Datenschutzkonzept zur Auftragsdatenverarbeitung

Technisch organisatorische Maßnahmen.

Stand: 25.05.2018

Softwarebüro Zauner GmbH & Co. KG

Rudolf-Braas-Straße 20
63150 Heusenstamm
Deutschland

Tel. +49(0)6104 699 170
Fax +49(0)6104 699 184

E-Mail info@zamik.de
Web www.zamik.de

Inhaltsverzeichnis

10 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 sz&p 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 Auftragsdatenverarbeitung.

Hinsichtlich der Datensicherheit sind drei Aspekte in diesem Datenschutzkonzept berücksichtigt:

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

20 Rahmenbedingungen

Personenbezogene Daten dürfen nur verarbeitet werden, soweit die gesetzlichen Vorschriften dies zulassen oder der Betroffene ausdrücklich zugestimmt hat. Für die Dienstleistungen der sz&p als datenverarbeitende nicht-öffentliche Stelle und als Telekommunikationsdiensteanbieter haben dabei insbesondere die Vorschriften der Datenschutz-Grundverordnung (DSGVO) datenschutzrechtliche Relevanz.

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

Das Datenschutzkonzept der Claranet GmbH ist in dem Datenschutzkonzept der Softwarebüro Zauner GmbH & Co. KG umgesetzt.

Gemäß der DSGVO ist im Falle der Auftragsdatenverarbeitung grundsätzlich der Auftraggeber der sz&p 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 im Rechenzentrum, die eine automatisierte Verarbeitung von personenbezogenen Daten zum Gegenstand haben oder bestimmungsgemäß voraussetzen, sind in entsprechenden Verfahrensbeschreibungen erfasst und werden durch den Datenschutzbeauftragten periodisch, mindestens zweimal jährlich anlassunabhängig 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 analog Bundesdatenschutzgesetz belehrt. Die Dokumentation der Belehrung erfolgt in Schriftform.

Der Prozess zur Zuteilung der Rechte zum Rechenzentrumszutritt auf den jeweiligen Zutrittskarten oder Token sieht wie folgt aus:

- Schriftliche Beantragung der Zutrittsrechte durch den Vorgesetzten des Mitarbeiters mit Begründung.
- Schriftliche Genehmigung der Rechtevergabe durch den Vorgesetzten des Vorgesetzten
- Vergabe der Zutrittsrechte.
- Die Freigabe des Zutritts zum Bereich der Auftragsdatenverarbeitung erfordert die besondere Genehmigung des Datenschutzbeauftragten.

Autorisierte Mitarbeiter der Softwarebüro Zauner GmbH & Co. KG sind:

- Herr Michael Grebe
- Herr Roman Sudhoff

30 sz&p Datenschutzbeauftragter

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

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

mecure GmbH
Herr Götz Blechschmidt
Bajuwarenring 19
82041 Oberhaching
Tel. 089 – 7168024-0
Mail: datenschutz@zamik.de

Der Datenschutzbeauftragte schult und verpflichtet die Mitarbeiter auf den 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. Die unabhängige und organisatorisch herausgehobene Stellung ist für eine wirkungsvolle Tätigkeit des Datenschutzbeauftragten von ausschlaggebender Bedeutung. Er darf bei der Wahrnehmung seiner Aufgaben nicht den Weisungen der Organisationeinheiten unterliegen, die er zu kontrollieren hat.

40 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.

40.1 Zutrittskontrolle

40.1.1 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. Letztere aber nur in Bezug auf ihre eigenen Systeme. Die autorisierten sz&p 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.

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

40.1.2 Software Büro Zauner GmbH und CO. KG

Der Zutritt zu den Räumlichkeiten des sz&p 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 der sz&p ist grundsätzlich nur im Besucherbereich / Besprechungsraum zugelassen.

Alle Mitarbeiter der sz&p sind hinsichtlich der Einhaltung des Datenschutzes belehrt. Eine Datenschutzverpflichtung analog dem Bundesdatenschutzgesetz liegt für jeden Mitarbeiter in den Personalunterlagen vor.

40.2 Zugangskontrolle

40.2.1 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.

40.2.2 Software Büro Zauner GmbH und CO. KG

Der Zugang zu Rechentechnik und Speichermedien der sz&p ist Kunden bzw. Betriebsfremden grundsätzlich nicht gestattet. Der Zugang zu sz&p Systemen über Netzwerk ist durch Firewalls und VPNs geschützt.

40.3 Zugriffskontrolle

40.3.1 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. Siehe auch

40.3.2 Software Büro Zauner GmbH und CO. KG

Der Zugriff auf Rechentechnik und Speichermedien der sz&p ist Kunden bzw. Betriebsfremden grundsätzlich 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 der sz&p und der Regelungen in der DSGVO Einzelvereinbarungen (Geheimhaltungs- und Datenschutzvereinbarungen) getroffen werden.

40.4 Weitergabekontrolle

40.4.1 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. Der Prozess zur Zuteilung eines Schlüssels zum Metallschrank sieht wie folgt aus:

- Schriftliche Beantragung des Schlüssels durch den Vorgesetzten des Mitarbeiters mit Begründung.
- Schriftliche Genehmigung der Schlüsselvergabe durch den Vorgesetzten des Vorgesetzten.
- Aushändigung des Schlüssels an den Mitarbeiter, schriftliche Empfangsbestätigung durch den Mitarbeiter.

- Die Freigabe des Zutritts zum Bereich der Auftragsdatenverarbeitung erfordert die besondere Genehmigung des Datenschutzbeauftragten.

40.4.2 Software Büro Zauner GmbH und CO. KG

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

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

40.5 Eingabekontrolle

Personenbezogene Daten im Sinne der DSGVO sind nur in den Datenbanken und Applikationen vorhanden. Zum Zwecke der Eingabekontrolle sind – falls technisch machbar – diese Komponenten so zu konfigurieren, dass ein entsprechendes Logging aktiviert ist und damit die Anforderungen einer lückenlosen Vorgangsprotokollierung für jeden Einzelfall möglich ist.

40.6 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.

40.7 Verfügbarkeitskontrolle

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

Für Festplattensysteme an Servern werden RAID-Mechanismen eingesetzt, die die Ausfallsicherheit erhöhen. Alle Systeme werden über die USVen in den Rechenzentren abgesichert. Über diese Systemeinrichtungen gewährleistet die Software Zauner GmbH & Co. KG, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

40.8 Trennungskontrolle

Im Rahmen der Trennungskontrolle gewährleistet die Software Zauner GmbH & Co. KG durch die getrennte Aufbewahrung von Datensicherungen und Produktivdaten eine logische Trennung 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.

40.9 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 kann nur durch einen Administrator von sz&p erfolgen. Ebenso verhält es sich mit der Zuweisung von Benutzerrechten. 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 Komplexitätsanforderungen (7 Zeichen Länge, Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen, keines der letzten 24 Passwörter) entsprechen muss. Die Passwörter müssen regelmäßig geändert werden. Die Benutzerkonten und Benutzerdaten von ausgeschiedene Mitarbeiter werden unverzüglich nach Beendigung des Arbeitsverhältnisses gelöscht.

40.10 Schutz der IT Infrastruktur des Softwarebüros 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, betreiben. 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.

50 Abschluss

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit spiegelt das Datenschutzkonzept, den jeweiligen Stand der Technik wieder. Die Software Zauner GmbH & Co. KG wird weitere adäquate Maßnahmen umsetzen und in weiteren Versionen dieses Konzeptes und der Dokumentation der Einzelsysteme dokumentieren. Dabei darf das jeweils zuvor gültige Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.