Anhang: Gegenstand der Auftragsverarbeitung

Zwecke der Auftragsverarbeitung

Personenbezogene Daten des Auftraggebers werden auf Grundlage dieses Auftragsverarbeitungsvertrages zu den folgenden Zwecken verarbeitet:

- IT-Beratung und Projektdurchführung
- IT-Betreuung und Support, insbesondere zur Fehlerbehebung
- Wartung und Aufrechterhaltung der technischen Funktion von IT und TK-Systemen

Arten und Kategorien von Daten

Zu den auf Grundlage dieses Auftragsverarbeitungsvertrages verarbeiteten Arten und Kategorien von personenbezogenen Daten gehören:

Auswahl	Datenkategorie	Datenbeispiele
X	Berufliche Kontakt- und (Arbeits-) Organisationsdaten	Name, Vorname, Geschlecht, Anschrift, E-Mail-Adresse, Telefonnummer, Mobiltelefonnummer, Gesellschaft, Bereich, Abteilung, Kostenstelle, Personalnummern, Zuständigkeiten, Funktionen, etc.
X	IT-Nutzungsdaten	User-ID, Rollen, Berechtigungen, Login-Zeiten, Rechnername, IP-Adresse, Software, Virenschutz, Softwareaktualisierung, Firewall- und Zugriffsprotokolle etc.
X	Vertrags- und Bestandsdaten	Beauftragte Leistungen, gekaufte Produkte, Datum Kaufvertrag, Kaufpreis, Garantien, etc.
X	Kommunikationsdaten und deren Historie	E-Mailverlauf, Anrufhistorie, Kommunikationsverlauf im CRM- und Ticket- System etc.
	Personaldaten	Tarifgruppe, Entgeltabrechnung, Sonderzahlungen, Pfändung, tägliche Anwesenheitszeiten, Abwesenheitsgründe, etc.
	Besonders sensible personenbezogene Daten	Rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.
	Bonitäts- und Bankdaten	Zahlungsverhalten, Bilanzen, Daten von Auskunfteien, Scorewerte, Vermögensverhältnisse, Kontoverbindung, Kreditkartennummer, etc.
X	Abrechnungsdaten	Rechnungen, Tätigkeitsnachweise, schriftliche Beauftragungen, Verlaufsdaten in Ticketsystemen
X	Sonstige Daten	Im Zuge der Leitungserbringung kann ein vorübergehender Zugriff auf weitere Datenarten des Auftraggebers und/oder dessen Kunden erfolgen, wenn bspw. eine Wiederherstellung aus der Datensicherung erforderlich ist.

Kategorien der betroffenen Personen

Zu den durch die Verarbeitung von personenbezogenen Daten auf Grundlage dieses Auftragsverarbeitungsvertrages betroffenen Personengruppen gehören:

- Mitarbeiter des Auftraggebers
- Ggfs. Kunden und Geschäftspartner des Auftraggebers (Dritte)

Quellen der verarbeiteten Daten

Die auf Grundlage dieses Auftragsverarbeitungsvertrages verarbeiteten Daten werden aus den im Folgenden genannten Quellen, bzw. im Rahmen genannter Verfahren erhoben oder sonst empfangen:

- Erhebung im Rahmen von Supporttätigkeiten während dem Remote-Access
- Erhebung im Rahmen der Nutzung von Software, Applikationen, Webseiten und anderen Onlinediensten

Anhang: Unterauftragsverarbeiter

Der Auftragsverarbeiter setzt die folgenden Unterauftragsverarbeiter im Rahmen der Verarbeitung von Daten für den Auftraggeber ein:

- TeamViewer: Software für Fernwartung; Dienstanbieter: TeamViewer GmbH, Jahnstr. 30, 73037 Göppingen, Deutschland; Datenverarbeitung: Europäischer Wirtschaftsraum (EWR)
- Noris Rechenzentrum: Bereitstellung von IT-Systemen und Betrieb Rechenzentrum; Dienstanbieter: Klausnerstraße 30, 85609 Aschheim; Datenverarbeitung: Deutschland

Weitere Unterauftragsverarbeiter können auftragsbezogen hinzugezogen und auf Anfrage mitgeteilt werden.

