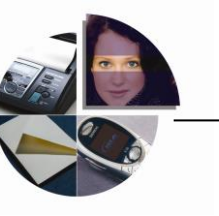


Technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DS-GVO für Auftragsverarbeiter (Art. 30 Abs. 1 lit. d)

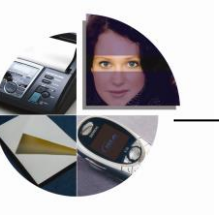
In dieser Übersicht stellen wir eine Übersicht der Technischen und organisatorischen Maßnahmen von FAX.de vor. Diese gelten als Anhang der FAX.de SLA (Vers. 1.2) bzw. der aktuellen Erklärung für die Auftragsdatenverarbeitung. FAX.de betreibt in Deutschland zwei Rechenzentren an unterschiedlichen Standorten. Beide Rechenzentren sind gespiegelte Systeme und können unabhängig vom anderen Rechenzentrum eigenständig die anfallenden Versandaufträge verarbeiten.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.	
Elektronische Zutrittstransponder/Zutrittscode	✓
Gesondert gesicherter Zutritt zum Rechenzentrum	✓
Aufbewahrung der Server in verschlossenen Räumen	✓
Aufbewahrung der Datenträger/Datensicherung im zutrittsgeschützem Safe	✓
Umfangreiches Sicherheitskonzept akkreditiert von der BNetzA	✓

Zugangskontrolle Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.	
Netzwerkzugang extern mit SSL-256 verschlüsselt	✓
Verschlossener Cage für Server	✓
Passwortsicherung der Bildschirmarbeitsplätze	✓
Verpflichtung zur Vertraulichkeit von allen Mitarbeitern unterzeichnet	✓

Zugriffskontrolle Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.	
Regelmäßige Auswertung von Protokollen/Logfiles	✓
Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen	✓
Einsetzen von entsprechenden Sicherheitssystemen (FortiNet, ESET)	✓
Verwendete Hash-Funktion: SHA2 (256 bit)	✓

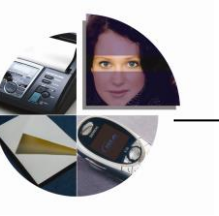


Trennungskontrolle Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.	
Funktionstrennung	✓
Dediziertes System	✓

Pseudonymisierung Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen	
Maßnahmen: Produktivdaten werden über ID's /AccountNr. organisiert	✓

2. Integrität (Art. 32 Abs 1 lit. b DS-GVO)

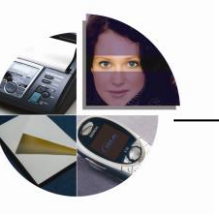
Weitergabekontrolle Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport sowie deren Kontrolle. Versendungsart der Daten zwischen Auftraggeber und Dritten:	
VPN-Verbindung (IP-Sec)	✓
Datenaustausch über https mit SSL-256 verschlüsselt	✓
Gesicherter Eingang für An- und Ablieferung	✓
Papierentsorgung: Shredder gem. DIN 66399, Sicherheitsstufe 4	✓
Dokumentation der Übermittlungswege	✓
Eingabekontrolle Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten	
Kennzeichnung erfasster Daten	✓
Differenzierte Benutzerberechtigungen	✓
Lesen, Ändern, Löschen	✓
Teilzugriff auf Daten bzw. Funktionen	✓
Organisatorische Festlegung von Eingabezuständigkeiten	✓
Protokollierung von Eingaben/Löschungen	✓
Verpflichtung auf das Datengeheimnis	✓



3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. B DS-GVO)

Verfügbarkeitskontrolle Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen	
Datensicherungs- und Backupkonzepte	✓
Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal	✓
Rauchmelder in Serverräumlichkeiten	✓
Wasserlose Brandbekämpfungssysteme in Serverräumlichkeiten	✓
Klimatisierte Serverräumlichkeiten	✓
Blitz-/Überspannungsschutz	✓
Serverräumlichkeiten in separatem Brandabschnitt	✓
Unterbringung Backupsystem in separaten Räumlichkeiten	✓
Lagerung von Archiven unter notwendigen Bedingungen	✓
CO2 Feuerlöscher in unmittelbarer Nähe der Serverräumlichkeiten	✓
Einbeziehung des Einflusses angrenzender baulicher Einrichtungen	✓
Aufbewahrung der Daten in Datensicherungsschränken/Tresoren	✓
USV-Anlage (Unterbrechungsfreie Stromversorgung)	✓

Widerstandsfähigkeit- und Ausfallsicherheitskontrolle Systeme müssen die Fähigkeit besitzen, mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.	
Redundante USV-Anlage	✓
Redundante Klimatisierung	✓
Festplattenspiegelung	✓
Loadbalancer	✓
Datenspeicherung auf RAID-Systemen	✓
Abgrenzung kritischer Komponenten	✓
Regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates	✓
Verwendung redundanter Systeme, um den Betrieb aufrecht zu erhalten	✓
Progressive Bereitstellung von Updates, um Probleme frühzeitig zu erkennen	✓
Begrenzung von Berechtigungen auf Bedarfsnotwendigkeit	✓
Abschluss einer IT/Cyber-Versicherung	✓



4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs 1 lit. d DS-GVO, Art 25 Abs 1 DS-GVO)

Kontrollverfahren Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren.	
Interne Verfahrensverzeichnisse werden jährlich aktualisiert	✓
Meldung neuer/veränderter Verfahren an den Datenschutzbeauftragten	✓
Meldung neuer/veränderter Verfahren an den IT-Sicherheitsbeauftragten	✓
Datenschutzfreundliche Voreinstellungen werden gewählt	✓
Sicherheitsmaßnahmen werden regelmäßig kontrolliert	✓

Auftragskontrolle Es ist sicherzustellen, dass Daten die im Auftrag durch Dienstleister verarbeitet werden, nur gemäß der Weisung des Auftragnehmers verarbeitet werden.	
Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DS-GVO)	✓
Zentrale Erfassung vorhandener Dienstleister	✓
Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn	✓
Überprüfung des Datensicherheitskonzepts beim Auftragnehmer	✓
Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer	✓

Genehmigte Subunternehmer	
Net@work Rechenzentrum	Hamburg/Wendenstr.
Colt GmbH	Hamburg/Div.
EWE GmbH	Oldenburg/Div.
Cosmos KG	Hamburg
BS PayOne GmbH	Frankfurt/Main