EDV-Ingenieurbüro GmbH

Technische und organisatorische Maßnahmen

Ergänzung zur Auftragsverarbeitung (AV) nach DS-GVO, Artikel 28

9607 29.11.2023

Vertraulichkeit - Zugangskontrolle 3

Vertraulichkeit - Zugriffskontrolle 3

Vertraulichkeit - Zutrittskontrolle 4

Integrität - 4

Integrität 5

Verfügbarkeit & Belastbarkeit 5

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung 5

Änderungs- und Versionshistorie 6

Kontakt 8

Zum Schutz der personenbezogenen Daten des Verantwortlichen, die sich entweder bei KSR befinden oder auf die KSR-Mitarbeiter per Fernwartung Zugriff haben, trifft KSR standardmäßig die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen.

Hinweis: Die genannten Datensicherheitsmaßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden.

Maßnahmenziel	**Maßnahmen**
Vertraulichkeit - Zugangskontrolle (Art. 32, Abs.1 b DS-GVO)	*Maßnahmen, die die unbefugte Nutzung der DV-Systeme bei KSR verhindern; Datenverarbeitungsanlagen nutzen, z. B. vom Home-Office aus* • Authentifizierung erforderlich an allen Rechnern mit Benutzername und Kennwort. • Passwortrichtlinie: mind. 8 Zeichen, Mischung aus Groß-/Kleinschreibung, Zahlen und Sonderzeichen (zentral geregelt über Active Directory). • Eindeutige Benutzerkennung für jeden Mitarbeiter und Berechtigungskonzept im Active Directory. • Anti-Viren-Software “Sophos Anti-Virus” • Hardware-Firewall inclusive Intrusion Detection System “Sophos UTM” • Software- und hardwarebasierte VPN-Technologien (Virtual Private Network) oder RemoteDesktop-Gateways für gesicherten Zugriff „von außen“ auf das KSR-Netzwerk (z. B. für Mitarbeiter in den Vertriebsbüros/im Home-Office).
Vertraulichkeit - Zugriffskontrolle (Art. 32, Abs.1 b DS-GVO)	*Maßnahmen, die bei und nach der Verarbeitung personenbezogener Daten die Vertraulichkeit sicherstellen;* *Zugriff auf bestimmte personenbezogene Daten, Programme, und Dokumente erhalten* • Anzahl der Systemadministratoren auf das „Notwendigste“ reduziert (2 Personen mit Informatik-Ausbildung). • Verwaltung der Rechte nur durch Systemadministration oder Geschäftsleitung. • Restriktives, bedarfsorientiertes Berechtigungskonzepts nach Abteilungszugehörigkeit und Funktion im Active Directory. • Eigenes Fremddatenverzeichnis für Dateien von Kunden mit eingeschränktem Benutzerkreis. Nach Abschluss der Bearbeitung eines Kundenproblems werden die zugehörigen Dateikopien sofort gelöscht, sofern nicht mehr benötigt. • Zentrale Ausgabe und Rückgabe von mobilen Datenträgern (z. B. Notebooks, externe Platten), sachgerechte Formatierung gebrauchter Geräte sofort nach der Rückgabe. • Bei allen Notebooks werden die Festplatte mittels BitLocker verschlüsselt, so das bei einem Verlust des Notebooks die Daten auf der Festplatte nicht ausgelesen werden können. • Smartphones werden mit einem Code verschlüsselt, z. B. Face-ID, Pin, Muster. • Mehrere elektrische Aktenvernichter zur Entsorgung gedruckter Screenshots oder Listen, handschriftlicher Aufschriebe und sonstiger Papiere mit vertraulichem Inhalt. • Professionelle Löschung/Vernichtung von alten oder defekten Datenträgern durch einen zertifizierten Entsorger. • Geheimhaltungspflicht der KSR-Mitarbeiter Alle Mitarbeiter der KSR sind schriftlich auf das Datengeheimnis verpflichtet und wurden mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht.

