Dokumentation der technischen und organisatorischen Maßnahmen (TOM) zur Einhaltung des Datenschutzes bei der netzfalken GmbH

Vorbemerkung

Als Auftragsdatenverarbeiter für verschiedene Software-Anwendungen (Tierarztsoftware debevet, ERP Software debecom, Konverter Bank2Swift, Webservice-Schnittstelle shopqueue) hat die netzfalken GmbH eine besondere Verantwortung für die Daten, die Kunden der netzfalken GmbH als Anwender in den über das Internet verfügbaren Anwendungen erfassen.

Ein Verlust dieser Daten oder aber ein Zugriff auf diese Daten, der nicht vom Kunden autorisiert wurde, hätte unter Umständen weitreichende Folgen.

Diese Dokumentation beschreibt die technischen und organisatorischen Maßnahmen zur Einhaltung und Umsetzung des Datenschutzes bei der netzfalken GmbH.

Datenkategorien

Es sind zwei Kategorien von (personenbezogenen) Daten zu unterscheiden. Bei beiden Datenkategorien wird davon ausgegangen, **dass keine personenbezogenen Daten der besonderen Kategorien gem. EU DSGVO (Art. 9) verarbeitet werden.**

Kundendaten

Im Rahmen eines gültigen Nutzungsvertrages erfassen bzw. übermitteln Kunden der netzfalken GmbH **eigenverantwortlich** über SSL-gesicherte Verbindungen Daten in die unter Vorbemerkung genannten Software-Anwendungen.

Zur technischen Wartung besteht die Möglichkeit des Zugriffs auf die Kundendaten durch die netzfalken GmbH. Bei gesonderter Beauftragung durch die netzfalken GmbH bei gleichzeitiger Weitergabe entsprechender Systemkennwörter besteht diese Möglichkeit theoretisch auch für den Rechenzentrumsbetreiber, sofern dessen Hilfe für die technische Wartung unerlässlich sein sollte.

Wird in diesem Dokument von Kundendaten gesprochen, so sind die in diesem Abschnitt beschriebenen Daten gemeint. Nur die Kundendaten sind Gegenstand der Auftragsdatenverarbeitung.

Verwaltungsdaten

Alle Daten, die durch die netzfalken GmbH zur Verwaltung der Kundenbeziehung bzw. Abrechnung mit den Kunden erhoben werden und in der Regel vom Kunden selbst über SSL-gesicherte Webseiten eingeben werden, werden im folgenden Verwaltungsdaten genannt. Dies sind im Wesentlichen:

- Firmenname des Kunden inkl. Rechtsform
- Anrede, Titel, Vorname und Nachname
- Anschrift(en) des Kunden (z.B. Rechnungsanschrift, Lieferanschrift)
- bei der netzfalken GmbH beauftragte/gentuzte Software-Anwendung und Version
- Bankverbindung mit optionalem SEPA-Basismandat zur Zahlungsabwicklung
- Rechnungen und Gutschriften der netzfalken GmbH an den Kunden im PDF-Format als Druckausgabe-Datei (unstrukturiert)
- Rechnungen und Gutschriften der netzfalken GmbH an den Kunden als Datenbank-Datensätze in der Datenbank (strukturiert)

Zur technischen Wartung kann die netzfalken GmbH dem Rechenzentrumsbetreiber bei Weitergabe entsprechender Systemkennwörter oder Schlüssel Zugriff auf die Verwaltungsdaten ermöglichen falls zur Aufrechterhaltung des Systems Hilfe durch das Rechenzentrum in Anspruch genommen werden muss.

Zutrittskontrolle

Über die Zutrittskontrolle wird Unbefugten der Zutritt verwehrt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden.
Bei den Räumlichkeiten, in denen sich die Datenverarbeitungsanlagen befinden, muss unterschieden werden zwischen dem Rechenzentrum, den Geschäftsräumen der netzfalken GmbH und dem Backup-Zentrum

Rechenzentrum

Im Rechenzentrum befinden sich die Server, auf denen sowohl die Kundendaten als auch die Verwaltungsdaten zentral gespeichert und verarbeitet werden. Die Zutrittskontrolle zu den Servern ist deshalb von besonderer Bedeutung. Das Rechenzentrum wird nicht durch die netzfalken GmbH, sondern von der Host Europe GmbH betrieben, mit der ein Vertrag zur Auftragsdatenverarbeitung geschlossen wurde.

