

**Vorbemerkung:**

Wir sind Softwarehersteller und nur nach jeweils individueller Beauftragung Auftragsdatenverarbeiter. In diesen Ausnahmefällen wird jeweils ein separater Verarbeitungsvertrag vereinbart. Die DSGVO ermöglicht uns als Kleinunternehmen erhebliche Erleichterungen bei den bürokratischen Auflagen zum Datenschutz. Das heißt aber keineswegs, dass wir die Themen Datenschutz und -sicherheit auf die leichte Schulter nehmen. Als Softwarehersteller haben wir selbstverständlich größtes Interesse an der Einhaltung von Sicherheitsstandards, da das für uns existenzielle Bedeutung hat.

<p>Organisatorische Maßnahmen</p>	<ul style="list-style-type: none"> <li>• Datenschutzbeauftragter aufgrund Unternehmensgröße nicht erforderlich</li> <li>• Wir sind ein inhabergeführtes Unternehmen und regelmäßig über datenschutzrechtliche Themen auf dem Laufenden.</li> <li>• Sicherheitsüberprüfungen müssen wir zwar nicht durchführen, haben aber die Themen Datenschutz und -sicherheit aufgrund ihrer existenziellen Bedeutung für unser Unternehmen zur Daueraufgabe gemacht.</li> <li>• Wir verwenden ausschließlich Dienstleister, die ihre Server in Deutschland betreiben.</li> </ul>
<p>Zutrittskontrolle</p>	<p>Kontrollierte Schlüsselvergabe</p>
<p>Zugangskontrolle</p>	<ul style="list-style-type: none"> <li>• Domänen abhängiger User</li> <li>• Sicherheitseinstellungen per Gruppenrichtlinie</li> <li>• komplexes Zugangspasswort             <ul style="list-style-type: none"> <li>▪ mind. 12-stellig</li> <li>▪ gemeinsame Verwendung von Zeichen aus mind. 3 der Gruppen Groß-, Kleinschreibung, Sonderzeichen und Ziffern</li> </ul> </li> <li>• Zwangsänderung nach 90 Tagen</li> <li>• Sperrung des Rechners bei Verlassen und nach Zeitablauf mit erneuter Kennworteingabe</li> <li>• Getrennte Konten von Systemadmin und Usern</li> </ul>
<p>Zugriffskontrolle</p>	<ul style="list-style-type: none"> <li>• Restriktive Zuweisung von Ordnerberechtigungen</li> <li>• Mandantenbezogene Ordnerstruktur</li> <li>• Zugriff eingeschränkt für Supportmitarbeiter</li> <li>• Mobile Datenträger dürfen nur nach Virenprüfung verwendet werden</li> <li>• Datenträger/Dokumente werden inhaus unwiederbringlich vernichtet</li> </ul>

<p>Transportsicherheit</p>	<ul style="list-style-type: none"> <li>• Software der edv-idee verwendet für den Datentransport das Tool 7-zip</li> <li>• Komprimierung der Daten</li> <li>• Verschlüsselung             <ul style="list-style-type: none"> <li>○ 256-bit AES</li> <li>○ Software der edv-idee: komplexes, 18 stelliges Passwort</li> <li>○ Individualaufträge: Passwort nach Vereinbarung</li> </ul> </li> </ul>
<p>Eingabekontrolle</p>	<ul style="list-style-type: none"> <li>• Daten werden im Original in maschinenlesbarer Form aus der jeweiligen Software angeliefert.</li> </ul>
<p>Auftragsdurchführung bei Supportabwicklung</p>	<ul style="list-style-type: none"> <li>• Eröffnung eines Supportfalles per Telefon oder eMail durch Auftraggeber</li> <li>• Auftragsdatenverarbeitung erfolgt nur, wenn eine Datenanalyse zur Ursachenlokalisierung erforderlich ist</li> <li>• Supportfunktion mit automatischer Verschlüsselung der Daten und Komprimierung (siehe Transport von Daten)</li> <li>• Datenanalyse durch Sichtung und/oder Testverarbeitung</li> <li>• Unverzügliche, endgültige Löschung der Daten nach Abschluss des Supportfalles</li> <li>• Rückmeldung per Telefon / E-Mail</li> </ul> <p>Eine Pseudonymisierung der Daten wird nicht vorgenommen, weil diese die Identifikation und Analyse der Fehler deutlich erschweren, meist sogar verhindern würde.</p>
<p>Auftragsdurchführung bei Individualaufträgen</p>	<ul style="list-style-type: none"> <li>• Auftragserteilung durch Zustellung von komprimierten und verschlüsselten Daten durch den Auftraggeber</li> <li>• Datenanalyse und Erstellung der Auswertungen durch den Auftragnehmer</li> <li>• Zustellung der Ergebnisse an den Auftraggeber</li> <li>• Löschung der Daten beim Auftragnehmer nach Auftragsabschluss spätestens nach Projektende</li> </ul>
<p>Verfügbarkeitskontrolle</p>	<ul style="list-style-type: none"> <li>• Plattenspiegelung RAID 1</li> <li>• Regelmäßige Datensicherung</li> <li>• Aktueller Virenschutz auf Server und Arbeitsplatz</li> <li>• Firewall auf Router und Workstations</li> <li>• Aktuelle Sicherheitsupdates für System und Programme</li> </ul>
<p>Trennungskontrolle</p>	<ul style="list-style-type: none"> <li>• Mandantenfähige Testsoftware</li> <li>• Getrennte Datenhaltung von             <ul style="list-style-type: none"> <li>○ Daten des Auftragnehmers</li> <li>○ Daten anderer Auftraggeber</li> <li>○ Entwicklungs-, Test- und Produktionsdaten</li> </ul> </li> </ul>