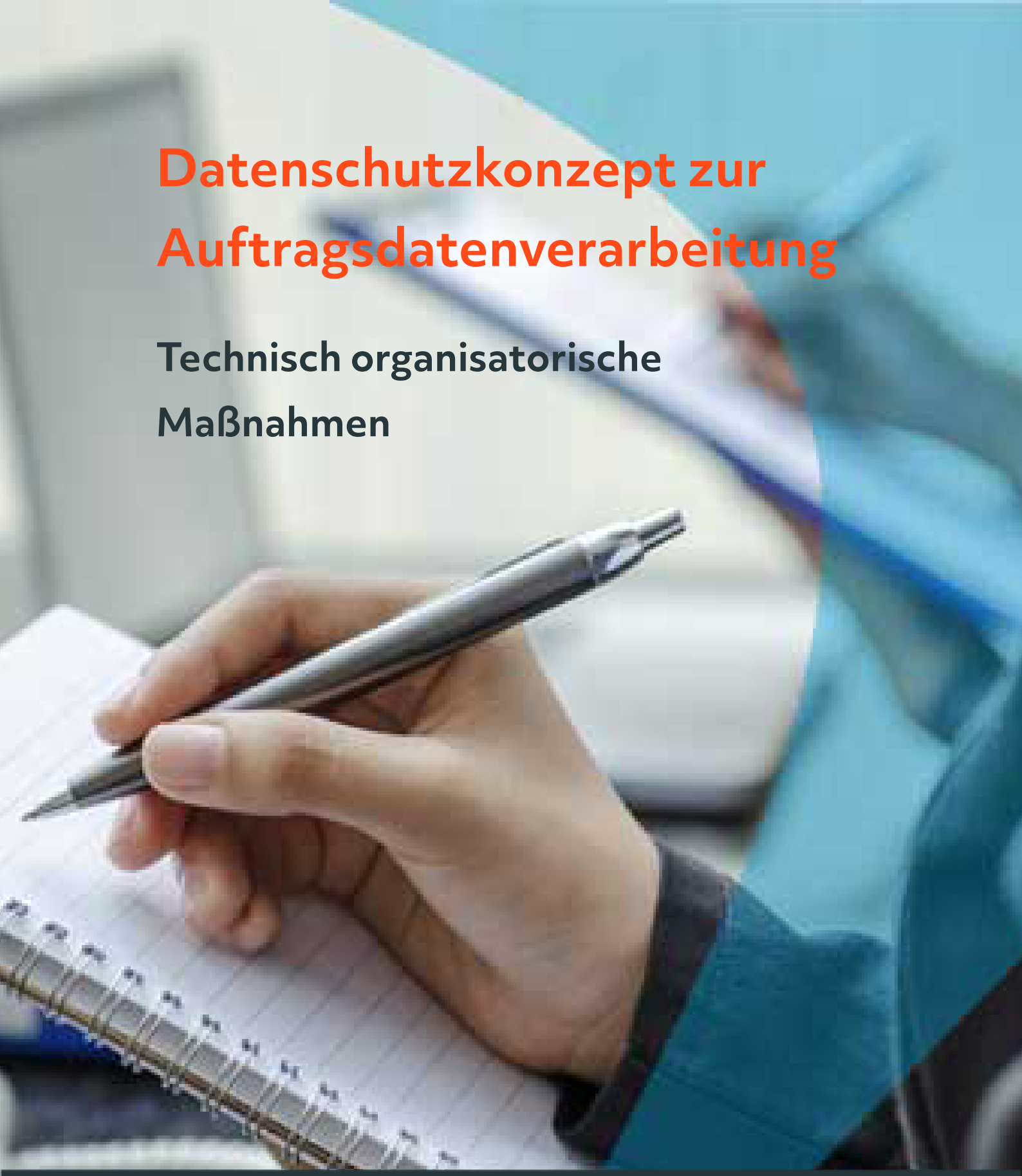
# Datenschutzkonzept zur Auftragsdatenverarbeitung

## Technisch organisatorische Maßnahmen




Softwarebüro Zauner

Softwarebüro Zauner GmbH & Co. KG
Jahnstraße 54 – 64
63150 Heusenstamm
Deutschland