Der Zugang zum Rechenzentrum wird durch den Rechenzentrumsbetreiber kontrolliert, wobei die Zutrittskontrolle einen sehr hohen Standard erfüllt. Näheres und vor allem aktuelle Informationen zu diesen Standards finden sich auf der Webseite des Anbieters www.hosteurope.de.

Geschäftsräume der netzfalken GmbH

Mit Geschäftsräumen sind zum einen die Räumlichkeiten am Firmensitz der netzfalken GmbH in Leverkusen gemeint und zum anderen weitere Arbeitsorte der Mitarbeiter der netzfalken GmbH bspw. mobile Heimarbeitsplätze.

Sofern Mitarbeiter von außerhalb für die netzfalken GmbH tätig werden (externe Arbeitsplätze), geschieht dies über eine gesicherte VPN-Verbindung des Mitarbeiters in die Geschäftsräume der netzfalken GmbH.

Nur wenn ein solcher VPN Tunnel aufgebaut ist, können Mitarbeiter prinzipiell auf Daten in den Geschäftsräumen oder über den WAN-Anschluss mit fester IP der Geschäftsräume der netzfalken GmbH auf den Wartungszugriff der Server im Rechenzentrum zugreifen.

Ein direkter Zugriff auf die Server im Rechenzentrum von externen Arbeitsplätze ist nicht möglich.

In den Geschäftsräumen befinden sich im Regelfall keine unverschlüsselten Kundendaten oder Verwaltungsdaten.

Die Geschäftsräume verfügen größtenteils über Video- und Alarmüberwachung und werden außerhalb der Büro- und Arbeitszeiten verschlossen.

Backup-Zentrum

Das Backup-Zentrum ist ein weiteres Rechenzentrum, das geographisch getrennt ist vom Rechenzentrum, in dem die Kundendaten und Verwaltungsdatum gespeichert und verwaltet werden.

Backups werden hier lediglich in komprimierter Form und verschlüsselt gespeichert. Der Schlüssel selbst variiert und ist nur der Geschäftsführung und der Leitung der Systemadministration bei der

netzfalken GmbH bekannt. Insofern ist das Auslesen der Backupdaten durch Mitarbeiter im Backup-Zentrum ausgeschlossen.

Zugangskontrolle

Über die Zugangskontrolle wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Server im Rechenzentrum

Nur auf den Servern im Rechenzentrum sind die Kundendaten und Verwaltungsdaten zentral und unverschlüsselt gespeichert. Die Zugangskontrolle zu diesen Servern ist deshalb von besonderer Bedeutung.

Die Server im Rechenzentrum verfügen zur Administration über entsprechende System-Benutzer. Die Administration der Server erfolgt über das Internet ausschließlich über ein verschlüsseltes Protokoll (https und ssh).

Die Kennwörter und Schlüssel für diese Benutzerkonten sind nur der Geschäftsführung und der Leitung der IT-Administration der netzfalken GmbH bekannt. Mitarbeiter des Rechenzentrums werden im Bedarfsfall gesondert beauftragt (Ticket-System) und erhalten einen zeitlich begrenzten Zugriff.

Die Server und Netze im Rechenzentrum werden durch den Rechenzentrumsbetreiber durch hardwarebasierte Firewalls geschützt, die durch das Rechenzentrum stetig überwacht, aktualisiert und gewartet werden.

Die Server im Rechenzentrum selbst verfügen jeweils über eine eigene software-basierte Firewall, die durch die netzfalken GmbH administriert wird.

Beide Firewalls sind so konfiguriert, dass nur der Datenverkehr zugelassen ist, der für den Betrieb der Software-Anwendungen zwingend erforderlich ist. Des weiteren sorgt die netzfalken GmbH dafür, dass Wartungszugriffe (vor allem via ssh) auf die Server nur von dezidierten Quellen bzw. Netzen aus möglich sind.

Zugang zu anderen Datenverarbeitungsanlagen

Der Zugang zu den Rechnern in den Geschäftsräumen der netzfalken GmbH wird über Benutzerkonten kontrolliert.

