

## Unser Fokus

Als Softwarehersteller fokussieren wir uns auf die Erstellung von standardisierter Software mit einer hohen Anpassbarkeit an individuelle Sichten und Prozesse. Das sichert eine wirtschaftlich vertretbare Entwicklung, die sich in bezahlbaren Preisen niederschlägt.

Wir haben aus Sicherheitsaspekten keinen direkten Zugriff auf die installierten Programme und bieten keine regelmäßigen Dienstleistungen als Auftragsverarbeiter an. Bei Supportfällen kann ein Austausch von Dateien zur Fehleranalyse notwendig sein. Für einen sicheren Datenaustausch integrieren wir eigenentwickelte Sicherheitskomponenten, um die Angreifbarkeit durch Dritte zu minimieren.

## Sicherheit basiert auf Vertrauen

Die rechtlichen Regelungen (EU-DSGVO, BSGG und einschlägige Richtlinien) stärken die juristische Position der Softwarenutzer sowie der Betroffenen bei der Verarbeitung von personenbezogenen Daten. Wirkliche Sicherheit wird unseres Erachtens nicht nur durch Gesetze und Vereinbarungen geschaffen, sondern vor allem im Vorfeld durch die Auswahl verlässlicher Partner, denen Sie ein Höchstmaß an Vertrauen entgegenbringen können.

Kleinunternehmen können Erleichterungen bei den bürokratischen Auflagen in Anspruch nehmen. Das schafft Freiraum für kreatives Unternehmertum und ermöglichen uns auch im Wettbewerb mit großen, finanzstarken Playern die Entwicklung von innovativen Produkten. Das heißt aber keineswegs, dass wir die Themen Datenschutz, -sicherheit und Softwarequalität auf die leichte Schulter nehmen. Über 30 Jahre Erfahrungen in der Finanzbranche sind die Basis für eine hohe Priorisierung der Einhaltung von Sicherheitsstandards. Zum Schutz der Beteiligten aber auch um die Existenz unseres Unternehmens und damit die Dienstleistungen für unsere langjährigen Partnerschaften sicher zu stellen.

In diesem Sinne verstehen und leben wir die Partnerschaft mit unseren Kunden:

- I Wir verarbeiten personenbezogene Daten ausschließlich im Rahmen getroffener Vereinbarungen und nach den Weisungen unserer Kunden. Wir verwenden die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden nicht ohne Ihr Wissen erstellt. Nicht mehr benötigte Unterlagen mit personenbezogenen Daten werden nach deren Verarbeitung umgehend und datenschutzgerecht vernichtet.
- II Wir geben jedem Kunden unser Einverständnis, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang kontrollieren zu können.
- III Sicherheit geht bei uns vor Zeit. Sicherheitsaspekte spielen bei uns in allen Phasen der Softwareentwicklung eine wichtige Rolle. In der Auswahl der Tools, bei der Codierung durch die Entwickler, bei den umfangreichen Funktionstests vor der Freigabe neuer Releases, bei der Priorisierung von Erkenntnissen und Rückmeldungen aus der Praxis.
- IV Wir verpflichten Mitarbeitende und Unterauftragsnehmer auf die Einhaltung aller sicherheitsrelevanten Regelungen.
- V Wir kommunizieren transparent über Änderungen, die die Organisation und Sicherheit der Softwareentwicklung und Datenverarbeitung und die dabei angewandten Verfahren betreffen.

## Entwicklung von Software

Gute Anwendungssoftware zeichnet sich durch folgende Merkmale aus:

- ⇒ Praxisbezug
- ⇒ Anwenderfreundlichkeit
- ⇒ stabiler Einsatz in diversen IT-Umgebungen
- ⇒ professionelles Fehlermanagement für Ermittlung, Dokumentation und Behebung
- ⇒ Datenintegrität

Diese Aspekte stehen bei unserer Softwareentwicklung im Vordergrund.

Zur Sicherstellung dieser hohen Qualität haben wir für die Entwicklung und Pflege unserer Softwareprodukte folgende Anforderungen:

### 1. Organisation des Entwicklungsprozesses

- Erfassung jedes Änderungsauftrages in einem Ticketsystem
- Information des Auftraggebers über Annahme, Entscheidung und Realisierung
- Dokumentation aller Teilschritte in der Programmierung

### 2. Einsatz von professionellen Softwaretools, für

- eine versionsbezogene Dokumentation
- eine beliebige Reorganisation jedes Softwarestandes
- detaillierte, funktionsbezogene Nachvollziehbarkeit aller im Rahmen der Programmierung erforderlichen Tätigkeiten (Status, Realisierung, Qualitätssicherung, usw.)

### 3. Definition von hierarchischen Testverfahren

- Umfassender Test der Datenverarbeitung
- spezifische Funktionstests für die durchgeführten Softwareänderungen
- Funktionsfähigkeit der Software in unterschiedlichen Systemumgebungen

## Technisch organisatorische Maßnahmen

Organisatorische Maßnahmen	<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>
Zutrittskontrolle	Kontrollierte Schlüsselvergabe
Zugangskontrolle	<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>
Zugriffskontrolle	<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>
Transportsicherheit	<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>
Eingabekontrolle	<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 Arbeitsplätzen</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>