Tel. +49 6104 699-170
Fax +49 6104 699-184

E-Mail office@zauner.software



Stand Mai 2022
Version 1.1

**Softwarebüro Zauner GmbH & Co.KG**
Jahnstraße 54-64
63150 Heusenstamm
**Tel.** +49 (0) 6104 699-170
**Mail** vertrieb@zauner.software

# Inhaltsverzeichnis

**1. Einleitung . . . . . 2**
**2. Rahmenbedingungen . . . . . 2**
**3. Zauner Datenschutzbeauftragter . . . . . 3**
**4. Technische und Organisatorische Maßnahmen . . . . . 3**
4.1 Zutrittskontrolle . . . . . 3
4.2 Zugangskontrolle . . . . . 4
4.3 Zugriffskontrolle . . . . . 4
4.4 Weitergabekontrolle . . . . . 5
4.5 Eingabekontrolle . . . . . 5
4.6 Auftragskontrolle . . . . . 5
4.7 Verfügbarkeitskontrolle . . . . . 5
4.8 Trennungskontrolle . . . . . 6
4.9 Benutzerverwaltung Zugriff IT System Softwarebüro Zauner GmbH & Co. KG . . . . . 6
4.10 Schutz der IT Infrastruktur der Softwarebüro Zauner GmbH und Co KG . . . . . 6
**5. Abschluss . . . . . 6**

**Softwarebüro Zauner GmbH & Co.KG**
Jahnstraße 54-64
63150 Heusenstamm
**Tel.** +49 (0) 6104 699-170
**Mail** vertrieb@zauner.software

# 1. Einleitung

Die Softwarebüro Zauner GmbH & Co. KG hat den umfassenden Datenschutz zum (Unternehmens)Ziel erklärt. Hierbei wird besonders auf den Schutz der Privatsphäre, personenbezogener Daten und Geheimhaltungsstufen Wert gelegt. Dies gilt für den Personenkreis der Kunden, Untervertragspartner, Lieferanten, Mitarbeiter und sonstigen Dienstleister. Das vorliegende Datenschutzkonzept hat zum Ziel, die bei Zauner eingesetzten Mechanismen zur Gewährleistung des Datenschutzes darzustellen, intern zu kommunizieren und als Grundlage für rechtliche Prüfungen zu dienen, z.B. für die Kunden der Softwarebüro Zauner GmbH & Co. KG im Rahmen der Auftragsverarbeitung.

Hinsichtlich der Datensicherheit sind drei Aspekte in diesem Datenschutzkonzept berücksichtigt:

1. Daten, die im Rahmen von Zauner - Serviceleistungen im Rechenzentrum der Claranet GmbH, Hanauer Landstraße 196, 60314 Frankfurt am Main verwaltet werden.
2. Daten, die als Datensicherung zur Überprüfung von Kundenanfragen Zauner zur Verfügung gestellt werden
3. Kenntnis zu Daten im Rahmen von Fernwartungs-Supportaufgaben

# 2. Rahmenbedingungen

Personenbezogene Daten werden nur verarbeitet, soweit die gesetzlichen Vorschriften dies erfordern oder der Betroffene ausdrücklich zugestimmt hat. Für die Dienstleistungen von Zauner als datenverarbeitende nicht-öffentliche Stelle hat im Sinne des Artikel 28 DSGVO dabei insbesondere die Vorschriften der Datenschutz-Grundverordnung (DSGVO) Relevanz.

Die Verarbeitung und Speicherung von Daten erfolgt im Rahmen der Erbringung der Betriebsdienst-leistungen in den Rechenzen tren der Claranet oder im Rahmen von Service Dienstleistungen (Support) in den Büroräumen von Zauner bzw. im Rahmen von Fernwartungsaktivitäten beim Kunden direkt.
Hier wird Zauner in konkreten Fällen durch die Kunden auch mit der „Datenverarbeitung im Auftrag“ gemäß DSGVO beauftragt.

Das Datenschutzkonzept der Claranet GmbH ist im Datenschutzkonzept der Softwarebüro Zauner GmbH & Co. KG berücksichtigt.

