Standard-Datenschutz-Maßnahmen (Standard-TOMs)

Maßnahmen zur Erfüllung der Gewährleistungsziele gemäß Art. 5 und 32 DS-GVO

Inhaltsverzeichnis

Einleitung

Inhalt

Dieses Dokument beschreibt die allgemeinen Maßnahmen (Standard-Datenschutz-Maßnahmen) der Schwarz Gruppe zur Gewährleistung der Verarbeitungsgrundsätze gemäß Art. 5 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) einschließlich der technischen und organisatorischen Maßnahmen (TOMs) gemäß Artikel 32 DS-GVO. Eventuell projekt- bzw. systemindividuelle Abweichungen oder Ergänzungen sind im jeweiligen Verarbeitungsformular, in der Checkliste TOMs zu Anwendungen und IT-Systemen bzw. ggf. im Vertrag zur Auftragsverarbeitung gesondert dokumentiert.

Dokumentenkontrolle

Datum	Version	Autor	Änderung
09.11.2017	1.0	Schmauß	Erstellung unter Berücksichtigung Anpassungen Schwarz IT und Dieter Schwarz Stiftung.

Kapitel 1: Maßnahmen zur Gewährleistung der Verarbeitungsgrundsätze

Gesetzliche Grundlage: *Art. 5 Abs. 1 DS-GVO*

Die folgenden Maßnahmen dienen der Gewährleistung der Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 DS-GVO (Verarbeitungsgrundsätze).

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz

Gesetzliche Grundlage: *Art. 5 Abs. 1 lit. a DS-GVO*

Alle Prozesse, IT-Systeme oder sonstigen Verarbeitungen, in denen jeweils personenbezogene Daten verarbeitet werden, werden vom für den Prozess verantwortlichen Fachbereich im Verzeichnis von Verarbeitungstätigkeiten dokumentiert. Das zum jeweiligen Prozess erfasste Verarbeitungsformular enthält sämtliche datenschutzrelevanten Angaben, insbesondere zu Zwecken, Umfang, Herkunft und Löschfristen der verarbeiteten personenbezogenen Daten. Darüber hinaus werden Angaben zu beabsichtigten Auswertungen, der Art und den Umfang der Information der Betroffenen, dem Datenfluss, die hierfür eingesetzten IT-Systeme sowie die Übermittlung an interne oder externe Stellen sowohl innerhalb, als auch außerhalb der EU/EWR erfasst.

Bei der Neugestaltung oder Änderung von Prozessen, IT-Systemen oder sonstigen Verarbeitungen besteht eine Verpflichtung zur Einbindung des Bereichs Datenschutz bereits in der Konzeptionsphase. Jeder erfasste Prozess wird auf Basis der Angaben im Verarbeitungsformular im Hinblick auf Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz bewertet und auf die Einhaltung der Grundsätze der Rechtmäßigkeit und Verarbeitung nach Treu und Glauben sowie die Erfüllung der Informationspflichten gegenüber dem Betroffenen hingewirkt, damit dieser die Art und Weise der Verarbeitung nachvollziehen kann. Auf Grundlage der Bewertung entscheidet der Freigabe-Verantwortliche des Bereiches über die Implementierung des Prozesses. Bei Änderungen von Prozessen, IT-Systemen oder sonstigen Verarbeitungen wird der Ablauf erneut angestoßen.

2. Zweckbindung

Gesetzliche Grundlage: *Art. 5 Abs. 1 lit. b DS-GVO*

Bei der Verarbeitung personenbezogener Daten werden die hierfür bestimmten Zwecke im Vorfeld definiert und im jeweiligen Verarbeitungsformular im Verzeichnis von Verarbeitungstätigkeiten schriftlich festgehalten. Um eine Weiterverarbeitung für nicht mit den festgelegten Zwecken vereinbare Weise zu verhindern, wird die Zweckbindung durch geeignete technische und organistorische Maßnahmen sichergestellt (vgl. dazu unten Kapitel 2).

3. Datenminimierung

Gesetzliche Grundlage: *Art. 5 Abs. 1 lit. c DS-GVO*

Im Rahmen der datenschutzrechtlichen Beratung bei der Einführung neuer Prozesse, IT-Systeme oder sonstigen Verarbeitungen, in denen jeweils personenbezogene Daten verarbeitet werden, wird unter Berücksichtigung der Anforderungen von *privacy by design* und *privacy by default* auf die Einhaltung des Grundsatzes der Datenminimierung hingewirkt, indem die Aspekte der Erheblichkeit der Datenverarbeitung für den verfolgten Zweck, der Erforderlichkeit, sowie der Angemessenheit bereits in der Gestaltungsphase Beachtung finden. Soweit jeweils möglich und mit verhältnismäßigem Aufwand umsetzbar, werden personenbezogene Daten in den Systemen pseudonymisiert. Ebenso werden in Systemen mit einem eigenen Usersteuerbereich Maßnahmen umgesetzt, die dem Betroffenen die Möglichkeit einräumen, selbst im einräumbaren Umfang über die Datenverarbeitung zu entscheiden, bzw. Einfluss zu nehmen.

4. Richtigkeit

Gesetzliche Grundlage: *Art. 5 Abs. 1 lit. d DS-GVO*

Im Rahmen der Konzeptionierung neuer bzw. Änderung bestehender Prozesse, IT-Systeme oder sonstigen Verarbeitungen, in denen jeweils personenbezogene Daten verarbeitet werden, wird bei automatisierten Verarbeitungen durch geeignete Maßnahmen zur Gewährleistung der Integrität der Daten (vgl. Abschnitt 2 Ziff. 2) sichergestellt, dass die Daten sachlich richtig und – sofern erforderlich – auf dem neuesten Stand sind. Durch Maßnahmen zur Gewährleistung der Lösch- und Korrekturfähigkeit wird sichergestellt, dass unrichtige Daten unverzüglich gelöscht oder berichtigt werden.

Darüber hinaus sind die verantwortlichen Bereiche angehalten, die Richtigkeit der ihnen anvertrauten personenbezogenen Daten zu gewährleisten.

5. Speicherbegrenzung (Löschung)

Gesetzliche Grundlage: *Art. 5 Abs. 1 lit. e DS-GVO*

Damit personenbezogene Daten nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, werden bei der Dokumentation der Prozesse, IT-Systeme und sonstigen Verarbeitungen im Verarbeitungsformular des Verzeichnisses von Verarbeitungstätigkeiten Regellöschfristen festgelegt. Nach Ablauf der Regellöschfristen werden die Daten gelöscht oder durch Entfernung des Personenbezugs vollständig anonymisiert. Die Umsetzung erfolgt – je nach Festlegung im Verarbeitungsformular – verarbeitungsindividuell automatisch oder manuell. In Systemen mit manuellen Löschroutinen werden geeignete Regelkontrollmechanismen implementiert, um die Prüfung der Löschung zu gewährleisten.