Maßnahmenziel	Maßnahmen
Vertraulichkeit - Zutrittskontrolle (Art. 32, Abs.1 b DS-GVO)	*Maßnahmen, die Unbefugten den Zutritt zu Räumen und Systemen mit personenbezogenen Daten verwehren;* *Physischen Zutritt zu Datenverarbeitungsanlagen erhalten. z. B. Mitarbeiter direkt am Firmen-PC, Elektriker zu Serveranlage* • Kein unbefugtes Betreten des KSR-Gebäudes oder des Server-Raums durch: - Alarmanlage mit Verbindung zu externem Wachdienst - Videoüberwachung - abgesicherte Gebäudeschächte, Sicherheitsschlösser - Durchgängig verschlossene Zugangstüren zu Gebäude und Server-Raum, Zugang zum Gebäude nur mit Transponder oder Schlüssel, Besucher müssen klingeln. - Zugang zum Serverraum nur nach Code-Eingabe. - Während der Geschäftszeiten durchgängig besetzter Empfang, Besucher-Einlass durch den Empfang entweder persönlich oder per elektronischem Türöffner. • Sichere Vergabe von Schlüsseln/Transpondern/Codes: - Transponderübergabe frühestens nach Ablauf der Probezeit - Schlüsselvergabe und Alarmanlagen-Code nur an langjährige Mitarbeiter und Geschäftsleitung, Aufbewahrung der restlichen Schlüssel im Tresor. - Schriftliche Belehrung/Information zur Aufbewahrung des Schlüssels/ Transponders mit sofortiger Informationspflicht bei Verlust. - Führen einer KSR-internen Schlüsselliste zur Dokumentation der verfügbaren Schlüssel/Transponder und der aktuellen Besitzer. • Reinigungsarbeiten erfolgen durch eine Gebäudereinigungsfirma, mit der eine Vereinbarung zur Verschwiegenheit besteht.
Integrität - (Art. 32, Abs.1 b DS-GVO)	*Maßnahmen, die bei Transport und elektr. Übertragung personenbezogener Daten die Vertraulichkeit sicherstellen* • Verwendung von VPN-Tunneln oder RemoteDesktop-Gateways zur Übertragung von Daten: - zwischen der KSR-Zentrale und den Mitarbeitern in Vertriebsbüros - zwischen den Mitarbeitern im Home-Office und ihren Firmen-PCs - vom Kunden zu KSR • Sichere Übertragung von Daten bei Fernwartungssitzungen durch: - Fernwartungsprogramme „TeamViewer"", der höchste Sicherheitsansprüche erfüllt (siehe Anlage). - KSRseitige Absicherung von Datenübertragungen an den Verantwortlichen durch Virenscanner, Firewall, unterbrechungsfreie Stromversorgung (USV). • Weitergabe von Datenträgern, Papieren, etc. nur durch eigene Mitarbeiter oder vertrauenswürdige Transporteure (z. B. Post) in sicherer Verpackung. Annahme und interne Verteilung aller Sendungen durch KSR-Zentrale.
	Maßnahmen, die die Verarbeitung personenbez. Daten nachvollziehbar machen **Hinweis:** Die Erfassung, Änderung oder Löschung von personenbezogenen Daten für den Verantwortlichen ist nicht Gegenstand des Auftrags. Sollte es zur Problemdiagnose erforderlich sein, einen einzelnen Datensatz temporär zu erfassen, zu ändern oder zu löschen gelten folgende Richtlinien:

Maßnahmenziel	Maßnahmen
	• Soweit möglich, werden Tests mit eigenen, erdachten Testdaten durchgeführt, die nach Testende sofort wieder gelöscht werden. • Tests mit echten Daten generell nur in Absprache mit dem Verantwortlichen. • Der Verantwortliche kann die Arbeiten und Tests jederzeit am Bildschirm beobachten oder unter Anleitung unserer Mitarbeiter selbst durchführen. • Unsere Mitarbeiter führen Tests und Arbeiten unter dem Benutzernamen „Support“ durch. In den KSR-Programmen wird dieser Name bei der Erfassung oder Änderung von Daten zusammen mit dem Datum am betreffenden Datensatz gespeichert und ermöglicht so die Unterscheidung von den eigenen Bearbeitungen des Verantwortlichen.
Integrität (Art. 32, Abs.1 b DS-GVO)	**Hinweis:** Manche Software-Probleme lassen sich unter dem Benutzernamen „Support“ nicht nachvollziehen. In diesem Fall müssen die Tests unter dem Benutzernamen des Mitarbeiters durchgeführt werden, der das Problem gemeldet hat. Nachdem sich dieser mit seinem Benutzernamen angemeldet hat, kann er die Tests entweder unter Anleitung von KSR selbst durchführen oder am Bildschirm beobachten.
Verfügbarkeit & Belastbarkeit (Art. 32, Abs.1 b DS-GVO)	*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.* **Hinweis:** Die Erfassung, Änderung oder Löschung von personenbezogenen Daten für den Verantwortlichen ist nicht Gegenstand des Softwarepflegevertrags. Daraus folgt, dass keine Original-Daten des Verantwortlichen bei KSR gespeichert sind. Folgende technische Maßnahmen dienen generell der ständigen Verfügbarkeit aller Daten bei KSR: • Feuer- und Rauchmeldeanlagen, generelles Rauchverbot innerhalb des Gebäudes • Unterbrechungsfreie Stromversorgung (USV) • Spezielle Schutzmaßnahmen für den Serverraum: - Alarmmeldung bei unberechtigtem Zutritt zum Serverraum - Klimaanlage, Feuerlöscher - Geräte zur Überwachung von Temperatur und Feuchtigkeit • Hohe Ausfallsicherheit der Server durch redundante Datenspeicher (RAID) • Automatisierte tägliche Sicherung der Server • Mindestens 1x jährlich Recovery-Test (Datenwiederherstellung) • Datensicherungen werden an einem sicheren Ort außerhalb des KSR-Gebäudes aufbewahrt.
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32, Abs. 1 d DS-GVO).	*Maßnahmen, die sicherstellen, dass keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers erfolgt.* • Die zu erbringenden Leistungen werden praktisch ausschließlich per Fernwartung oder telefonisch erbracht. Dabei sind unsere Mitarbeiter in direktem Kontakt mit dem Verantwortlichen, so dass schon dadurch eine Auftragskontrolle gegeben ist. • Das eingesetzte Fernwartungsprogramm „TeamViewer“ ist so konzipiert, dass Sicherheit und Kontrollierbarkeit einer Fernwartungssitzung oberste Priorität haben. Konkret bedeutet dies: - Eine Fernwartungssitzung ist nur möglich in Absprache mit dem Verantwortlichen, da dieser einen bestimmten Code eingeben muss. Dieser Code wird für jede Sitzung neu vergeben.

Maßnahmenziel	Maßnahmen
	- Jede Fernwartungssitzung kann vom Verantwortlichen am Bildschirm des gewarteten Rechners beobachtet werden. - Der Verantwortliche kann jederzeit wieder die Steuerung übernehmen. - Eine Fernwartungssitzung kann vom Verantwortlichen jederzeit abgebrochen werden.

Änderungs- und Versionshistorie

Version	Datum	Erläuterung	geändert durch
1.2	29.11.2023	- Übertragung des Kapitels "Geheimhaltungspflicht der KSR-Mitarbeiter" aus dem AV-Vertrag in die TOMs - Ergänzung des Punktes Vertraulichkeit um die Begriffe Zugangs-, Zugriffs- und Zutrittskontrolle	KSR EDV GmbH / GRE
1.1	06.10.2022	Ergänzung: Bei allen Notebooks wird die Festplatte mittels BitLocker verschlüsselt, so das bei einem Verlust des Notebooks die Daten auf der Festplatte nicht ausgelesen werden können.	KSR EDV GmbH / FGR / GRE
	31.05.2022	Aktualisierung auf 2022	KSR EDV GmbH / PRI / GRE
1.0	30.03.2018	Freigabe als Kapitel im AVV	KSR EDV GmbH / AST

Notizen

Kontakt

KSR EDV-Ingenieurbüro GmbH
Adenauerstraße 13/1
D-89233 Neu-Ulm

Sie erreichen uns **telefonisch** unter
+49 (0) 731 / 20 555 - 0

Per **Fax** unter
+49 (0) 731 / 20 555 - 450

Öffnungszeiten

Montag - Donnerstag	08.00 bis 18.00 Uhr
Freitag	08.00 bis 16.30 Uhr

Geschäftsleitung
Peter Ringhut Dipl.-Ing. Elektrotechnik (FH) Techn. Informatik

Direkt per **E-Mail**
info@ksredv.de

Datenschutzbeauftragter (DSB)
datenschutz@ksredv.de