Hierzu hat jeder Mitarbeiter ein eigenes passwortgeschütztes Benutzerkonto sowohl für den lokalen Rechner, als auch für die Verwaltungssoftware, mit der auf die Kundendaten (bei Aktivierung des Service-Benutzers s.u.) und Verwaltungsdaten im Rahmen des Supports kontrolliert zugegriffen werden kann (s. Zugriffskontrolle).

Kennwörter sind mindestens 12 Zeichen lang. Des weiteren gelten strikte Kennwortrichtlinien als auch die Pflicht zur Abänderung von Kennwörtern alle 6 Wochen.

Arbeitsplatzrechner sperren sich automatisch nach wenigen Minuten, sollten Mitarbeiter den Arbeitsplatz verlassen bzw. inaktiv sein.

Zugang zu dem Server im Backup-Rechenzentrum haben nur Mitglieder der Geschäftsführung sowie im Bedarfsfall die Leitung der IT-Administration.

Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Zugriff auf Kundendaten durch den Support der netzfalken GmbH

Support-Mitarbeiter haben immer nur Zugriff auf die Kundendaten, die sie im Rahmen ihrer Tätigkeit gerade benötigen. Die Möglichkeit des gleichzeitigen Zugriffs auf alle Kundendaten ist der Geschäftsführung vorbehalten.

Zur Kontrolle des Zugriffs auf die Kundendaten verfügt jeder Kunde über die Option, den Zugriff für den sogenannten (virtuellen) Service-Benutzer zu aktivieren. Dieser Service-Benutzer kann allein durch den Kunden in der Anwendungs-Software aktiviert werden. Aktiviert der Kunde in seiner Anwendung den Service-Benutzer, so kann ein Mitarbeiter der netzfalken GmbH, der ein gültiges Benutzerkonto in der Verwaltungssoftware der netzfalken GmbH hat über einen Link in der Verwaltungssoftware für die Dauer bis zur Deaktivierung des Service-Benutzers durch den Kunden (jedoch nicht länger als maximal 24 Stunden ab Aktivierung) in die Software-Anwendung des Kunden wechseln und so in der Software-Anwendung wie der Kunde arbeiten.

Zugriff, aber vor allem auch Manipulationen an Kundendaten als Service-Benutzer werden von der der netzfalken GmbH protokolliert mit dem Benutzernamen des Mitarbeiters aus dem Support der netzfalken GmbH.

Für einige eher seltene speziellere Support-Aufgaben ist es erforderlich, auf technischer Ebene auf Kundendaten zuzugreifen (z.B. zur Fehlersuche mittels Debugger). In diesem Fall meldet sich ein Mitglied der Geschäftsführung oder die Leitung der IT-Administration auf dem Server im Rechenzentrum an und stellt die Kundendaten des betroffenen Kunden dem Support-Mitarbeiter der netzfalken GmbH als lokale Kopie zur Verfügung. Die Kundendaten werden ausschließlich in passwortgeschützten und verschlüsselten Verzeichnissen auf dem Arbeitsplatzrechner des Support-Mitarbeiters gespeichert. Somit ist ein Auslesen der Daten bei Verlust der Arbeitsplatzrechner prinzipiell ausgeschlossen. Solche Tätigkeiten werden nur in den Geschäftsräumen der netzfalken GmbH durchgeführt und nicht an externen Arbeitsplätzen.

Die Mitarbeiter sind angewiesen, direkt nach Abschluss der Support-Tätigkeit die lokale Datenkopie zu löschen.

Alle Mitarbeiter der netzfalken GmbH sind hinsichtlich Datenschutz und Datensicherheit geschult und auf ihre Verschwiegenheitsverpflichtung schriftlich unterwiesen.

Zugriff auf Sicherungskopien

Sicherungskopien werden grundsätzlich mit einem gängigen und als sicher geltenden Verfahren auf den Servern im Rechenzentrum verschlüsselt. Das Kennwort zur Entschlüsselung der Sicherungskopien ist nur den Mitgliedern der Geschäftsführung und der Leitung der IT-Administration bekannt. So ist sichergestellt, dass nur befugte Personen Zugriff auf die Sicherungskopien der Kundendaten und Verwaltungsdaten haben, auch wenn unbefugte Personen Zutritt oder Zugang zu einer Sicherungskopie erlangen sollten.