6. Rechenschaftspflicht

Gesetzliche Grundlage: *Art. 5 Abs. 2 DS-GVO*

Durch die Dokumentation der relevanten Angaben im Verzeichnis von Verarbeitungstätigkeiten und deren regelmäßige Aktualisierung sowie der Festlegung von Vorgaben zu verarbeitungsspezifischen Dokumentationspflichten, z.B. bei Einwilligungen, werden die verarbeitungsspezifischen Rechenschaftspflichten nach Art. 5 Abs. 2 DS-GVO gewährleistet.

Kapitel 2: Technische und organisatorische Maßnahmen (TOMs)

Gesetzliche Grundlage: *Art. 32 DS-GVO*

Die folgenden Maßnahmen dienen der Gewährleistung der Anforderungen an die Sicherheit der Verarbeitung personenbezogener Daten durch das Treffen geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 32 DS-GVO (Technische und organisatorische Maßnahmen – TOMs).

1. Vertraulichkeit

Gesetzliche Grundlage: *Art. 5 Abs. 1 lit. f i.V.m. Art. 32 Abs. 1 lit. b DS-GVO*

Die folgenden Maßnahmen werden zur dauerhaften Sicherstellung der Vertraulichkeit der Daten ergriffen.

1.1 Zugangskontrolle

Die folgenden Maßnahmen verhindern, dass Unbefugte physischen Zugang zu Anlagen erlangen, in denen die Datenverarbeitung durchgeführt wird.

1.1.1 Einbruchsschutzmaßnahmen, Brand- und Blitzschutz

Gebäude sind im Regelfall umzäunt und Zufahrten mit Toren gesichert. Sofern dies im Einzelfall nicht der Fall ist, wird durch die nachfolgenden und ggf. weiteren Maßnahmen eine angemessene Zugangskontrolle gewährleistet. Außentüren sind mit Sicherheitsschlössern gesichert. Blitzschutzanlagen bei den Gebäuden stellen sicher, dass Energiespitzen und Überlastungen abgeführt werden. Die Rechenzentren sind mit Einbruchmeldeanlagen ausgestattet. Wird eine RZ-Tür aufgebrochen, wird der Leitstand alarmiert. Räumlichkeiten sind mit Branderkennungsgeräten ausgestattet. Alarme über Brandmeldungen, Löschmitteleinsätze, Wassereinbrüche und Stromausfälle werden zentral vom Leitstand überwacht. Andere Alarmmeldungen erhält der Sicherheitsdienst oder die Notrufzentrale. Von dort werden die zuständigen Personen aus der Alarmbenachrichtigungsliste informiert.

Die Feuerlöschanlage im RZ nutzt Löschgas. Im RZ und Serverräumen stehen CO2-Handlöscher in ausreichender Menge in der Nähe der Türen.

1.1.2 Schlüsselverwaltung

Bürogebäude sind stets verschlossen. Türen können nur durch Berechtigte durch elektronische Zugangskarten oder mechanische Schlüssel geöffnet werden. Büroschlüssel und Schlösser folgen funktional der Unternehmensorganisation, so dass unmittelbare Vorgesetzte Zutritt zu den Büros ihrer Mitarbeiter haben. Büros, in denen personenbezogene Daten verarbeitet werden, werden bei längerer Abwesenheit der Mitarbeiter und nach Dienstschluss verschlossen und vertrauliche Daten in Großraumbüros in Büromöbeln unter Verschluss gehalten.

Für zentrale Standorte sind Generalschlüssel verschlossen und alarmgesichert beim Sicherheitsdienst oder Leitstand hinterlegt, um im Brandfall durch den Sicherheitsdienst für den gewaltfreien Zutritt an die Feuerwehr auszuhändigen. Die Aus- und Rückgabe von Schlüsseln wird protokolliert.

1.1.3 Elektronischer Zugangsschutz

Die personalisierten, elektronischen Unternehmensausweise öffnen und schließen durch Vorhalten Eingangstüren zu Gebäuden, Etagen- und Flurtüren sowie Zugangstüren zu Sicherheitsbereichen. Die elektronischen Zutrittsprofile folgen i.d.R. den Arbeitsbereichen und der Position eines Mitarbeiters. Dazu kommen Funktionsprofile z.B. für die Gebäudereinigung und Gebäudetechnik.

Die Ausgabe, die jeweiligen Zutrittsberechtigungen und Nutzung der elektronischen Unternehmensausweise sind protokolliert. Der Zugriff auf diese Daten erfolgt gemäß des dokumentierten Berechtigungskonzepts durch die Fachverantwortlichen des Gebäudemanagements, den Sicherheitsdienst und den jeweiligen Systemadministratoren.

1.1.4 Zutritt für Gäste

Zentrale Standorte verfügen über Empfänge, an denen sich Besucher während der Öffnungszeiten anmelden. Ein Mitarbeiter holt Gäste vom Wartebereich ab und begleitet sie während des Aufenthalts auf dem Gelände. Außerhalb der Empfangsöffnungszeiten und wenn kein Empfang vorhanden ist, sind die Türen verschlossen. Besucher melden sich dann mittels Telefons im Eingangsbereich beim Mitarbeiter oder an zentralen Standorten beim Sicherheitsdienst.

Handwerker und Personal von Reinigungs- und Wartungsunternehmen erhalten elektronische Unternehmensausweise mit erweiterten Zutrittsrechten, jedoch ohne Berechtigung zu den Sicherheitsbereichen. Sie werden für ihre Tätigkeiten in den Gebäuden von Mitarbeitern des zuständigen Fachbereichs eingewiesen und betreut und auf Anforderung der Fachbereiche durch den Sicherheitsdienst begleitet.

1.1.5 Rechenzentren

Lage, Gebäude, Räume etc. unterliegen fest definierten baulichen Vorgaben gemäß der aktuellen Baubeschreibungen und dem Sicherheitskonzept für Rechenzentren. Zentrale IT Komponenten sind ausschließlich in abschließbaren Räumen untergebracht. Gleiches gilt für die zentralen Komponenten der Telekommunikationsanlage. Die Stromversorgung ist über separate Elektro-Unterverteilung mit USV und Notstromaggregat gesichert. Die USV ist für eine definierte Mindestversorgungszeit ausreichend ausgelegt. Messgeräte sind im Einsatz. Funktionstests finden regelmäßig statt.

