Technische und organisatorische Maßnahmen

Präambel

Die technischen und organisatorischen Maßnahmen sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechten und Freiheiten natürlicher Personen zu treffen. Insofern ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei muss ein dem Risiko angemessenes Schutzniveau gewährleistet werden. Wesentliche Änderungen sind zu dokumentieren.

§ 1 Zutrittskontrolle

Die Zutrittskontrolle regelt die Annäherung und den physischen Zutritt zu Bereichen, in denen sich IT-Systeme befinden und mit deren Hilfe personenbezogene Daten verarbeitet werden.

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Die Zutrittskontrolle wird durch folgende Maßnahmen gewährleistet:

(1) Alle Stellen, in denen Daten des Auftragnehmers verarbeitet werden, werden durch ein geeignetes Zutrittskontrollsystem geschützt (Schlüssel, Zahlenschlösser, Kartenlesesystem).

(2) Die befugten Personen sind festgelegt und mit den entsprechenden Zutrittsmitteln wie Schlüssel und / oder Chipkarten ausgestattet. Die Vergabe von Zutrittsberechtigung wird dokumentiert. Die Schlüsselausgabe an Berechtigte erfolgt am Empfang durch den Wachdienst.

(3) Bereiche mit erhöhter Schutzbedürftigkeit wie Serverräume oder Netzwerktechniken sind gesondert geschützt und nur einem begrenzten Personenkreis zugänglich.

(4) Alle Zutrittsrechte werden restriktiv vergeben, dokumentiert und vor Manipulationen geschützt. Dies beinhaltet auch eine regelmäßige Überprüfung der Berechtigungen bzgl. Aktualität und Notwendigkeit. Nicht mehr benötigte Berechtigungen werden zeitnah entzogen.

(5) Veränderungen und Löschungen von Zutrittsberechtigungen auf Grund von Mitarbeiterwechsel oder- ausscheiden werden sofort umgesetzt und dokumentiert.

(6) Zutritte von betriebsfremden Personen werden durch einen Wachdienst / Pförtnerdienst mittels Besuchskontrollverfahren dokumentiert. Gäste müssen während Ihres Besuchs in den Geschäftsräumen von einem Mitarbeiter des Auftragnehmers begleitet werden.

(7) Das Firmengelände wird mittels einer Videokamera überwacht. Die Geschäftsräume werden nachts ebenfalls durch einen Wachdienst überwacht.

(8) Zur Alarmsicherung, von Bereichen mit erhöhter Schutzbedürftigkeit wie Serverräume, ist eine Meldeanlage mit Anbindung an Polizei und / oder Rettungsdienste installiert.

(9) Türen und Fenster sind außerhalb der Betriebszeiten fest verschlossen.

§ 2 Zugangskontrolle

Die Zugangskontrolle verfolgt das Ziel, Unbefugten den Zugang zu IT-Systemen zu verwehren. Sie bildet die zweite Sicherheitsebene nach der Zutrittskontrolle und regelt damit die Möglichkeit des Einwirkens auf die Datenverarbeitung im IT-System selbst.

Das Eindringen Unbefugter in IT-Systeme ist zu verhindern.

Die Zugangskontrolle wird durch folgende Maßnahmen gewährleistet:

(1) Im Rahmen der Auftragsverarbeitung wurden technische (Kennwort- / Passwortschutz) und organisatorische Maßnahmen, hinsichtlich der Benutzeridentifikation und Authentifizierung, getroffen.

(2) Zugriffsprotokolle werden, soweit technisch möglich, mittels einem Verzeichnisdienst gesteuert (LDAP).

(3) Jeder Benutzer erhält einen eindeutigen, ihm zugewiesenen Nutzeraccount, welcher durch ein Passwort geschützt ist.

(4) Die Regelung des Passwortverfahrens erfolgt über eine Passwortrichtlinie mit folgenden Anforderungen:

Das Kennwort muss eine Mindestlänge von 8 Zeichen haben.

Kennwörter werden regelmäßig gewechselt.

Das Kennwort muss eine Komplexität von drei aufweisen (Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen).

Initialkennwörter und voreingestellte Kennwörter sind sofort zu ändern.

Nach mehreren fehlgeschlagenen Kennworteingaben erfolgt eine automatische Sperrung.

(5) Kennwörter werden im System zugriffssicher gespeichert (virtueller Tresor). Vorläufige Kennwörter werden den Benutzern auf sichere Art übergeben.

(6) Pro User wird ein Benutzerstammsatz eingerichtet und gepflegt.

(7) Mobile Datenträger wie Laptops, externe Festplatten, USB Sticks sind verschlüsselt soweit die Datenklassifizierung dies notwendig macht.