Anhang: Technische und organisatorische Maßnahmen (TOMs)
Stand: 13.11.2024

M.1 Maßnahmen zur Vertraulichkeit
M.1.1 Beschreibung der Zutrittskontrolle:

- Außentüren - Die Zugänge zum Bürohaus und auch zu den Büroräumen sind Tag und Nacht verschlossen.
- Videoüberwachung – Videoüberwachung der Eingangsbereiche.
- Besucherregelung - Besucher erhalten erst nach Türöffnung durch den Empfang Zutritt zu dem Bürohaus und dann den Büroräumen. Der Empfang kann die Eingangstür einsehen und trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet.
- Home-Office - Es ist sichergestellt, dass erforderliche Sicherheitsmaßnahmen für Beschäftigte im Home-Office eingehalten werden.
- IT-Schränke - Server- und Netzwerkschränke (Racks) sind verschlossen und werden nur bei Wartungsarbeiten geöffnet. Die Schlüsselausgabe ist geregelt.
- Manuelles Schließsystem - Manuelles Schließsystem mit Schließzylinder.
- Schließanlage - Einsatz einer Schließanlage.
- Schlüsselverwaltung - Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt
- Büroräume des Auftragnehmers
- Die Büroräume des Auftragnehmers sind mit Sicherheitsschlössern versehen und alle Schlüsselinhaber werden in einem Schlüsselverzeichnis geführt. Besucher werden innerhalb der Räumlichkeiten durch einen Mitarbeiter des Auftragnehmers begleitet.
- IT-Outsourcing / Software-Hosting in Aschheim
- Der Auftragnehmer hat Netzwerkschränke bei der noris network AG in Aschheim gemietet. Die Räume der noris network AG können nur durch berechtigte Personen mit 2 Faktor Authentifizierung betreten werden. Die Räume bzw. das Gebäude der noris network AG ist videoüberwacht und durch Sicherheitspersonal gesichert. Alle Zutritte werden protokolliert. Die Schränke des Auftragnehmers sind durch spezielle Schlüssel abgesichert und können nur durch die Mitarbeiter des Auftragnehmers geöffnet werden (zu Wartungszwecken auch durch Mitarbeiter der noris network AG). Nichtberechtigte Personen haben keinen Zugriff zu den Räumlichkeiten des Rechenzentrums.
- Cloud-Dienste bei externen Providern
- Der Auftragnehmer hat keinen Zutritt zu Räumlichkeiten von externen Cloud-Providern. Die Zutrittsregelung ist in dem mit dem jeweiligen Anbieter abgeschlossenen Vertrag zur Auftragsvereinbarung geregelt.

M.1.2 Beschreibung der Zugangskontrolle:

- Abwesenheit Arbeitsplatz - Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen. Alternativ wird diese Maßnahme durch dementsprechende technische Maßnahmen umgesetzt
- Authentifikation mit Benutzer + Passwort - Authentifikation an den IT-Systemen mit Benutzername + Passwort
- Besucherregelung - Es existiert eine Regelung, die die Verwendung privater Smartphones der Mitarbeiter und Geräte der Besucher ausschließlich im Gäste-WLAN garantiert.
- Firewall - Einsatz von Firewalls zum Schutz des Netzwerkes. Das Regelwerk der Firewall beinhaltet eine Sperrung nicht benötigter Ports und Dienste.
- Internetzugriff - Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.
- MDM - Einsatz von Mobile Device Management.
- Monitoring - Auf der Firewall ist ein Intrusion-Prevention-System im Einsatz. Alle Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist.
- Netzwerk-Segmentierung - Es besteht eine Netzwerksegmentierung und das interne Netzwerk bzw. WLAN ist vom Gäste-WLAN physisch oder per VLAN getrennt. Diese Maßnahme wird in einem grafischen Netzwerkplan dokumentiert.
- Regelung zu mobilen Geräten - Mitarbeiter verpflichten sich zur Einhaltung der Vorgaben zur Verwendung dienstlicher Smartphones / Notebooks bzw. existiert eine BYOD-Regelung.
- Remote Access - Remote-Zugriffe auf IT-Systeme erfolgen stets über verschlüsselte Verbindungen