Wartungstechniker (Strom, Wasser, Löschanlagen) ohne personalisierte Zutrittskarten erhalten bei der Anmeldung eine Besucherkarte und werden vom Sicherheitsdienst oder einem Mitarbeiter des RZ-Betreibers mit personalisierter Karte begleitet. Wartungstechniker für IT-Equipment werden von den Fachteams oder dem Sicherheitsdienst begleitet.

1.1.6 Videoüberwachung

Zutritte zu sensiblen Bereichen der Gebäude werden mit Videokameras überwacht. Die Speicherdauer des Bildmaterials beträgt im Regelfall 7 Tage.

1.1.7 Netzwerk

Das Local Area Network (LAN) besteht aus unterschiedlichen funktionalen und sicherheitstechnischen Zonen. Der Zugriffsschutz zwischen den Zonen wird mit Firewall-Regelwerken oder Accesslisten hergestellt.

Aktive Netzwerkkomponenten außerhalb des Rechenzentrums befinden sich in geschlossenen Technikräumen. Wenn nicht, sind sie in abschließbaren Schränken montiert. Davon ausgenommen sind Access Points, die zur Ausleuchtung der Räumlichkeiten an der Decke angebracht sind.

Standortabhängig finden Zugangskontrollen zum Netzwerk über entsprechend sichere Protokolle (z.B. 802.1x) statt. Vor der Vergabe der IP-Adresse an Anwender / Endgeräte beim Zugang zum Netzwerk werden diese identifiziert.

WLAN-Verbindungen sind verschlüsselt, WLAN-Teilnehmer authentifiziert, teils zertifikatsbasiert. Zertifikate und WLAN-Zugriffe werden zentral verwaltet. Teilnehmern des Gäste-WLANs steht ausschließlich eine Verbindung zum Internet zur Verfügung.

1.2 Benutzer-, Zugriffs-, Datenträger- und Speicherkontrolle

Die folgenden Maßnahmen gewährleisten, dass personenbezogene Daten auf Datenträgern und in Datenverarbeitungssystemen nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden und gewährleisten, dass die zur

Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

1.2.1 Berechtigungskonzepte

Berechtigungskonzepte sind Teil der Systemdokumentationen. Die Vergabe der Berechtigungen folgt dem „Need-to-know-Prinzip“. Die Einhaltung der jeweiligen Berechtigungskonzepte wird regelmäßig geprüft. Nicht mehr benötigte Nutzerkonten werden gelöscht.

Berechtigungskonzepte in Summe, angefangen bei der zentralen Benutzerverwaltung bis hin zu Server- und Ordnerberechtigungen in Kombination mit den Zugangskontrollen der Netzwerksegmentierung gewährt Anwendern abhängig von ihren Rollen und Aufgaben im Unternehmen system- und anwendungsübergreifend Zugang auf IT Ressourcen, die für die Arbeit benötigt werden.

1.2.2 Kennwörter und PINs

Über Kennwörter und Benutzerkonten werden sämtliche Zugriffe auf IT-Systeme reguliert. Benutzerkonten sind regelmäßig eindeutig einer Person zugeordnet. Bei der ersten Anmeldung eines Benutzers wird ein persönliches Kennwort vergeben. Die von den Systemen vorgegebenen Kennwortverfahren erfüllen die unterschiedlichen funktionalen Anforderungen der Benutzerkonten bis hin zum hohen Schutzbedarf von Daten und Systemen. Kennwörter werden abhängig vom Schutzbedarf und der Gefahrensituation in regelmäßigen Abständen geändert.

Kleine, mobile Geräte wie z.B. Smartphones und Tablets sind den jeweiligen Anwendern fest zugeordnet. Aus wirtschaftlichen und ergonomischen Gründen gilt eine Ausnahme zur Kennwortrichtlinie für die Länge der Geräte-PINs. Abhängig von der Ausstattung mobiler Geräte werden diese anhand zentral verwalteter Gerätezertifikate identifiziert, um in Reichweite eines Firmen-WLANs automatisch eine Verbindung mit dem Netzwerk herzustellen.

1.2.3 Diebstahlschutz für Laptops

Die Festplatten von Laptops sind verschlüsselt, somit erfordert der Start eines Laptops die Eingabe des persönlichen Kennworts.

1.2.4 Administration von IT-Systemen

Im Regelfall setzt der Auftragnehmer eigene Mitarbeiter zur Administration der betreuten IT-Systeme ein. Mitarbeiter der IT sind gemäß Anstellungsvertrag auf das Fernmeldegeheimnis und das Datengeheimnis verpflichtet.

Administrationszugänge werden ausschließlich für administrative Zwecke genutzt und unterliegen umfangreichen Protokollierungsmaßnahmen. Protokolle werden vor Änderungen geschützt aufbewahrt und anlassbezogen und in regelmäßigen Abständen stichprobenartig ausgewertet.

Rollenkonzepte stellen sicher, dass die für die Aufgaben benötigten administrativen Rechte dokumentiert und überprüfbar eingerichtet sind. Administrationskonten sind personalisiert. Administrationskonten sind durch eine Kennzeichnung im Benutzernamen von normalen Benutzerkonten separiert.

Administrative Berechtigungen auf Systeme mit personenbezogenen Daten werden im Vier-Augen-Prinzip freigegeben und regelmäßig überprüft.

Die Administration der Netzwerkinfrastrukturkomponenten erfolgt über kontrollierte Verbindungen von berechtigten Managementsystemen. Netzwerkadministratoren werden über zentrale Authentifizierungsmechanismen identifiziert.

1.2.5 Starke Authentifizierung

Zugriffe externer Anwender aus öffentlichen Netzen werden mit einer Zwei-Faktor-Authentifizierung identifiziert. Die zwei Faktoren sind Einmalkennwort und persönliche Benutzerkennung. Einmalkennwörter haben eine begrenzte Gültigkeit und werden nach Eingabe eines persönlichen PINs am physischen Token-Generator/Software-Token o.ä. angezeigt. Die Ausgabe der physischen Token-Generatoren erfolgt durch den Service Desk. Der Empfang wird schriftlich bestätigt und der Anwender darauf hingewiesen dem Service Desk einen eventuellen Verlust unmittelbar mitzuteilen, um den Token-Generator sperren zu lassen. Eine automatische Sperre erfolgt nach einer gewissen Anzahl von Anmeldefehlern. Die Freigabe des Antrags auf Fernzugriff und der Betrieb der Verwaltungssysteme für Token-Generatoren erfolgt von voneinander unabhängigen Abteilungen.

Für die Kommunikation von und zu externen IT-Systemen mit Vertragspartnern sind Site-2-Site VPN-Tunnel (S2S-VPN) eingerichtet. Die öffentlichen IP-Adressen der Firewalls auf beiden Seiten, fest eingestellte Verschlüsselungsparameter und ein telefonisch vereinbartes Kennwort sorgen für sichere Authentifizierung und Verschlüsselung.