(8) Nach längerer Inaktivität eines Nutzers erfolgt eine automatische Sperre des Rechners sowie des Bildschirms, welche nur durch Passworteingabe durch den Nutzer aufgehoben werden kann.

§ 3 Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung Berechtigten nur auf die ihrer jeweiligen Berechtigung unterliegenden Daten zugreifen können („Need-to-Know-Prinzip“). Sie bildet die dritte Sicherheitsebene.

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Die Zugriffskontrolle wird durch folgende Maßnahmen gewährleistet:

(1) Es liegt eine IT-Sicherheitsrichtlinie vor.

(2) Zwei-Faktor-Authentisierung.

(3) Für die Auftragsverarbeitung wird eine bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung eingerichtet. Unterschiedliche Funktionen sind mit differenzierten Berechtigungen in Form von Profilen, Rollen, Transaktionen oder Objekten versehen. Alle Rechte werden restriktiv vergeben, dokumentiert und vor Manipulationen geschützt. Dies beinhaltet auch eine regelmäßige Überprüfung der Berechtigungen bzgl. Aktualität und Notwendigkeit.

(4) Veränderungen und Löschungen von Zugriffsberechtigungen auf Grund von Mitarbeiterwechsel oder- ausscheiden werden zeitnah, umgesetzt und dokumentiert.

(5) Zum Zwecke der Administration werden gesonderte Benutzerkennungen eingerichtet

(6) Es wird geprüft, wann personenbezogene Daten ohne Beeinträchtigung gesetzlicher, vertraglicher oder interner Interessen vernichtet werden können. Hierbei werden die Maximal-Aufbewahrungsfristen, sofern vorhanden, der Entscheidung zugrunde gelegt. Sobald kein Erfordernis zur Aufbewahrung vorliegt, werden die Daten unabhängig von ihrer Form (digital / Papier). Entsprechend der zu löschenden Daten und deren Schutzbedarf wird eine geeignete Löschmethode gewählt:

a) Löschkommandos
b) Formatieren
c) Überschreiben
d) Zerstörung

Technische und organisatorische Maßnahmen

§ 4 Weitergabekontrolle

Durch die Weitergabekontrolle soll sichergestellt werden, dass personenbezogene Daten während einer elektronischen Übertragung, eines Transports oder der Speicherung auf mobilen Datenträgern nicht unberechtigt eingesehen, kopiert, verändert oder gelöscht werden können.

Die Weitergabekontrolle wird durch folgende Maßnahmen gewährleistet:

(1) Im Rahmen der Auftragsdatenverarbeitung wurden Maßnahmen für den Transport, die Übertragung und Übermittlung oder die Speicherung auf Datenträger getroffen (z.B. mittels Passwortschutz).

(2) Mobile Datenträger wie Laptops, externe Festplatten, USB Sticks sind verschlüsselt. Nicht verschlüsselbare Medien dürfen nicht für den Transfer von Daten des Auftraggebers benutzt werden.

(3) Alle Datenübertragungen werden durch das Personal des Auftraggebers initiiert oder werden diesem durch den Auftragnehmer ersichtlich gemacht. Der Auftraggeber kann jederzeit der Datenübertragung widersprechen. Daten die zum Transfer vom Auftraggebernetz ins Auftragnehmernetz auf ein Transportmedium zwischengespeichert werden, werden nach der Übertragung sofort unwiderruflich gelöscht.

(4) Nicht mehr benötigte Datenträger werden datenschutzkonform / BSI-konform vernichtet.

(5) Ein Datenaustausch über das Internet / per E-Mail erfolgt mittels einer verschlüsselten Verbindung (z. B. https).

§ 5 Eingabekontrolle

Die Eingabekontrolle gewährleistet, dass nachvollziehbar protokolliert wird, welcher Nutzer einer Applikation personenbezogene Daten verarbeitet hat. Ein weiteres Ziel der Eingabekontrolle ist die Nachvollziehbarkeit von Fehleingaben.

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege wird durch folgende Maßnahmen gewährleistet:

(1) Bezüglich Daten, die zur Leistungserbringung im Rahmen der Auftragsverarbeitung eingegeben, verändert oder gelöscht werden, erfolgt eine Protokollierung der einzelnen Zugriffe.

(2) Der Auftragnehmer protokolliert sämtliche Veränderungen an Daten in Systemen des Auftragnehmers und macht diese über Auswertungen nachvollziehbar, sofern technisch möglich.

(3) Protokolldaten werden nicht nachträglich verändert.

(4) Ein Zugriff auf Protokolldaten erfolgt nur durch autorisierte Nutzer mit gesonderten Zugriffsrechten.

§ 6 Auftragskontrolle

Die Auftragskontrolle gewährleistet, dass personenbezogene Daten im Rahmen einer Auftragsverarbeitung nur nach den Weisungen des Auftraggebers durch den Auftragnehmer verarbeitet werden.

