1 Gewährleistung der Vertraulichkeit

(Rechtsgrundlage Art. 32 Abs. 1 Buchst. b DSGVO)

1.1 Zutrittskontrolle (kein unbefugter Zutritt zu Datenverarbeitungsanlagen)

Die Betriebsstätten des ReNoStar Firmenverbundes befinden sich innerhalb eines Bürogebäudes in einem Gewerbegebiet. Dazu zählen die Büroräume der Mitarbeiter, Serverraum, Kopierräume, Besprechungsräume, Technik-Räume, Buchhaltungs- und Personal(-archiv).

Die Türen der Ein- und Ausgänge sind Rauchschutztüren und mit Sicherheitsschlössern versehen, die von außen nur über einen Knauf mit Transponder zu öffnen sind. Diese werden videoüberwacht. Die Verhältnismäßigkeit dieser Überwachung wurde durch die Landesdatenschutzaufsicht geprüft.

Schlüssel (Transponder) haben alle Mitarbeiter und die Geschäftsleitung. Damit können Sie das elektronische Zeiterfassungssystem bedienen und haben Zutritt in das Gebäude und zu den Räumlichkeiten der ReNoStar Firmenverbundes.

Besonders sensible Räume sind der Serverraum, Technik-Raum, Buchhaltung/Personal und Räume der Geschäftsleitung. Diese sind abschließbar und die Transponder nur für das dort arbeitende Personal freigeschaltet. Die Server befinden sich in gesonderten Räumlichkeiten ohne Fenster und sind mit einer eigenen Zutrittskontrolle gesichert. Hier hat lediglich dazu autorisiertes (Netzwerk-Administratoren) Personal und die Geschäftsleitung zutritt.

Mit einer Software werden die Transponder verwaltet und die Zutrittsberechtigungen vergeben. Außerhalb der Bürozeiten sichert ein Alarmsystem die Geschäftsräume.

Besucher müssen sich generell am Empfang anmelden. Aus einem Wartebereich werden sie abgeholt. Sie dürfen sich nur in Begleitung eines Mitarbeiters und nur außerhalb sensibler Räume bewegen. Nach Abschluss des Besuches werden sie zum Empfang zurückgebracht und zum Ausgang begleitet.

1.2 Zugangskontrolle (Keine unbefugte Systembenutzung)

Alle Mitarbeiter arbeiten EDV-gestützt, entsprechend haben auch alle Mitarbeiter, die Zutritt zu den Räumen besitzen, einen EDV-Zugang. Darüber hinaus können Mitarbeiter standort-unabhängig über einen VPN-Zugang auf das System zugreifen. Der Zugang wird durch die Geschäftsleitung genehmigt und durch den Admin eingerichtet und kontrolliert. Zugriff über einen VPN-Zugang auf bestimmte Anwendungen hat auch ein Hotline-Dienstleister. Hier sind die entsprechenden Datenschutz-Vereinbarungen (anwaltliche Verschwiegenheit, Vereinbarung zur Auftragsdatenverarbeitung) mit dem Dienstleister geschlossen.

Der Zugang in das EDV-System ist nur mit Benutzerkennung und persönlichem Kennwort möglich. Das Kennwortverfahren erfordert neben einer Mindestlänge noch den Gebrauch von Sonderzeichen, Groß-/Kleinschreibung und einen vom System erzwungenen regelmäßigen Kennwortwechsel.

Zusätzlich ist das Netzwerk gegen unautorisierte Zugänge durch Firewall und Virenschutz geschützt, das auf dem jeweils aktuellen technischen Stand betrieben wird.

1.3 Zugriffskontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems)

Die Zugriffsberechtigung auf die Daten innerhalb der EDV-Systeme ist personalisiert. D.h. die Mitarbeiter haben gemäß ihren Arbeitsplatzprofilen Zugriff auf für sie relevante und zur Erfüllung ihrer Aufgaben erforderliche Ordner, Dokumente und Anwendungen. Auch wird zwischen Lese- und Schreibberechtigungen unterschieden. Darüber hinaus gehende Berechtigungen sind zu vermeiden bzw. zu entziehen. Die Zugriffsrechte werden durch die Geschäftsleitung vergeben und den EDV-Administrator verwaltet. Veränderungen werden protokolliert und Löschungen sind über die kontinuierliche Datensicherung nachvollziehbar und wiederherstellbar.

Zusätzlich sind die Daten im Netzwerk logisch segmentiert und die Zugriffe darauf ebenfalls auf dieses Konzept abgestimmt. Es gibt verschiedene Laufwerke, die für unterschiedliche inhaltliche Bereiche genutzt werden. Innerhalb der Laufwerke sind Ordnerstrukturen nach Themen oder Abteilungen angelegt. Zudem gibt es ein Warenwirtschaftssystem mit dem auch Kundenrechnungen geschrieben und die Finanzbuchhaltung abgewickelt wird. Auf Kundendaten haben Hotline, Vertrieb und Auftragskoordination Zugriff. Auf Buchhaltungsdaten die Buchhaltung und auf Personaldaten Personalverantwortliche. Das System protokolliert Veränderungen und Entfernen der Daten.

1.4 Trennungsgebot
(Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden)

Personenbezogene Daten werden projektbezogen im Warenwirtschaftssystem bzw. definierten EDV-Laufwerken bearbeitet und gespeichert.

Mit dem Warenwirtschaftssystem und der definierten Laufwerksstruktur im EDV-Netz ist die Mandantenfähigkeit gewährleistet.