1.2.6 Fernzugriffe

Fernzugriffe von Administratoren sind mehrstufig gesichert. Administratoren arbeiten auf einer oder mehreren virtuellen Arbeitsumgebungen. Aktivitäten werden aufgezeichnet und bei begründetem Verdacht geprüft.

1.2.7 Fernwartungszugriffe vom Service Desk

Mitarbeitern aus dem Service Desk ist die Kontrolle über einen IT-Arbeitsplatz erlaubt, wenn ein angemeldeter Benutzer die Fernzugriffsanfrage bestätigt. Fernwartungssitzungen sind auf dem Bildschirm sichtbar gekennzeichnet und der Benutzer kann jederzeit mit Maus und Tastatur eingreifen. Ist ein Rechner ausgeschaltet oder der Arbeitsplatz gesperrt, ist das Aufschalten nicht möglich. Fallen einem Service Desk Mitarbeiter während eines Fernwartungszugriff geöffnete Dokumente oder Anwendungen mit vertraulicher Information auf, ist er angehalten den Mitarbeiter aufzufordern, die Dokumente und Anwendungen zu schließen, bevor er die Arbeit fortsetzt.

1.2.8 Client-Schutzmaßnahmen

Durch BIOS-Kennwörter und Software zur Schnittstellenkontrolle ist gewährleistet, dass Anwender ausschließlich unterstützte Hardware im Sinne des Verwendungszecks nutzen. Die Datenübertragung auf Wechseldatenträger, z.B. USB-Sticks, ist reguliert. Wechseldatenträger werden einzeln auf Antrag freigeschaltet und vor der ersten Nutzung automatisch verschlüsselt. Unverschlüsselten Wechseldatenträgers werden nur mit einer Ausnahmegenehmigung durch den Informationssicherheitsbeauftragten freigeschaltet.

Die Netzwerkkommunikation von Clients ist mit Hilfe von zentral verwalteten Systemeinstellungen und Tools zur Hardwarekontrolle auf das Notwendigste reduziert. Laptops verfügen zudem über lokale, zentral verwaltet Firewalls. Außerhalb des Firmennetzwerks ist es Laptops kurzzeitig gestattet, fremde Netzwerkzugänge für den Aufbau des VPN-Tunnels zum Firmennetzwerk zu nutzen. Besteht eine Verbindung zum Firmennetzwerk, wird das gleichzeitige Nutzen anderer Netzwerkverbindungen z.B. über Hotspots unterbunden.

Die Installation von Software ist zentral verwaltet. Anwender können Software aus dem zentralen Softwarekatalog beantragen. Nach der Freigabe durch den Vorgesetzten wird die Anwendung zur Installation zur Verfügung gestellt. Die Installation von Software außerhalb des Katalogs wird einzeln betrachtet.

PC-Arbeitsplätze werden nach einer bestimmten Dauer der Inaktivität automatisch gesperrt. Im gesperrten Zustand können weder Dokumente eingesehen noch Programme gestartet werden. Entsperrt werden PC-Arbeitsplätze durch das Kennwort des angemeldeten Benutzers oder der Anmeldung eines Administrators.

1.2.9 Berechtigungsanforderungen

Das Stellen von Berechtigungsanforderungen ist Mitarbeitern selbst, den Vorgesetzten oder dem jeweils zuständigen Sekretariat möglich. Nach der Freigabe durch den Vorgesetzten werden diese zentral umgesetzt. Zugriffsberechtigungen auf besonders schützenswerte Ressourcen benötigen darüber hinaus die Freigabe des jeweiligen Dateneigentümers. Das Löschen von Berechtigungen wird beantragt, begründet und dokumentiert. Die Betriebsprozesse sind im IDM (Identity Management)-Handbuch dokumentiert. Daten- und Systemeigentümer erhalten regelmäßig Berichte über Anwender und Berechtigungen. SAP-Berechtigungen werden mit Hilfe einer speziellen Softwarelösung automatisch geprüft. Problematische Rechtekombinationen und verwaiste Accounts werden gelöscht.

1.3 Übertragungskontrolle

Die folgenden Maßnahmen gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

1.3.1 Protokollierung

Generell sind die Protokollierungseinstellungen abhängig von den Systemspezifikationen, den betrieblichen Anforderungen und dem Schutzbedarf. Bei hohem Schutzbedarf werden Protokolldaten gemäß der systemspezifisch vereinbarten Vorhaltezeiten und vor Manipulation geschützt archiviert.

1.3.2 Funktionale Zonen

Es existieren regelmäßig funktionale Zonen. Zugriffe und Datenflüsse von und in diesen Zonen werden durch Firewalls reguliert.

1.3.3 Drucken

Drucker, Kopierer und Multifunktionsgeräte besitzen Lesegeräte für die elektronischen Unternehmensausweise.Sofern der Anwender Druckaufträge als vertraulich gekennzeichnet hat, werden diese erst nach der Authentifizierung des Anwenders ausgeführt.

1.3.4 Interner Datenaustausch

Authentifizierten und autorisierten Mitarbeitern stehen für den Datenaustausch Netzlaufwerke und datenbankgestützte Anwendungen zur Verfügung. Zugriffsberechtigungen sind mit Hilfe der Berechtigungskonzepte und zentralen Benutzerverwaltung umgesetzt und werden von den eingesetzten Systemen protokolliert. Die Netzwerk- und Systemumgebungen sind dokumentiert.

1.3.5 Schnittstellenkontrolle mit Datenträgerverschlüsselung

Zum Schutz vor unbefugter Weitergabe und unkontrolliertem Abfluss elektronischer Informationen wird der Umgang mit Hardware, insbesondere mit Wechselmedien und Geräten, die über USB-Schnittstellen oder ähnliche Anschlüsse an PCs oder Laptops angeschlossen werden können, kontrolliert.

Der Einsatz mobiler Speichermedien, wie z.B. USB-Sticks, ist mit Blick auf Schreibrechte nur auf Antrag und mit Freigabe durch den Vorgesetzten möglich.

Die Daten auf dem Wechseldatenträger sind passwortgeschützt.

Datenspeicher von iOS Geräten werden AES-256 verschlüsselt. Anwender mit Android Geräten werden dazu angehalten, die Verschlüsselung zu aktivieren.

Einzelne Dateien können bei Bedarf mit Hilfe eines Programms zur Komprimierung, das auf allen Arbeitsplätzen verfügbar ist, mit Kennwort geschütztem AES-256 verschlüsselt werden.

