich sein, muss die Organisation sicherstellen, dass die Zugriffsberechtigungen sowie die technischen und organisatorischen Maßnahmen vergleichbar sind wie die auf die entsprechenden Echtdaten zur Anwendung kommenden Berechtigungen sowie technische und organisatorische Maßnahmen.

A 6 Trennung von Daten

A 6.1 Die Organisation muss sicherstellen, dass Daten von unterschiedlichen Auftraggebern sicher voneinander getrennt sind.