

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 comfax vor. Diese gelten als Anhang der comfax SLA (Vers. 1.2) bzw. der aktuellen Erklärung für die Auftragsdatenverarbeitung. Die Daten werden mehrfach auf unterschiedlichen Datenträgern gesichert.

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	✓
Zutrittsberechtigungskonzept	✓
Videoüberwachung	✓
Alarmanlage mit Aufschaltung Wachdienst	✓
Schlüsselregelung	✓
Begleitung von Besucherzutritten durch eigene Mitarbeiter	✓
Abgestufte Sicherheitsbereiche und kontrollierter Zutritt	✓
Gesondert gesicherter Zutritt zum Rechenzentrum	✓
Aufbewahrung der Server in verschlossenen Räumen	✓
Aufbewahrung der Datenträger/Datensicherung im zutrittsgeschütztem 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	✓
Funktionelle Vergabe von Benutzerberechtigungen	✓
Automatische passwortgesicherte Bildschirmspernung nach Inaktivität	✓
Passwortpolicy mit mindestens 8 Ziffern, 3 Kriterien (Optional OTP) *1	✓
Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern	✓
Prozess zur Rechtevergabe bei Austritt von Mitarbeitern	✓
Verpflichtung zur Vertraulichkeit von allen Mitarbeitern unterzeichnet	✓
Protokollierung und Auswertung der Systembenutzung	✓
Kontrollierte Vernichtung von Datenträgern	✓

<u>Zugriffskontrolle</u>	
Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.	
Festlegung der Zugriffsberechtigung, Berechtigungskonzept	✓
Regelung zur Wiederherstellung von Daten aus Backups	✓
Beschränkung der freien Abfragemöglichkeit von Datenbanken	✓
Regelmäßige Auswertung von Protokollen/Logfiles	✓
Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen	✓
Protokollierung von Zugriffen und Löschungen	✓
Einsetzen von entsprechenden Sicherheitssystemen (FortiNet, ESET)	✓
Virens Scanner	✓
Intrusion detection (IDS)	✓
Verwendete Verschlüsselungsalgorithmen: AES	✓
Verwendete Hash-Funktion: SHA2 (256 Bit)	✓

<u>Trennungskontrolle</u>	
Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.	
Logische Datentrennung auf Basis von Mandaten Nummern	✓
Funktionstrennung	✓
Trennung von Entwicklungs- und Produktivsystem	✓
Dediziertes System	✓

<u>Pseudonymisierung</u>	
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 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	✓
Datenträgerentsorgung: Sichere Löschung von Datenträgern	✓
Papierentsorgung: Shredder gem. DIN 66399, Sicherheitsstufe 4	✓
Regelung zur Anfertigung von Kopien	✓
Dokumentation der Übermittlungswege	✓

Eingabekontrolle	
Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten	
Kennzeichnung erfasster Daten	✓
Festlegung von Benutzerberechtigungen (Profile)	✓
Differenzierte Benutzerberechtigungen	✓
Lesen, Ändern, Löschen	✓
Teilzugriff auf Daten bzw. Funktionen	✓
Organisatorische Festlegung von Eingabezuständigkeiten	✓
Protokollierung von Eingaben/Löschungen	✓
Verpflichtung auf das Datengeheimnis	✓

Verfügbarkeitskontrolle	
Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen	
Datensicherungs- und Backupkonzepte	✓
Durchführung der Datensicherungs- und Backupkonzepte	✓
Zutrittsbegrenzung in Serverräumen auf notwendiges Personal	✓
Brandmeldeanlagen in Serverräumen	✓
Rauchmelder in Serverräumen	✓
Wasserlose Brandbekämpfungssysteme in Serverräumen	✓
Klimatisierte Serverräume	✓
Blitz-/Überspannungsschutz	✓
Wassersensoren in Serverräumen	✓
Serverräume in separaten Brandabschnitt	✓
Unterbringung Backupsystem in separaten Räumen	✓
Gewährleistung der technischen Lesbarkeit von Backup für die Zukunft	✓
Lagerung von Archiven unter notwendigen Bedingungen	✓
CO2 Feuerlöscher in unmittelbarer Nähe der Serverräume	✓
Vereinbarung bzgl. Übergabe der Datensicherungen	✓
Notfallplan (z.B. Wasser, Feuer, Explosion, Absturz, Anschlag)	✓
Einbeziehung des Einflusses angrenzender baulicher Einrichtungen	✓
Schwachstellenanalyse (Gebäudeschutz, Eindringen in Rechner/Netze)	✓
Aufbewahrung der Daten in Datensicherungsschränken/Tresoren	✓
USV-Anlage (Unterbrechungsfreie Stromversorgung)	✓
Stromgenerator für RZ	✓

Widerstandsfähigkeit- und Ausfallsicherheitskontrolle	
Systeme müssen die Fähigkeit besitzen, mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.	
Redundante Stromversorgung	✓
Redundante USV-Anlage	✓
Redundante Klimatisierung	✓
Festplattenspiegelung	✓
Loadbalancer	✓
Datenspeicherung auf RAID-Systemen	✓
Abgrenzung kritischer Komponenten	✓
Durchführung von Penetrationstests	✓
Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)	✓
Regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates	✓
Identifikation verschiedener Geräte, aus denen sich das Netzwerk zusammensetzt	✓
Kommunikationskanal mit den Herstellern, um neue Updates zu erhalten	✓
Definition von Zeiträumen, in denen Updates implementiert werden	✓
Verwendung redundanter Systeme, um den Betrieb aufrecht zu erhalten	✓
Progressive Bereitstellung von Updates, um Probleme frühzeitig zu erkennen	✓
Definition von Sicherheitsmaßnahmen zur Validierung der Systemkomponenten	✓
Begrenzung von Berechtigungen auf Bedarfsnotwendigkeit	✓
Externe Auftragnehmer/Wartungspersonal erhalten einen zeitlich limitierten Zugang	✓
Sensibilisierungskampagnen um die Benutzer über die Sicherheitskonzepte zu informieren	✓
Sicherheitstraining für Sicherheitsmaßnahmen der täglichen Prozesse	✓
Abschluss einer IT/Cyber-Versicherung	✓
Risikoanalyse aller Systeme, Geräte, Vermögenswerte	✓

3. 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	✓
Vor Ort Kontrollen beim Auftragnehmer	✓
Überprüfung des Datensicherheitskonzepts beim Auftragnehmer	✓
Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer	✓

Genehmigte Subunternehmer	
Colt GmbH	Hamburg/Div.
EWE GmbH	Oldenburg/Div.
Cosmos KG	Hamburg