Im Rahmen der Softwareentwicklung erfolgt die Verifizierung und Validierung in einer getrennten Testumgebung mit anonymisierten Datensätzen (Musteranwendungen).

Wenn Validierungen unter Anwenderbedingungen beim Kunden stattfinden, werden dazu gesonderte Vereinbarungen getroffen (Pilotkunden).

1.5 Pseudonymisierung

(Art. 32 Abs. 1 Buchst. a DSGVO; Art. 25 Abs. 1 DSGVO)

Personenbezogene Daten werden, soweit möglich, unter einem Pseudonym gespeichert. Dies betrifft insbesondere in Testumgebungen genutzte Datensätze.

2 Gewährleistung der Integrität

(Art. 32 Abs. 1 Buchst. b DSGVO)

2.1 Weitergabekontrolle
(Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)

In der Kommunikation kann eine gesicherte Kontaktaufnahme auf der Webseite der ReNoStar über das Kontaktformular via HTTPS-Verschlüsselung erfolgen.

Sofern personenbezogenen Daten im Rahmen der Leistungserbringung verwendet werden, erfolgt dies in Abstimmung mit dem Auftraggeber und in dessen Auftrag. Solche Daten werden verschlüsselt oder durch einen VPN-Tunnel übermittelt.

Bei von Kunden gewünschten Datenträgertransporten wird auf das entstehende Risiko hingewiesen und verschiedene Lösungswege vorgeschlagen. Eine Abholung der Datenträger durch eigenes Personal ist ein Weg. Ein anderer ist die Verschlüsselung und der Versand über gesicherte und nachvollziehbare Wege.

Ausgelagerte Speichermedien werden in gesicherten Bereichen gelagert. Datenträger und Papierdokumente im Eigentum des werden am Nutzungsende weisungsgemäß zurückgegeben oder vernichtet.

2.2 Eingabekontrolle
(Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)

Jeder Datenverkehr zwischen dem lokalen und externen Netz unterliegt einer automatischen Protokollierung. Die Verarbeitung, Nutzung und Speicherung ist nur bestimmten, dafür vorgesehenen Personen möglich.

Veränderungen im Warenwirtschaftssystem werden benutzerbezogen durchgeführt und protokolliert. Veränderungen können somit Nutzern zugeordnet und so nachvollzogen werden.

Auch die Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, ist für die Nutzung von Internet, Email-System und der System-Laufwerke möglich. Gemäß der internen QM-Richtlinien zum Dokumentenmanagement werden Dokumente gelenkt.

3 Gewährleistung der Verfügbarkeit und Belastbarkeit

(Rechtsgrundlage Art. 32 Abs. 1 Buchst. b DSGVO)

3.1 Verfügbarkeitskontrolle
(Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust)

Alle EDV-Systeme werden durch Full-Backup kontinuierlich gesichert. Es findet eine tägliche Vollsicherung auf einem Netzwerkspeicher statt. Eine laufende Spiegelung der Daten erfolgt über ein SAN (Storage Attached Network). Darüber hinaus gibt es eine wöchentliche Bandsicherung, die in einem Tresor außerhalb des Serverraums ausgelagert wird.

Alle Systeme (Server und Clients) des ReNoStar Firmenverbundes sind mit Virenscannern der neuesten Generation ausgestattet. Dabei werden die Signaturen automatisch aktualisiert. Gegen Feuer / Brand sind alle Bereiche mit Rauchmeldern und Feuerlöschern ausgestattet, das Personal ist darin eingewiesen. Stromausfälle werden durch mehrere unterbrechungsfreie Stromversorgungen (USV) kompensiert.

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

(Rechtsgrundlage Art. 32 Abs. 1 Buchst. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1 Datenschutz-Management

Es ist ein Datenschutzbeauftragter bestellt. Die Mitarbeiter sind im Hinblick auf Datenschutz und Datensicherheit verpflichtet. Dazu gehört auch die Kenntnis und Einhaltung der besonderen anwaltlichen und notariellen Verschwiegenheit.

Verantwortlichkeiten und Zuständigkeiten sind verbindlich geregelt. Die Umsetzung wird über ein Datenschutzmanagementsystem mit Prozessbeschreibungen, Arbeitsanweisungen, Formularen und Dienstanweisungen gesteuert. Ein Prozess zur kontinuierlichen Verbesserung ist etabliert.

4.2 Incident-Response-Management

Dokumentierte Prozesse zur Erkennung und Meldung von Sicherheitsvorfällen und Daten-Pannen sind vorhanden. Dazu gehört die Einbindung des Datenschutzbeauftragten bei solchen Vorfällen und die Dokumentation dieser in Form von festgelegten Aufzeichnungen.

Regelmäßige Aktualisierung von Firewall, Spamfilter und Virenscanner zur frühzeitigen Identifikation bzw. Abwehr möglicher sicherheitsrelevanter Vorkommnisse.

4.3 Datenschutzfreundliche Voreinstellungen

(Rechtsgrundlage. Art. 25 Abs. 2 DS-GVO)

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

4.4 Auftragskontrolle

Auftragsdatenverarbeitungen erfolgen auf Basis entsprechender Vereinbarungen nach Art. 28 DSGVO sowie nach Weisung durch den Auftraggeber. Weisungen können über jeden Kommunikationskanal an dafür bestimmte Personen beim Auftragnehmer eingehen.