1.3.6 Vorgehensweise bei Hardwareverlust

Mitarbeiter sind über die Vorgehensweise bei Schäden und Verlust von Hardware informiert. Bei Verlust oder Schäden werden angemessene Maßnahmen eingeleitet, die dem Schutz der Daten dienen. Hierzu können beispielsweise die lokal gespeicherten Nutzerdaten durch Rücksetzen auf die Werkseinstellungen unbrauchbar gemacht oder der ans Gerät gebundenen Account für die Nutzung zentraler Unternehmensdienste gesperrt werden.

1.3.7 Transport (Post)

Der Transport bzw. Versand von Datenträgern ist streng limitiert und nur für den Datenaustausch mit Partner und Dienstleistern vorgesehen. Für den Versand von personenbezogenen Daten auf Wechseldatenträgern über externe Postdienstleister werden Einschreiben oder vergleichbare Zusatzleistungen verwendet. Eingehende Post wird von den Postabteilungen entgegengenommen, ggf. quittiert und intern weitergeleitet.

1.3.8 Nutzung von Internet und E-Mail

Anwender nutzen vordefinierte Webbrowser (z.B. Internet Explorer, Firefox) für das Aufrufen von Webseiten. Bei kritischen Schwachstellen wird der betroffene Browser bis zur Beseitigung der Schwachstelle für die Internetnutzung zentral gesperrt und eine Informationsseite eingeblendet.

Die private Nutzung von dienstlichen E-Mail-Accounts ist untersagt.

E-Mail-Benutzer erhalten bei der Erstellung des E-Mail-Accounts eine neue, individuelle Kennung (ID), die dem jeweiligen Benutzer vorgehalten bleibt. E-Mails innerhalb der Unternehmensgruppe werden intern versendet und zugestellt. E-Mails zu externen Empfängern können vom Versender mit Hilfe von „Secure/Multipurpose Internet Mail Extension“ (S/MIME) und TLS verschlüsselt werden. Die Nutzung von S/MIME muss beantragt werden und wird an zentraler Stelle eingerichtet.

1.4 Datenträgervernichtung

Aussortierte Datenträger wie Festplatten und Backup-Bänder werden durch angemessene Maßnahmen sicher vernichtet. Hierzu kann beispielsweise die Einschaltung eines zertifizierten Dienstleisters zur fachmännischen Vernichtung gehören. Die Datenträger werden formatiert und mehrfach überschrieben. Bei physikalischen Defekten der Datenträger werden diese durch Degausern unleserlich gemacht.

2. Integrität

Gesetzliche Grundlage: *Art. 5 Abs. 1 lit. f i.V.m. Art. 32 Abs. 1 lit. b DS-GVO*

Die folgenden Maßnahmen werden zur dauerhaften Sicherstellung der Integrität der Daten ergriffen.

2.1 Eingabekontrolle

Die folgenden Maßnahmen gewährleisten, dass überprüft und festgestellt werden kann, ob, von wem und zu welcher Zeit personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind.

2.1.1 Berechtigungskonzepte, Protokollierungs- und Protokollauswertungssysteme

Mit Hilfe der zentralen Benutzerverwaltung, wie ausführlich im Abschnitt „Benutzer- und Zugriffskontrollen“ beschrieben, ist gewährleistet, dass IT-Systeme gemäß dem jeweiligen Rollen- und Berechtigungskonzept genutzt werden. Abhängig von den Aufgaben und der Position eines Mitarbeiters wird bei den Benutzerrechten zwischen Lesen, Schreiben und Löschen unterschieden. Daten mit besonders hohem Schutzbedarf werden verschlüsselt bevor sie in der Datenbank gespeichert werden, sodass sie durch Datenbankadministratoren nicht eingesehen werden können.

Mithilfe der Protokollierung kann der Zugriff auf personenbezogene Daten nachvollzogen werden. Systemverantwortliche können Protokolldaten einsehen, aber nicht ändern. Die manuelle Auswertung von Protokolldaten erfolgt bei festgestellten Unregelmäßigkeiten oder Sicherheitsverstößen. Bei hohem Schutzbedarf werden Protokolle regelmäßig stichprobenartig auf Unregelmäßigkeiten überprüft, teils unterstützt durch Protokollierungs- und Protokollauswertungssystemen.

Änderungen an Benutzerrechten werden unabhängig vom System zur Rechteverwaltung aufgezeichnet und bei einem Fehler rückgängig gemacht.

2.2 Datenintegrität

Die folgenden Maßnahmen gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

2.2.1 Datenbanken

Direkte Zugriffe von Clients und Anwendern auf Datenbanken sind durch die Netzwerksegmentierung und Firewallregeln im Regelfall unterbunden. Datenbankzugriffe werden für Anwendungen durch kennwortgeschützte Datenbank-Benutzerkonten authentifiziert. Abhängig vom Schutzbedarf der Daten wird das Kennwort in regelmäßigen Abständen geändert.

2.2.2 Funktionale Zonen

Um die Wahrscheinlichkeit von negativen Auswirkungen durch Software- und Anwenderfehler gering zu halten und die Wirkung der eingesetzten organisatorischen und technischen Maßnahmen aufrecht zu erhalten, sind produktive Systeme, Entwicklungs- und Testsystemen regelmäßig voneinander getrennt.

2.2.3 Schutz gegen Schadsoftware und Maßnahmen bei Sicherheitsvorfällen

Der Schutz vor Schadsoftware erfolgt durch signaturbasierte Erkennungstechnik. Daneben kommen heuristische und verhaltensbasierte Methoden zum Einsatz. Die Signaturen der Endgeräte werden täglich automatisch aktualisiert.

Bei verdächtigen Aktivitäten durch Malware werden die Sicherheitsadministratoren über das zentrale Managementsystem alarmiert. Infizierte Daten werden zur späteren Analyse in Quarantäne-Ordner verschoben und die Malware gelöscht. Sollten Programmdateien unbrauchbar werden, werden die betroffenen Clients neu installiert. Ist das Löschen der Malware nicht erfolgreich, werden infizierte Systeme vom Netzwerk isoliert und mit einem Antiviren-Programm geprüft, das keine Netzwerkverbindung benötigt. Infektionsquellen werden nach der Isolation und Desinfektion bis zum Ursprung zurückverfolgt und Gegenmaßnahmen etabliert, die eine erneute Infektion verhindern sollen.