Weitergabekontrolle

Die Weitergabekontrolle gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Die Weitergabekontrolle wird bei der netzfalken GmbH durch die Reduktion der Speicherung unverschlüsselte Kundendaten und Verwaltungsdaten auf die Speicherung im Rechenzentrum und die restriktive Zutritts- und Zugangskontrolle zu diesem Speicherort sichergestellt.

Das unbefugte lesen, kopieren, verändern oder entfernen von im Rechenzentrum gespeicherten Daten durch den Rechenzentrumsbetreiber ist vertraglich ausgeschlossen. Die Daten werden nur in verschlüsselter Form nach außerhalb des Rechenzentrums übertragen oder in verschlüsselter Form außerhalb des Rechenzentrums gespeichert.

Das Kennwort zur Entschlüsselung der Daten ist nur den Mitgliedern der Geschäftsführung oder der Leitung der IT-Administration bekannt, so dass eine unberechtigte Weitergabe ausgeschlossen werden kann.

Auf den Übertragungswegen selbst werden nur geschützte Datenprotokolle eingesetzt (https, ssh).

Das Rechenzentrum sichert zu, dass defekte Festplatten sicher zerstört und entsorgt werden, so dass ein nachträgliches Auslesen nicht möglich ist.

Eingabekontrolle

Die Eingabekontrolle gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die Kontrolle der Eingabe hinsichtlich der Kundendaten, übernimmt der Kunde selbst, da nur er die Kontrolle über die Zugriffe hat. Gewährt der Kunde dem Support durch Aktivierung des Service-Benutzers Zugriff, werden diese Zugriffe durch die netzfalken GmbH dokumentiert.

Zum anderen haben Kunden die Möglichkeit in ihrem Programm selbst zu sehen, welcher Benutzer zu welchem Zeitpunkt einen Datensatz (z.B. Kunde) zuletzt geändert hat.

Sollte der Kunde den begründeten Verdacht einer unerklärlichen Manipulation an seinen Kundendaten haben, so kann dies anhand der retrograden Backups (10 Tage) überprüft werden.

Auftragskontrolle

Die Auftragskontrolle stellt sicher, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Als einziger Datenverarbeiter mit möglichem Zugang zu den Daten ist der Rechenzentrumsbetreiber (Host Europe GmbH) beauftragt.

Mit dem Rechenzentrumsbetreiber besteht eine schriftliche Vereinbarung zur Auftragsdatenverarbeitung über die sichergestellt ist, dass die Daten nur entsprechend den Weisungen der netzfalken GmbH verarbeitet werden.

Eine Nutzung oder Weitergabe der Daten durch Mitarbeiter des Rechenzentrums ist vertraglich ausgeschlossen.

Support-Aufträge werden beim Rechenzentrumsbetreiber nur durch Mitarbeiter der Geschäftsführung der netzfalken GmbH oder der Leitung der IT-Administration in das Auftragssystem des Rechenzentrumsbetreibers eingestellt. Die Aufträge der netzfalken GmbH an das Rechenzentrum liegen damit schriftlich vor und können nachträglich überprüft werden.

Des weiteren erhält das Rechenzentrum nur im Rahmen einer solchen gesonderten Einzelbeauftragung Kennwörter um zuzugreifen. Daher ist ein Zugriff außerhalb einer gesonderten Einzelbeauftragung prinzipiell ausgeschlossen. Die Gültigkeit bzw. Verwendbarkeit solcher Kennwörter für das Rechenzentrum ist zeitlich auf das notwendige Maß beschränkt.

Hinweis zur Einordnung: Die Tätigkeit des Supports im Rechenzentrum vor Ort beschränkt sich normalerweise auf Einsätze hinsichtlich Defekten an der Hardware der Server oder der Netzwerkwege zu den Servern bzw. von den Server ins Internet. Insofern ist das Szenario der Weitergabe von Support-Kennwörtern an das Rechenzentrum eher theoretischer als praktischer Relevanz.

Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die Verfügbarkeit der Verwaltungsdaten als auch Kundendaten wird durch verschiedene Maßnahmen gewährleistet.

RAID-System

Die Server der netzfalken GmbH im Rechenzentrum verfügen über ein gespiegeltes Festplatten-System (mindestens RAID1). Eine defekte Festplatte kann im laufenden Betrieb getauscht werden (HOT-Plugfähig). Funktionstüchtigkeit als auch Fehlerraten der Speichermedien werden im laufenden Betrieb permanent überwacht.

