

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO und § 64 BDSG (neu)

1 Pseudonymisierung und Verschlüsselung

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

Die Elektronische Kommunikation per E-Mail findet nach vorheriger Angemessenheitsprüfung unter dem Einsatz von folgenden Verschlüsselungstechniken statt:

- Transportverschlüsselung
- Ende-zu-Ende Verschlüsselung oder Dateianhangverschlüsselung

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

2 Gewährleistung der Vertraulichkeit

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

2.1 Zutrittskontrolle (kein unbefugter Zutritt zu Datenverarbeitungsanlagen)

Die Betriebsstätte der Renostar GmbH & Co. KG befindet sich innerhalb eines Bürogebäudes in einem Gewerbegebiet am Betriebsstandort in Großwallstadt. Diese beinhaltet Büroräume für Mitarbeiter und Geschäftsleitung, 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 sind mit Videokameras versehen, über die, bei Bedarf, eine Überwachung stattfinden kann. Die Verhältnismäßigkeit dieser Überwachungsmaßnahmen wurde durch die Landesdatenschutzaufsicht geprüft.

Schlüssel (Transponder) haben alle Mitarbeiter und die Geschäftsleitung, diese haben damit Zutritt in das Gebäude und die Räumlichkeiten der Renostar GmbH & Co. KG.

Besonders sensible Räume sind der Serverraum, Technik-Raum, Buchhaltung/Personal und die Räume der Geschäftsleitung. Diese sind abschließbar und die Transponder nur für das dort arbeitende Personal freigeschaltet. Die Server befinden sich in Abhängigkeit von den Anwendungen in Rechenzentren an externen Standorten in Deutschland oder in gesonderten Räumlichkeiten in der Betriebsstätte der Renostar GmbH & Co. KG, ausgestaltet ohne Fenster und mit einer eigenen Zutrittskontrolle gesichert. Hier hat lediglich autorisiertes (Netzwerk-Administratoren) Personal und die Geschäftsleitung Zutritt. Mit den Rechenzentren sind entsprechende Datenschutz-Vereinbarungen geschlossen.

Mit einer Software werden die Transponder verwaltet und die Zutrittsberechtigungen vergeben.

Besucher müssen sich generell am Eingang anmelden. Sie dürfen sich nur in Begleitung von Mitarbeitern und nur außerhalb sensibler Räume bewegen. Nach Abschluss des Besuches werden sie zum Ausgang begleitet.

2.2 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 VPN- oder Cloudzugänge auf die Systeme zugreifen. Der Zugang wird durch die Geschäftsleitung genehmigt und durch die Administratoren eingerichtet und kontrolliert.

Der Zugang in das EDV-System ist nur mit Benutzererkennung 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.

2.3 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 Bereiche, Dokumente und Anwendungen. Auch wird zwischen Lese- und Schreibberechtigungen unterschieden. Die Zugriffsrechte werden durch die Geschäftsleitung vergeben und die EDV-Administratoren 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.

2.4 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).

3 Gewährleistung der Integrität

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

3.1 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 GmbH & Co. KG über das Kontakt-formular 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, wie z.B. die Abholung der Datenträger durch eigenes Personal oder 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.

3.2 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, E-Mail-System und der System-Laufwerke möglich. Gemäß der internen

QM-Richtlinien zum Dokumentenmanagement werden Dokumente gelenkt.

4 Gewährleistung der Verfügbarkeit und Belastbarkeit

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

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

Alle EDV-Systeme werden durch ein Full-Backup kontinuierlich gesichert. Die Sicherung findet auf gespiegelten Netzwerkspeichern an getrennten Standorten statt.

Stromausfälle werden durch mehrere unterbrechungsfreie Stromversorgungen (USV) kompensiert.

Alle Systeme (Server und Clients) sind mit Virensclannern der neuesten Generation ausgestattet. Dabei werden die Signaturen automatisch aktualisiert.

Gegen Feuer / Brand sind alle Bereiche in den Betriebsstätten der Renostar GmbH & Co. KG und im Rechenzentrum mit Rauchmeldern und Feuerlöschern ausgestattet, das Personal ist darin eingewiesen.

5 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)

5.1 Datenschutz-Management

Es ist eine Datenschutzbeauftragte bestellt.

Name und Kontaktmöglichkeiten sind einsehbar unter: <https://www.renostar.de/info-zur-datenerhebung>

Die Mitarbeiter sind auf Datenschutz und Datensicherheit verpflichtet. Dazu gehört auch die Kenntnis und Einhaltung der besonderen anwaltlichen und notariellen Verschwiegenheitspflichten.

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

Eine Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt.

5.2 Incident-Response-Management

Die Mitarbeiter sind auf die Erkennung und Meldung von Sicherheitsvorfällen und Daten-Pannen, auch im Hinblick auf Meldepflicht gegenüber der Aufsichtsbehörde geschult.

Es gibt eine dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen und Datenpannen unter Einbindung der Datenschutzbeauftragten.

Die Dokumentation von Sicherheitsvorfällen und Datenpannen erfolgt im Datenschutzmanagementsystem. In jedem Einzelfall erfolgt eine Nachbearbeitung.

Durch den Einsatz und die regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen werden Sicherheitsvorfälle und Datenpannen, soweit möglich, durch das Unternehmen verhindert.

Sicherheitsvorfälle, die durch böswillige äußere Einflüsse ausgelöst werden könnten, werden insbesondere verhindert durch:

- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virensclannern und regelmäßige Aktualisierung

5.3 Datenschutzfreundliche Voreinstellungen

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

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.
Eine einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen ist etabliert.

5.4 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.

Bei jeder Verarbeitung im Auftrag wird sichergestellt, dass die Verarbeitung nur einem bestimmten Zweck dient und dieser rechtmäßig ist.

Auftragsdatenverarbeiter werden nach einer vorherigen Prüfung der getroffenen Sicherheitsmaßnahmen und deren Dokumentation sorgfältig ausgewählt. Mit Auftragsverarbeitern werden entsprechende Datenschutzvereinbarungen (anwaltliche/notarielle Verschwiegenheit, Vereinbarung zur Auftragsdatenverarbeitung) geschlossen.

Auftragsverarbeiter werden nur unter folgenden Voraussetzungen tätig:

- der Auftragsverarbeiter verarbeitet nur nach schriftlicher Weisung des Unternehmens
- der Auftragsverarbeiter verpflichtet seine Mitarbeiter auf Berufs- und Datengeheimnis
- der Auftragsverarbeiter verpflichtet sich zur Bestellung eines Datenschutzbeauftragten bei Vorliegen der Bestellopflicht
- der Auftragsverarbeiter gewährt wirksame Kontrollrechte insbesondere zur Überprüfung seines Schutzniveaus
- der Auftragsverarbeiter informiert bei Einsatz weiterer Subunternehmer
- der Auftragsverarbeiter stellt die Vernichtung von Daten nach Beendigung des Auftrags sicher