- Sorgfältige Personalauswahl - Sorgfältige Auswahl der Beschäftigten sowie von von Reinigungs- und Sicherheitspersonal
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren
- Verwaltung der Adminpasswörter - Administratorpasswörter werden zentral und verschlüsselt unter Verwendung eines Passworttools gespeichert. Der Leitung bzw. Geschäftsführung sind die Passwörter regelmäßig gesichert auszuhändigen.
- Zugang zu Clouddiensten - Kritische interne IT-Systeme und cloudbasierte Anwendersoftware werden zusätzlich durch eine Zwei-Faktor-Authentifizierung gesichert.
- Der Auftragnehmer sichert die eigenen Systeme und die Systeme des Auftraggebers durch diverse Schutzmechanismen ab.
- Zugriffe von außen sind durch Firewalls des Auftragnehmers geschützt. Die Firewalls des Auftragnehmers schützen durch mehrstufige Kontrollen und Mechanismen den Zugriff von außen ab. Die Wartung der Firewall-Systeme erfolgt ausschließlich durch den Auftragnehmer. Der Zugriff von außen für Smartphones oder Tablets zur Synchronisation von E-Mails/Kontakten/Kalendern erfolgt durch eine Verschlüsselung auf dem aktuellen Stand der Technik.
- Der Zugriff innerhalb des Systems auf Internetdienste wird durch Web-Filterung kontrolliert. Antivirenprüfung und Content-Filter schützen vor Viren und Trojanern.
- Die E-Mail-Abholung (falls genutzt) wird durch Virenscan und Spamfilterung gewährleistet.
- Die Systeme der Kunden sind untereinander durch Schutzmechanismen getrennt. Die Server der Kunden werden durch Einsatz von VLAN-Technik getrennt. Die Server der Kunden werden zusätzlich durch Netztrennung auf Ebene von TCP/IP voneinander getrennt. Die Systeme werden zusätzlich durch Firewall-Regeln voneinander abgeschottet.
- Die Systeme sind innerhalb der Maschinen mit Benutzername und Kennwort geschützt. Die Kennwörter werden pro Mitarbeiter individuell vergeben. Dem Auftragnehmer sind die Kennwörter der Benutzer in der Regel nicht bekannt. Der Auftragnehmer kann die Kennwörter nur zurücksetzen aber nicht auslesen.

M.1.3 Beschreibung der Zugriffskontrolle:

- Adminrechte - Berechtigungen für IT-Systeme und Applikationen werden ausschließlich von Administratoren eingerichtet.
- Berechtigungskonzept - Es besteht ein dokumentiertes Berechtigungskonzept, dass Zugriffsberechtigungen und Passwortverfahren pro genutzter Anwendung und Dateisystem beschreibt. Ferner werden die Zugriffsrechte der Benutzer personen- oder rollenbasiert beschrieben.
- Datenlöschung - Sichere Löschung von Datenträgern vor deren Wiederverwendung (z.B. durch mehrfaches Überschreiben)
- Dokumentenvernichtung - Alle Mitarbeiter sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen oder mit dem Schredder zu vernichten.
- IT-Infrastruktur physisch - Der physische Zugriff auf Server und zentrale Netzwerkkomponenten ist durch die Installation in IT-Schränken (Racks) abgesichert.
- On- und Offboarding - Es ist ein Verfahren etabliert, dass mit der Einstellung und dem Ausscheiden von Beschäftigten den Zugriff auf IT-Systeme berechtigt bzw. entzieht.
- Passwortregelung 2020 - Es ist eine Passwortrichtlinie, die Länge und Komplexität technisch vorgibt, etabliert. Der Benutzer muss sein Initialpasswort mit der ersten Anmeldung wechseln und eine automatische Sperrung erfolgt bei wiederholter Falscheingabe.
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren.
- Zentrale Benutzerverwaltung - Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.
- Der Zugriff auf Systeme des Auftragnehmers kann ausschließlich durch Eingabe von Benutzername und Kennwort erfolgen. Der Benutzer muss sein Kenn-wort in regelmäßigen Abständen nach den Vorgaben der Passwortrichtlinie des Auftragnehmers erneuern. Das interne Berechtigungskonzept stellt sicher, dass jeder Mitarbeiter nur Zugriff auf die Daten erhält, die zur Erfüllung seiner Tätigkeit notwendig sind. Administratorzugang haben nur die Leiter der jeweiligen Projektteams und der Leiter der Datenverarbeitung.

M.1.4 Beschreibung der Weitergabekontrolle:

- Datenweitergabe - Eine Weitergabe von personenbezogenen Daten darf jeweils nur in dem Umfang erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.
- E-Mail-Verschlüsselung - E-Mail-Verschlüsselung mit S/MIME oder PGP-Verfahren wird dem Kunden grundsätzlich angeboten.
- Externe Datenträger - Die Nutzung von privaten Datenträgern ist den Beschäftigten im Zusammenhang mit Kundenprojekten untersagt.
- Kundenprojekt - Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.
- Mitarbeiterschulung - Die Mitarbeiter werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.
- SSL / TLS Verschlüsselung - Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet
- VPN-Tunnel - Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen
- Der Zugriff des Auftraggebers und des Auftragnehmers und die Übertragung von Benutzereingaben und Bildschirminhalten erfolgt durch VPN-Tunnel. Die VPN-Tunnel werden durch IPsec mit PreShared Key und Zertifikaten abgesichert. IPsec ist ein weltweit gültiger Standard auf dem aktuellen Stand der Technik. Der Zugriff von einzelnen Mitarbeitern von Heimarbeitsplätzen erfolgt durch SSL-VPN. Der SSL-VPN -Zugang ist durch persönliche Benutzernamen und Kennwörter abgesichert.