Die weisungsgemäße Auftragsverarbeitung wird durch einen Vertrag zur Auftragsverarbeitung gewährleistet.

Alle für die Auftragsverarbeitung relevanten Punkte sind im Hauptvertrag sowie dessen Anlagen konkretisiert.

§ 7 Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle beinhaltet Maßnahmen zum Schutz von personenbezogenen Daten vor einem zufälligen Verlust oder einer Zerstörung (bspw. Wasserschäden, Brand, Blitzschlag, Stromausfall usw.).

Die Verfügbarkeitskontrolle wird durch folgende Maßnahmen gewährleistet:

(1) Im Rahmen der Auftragsverarbeitung werden physikalische als auch logische Maßnahmen zur Datensicherung getroffen. Alle für die Leistungserbringung notwendigen Daten werden durch ein geeignetes Backupverfahren vor Verlust und Zerstörung gesichert.

(2) Alle eingesetzte Software wird einmal voll gesichert, entweder mittels der Originaldatenträger oder als selbst erstellte Kopie.

(3) System- und Protokolldaten werden regelmäßig voll gesichert. Die Sicherung erfolgt im Drei-Generationen-Prinzip auf geeigneten Datenträgern. Alle Anwendungsdaten werden täglich inkrementell gesichert und zusätzlich wöchentlich voll, jeweils im Drei-Generationen-Prinzip. Die Datenträger werden in geeigneter Weise aufbewahrt.

(4) Die im Rahmen der Auftragsverarbeitung eingesetzten Mitarbeiter sind zur Datensicherung verpflichtet.

(5) Anwendungsdaten werden auf zentralen Servern, die vom Backupkonzept abgedeckt sind, abgelegt. In Fällen, in denen der Mitarbeiter keinen Netzzugang hat, muss der Mitarbeiter die Datensicherung selbst vornehmen. In diesem Fall muss das in Abs. (3) angegebene Minimaldatensicherungskonzept eingehalten werden.

(6) Im Rahmen eines Desaster-Recovery-Plans werden alle Datensicherungen bzgl. der Wiederherstellung regelmäßig getestet.

(7) Alle für die Leistungserbringung relevanten Systeme sind durch eine aktuelle Virenschutzsoftware gesichert. Zugänge zu externen Netzen sind durch eine Firewall geschützt.

(8) Alle Datensicherungen werden in einem Tresor aufbewahrt.

(9) Zur unterbrechungsfreien Stromversorgung wird ein Notstromaggregat eingesetzt.

(10) Der Serverraum ist durch eine Klimaanlage sowie eine Brandmeldeanlage geschützt.

Technische und organisatorische Maßnahmen

§ 8 Trennungsgebot

Das Trennungsgebot regelt (technisch und organisatorisch) die getrennte Verarbeitung von personenbezogenen Daten je nach dem Zweck ihrer Erhebung.

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Das Trennungsgebot wird durch folgende Maßnahmen gewährleistet:

(1) Im Rahmen der Auftragsverarbeitung werden Maßnahmen zur getrennten Verarbeitung von Daten mit unterschiedlichen Zwecken getroffen. Die Systeme des Auftragnehmers bilden eine interne Mandantenfähigkeit ab. Daten des Auftraggebers werden sowohl physikalisch als auch logisch von Daten anderer Auftraggeber getrennt. Diese Trennung wird zum einen durch entsprechende Berechtigungen als auch durch physikalisch getrennte Speichermedien oder Dateiseparierung realisiert.

(2) Daten die beim Auftraggeber zu unterschiedlichen Zwecken erhoben und verarbeitet werden, werden beim Auftragnehmer nicht zusammengefasst.

(3) Bei der Durchführung der Leistungserbringung erfolgt eine Funktionstrennung von Test- und Produktivdaten.

(4) Zur Durchführung von Tests, werden die Daten zuvor anonymisiert, mindestens jedoch pseudonymisiert soweit technisch möglich.

§ 9 Organisationskontrolle

Über die technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO hinaus ist die innerbetriebliche Organisation beim Auftragnehmer durch folgende Maßnahmen so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird:

a) Nachweise über durchgeführte Mitarbeiterschulungen liegen vor.

b) Nachweise über Verpflichtungen auf Vertraulichkeit liegen vor.

c) Datenschutzbeauftragter ist schriftlich bestellt.

d) Fachkundenachweise des Datenschutzbeauftragten liegen vor.

e) Eine Datenschutzrichtlinie liegt vor.

f) Ein IT-Sicherheitskonzept liegt vor.

g) Schriftliche Arbeitsanweisungen / Richtlinien / Merkblätter liegen vor.