Schwachstellenscanner sind im Einsatz. Schwachstellenberichte für externe IP-Adressen werden regelmäßig an die Systemverantwortlichen gesendet und nicht kritische Schwachstellen mit Hilfe des Patchmanagement behoben. Kritische Schwachstellen werden abhängig von den Angriffsvektoren mit Hilfe einer Notfallprozedur schnellstmöglich beseitigt und der Fortschritt permanent nachgehalten. Zusätzlich werden Schwachstellen und aktuelle Angriffe von einschlägigen Internetseiten und anderen Kanälen in Erfahrung gebracht, u.a. dem IT-Lagezentrum des BSI (Bundesamt für Sicherheit in der Informationstechnik) und privaten Dienstleistern. Die Informationen werden auf Relevanz geprüft und in kritischen Fällen Sofortmaßnahmen zentral koordiniert. Als Sofortmaßnahmen werden Regeln auf den zentralen Sicherheitssystemen eingerichtet und Internet, E-Mail oder andere Netzwerkverbindungen teilweise oder vollständig ausgeschaltet. Sofortmaßnahmen bleiben solange aktiv, bis die ursächliche Schwachstelle nachhaltig beseitigt ist. Sollte bei der Bearbeitung eines Vorfalls absehbar sein, dass sensible Systeme oder Daten beeinträchtigt worden sind oder z.B. die Ausbreitung von Malware über einzelne

Systeme hinausgeht, wird umgehend die Geschäftsleitung informieren und ein Team aus Systemadministratoren und IT Sicherheitsfachleuten zusammengestellt, bis die Auswirkungen eingedämmt und die Gefahr beseitigt ist. Kritische Vorfälle werden umfassend dokumentiert und Folgemaßnahmen initiiert, um ein erneutes Auftreten dieser oder ähnlicher Vorfälle nachhaltig zu vermeiden.

2.2.4 URL- und Spamfilter

Der Aufruf von Webseiten wird durch URL-Filter mit Schadsoftware-Schutz auf den Internet-Proxys gesichert. Zugriffe auf jugendgefährdende, illegale und schädliche Inhalte werden geblockt, die Filterlisten automatisch aktualisiert. Zusätzlich werden manuell erstellte Filterlisten eingesetzt, um vor gefährlichen Internetverbindungen zu schützen, die vom Proxy-Hersteller noch nicht kategorisiert worden sind, und aus den oben genannten Quellen bekannt geworden sind.

Zur Abwehr von Spam- und Phishing-E-Mails werden u.a. Spamfilter eingesetzt. Die Filter werden mehrmals täglich automatisch aktualisiert. Eindeutig erkannte Spam- und Phishing-E-Mails werden von den Email-Servern nicht angenommen. Es folgt eine automatische Aussortierung von Emails mit ungültigen E-Mail-Empfänger und im Anschluss die Signatur- und Mustererkennung sowie die Reputationsprüfung. Falls Spam oder andere verdächtige Emails nicht richtig erkannt werden, werden diese vom Empfänger abgespeichert und an den Service Desk gesendet oder direkt an die E-Mail-Adresse für Spam- und Phishing-Support gesendet. Handelt es sich tatsächlich um Spam oder Phishing, werden entsprechende Filterregeln erstellt.

2.2.5 Softwarekontrolle und Aktualisierungen

Windows-Anwendungen und Betriebssystemaktualisierungen werden zentral verwaltet. Aktualisierungen werden im Rahmen des Change- und Patch-Management-Prozesses in dedizierten Testumgebungen geprüft. Nach erfolgreichen Tests wird das Änderungspaket zentral zur Verfügung gestellt. Die Verteilung erfolgt zeitversetzt, um Störungen, die während der Tests ggfs. nicht auftraten, rechtzeitig zu erkennen und zu beseitigen. Zusätzlich hängt die Verteilung von der Dringlichkeit, den Auswirkungen und den Wartungsfenstern ab. Für Notfälle gilt ein beschleunigtes Verfahren. Die jeweiligen Produktverantwortlichen informieren betroffene Mitarbeiter über die etablierten zentralen Kommunikationskanäle.

Bei Geräten ohne zentrale Verwaltung der Einstellungen liegt die Aktualisierung in der Verantwortung des Anwenders. Mit der Ausgabe eines Geräts wird der Benutzer über die Pflicht zur Systempflege in Kenntnis gesetzt. Aktualisierungen von mobilen Geräten mit zentraler Verwaltung der Systemeinstellungen werden gemäß Change und Patch Management getestet. Nach erfolgreichen Tests und bei kritischen Updates werden die Anwender informiert, um die Aktualisierung zeitnah zu installieren. Der Versionsstand wird zentral überwacht und dokumentiert.

3. Verfügbarkeit

Gesetzliche Grundlage: *Art. 5 Abs. 1 lit. f i.V.m. Art. 32 Abs. 1 lit. b DS-GVO*

Die folgenden Maßnahmen werden zur dauerhaften Sicherstellung der Verfügbarkeit der personenbezogenen Daten ergriffen.

3.1 Verfügbarkeitskontrolle

Die folgenden Maßnahmen gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

3.1.1 Firewall- und Virenschutz-Systeme

Die gesamte IT-Infrastruktur wird durch mehrfach redundante Firewall- und Virenschutz-Systeme vor Denial of Service (DoS) oder anderen Überlastangriffen, sowie Schadsoftware und unbefugtes Eindringen über Netzwerkverbindungen geschützt.

3.1.2 Entwicklungs- und Testsysteme

Entwicklungssysteme entsprechen in den wesentlichen Funktionen den Produktivsystemen. Testsysteme sind bei Bedarf mit einem realitätsnahen Datenbestand ausgestattet. Damit ist gewährleistet, dass Softwareaktualisierungen, Erweiterungen und Änderungen entwickelt und auf Interoperabilität, Kompatibilität und Erfüllung der Anforderungen geprüft werden können, ohne die produktive Umgebung zu beeinträchtigen.

3.1.3 Zentrale Dateiablage

Anwender sind angehalten produktive Daten auf den zentralen Datenspeicher im gesicherten Unternehmensnetzwerk abzulegen. Daten auf Fileserver werden täglich gesichert.

3.1.4 Datensicherungsschränke

Der Zugriff auf Datentresore ist streng limitiert. Sie befinden sich in anderen Brandabschnitten oder Gebäuden als Server, haben Doppelbartschlösser, sind feuerfest und mit separaten Datenträgerarchive nach S 120 DIS ausgestattet. Die Vorgaben für Tresore sind dokumentiert.

3.1.5 Klimatisierung des Rechenzentrums

Das Rechenzentrum ist mit einer elektronisch geregelten Klimaanlage ausgestattet. Die Temperaturen werden permanent überwacht. Die abschließbaren Server-Schränke befinden sich in einer sogenannten Kaltgangeinhausung.

3.1.6 Brandschutzmaßnahmen

Die Brandmeldeanlagen mit automatischer Benachrichtigung entsprechen gängigen Standards. Brandabschnitte im RZ haben feuerfesten Türen mit einem Brandwiderstand und Rauchschutz von jeweils 90 Minuten (F90/T90). Beim Brand werden die Serverräume über die Gaslöschanlage geflutet. Eine ausreichende Anzahl an Feuerlöschern steht in den Fluren gut sichtbar markiert bereit.