Gemäß DSGVO ist im Falle der Auftragsdatenverarbeitung grundsätzlich der Auftraggeber von Zauner für die Einhaltung des Datenschutzes gesamtverantwortlich. Die generellen Weisungen des Auftraggebers werden zum Zeitpunkt der Vertragsunterschrift in Form einer Einzelvereinbarung dokumentiert und den notwendigen Beteiligten im Rahmen einer Einweisung in der Setup-Phase bekannt gemacht.

Die Prozesse, die eine automatisierte Verarbeitung von personenbezogenen Daten zum Gegenstand haben oder bestimmungsgemäß voraussetzen, sind in entsprechenden Verfahrensbeschreibungen erfasst und werden durch den Datenschutzbeauftragten regelmäßig sowie anlassbezogen überprüft. Im Übrigen findet eine Kontrolle und Berichtigung der Verfahrensbeschreibungen bei jeder Änderung statt.

Alle Mitarbeiter des Softwarebüro Zauner GmbH & Co. KG werden bei Ihrer Einstellung zu den geltenden Bestimmungen des Datenschutzes und den internen Regelungen zur Informationssicherheit belehrt und auf das Datengeheimnis verpflichtet. Die Dokumentation der Verpflichtung erfolgt in Schriftform.

Die Erteilung von Berechtigungen erfolgt nach den Regelungen des implementierten Informationssicherheitsmanagementsystems unter Anwendung des 4-Augen-Prinzips und wird mittels Mehrfaktorenauthen-

**Softwarebüro Zauner GmbH & Co.KG**
Jahnstraße 54-64
63150 Heusenstamm
**Tel.** +49 (0) 6104 699-170
**Mail** vertrieb@zauner.software

tifizierung (Ausweis + Zutrittskarte / Token) realisiert und zyklisch kontrolliert.

# 3. Zauner Datenschutzbeauftragter

Die Softwarebüro Zauner GmbH & Co. KG hat einen Datenschutzbeauftragten zu bestellen.

Der Datenschutzbeauftragte der Softwarebüro Zauner GmbH & Co. KG ist:

msecure GmbH
Herr Götz Blechschmidt
Bajuwarenring 21
82041 Oberhaching
Tel. 089 – 7168024-0
Mail: datenschutz@zauner.software

Die Softwarebüro Zauner GmbH & Co. KG Verpflichtet die Mitarbeiter auf den Datenschutz. Der Datenschutzbeauftragte führt regelmäßig Schulungen für die Mitarbeiter durch. Die Schulungen finden regelmäßig und mindestens jährlich statt. Zu seinen Aufgaben zählen außerdem Beratung, Vorabkontrollen, Führung von Verfahrensverzeichnissen, Kontrolle der datenschutzrechtlichen Einhaltung sowie Mitwirkung beim Audit. Der Datenschutzbeauftragte ist in seiner Tätigkeit neutral, unabhängig und keinen fachlichen Weisungen der Organisation unterworfen.

# 4. Technische und Organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen werden detailliert innerhalb der kundenspezifischen Einzelvereinbarung zum Datenschutz dokumentiert und sind damit vertragswirksam.

Im Folgenden werden die unter datenschutzrechtlichen Gesichtspunkten relevanten Maßnahmen grob vorgestellt, die in Bezug auf die Betriebsleistungen der Softwarebüro Zauner GmbH & Co. KG eingesetzt werden. Eine detaillierte Beschreibung wird in der jeweiligen kundenspezifischen Einzelvereinbarung dokumentiert.

## 4.1 Zutrittskontrolle

### 4.1.1 Rechenzentrum Claranet

Die Claranet verfügt über ein elektronisches Zutrittssystem für das Rechenzentrum, separierte Bereiche des Rechenzentrums sowie die Büroräumlichkeiten. Die Zutrittsrechte werden auf den jeweiligen Zutrittskarten oder Tokens der Mitarbeiter gespeichert und sind zeitlich begrenzt. Der Zutritt zu den Räumlichkeiten der Claranet ist nur nach Klingeln und anschließender Anmeldung möglich. Der Zutritt zu den Rechenzentren, in denen sich sämtliche verarbeitenden Systeme und Speichersysteme befinden, ist physisch besonders gesichert. Zutritt wird nur autorisierten Personen gegeben.