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung - Die eingesetzten IT-System verfügen über eine logische Mandantentrennung (softwareseitig). Die Trennung von Daten von verschiedenen Kunden/Projekten ist stets gewährleistet.
- Durch regelmäßige Unterweisungen zum Datenschutz sensibilisiert der Auftragnehmer die Mitarbeiter im Umgang mit dem Trennungsgebot.

M.1.7 Beschreibung der Verschlüsselung:

- Festplattenverschlüsselung - Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungssysteme im Einsatz.
- Serverzugriff - Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

M.2 Maßnahmen zur Integrität

M.2.1 Beschreibung der Eingabekontrolle:

- Benutzerkonten - Die Beschäftigten sind verpflichtet, stets mit ihren eigenen Benutzerkonten zu arbeiten. Benutzerkonten dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.
- Personalisierte Benutzernamen - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen).
- Zugriffsrechte - Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Aktualisierung von Anwendersoftware - Es ist ein Verfahren etabliert, dass die regelmäßige Aktualisierung der Standard- und Individualsoftware sicherstellt. Dieses Verfahren beinhaltet automatisierte Verfahren mit zentraler Steuerung, als auch manuelle Prozesse, die je nach technischer Vorrausetzung der Anwendersoftware geplant werden.
- Auslagerung Datensicherung - Die Aufbewahrung der Datensicherung erfolgt an einen sicheren, ausgelagerten Ort. Die Datensicherung wird verschlüsselt.
- Backup- & Recoverykonzept - Es existiert ein dokumentiertes Backup- & Recoverykonzept, das täglich überprüft wird.
- Monitoring - Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.
- Patchmanagement - Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits- und Software-Updates aktualisiert.
- Umgebungssicherheit für Serverräume und RZ - Der Serverbetrieb ist ausschließlich an Dienstleister ausgelagert. Die Dienstleister verfügen über ein zertifiziertes Betriebskonzept. Dies wird regelmäßig geprüft.
- Viren- und Malwareschutz - Einsatz einer mehrstufigen Absicherung gegenüber Viren und Malware. Es ist gewährleistet, dass die Absicherung der IT-Systeme tagesaktuell ist und der Status in regelmäßigen Abständen überwacht wird.
- IT-Outsourcing / Software-Betreuung in Aschheim
- Die Netzwerkschränke des Auftragnehmers (Schränke bei der noris network AG Aschheim) sind durch zertifizierte Systeme geschützt. Aktuelle Brandschutzmaßnahmen, Überspannungsschutz und unterbrechungsfreie Stromversorgung mit Dieselaggregaten sind vorhanden. Die Räume sind klimatisiert und werden durch Temperatursensoren überwacht. Eine Überschreitung der zulässigen Temperaturen wird dem Betreiber signalisiert, dadurch werden weitere Maßnahmen veranlasst.
- Die Systeme sind durch die Zugangskontrolle und diverse Überwachungsmechanismen vor Diebstahl geschützt.
- Die Systeme des Auftragnehmers sind hochwertige Markensysteme (überwiegend HPE-Server und HPE-Storage-Systeme). Die Systeme sind unterschiedlich zusammengestellt, um flexibel auf Änderungen und Kundenanforderungen reagieren zu können. Die Serversysteme sind durch redundante Komponenten überwiegend gegen Ausfall abgesichert, einzelne nicht redundante Komponenten könnten aber zu einem Ausfall eines Serversystems führen. Sollten nicht redundante Komponenten einen Ausfall verursachen, können diese durch immer verfügbare Ersatzgeräte in der Regel innerhalb weniger Stunden wieder repariert oder durch ein gleichwertiges System wiederhergestellt werden. Sollten Kundenserver defekt oder durch einen Hardwarefehler zerstört worden sein, müssen die Server von der Datensicherung wiederhergestellt werden. Eine Rücksicherung von Kundenservern aus der Datensicherung kann je nach Größe der Daten bis zu 1-2 Tage dauern.