In den Gebäuden gilt Rauchverbot. Auf den Etagenfluren sind Feuerlöscher vorhanden. Die Brandschutzordnungen für Gebäude sind im Fachbereich Arbeitssicherheit und Umweltschutz einsehbar. Regelmäßig finden Übungsalarme und -evakuierungen mit Hilfe von Evakuierungshelfern statt. Das System zur Evakuierung entspricht BGV A1.

3.1.7 Stromausfall oder -überlastung

Sensible Systeme sind an eine passive und aktive Notfallstromversorgung angeschlossen. Bei Stromausfall sichert die batteriebetriebene, unterbrechungsfreie Stromversorgung (USV) den Betrieb deutlich über die Zeit hinaus, bis der Dieselgenerator die Stromversorgung übernimmt. Der Überspannungsschutz der USV schützt die Stromabnehmer vor Beschädigungen durch Spannungsspitzen. Die Einsatzbereitschaft und ordnungsgemäße Funktion der Notfallstromversorgung werden regelmäßig getestet.

3.1.8 Notfallmanagement

Unter Berücksichtigung der Möglichkeiten für einen eingeschränkten IT-Betrieb halten Ausfall- und Notfallkonzepte die IT-gestützten Geschäftsprozesse aufrecht. Die Konzepte enthalten die notwendigen Details für die technischen und organisatorischen Sofort- und Notfallmaßnahmen

3.2 Belastbarkeit

Durch Redundanz ist die Verfügbarkeit wesentlicher IT-Dienste und Daten gegen Hardwareausfälle gesichert. Die Hardware in den Rechenzentren insbesondere Server, Netzteile, Netzwerkkarten, Festplatten und Lüfter sind hochverfügbar ausgelegt. Daten sind gespiegelt.

3.3 Wiederherstellung der Verfügbarkeit

Die folgenden Maßnahmen gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

3.3.1 Datensicherung und Wiederherstellung

Um Auswirkungen von Systemfehlern entgegenzuwirken, werden Server täglich gesichert: Werktags mit inkrementellen Backups und an den Wochenenden mit vollständigen Backups. Das dokumentierte Backup-Verfahren ist zweistufig, um die Auswirkung von Backups zu minimieren. Teilweise erfolgt eine Auslagerung von Backup-Bändern aus den Datensicherungsgeräten.

Zerstörte oder verlorene Daten werden abhängig von ihrer Kritikalität mit Hilfe der Hochverfügbarkeitsmaßnahmen oder Datensicherungsverfahren wiederhergestellt. Die Kritikalität für die Wiederherstellung basiert auf dem Schutzbedarf für die Verfügbarkeit. Die Länge der tolerierbaren Ausfallzeit definiert die maximale Dauer der Wiederherstellungszeit und damit das Vorgehen bei einer Wiederherstellung.

3.3.2 Wiederherstellung von Dateien

Anwender können versehentlich gelöschte Daten teilweise selbst wieder herstellen. In anderen Fällen erfolgt eine Wiederherstellung unter Einbeziehung des ServiceDesks.

4. Pseudonymisierung

Gesetzliche Grundlage: *Art. 32 Abs. 1 lit. a DS-GVO*

Soweit möglich und dem verfolgten Verarbeitungszweck angemessen, werden personenbezogene Daten pseudonymisiert verarbeitet. Die entsprechenden Maßnahmen sind je Prozess, IT-System oder sonstiger Verarbeitung dokumentiert.

5. Verschlüsselung

Gesetzliche Grundlage: Art. 32 Abs. 1 lit. a DS-GVO

5.1 Verschlüsselungsverfahren

5.1.1 Allgemeine Richtlinien

Die Wirksamkeit der zur Verschlüsselung eingesetzten Methoden und Verfahren sowie der zugehörigen Prozesse zur Verwaltung der elektronischen Schlüssel und Zertifikate werden in regelmäßigen Abständen geprüft und bei Bedarf angepasst. Sind neue Methoden und Verfahren notwendig, gelten für Bestandssysteme wirtschaftlich angemessene Übergangszeiten bei gleichzeitigem Einsatz von kompensierenden Maßnahmen.

5.1.2 Datenbanken

Datenbanken und Datenquellen sind gemäß Schutzbedarf der vorgehaltenen Daten klassifiziert. Je nach Anforderungen gemäß Schutzbedarf wird für Datenbanken Transparent Data Encryption (TDE – Verschlüsselung) eingesetzt. Datenbanken mit unterschiedlichem Schutzbedarf werden auf getrennten Systemen betrieben. Bei Datenbankexporten in Umgebungen mit niedrigerem Schutzbedarf werden sensible Daten unkenntlich gemacht.

Datenbankzugriffe und Datenbankaktivitäten von Administratoren werden protokolliert und bei Verdacht auf Unregelmäßigkeiten überprüft.

5.2 Transportkontrolle

Die folgenden Maßnahmen gewährleisten, dass bei der Übermittlung personenbezogener Daten, sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird.

Der Transport von Daten mit hohem Schutzbedarf auf zentralen Systemen ist verschlüsselt. Je nach Einsatzzweck nutzen Verbindungen das Protokoll https oder VPN-Tunnel mit den aktuell als sicher geltenden Verschlüsselungsparametern. Das Verschlüsseln von Datenspeichern wie Festplatten in Laptops wird ohne Zutun der Anwender mit Hilfe von Software automatisch umgesetzt. Werden Zertifikate für die Verschlüsselung und Signaturen verwendet, werden diese zentral verwaltet.

6. Überprüfung, Bewertung und Evaluierung der Wirksamkeit

Gesetzliche Grundlage: Art. 32 Abs. 1 lit. d DS-GVO

6.1 Zuverlässigkeit

Die folgenden Maßnahmen gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

6.1.1 Prozesse und Prozeduren

Die Prozesse und Prozeduren der Informationssicherheit sind als Teil des Informationssicherheitsmanagementsystems (ISMS) definiert, angelehnt an ISO/IEC 27001 ff. Sie werden regelmäßig geprüft und bei Bedarf aktualisiert. Das ISMS beinhaltet die Informationssicherheitspolitik, die Grundsätze der Informationssicherheit, Standards und Prozesse zum umfassenden Schutz von Informationen und Daten sowie der Kontinuität IT-gestützter Geschäftsprozesse.