Autorisierte Personen sind in diesem Zusammenhang die Rechenzentrumsbetreuer der Claranet sowie die autorisierten Mitarbeiter der Softwarebüro Zauner GmbH & Co. KG. L etztere aber nur in Bezug auf ihre eigenen Systeme. Die autorisierten Zauner Mitarbeiter müssen sich vor dem Zutritt zum Rechenzentrum anmelden, identifizieren und registrieren. Kunden der Claranet GmbH und der Softwarebüro Zauner GmbH & Co. KG erhalten grundsätzlich keinen Zutritt zu diesem Abschnitt.

**Softwarebüro Zauner GmbH & Co.KG**
Jahnstraße 54-64
63150 Heusenstamm
**Tel.** +49 (0) 6104 699-170
**Mail** vertrieb@zauner.software

Lieferanten, Kunden und sonstigen Dienstleistern werden nur nach Anmeldung, Identifikation und Registrierung sowie in Begleitung der Zutritt zum Rechenzentrum gewährt.

### 4.1.2 Softwarebüro Zauner GmbH & Co. KG

Der Zutritt zu den Räumlichkeiten von Zauner ist nur nach Klingeln und anschließender Anmeldung möglich.Die Arbeitsträume der Supportabteilung sowie sicherheitstechnisch relevante Bereiche der Abteilung Softwareentwicklung sind als Sicherheitsbereich deklariert und der Zutritt ist Betriebsfremden untersagt. Die Zugänge zu diesen Bereichen ist nur mittels Zugangscode möglich.

Der Aufenthalt für Gäste von Zauner ist grundsätzlich nur im Besucherbereich / Besprechungsraum zugelassen. Alle Mitarbeiter von Zauner sind hinsichtlich der Einhaltung der Regelungen zur Informationssicherheit und des Datenschutzes belehrt und verpflichtet.

## 4.2 Zugangskontrolle

### 4.2.1 Rechenzentrum Claranet

Zur Zugangskontrolle zu den Systemen sind technische und organisatorische Maßnahmen getroffen worden. Der elektronische Zugang zu Systemen über Netzwerk ist durch Firewalls und VPNs geschützt. Die administrativen Zugangsdaten zu den jeweiligen Serversystemen sind innerhalb der Claranet GmbH und der Softwarebüro Zauner GmbH & Co. KG nur den Administratoren bekannt.

Elektronischer Zugang zu Systemen ist schriftlich durch den Vorgesetzten zu beantragen und durch den Vorgesetzten des Vorgesetzten zu genehmigen. Zugang zu Systemen, die der Auftragsdatenverarbeitung unterliegen, bedarf der Genehmigung des Datenschutzbeauftragten, der diese Zugänge dokumentiert und regelmäßig auf deren Notwendigkeit validiert. Jeder Nutzer erhält einen personalisierten, passwortgeschützten Account. Das Passwort ist im Abstand von 42 Tagen zu ändern und muss eine Kombination aus Buchstaben und Ziffern beinhalten. Dabei können die letzten 5 Passworte nicht wiederverwendet werden. Zu Kundensystemen erhalten nur die Administratoren Zugriff, die den Kunden betreuen. Wird ein Passwort nicht innerhalb der Frist geändert, wird der Account gesperrt.

### 4.2.2 Softwarebüro Zauner GmbH & Co. KG

Der Zugang zu Rechentechnik und Speichermedien von Zauner ist Kunden bzw. Betriebsfremden grundsätzlich nicht gestattet. Berechtigungen von Mitarbeitern werden über die Informationssicherheits-Richtlinie zur Verwaltung von Identitäten und Zugängen geregelt. Der Zugang zu Zauner Systemen über Netzwerk ist durch Firewalls und VPNs geschützt.