Tägliches Full-Backup

Einmal täglich wird ein Full-Backup der Server durchgeführt. Die Sicherungsdaten werden komprimiert und verschlüsselt abgelegt. Aus den Sicherungsdaten könnte im Worst-Case ein Stand-By-Server voraussichtlich innerhalb von weniger als 4 Stunden wiederhergestellt und über das Internet erreichbar gemacht werden.

Transfer Backup

Nach erfolgreicher Durchführung des Fullbackup werden die verschlüsselten Sicherungsdaten in das Backup-Zentrum über gesicherte Transferprotokolle übertragen. Aus den Sicherungsdaten lässt sich das komplette Server-System samt Kundendaten und Verwaltungsdaten 14 Tage rückwirkend wiederherstellen.

Kopie der Sicherungsdaten

Optional wird in sporadischen Zeitabständen eine verschlüsselte Sicherungskopie zusätzlich in den Geschäftsräumen der netzfalken GmbH gespeichert.

Ausstattung Rechenzentrum

Im Rechenzentrum bieten vollklimatisierte Sicherheitsräume Schutz vor Gas, Wasser und Feuer. Der zusätzliche Speicherort im Backuprechenzentrum sichert darüber hinaus auch größte anzunehmende Unfälle ab.

Vorbereitung für mögliche Ausfallszenarien

Des weiteren wird die Verfügbarkeit der Systeme durch die netzfalken GmbH selbst erhöht durch

- trainierte Recovery-Szenarien
- Wiederherstellung Server aus Backup-Dateien zur Sicherstellung der Backup-Qualität in sporadischen Abständen
- Parallel-System-Betrieb mit Testdaten in weiteren Rechenzentrum, das prinzipiell mit den Kunden- und Verwaltungsdaten aus den Backups bestückt werden könnte und mittels Schwenkung des DNS-Records kurzfristig einsatzbereits wäre

- Automatische Überwachung und Monitoring der Vitalparameter: alle Server haben modernste Monitoring-Software, die rechtzeitig Defekte (RAM, Festplatten, Temperatur u.a.) als auch Kapazitätsprobleme (Datenspeicher, Auslastung) melden, bevor der Betrieb nachhaltig gestört würde.

Getrennte Verarbeitung

Die getrennte Verarbeitung gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Der getrennten Verarbeitung kommt bei der netzfalken GmbH eine besondere Bedeutung zu, da die Kundendaten vieler Kunden gleichzeitig auf einem Server verarbeitet werden. Gleichzeitig werden Vertragsdaten der netzfalken GmbH ebenfalls auf dem selben Server wie die Kundendaten oder zumindestens im gleichen Rechenzentrum gespeichert bzw. verarbeitet.

Kundendaten und Verwaltungsdaten auf Servern der netzfalken GmbH sind grundsätzlich nie in einer Datenbank gespeichert. Die verschiedenen Datenbanken sind durch verschiedene Benutzer mit sicheren Kennwörtern gesichert.

Zur Gewährleistung der getrennten Verarbeitung der Kundendaten sind die unstrukturierten Daten (z.B. PDF-Dokumente wie Rechnungen, Bilder) unterschiedlicher Kunden auf dem Server nach Verzeichnissen getrennt gespeichert, d.h. für jeden Kunden existiert ein eigenes Verzeichnis, in dem nur die Dokumente dieses einen Kunden gespeichert sind.

Datenbanken in denen Kundendaten gespeichert werden, haben ein eindeutiges und einmaliges Kennzeichen (Kunden-Attribut) in allen Datensätzen. Alle lesenden als auch schreibenden Zugriffe auf Datensätze sind in der serverseitigen Datenzugriffsschicht der Anwendungen so gestaltet, dass ein Zugriff ohne Filter-Verwendung des eindeutigen Kunden-Attributs nicht möglich ist. Somit ist prinzipiell ausgeschlossen, dass Zugriffe eines Kunden Kundendaten in Datensätzen eines anderen Kunden lesen oder verändern.

Nach dem selben Prinzip findet der Zugriff eines Kunden auf seine bei der netzfalken GmbH gespeicherte Verwaltungsdaten statt.

Nur Zugriffe die netzfalken GmbH selbst hat über ihre Verwaltungssoftware mittels Benutzer und Kennwort Zugriff auf Verwaltungsdaten ohne Verwendung des Kunden-Attribut.