ReNoStar FIRMENGRUPPE	**PB_DSM_Technische und organisatorische Maßnahmen zur Datensicherheit**

1 Prozesszuordnung:

Prozess:	**Technische und organisatorische Maßnahmen zur Auftragsdatenverarbeitung**
Geltungsbereich:	Alle erforderlichen Maßnahmen zur Datensicherheit im ReNoStar Firmenverbund
Hinweise:	Mit dieser Anweisung werden die Anforderungen gemäß § 9 BDSG umgesetzt.

2 Inhalt

3 Zutrittskontrolle zu den Geschäftsräumen

Die sicherheitsrelevanten Betriebsstätten der ReNoStar-Firmengruppe in Großwallstadt befinden sich innerhalb eines Bürogebäudes in einem Gewerbegebiet. Sie bilden darin einen in sich abgeschlossenen Bereich im 1. OG. Sämtliche Ein- und Ausgänge (inkl. Notausgänge) sind videoüberwacht und mit Sicherheitsschlössern versehen. Schlüssel (Transponder) haben nur autorisierte Mitarbeiter und die Geschäftsleitung. Die Server befinden sich in einem gesonderten Raum ohne Fenster und sind mit einer eigenen Zutrittskontrolle. Zugang haben nur die Geschäftsleitung und besonders autorisiertes Personal. 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 außerhalb sensibler Räume bewegen. Nach Abschluss des Besuches werden sie zum Empfang zurückgebracht und zum Ausgang begleitet.

4 Zugangskontrolle zum IT-System

Der Zugang in das EDV-System ist nur für Personen mit Benutzerkennung und persönlichem Passwort möglich. Sollten Zugänge von außerhalb erfolgen, geschieht dies ausschließlich über verschlüsselte Leitungen / Verbindungen. Zusätzlich ist das Netzwerk gegen unautorisierte Zugänge durch Firewalling geschützt, das auf dem jeweils aktuellen technischen Stand betrieben wird.

5 Zugriffskontrolle auf Daten

Die Zugriffsberechtigung auf die Daten innerhalb der EDV-Systeme ist personalisiert. Die Zugriffsrechte werden durch die Geschäftsleitung und den Datenschutzbeauftragten vergeben und den EDV-Administrator verwaltet. Zusätzlich sind die Daten im Netzwerk logisch segmentiert, die Zugriffe darauf ebenfalls auf dieses Konzept abgestimmt. Alte bzw. defekte Datenträger werden bis zu ihrer zertifizierten Vernichtung zugriffsgeschützt gelagert.

6 Weitergabekontrolle von Daten

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

Datenträgertransporte von Kunden werden nur in Ausnahmefällen vorgenommen und die Absicherungsmöglichkeiten (z.B. Einschreibversand) mit dem Kunden geklärt.

Werden physische Datenträger oder Papierdaten weitergegeben, werden diese eindeutig gekennzeichnet und nur durch eigenes Personal transportiert.

Ausgelagerte Speichermedien werden in gesicherten Bereichen gelagert.

Datenträger und Papierdokumente im Eigentum des Auftraggebers werden am Nutzungsende weisungsgemäß zurückgegeben oder vernichtet.

7 Eingabekontrolle zum IT-System

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

Personenbezogene Daten im Warenwirtschaftssystem sind über die personalisierten Zugriffe auf dieses System geschützt. Der Zugriff ist nachvollziehbar.

Personenbezogene Daten, die auf Laufwerken abgespeichert sind, unterliegen einer Zugriffsbeschränkung. Veränderungen sind über die Dokumenteneigenschaften rückverfolgbar.

8 Auftragskontrolle zur Datenverarbeitung

Jegliche Auftragsdatenverarbeitung erfolgt nur auf Basis entsprechender Vereinbarungen nach § 11 BDSG sowie nach Weisung durch den Auftraggeber. Weisungen können über jeden Kommunikationskanal an dafür bestimmte Personen beim Auftragnehmer eingehen.

Bei jeder Verarbeitung im Auftrag muss vorher sichergestellt, dass die Verarbeitung nur einem bestimmten Zweck dient, dieser rechtmäßig ist und wie lange die Daten beim Auftragnehmer verbleiben bzw. was danach mit ihnen zu geschehen hat (Rückgabe / Löschung etc.).

Alle beteiligten Personen werden in das Datengeheimnis nach § 5 BDSG unterwiesen und verpflichtet.

Einzelheiten sind in den als Dienstanweisungen hinterlegten Verpflichtungserklärungen definiert.

9 Verfügbarkeitskontrolle durch Datensicherung

Alle EDV-Systeme des Auftragnehmers werden durch Full-Backup kontinuierlich gesichert.

Alle Systeme (Server und Clients) der ReNoStar-Firmengruppe 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.

10 Trennungsgebot zu Daten im IT-System

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).