## 4.3 Zugriffskontrolle

### 4.3.1 Rechenzentrum Claranet

Zu Kundensystemen erhalten nur die Administratoren Zugriff, die den Kunden betreuen. Zugriff auf Applikationen und Datenbanken wird – wo technisch realisierbar – rollenbasierend vergeben. Wo dies technisch nicht realisierbar ist, wird der Zugriff personenabhängig und individuell, je nach Aufgabenart, vergeben. Die Einräumung administrativer Privilegien auf Applikations- und Datenbankebene, die in der Verantwortung der Claranet sind, bedarf ebenfalls der schriftlichen Genehmigung des Vorgesetzten und dessen Vorgesetzten sowie der schriftlichen Genehmigung des Datenschutzbeauftragten. Eine Erweiterung der Zugriffsrechte erfordert die Zustimmung des Datenschutzbeauftragten.

### 4.3.2 Softwarebüro Zauner GmbH & Co. KG

Der Zugriff auf Rechentechnik und Speichermedien von Zauner ist Kunden bzw. Betriebsfremden grund-

**Softwarebüro Zauner GmbH & Co.KG**
Jahnstraße 54-64
63150 Heusenstamm
**Tel.** +49 (0) 6104 699-170
**Mail** vertrieb@zauner.software

sätzlich nicht gestattet.
Die Mitarbeiter des Supports sind in Rahmen Ihrer Tätigkeit für den Zugriff auf IT Systeme und Datensicherungen Ihrer Kunden autorisiert. Für die Supportunterstützung steht die Fernwartungssoftware TEAMVIEWER zur Verfügung. Diese Software gestattet einen Zugriff auf das Kundensystem erst nach Freigabe durch den Kunden und protokolliert den Ablauf der Fernwartungssitzung. Das Protokoll ist auf Verlangen des Kunden nach der Fernwartungssitzung zur Verfügung zu stellen.

Mit den Kunden können auf Basis dieses Datenschutzkonzeptes von Zauner und der Regelungen in der DSGVO Einzelvereinbarungen (Geheimhaltungs- und Datenschutzvereinbarungen) getroffen werden.

## 4.4 Weitergabekontrolle

### 4.4.1 Rechenzentrum Claranet

Außer zum Zwecke der Datensicherung erfolgt die Weitergabe personenbezogener Daten nur auf explizite Anweisung durch den Kunden (schriftlicher Change-Request). Innerhalb des Claranet-Netzwerkes und auf der Rechentechnik der Software Zauner GmbH & Co. KG werden elektronisch übertragene Daten verschlüsselt.

Die Auslagerung von Datensicherungen erfolgt über gesicherte Internetverbindungen in den Räumen der Software Zauner GmbH & Co. KG. Die Speicherung erfolgt auf transportgesicherten Medien. Diese befinden sich in einem verschlossenen Schrank. Die Schlüsselvergabe ist geregelt und auf wenige Personen begrenzt.

### 4.4.2 Softwarebüro Zauner GmbH & Co. KG

Die durch den Kunden zu Testzwecke ggf. zur Verfügung gestellten Datensicherungen werden getrennt von den eigenen Systemsicherungen auf Zauner eigenen Speichermedien gespeichert und unmittelbar nach Abschluss der Bearbeitung gelöscht.

Die Weitergabe von Kunden - Daten an Dritte außerhalb gesetzlicher Pflichten ist nur mit ausdrücklicher Zustimmung des Eigentümers der Daten gestattet.

## 4.5 Eingabekontrolle

Personenbezogene Daten im Sinne der DSGVO sind nur in den Datenbanken und Applikationen vorhanden. Zum Zwecke der Eingabekontrolle erfolgt ein entsprechendes Logging um damit die Anforderungen einer lückenlosen Vorgangsprotokollierung für jeden Einzelfall zu erfüllen.

## 4.6 Auftragskontrolle

Zur Auftragskontrolle sind die mit dem Kunden in den Einzelvereinbarungen zum Datenschutz vereinbarten Richtlinien zu befolgen. Darüber hinaus folgen weitergehende Aufträge des Kunden (z.B. Übertragung von Daten) dem Change-Request-Verfahren und sind somit schriftlich zu dokumentieren. Kenntnisse über die Nicht-Einhaltung der Vorgaben des Kunden sind dem Datenschutzbeauftragten zur Kenntnis zu bringen.