- Der Auftragnehmer sichert täglich die Server der Kunden. Die Datensicherungen werden über 28 Tage verfügbar gehalten. Die Datensicherung erfolgt mindestens einmal täglich (in der Regel nachts). Bei Ausfall eines kompletten Servers oder bei Verlust von einzelnen Dateien (unabsichtliches löschen durch Auftraggeber) können diese Server/Daten in der Regel innerhalb von wenigen Minuten/Stunden wiederhergestellt werden. Eine genaue Zusage der Wiederherstellung kann nicht festgelegt werden, da die Wiederherstellung je nach Größe/Ausmaß unterschiedlich sein kann. Die Verfügbarkeit der Serversysteme des Auftragnehmers sind mit 99% festgelegt.
- Cloud-Dienste bei externen Providern
- Die Verfügbarkeitskontrolle ist in dem mit dem jeweiligen Anbieter abgeschlossenen Vertrag zur Auftragsvereinbarung geregelt.

M.3.2 Beschreibung der raschen Wiederherstellbarkeit:

- Incidentmanagement - Es besteht ein Verfahren (bspw. nach ITIL-Standard), dass zwischen Ausfällen / Störungen und Sicherheitsvorfällen unterscheidet. Meldungen werden zentral in einem Ticketsystem protokolliert und die Bearbeitung dokumentiert. In regelmäßigen Abständen werden Vorfälle ausgewertet, um Schwachstellen in IT-Systemen proaktiv entgegenzuwirken.
- Notfallkonzept und Datenwiederherstellung - Tolerierbare Ausfallzeiten sind mit den Dienstleistern festgelegt und insbesondere für kritische IT-Systeme geprüft.
- Mit der Wiederherstellung ist eine Reihenfolge der IT-Systeme festgelegt, damit der Wiederanlauf fehlerfrei ablaufen kann.

M.4 Weitere Maßnahmen zum Datenschutz

M.4.1 Beschreibung der Auftragskontrolle:

- Audits - Regelmäßige Datenschutzaudits der beauftragten Dienstleister durch den Datenschutzbeauftragten.
- Auswahl - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit und Subdienstleister)
- Datenverarbeitung - Die Verarbeitung der Datenhaltung erfolgt ausschließlich in der Europäischen Union oder im Europäischen Wirtschaftsraum.
- Dienstleister - Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts eine angemessene Datenschutzregelung getroffen. Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO.
- DSB - Benennung eines externen Datenschutzbeauftragten: Stephan Krischke, erreichbar unter datenschutz@sbsgmbh.com
- Laufende Überprüfung - Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.
- Schulung - Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen.
- Verpflichtung - Verpflichtung der Dienstleister auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, Art. 29, Art. 32 Abs. 4 DS-GVO
- Es ist sichergestellt, dass personenbezogene Daten die im Auftrag verarbeitet werden, gemäß den Weisungen des Auftraggebers verarbeitet werden. Alle Mitarbeiter des Auftragnehmers sind bis auf Weiteres auf das Datengeheimnis verpflichtet.
- Die Auswahl von Dienstleistern erfolgt erst nach sorgfältiger Vorab-Prüfung durch den Auftragnehmer und allen involvierten Fachabteilungen. Eine Auftragserteilung erfolgt ausschließlich nach Abschluss eines schriftlichen Vertrages zur Auftragsverarbeitung (Art. 28 Abs. 9 DS-GVO).

M.4.2 Beschreibung des Managementsystems zum Datenschutz:

- DSMS - Im Unternehmen ist ein Datenschutzmanagementsystem (DSMS) implementiert. Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.
- DST - Es ist Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, dass Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.
- Incident-Response-System - Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.
- Meldung Aufsichtsbehörde - Bei der Verarbeitung von Daten für eigene Zwecke wird im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Kenntnis von dem Vorfall erfolgen.
- Regelungen zum Datenschutz und der IT-Sicherheit - Es bestehen schriftliche Regelungen zum Datenschutz und Datensicherheit (Arbeitsvertrag, Datenschutzhandbuch). Beschäftigte werden auf die Einhaltung der dieser Regelungen geschult und verpflichtet.
- Verpflichtung der Beschäftigten - Beschäftigte werden zur Vertraulichkeit im Umgang mit personenbezogenen Daten sowie der Verschwiegenheit gegenüber dem Geschäftsgeheimnis verpflichtet. Diese Verpflichtung beinhaltet auch die Nutzung sozialer Medien.