Mit Hilfe der Sicherheitsprozesse und Prozeduren des Sicherheitsmanagement und der Berichterstattung wird die Effizienz und Effektivität der Schutzmaßnahmen sichergestellt. Dafür werden auf Basis eines risikobasierten Ansatzes IT-Systeme gemäß ihres Schutzbedarfs klassifiziert. Verfahren für akute Notfälle und Sicherheitsvorfälle sichern die Verfügbarkeit in Krisenfällen. Vorbeugende Maßnahmen zur Feststellung von Schwachstellen helfen diese zu beseitigen, bevor Auswirkungen wirksam werden können. Schulungen und Sensibilisierung fördern die Unterstützung der Schutzmaßnahmen durch die Belegschaft.

6.1.2 Richtlinien und Standards

Technische Standards und organisatorische Richtlinien sind dokumentiert und bindend. Sie werden den betroffenen Anwendern zur Kenntnis gebracht und deren Anwednung vermittelt. Abweichungen werden beantragt, freigegeben und zentral dokumentiert.

6.1.3 Schutzbedarfsfeststellung

Das Vorgehen zur Feststellung des Schutzbedarfs von Daten und IT-Systemen ist im Prozess Schutzbedarfsfeststellung (SBF) beschrieben. Der Prozess gilt für neue Systeme, aber auch für Bestandssysteme bei neuen Schnittstellen; ausschlaggebend sind Änderungen am Datenfluss oder dem Informationsgehalt der Daten.

Der Schutzbedarf dient als Grundlage für die Schutzmaßnahmen. Reichen bestehende Schutzmaßnahmen nicht aus, werden neue Maßnahmen entwickelt, geplant und umgesetzt. Bei regelmäßiger Anwendung neuer Maßnahmen werden diese zum Standard bzw. zur Richtlinie.

Die Einhaltung oder Nicht-Einhaltung von Schutzmaßnahmen wird durch Stichproben, Sicherheitsaudits und Revisionen festgestellt.

6.1.4 Sicherheitsüberprüfungen / Audit-Rahmenwerk

Neue Systeme werden im Rahmen der Abnahmeprüfung einer Sicherheitsprüfung unterzogen. Eine Freigabe für den Betrieb erfolgt erst, wenn keine kritischen Schwachstellen festgestellt werden können. Ausnahmen sind nur durch Risikoübernahmen möglich, allerdings nicht bei öffentlichen Internetauftritten.

7. Weisungsgemäße Verarbeitung

Gesetzliche Grundlage: *Art. 32 Abs. 4 DS-GVO*

Die folgenden Maßnahmen gewährleisten, dass personenbezogene Daten, nur entsprechend der Weisungen der verantwortlichen Stellen verarbeitet werden.

7.1.1 Mitarbeitersensibilisierung

Mitarbeiter sind auf das Datengeheimnis verpflichtet und werden angemessen, z.B. durch Schulungs- und Sensibilisierungsmaßnahmen, zu den Themen Datenschutz und Informationssicherheit informiert.

7.2 Auftragskontrolle

Die folgenden Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend der Weisungen des Verantwortlichen verarbeitet werden.

7.2.1 Datenverarbeitung im Auftrag

Bei der Verarbeitung im Auftrag eines Verantwortlichen wird die ordnungsgemäße Vertragsgestaltung und Auftragserteilung i.d.R. durch die Verwendung von Musterverträgen sichergestellt. Wird eine Gesellschaft der Schwarz Gruppe mit der Verarbeitung personenbezogener Daten beauftragt, erfolgt dies auf Grundlage der jeweils gültigen Rahmenvereinbarung zu Datentransfers personenbezogener Daten innerhalb der Unternehmensgruppe Schwarz und Nutzung des Vertragsmusters für die Verarbeitung personenbezogener Daten im Einzelfall („Einzelauftrag“).

Auftragsverarbeiter haben die getroffenen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung offenzulegen. Einzelfallabhängig wird entschieden, ob neben der dokumentenbasierten Prüfung der technischen und organisatorischen Maßnahmen, weitere Prüfungsmaßnahmen eingeleitet werden.

7.2.2 Sicherheitsüberprüfung des Auftragsverarbeiters

Vor der Beauftragung einer Verarbeitung im Auftrag eines Verantwortlichen überzeugt sich der Verantwortliche in geeigneter Weise beim Auftragsverarbeiter von der Einhaltung der zugesicherten technischen und organisatorischen Maßnahmen. Abhängig von den Antworten und den vom Auftragsverarbeiter bereitgestellten Dokumente wird entschieden, ob weitergehende Maßnahmen wie z.B. eine Begehung und Sichtung vor Ort oder die Beauftragung Dritter zur Überprüfung des Datenschutzniveaus erforderlich sind.

8. Datenportabilität

Gesetzliche Grundlage: *Art. 20 DS-GVO*

Wenn Betroffene selbst personenbezogene Daten bereitstellen, werden diese auf Anforderung durch den Betroffenen diesem oder – sofern dies technisch machbar ist – auf Weisung des Betroffenen an eine andere Verantwortliche Stelle in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt.

9. Mandantenfähigkeit

Gesetzliche Grundlage: *Art. 5 Abs. 1 DS-GVO*

Die folgenden Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

9.1 Trennung nach Mandanten

Wenn IT-Systeme personenbezogene Daten mehrerer verantwortlicher Stellen verarbeiten, werden die Datenbestände getrennt verarbeitet (Mandantentrennung). Die Dokumentation der Maßnahmen zur Umsetzung der Mandantentrennung erfolgt zum jeweiligen Prozess, IT-System oder sonstigen Verarbeitung.

9.2 Datenhaltungszone

Netzwerksegmente zur Datenhaltung beinhalten ausschließlich Datenbankserver. Datenbankzugriffe werden zwangsprotokolliert.

Datenbanken mit unterschiedlichem Schutzbedarf werden auf separaten Datenbankservern betrieben.

10. Trennbarkeit

Gesetzliche Grundlage: *Art. 5 Abs. 1 DS-GVO*

Die folgenden Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

Systeme mit hohem Schutzbedarf sind nach der Drei-Schichten-Architektur aufgebaut. Je Schicht gibt es ein Netzwerksegment. Firewalls erlauben nur Punkt-zu-Punkt-Verbindungen zwischen den Systemen der Präsentationsschicht und der Anwendungsschicht sowie der Anwendungsschicht und der Datenhaltungsschicht. Anwendern ist der Zugriff in die Präsentationsschicht erlaubt. Von der Präsentationsschicht zur Anwendungsschicht und von der Anwendungsschicht zur Datenhaltungsschicht sind nur Systemzugriffe erlaubt. Kann ein System die zugehörige Datenbank oder andere Komponente zur Datenhaltung nicht von der zugehörigen Anwendung trennen, gehört das System zur Anwendungsschicht. Somit ist gewährleistet, dass Auswirkungen von Fehlern oder Schwachstellen von Betriebssystemen oder Anwendungen auf angrenzende Systeme und Datenbestände minimal sind.