## 4.7 Verfügbarkeitskontrolle

Grundsätzlich sind die Systeme, die die Software Zauner GmbH & Co. KG im Rahmen der Auftragsverarbeitung betreut, im Rahmen des Backup-Dienstes regelmäßig zu sichern und die Konsistenz der Sicherung ist zu prüfen. Datensicherungsmedien werden in einem getrennten Gebäude aufbewahrt.

**Softwarebüro Zauner GmbH & Co.KG**
Jahnstraße 54-64
63150 Heusenstamm
**Tel.** +49 (0) 6104 699-170
**Mail** vertrieb@zauner.software

Für Festplattensysteme an Servern werden RAID-Mechanismen eingesetzt, die die Ausfallsicherheit erhöhen. Alle Systeme werden über die USV in den Rechenzentren abgesichert. Über diese Systemeinrichtungen sowie das im Rahmen des Informationssicherheitsmanagementsystems implementierte Backupkonzept gewährleistet die Softwarebüro Zauner GmbH & Co. KG, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

## 4.8 Trennungskontrolle

Im Rahmen der Trennungskontrolle gewährleistet die Softwarebüro Zauner GmbH & Co. KG durch die getrennte Aufbewahrung von Datensicherungen und Produktivdaten eine logische und physischeTrennung der Systeme.Darüber hinaus werden auch die Daten von Test- und Produktivsystemen getrennt abgelegt. Logdateien werden auf einem eigenen Log-System gespeichert. Dadurch werden zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet.

## 4.9 Benutzerverwaltung Zugriff IT System Softwarebüro Zauner GmbH & Co. KG

Benutzerkonten und deren Berechtigungen werden zentral über einen Verzeichnisdienst angelegt und verwaltet. Jedes Benutzerkonto hat eine eindeutige Zuweisung zu einer Person. Die Anlage, Änderung und Löschung von Benutzerkonten und die Zuweisung von Benutzerrechten erfolgt nach der Richtlinie zur Verwaltung von Identitäten und Zugängen. Mitarbeiter erhalten abhängig von ihrer Tätigkeit im Unternehmen ausschließlich Zugriffe, die für ihre tägliche Arbeit notwendig sind (Minimalprinzip). Nutzeraktivitäten werden protokolliert.

Jeder Benutzer erhält sein persönliches Kennwort, welches den Regeln zur Komplexitätsanforderung entspricht. Die Passwörter müssen regelmäßig geändert werden. Die Benutzerkonten und Benutzerdaten von ausgeschiedene Mitarbeiter werden unverzüglich nach Beendigung des Arbeitsverhältnisses gelöscht.

## 4.10 Schutz der IT Infrastruktur der Softwarebüro Zauner GmbH und Co. KG

Die Infrastruktur des Softwarebüros Zauner wird mittels Einsatz einer Hardwarefirewall geschützt, welche regelmäßig aktualisiert wird. Alle Dienste, welche über das Internet erreichbar sein müssen, werden in einer demilitarisierten Zone, logisch vom internen Netzwerk getrennt, betrieben. Des Weiteren sind aktuelle Anti-Virenprogramme auf allen Arbeitsstationen installiert und werden regelmäßig aktualisiert. Jeder Zugriff auf Systeme erfolgt über personalisierte Zugangsdaten und wird entsprechend protokolliert. Zum Zwecke der Eingabekontrolle erfolgt ein entsprechendes Logging um damit die Anforderungen einer lückenlosen Vorgangsprotokollierung für jeden Einzelfall zu erfüllen.

# 5. Abschluss

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit bildet das Informationssicherheits- und Datenschutzkonzept den jeweiligen Stand der Technik ab. Die Softwarebüro Zauner GmbH & Co. KG wird weitere adäquate Maßnahmen umsetzen und in weiteren Versionen dieses Konzeptes und der Dokumentation der Einzelsysteme dokumentieren. Dabei wird das jeweils zuvor gültige Sicherheitsniveau der festgelegten Maßnahmen stets weiterentwickelt und entsprechend angepasst.