Vereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen gem. Art. 28 DSGVO (Auftragsdatenverarbeitung)

zwischen dem Auftraggeber:

⌜ ⌝

⌞ ⌟

(nachstehend „AG“genannt)

und

ISN-Services KG
Richard-Wagner-Str. 6
96472 Rödental

(nachstehend zusammen „ISN“ genannt)

Präambel

Der AG hat die ISN vertraglich zur Erbringung definierter Leistungen beauftragt. Darüber liegen gesonderte Leistungsverträge vor. Bei diesen Leistungen kann die ISN auch Zugriff auf die vom AG gespeicherte oder vom AG anderweitig ISN zur Verfügung gestellte personenbezogene Daten zugreifen, so dass es sich bei der Leistung von ISN um Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO handeln kann. Zum Schutz der personenbezogenen Daten treffen die Vertragspartner die nachfolgenden Vereinbarungen zum Datenschutz.

§ 1 Datenschutz, Auftragsdatenverarbeitung

1.1 ISN beachtet das jeweils geltende Datenschutzrecht und trifft alle notwendigen organisatorischen Maßnahmen, um die Einhaltung des Datenschutzrechts zu gewährleisten.

1.2 ISN wird nur solche Mitarbeiter einsetzen, die ISN vorab auf das Datengeheimnis sowie, falls einschlägig, auf das Fernmeldegeheimnis gem. § 88 TGK und/oder das Sozialgeheimnis gem. § 35 SGB I verpflichtet hat. ISN hat die Mitarbeiter über einschlägige Strafbestimmungen, insbesondere § 203 StGB, belehrt.

1.3 Der Auftragnehmer führt im Auftrag des Auftraggebers Wartungs- und/oder Pflegearbeiten an IT-Systemen des Auftraggebers durch. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis erlangt oder personenbezogene Daten verarbeitet, um die Wartung und Pflege von IT-Systemen durchzuführen oder durchführen zu können.

§ 2 Definitionen und Festlegungen

2.1 Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist der Auftragnehmer auf Wunsch verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

2.2 Für den Fall, dass der Auftraggeber einer Berufsgeheimnispflicht i.S.d. § 203 StGB unterliegt, hat dieser Sorge dafür zu tragen, dass eine unbefugte Offenbarung i.S.d. § 203 StGB durch die Fernwartung nicht erfolgt. Der Auftragnehmer ist diesbezüglich verpflichtet, Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglicht, sondern dem Auftraggeber auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

2.3 Soweit ISN Zugriff auf personenbezogene Daten hat, der AG speichert oder das der AG anderweitig ISN zur Verfügung stellt und die ISN zur Erbringung der von ISN geschuldeten Leistungen verarbeitet oder nutzt (diese Daten werden im Folgenden die „Nutzerdaten “genannt), erfolgt dies im Auftrag und auf Weisung von AG gemäß Art. 28 DSGVO.

2.4 Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2.5 Die Nutzerdaten sind in Anlage 1 genannt.

§ 3 Weisungsgebundenheit; Erhebung, Nutzung und Verarbeitung der Daten durch ISN

3.1 ISN wird die Nutzerdaten nur im Rahmen der dokumentierten Weisungen von AG erheben, verarbeiten oder nutzen. AG wird mündliche Weisungen unverzüglich schriftlich bestätigen, E-Mail genügt. ISN wird die Nutzerdaten nur in dem Maße nutzen und verarbeiten, wie es für die Erfüllung der von ISN nach dem in der Präambel genannten Vertrag geschuldeten Leistungen erforderlich ist.

3.2 ISN wird alle technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die für ISN anwendbaren Vorschriften der DSGVO zu erfüllen, insbesondere die in Art. 32 DSGVO genannten Anforderungen.

Die konkreten Maßnahmen ergeben sich aus dem Dokument „Technische und Organisatorische Maßnahmen", das dieser Vereinbarung als Anlage 2 beigefügt ist.

§ 4 Pflichten von ISN, Rechte von AG

4.1 ISN wird AG auf schriftliches Verlangen von AG bei der Wahrung der Rechte der Betroffenen, insb. im Hinblick auf die Benachrichtigung, Auskunftserteilung sowie die Berichtigung, Sperrung oder Löschung der Nutzerdaten im Rahmen der Möglichkeiten von ISN unterstützen, insbesondere wird ISN

- angesichts der Art der Verarbeitung AG nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, der Pflicht von AG zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen, wenn AG ISN diese Anträge übermittelt und unter Zitat des entsprechenden Gesetzestexts nachweist, dass diese Anträge berechtigt sind.
- AG unter Berücksichtigung der Art der Verarbeitung und von ISN zur Verfügung stehenden Informationen unterstützen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten von AG (Sicherheit der Verarbeitung; ggf. Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde; ggf. Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person; bei voraussichtlich hohem Risiko für die Rechte und Freiheiten natürlicher Personen Datenschutz-Folgenabschätzung mit ggf. vorheriger Konsultation der Datenschutzbehörde), soweit AG gegenüber ISN nachweist, dass AG im konkreten Einzelfall, für den AG Unterstützung verlangt, derartige Pflichten hat.

4.2 ISN wird alle Nutzerdaten vertraulich behandeln und sicher verwahren. ISN darf die Nutzerdaten nicht an Dritte weitergeben, außer AG hat zuvor ausdrücklich zugestimmt. ISN gewährleistet, dass ISN die Pflichten aus Art. 28 DSGVO erfüllt. Insbesondere gewährleistet ISN, dass der Datenschutzbeauftragte von ISN, und die für ISN im Bereich Datenschutzrecht zuständigen Aufsichtsbehörden ihre gesetzlichen Aufsichts- und Kontrollrechte wahrnehmen können.

4.3 ISN ist berechtigt, für die Datenverarbeitung gemäß dieser Zusatzvereinbarung Unterauftragnehmer einzusetzen. ISN wird AG immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informieren, wodurch AG die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (siehe Anlage 3).

Soweit ISN von diesem Recht Gebrauch macht, hat ISN sicherzustellen, dass alle in dieser Vereinbarung und in Art. 28 DSGVO genannten Pflichten von ISN auch von den betreffenden Unterauftragnehmern eingehalten werden, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

4.4 ISN wird AG auf Anforderung von AG alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO beschriebenen Pflichten von ISN zur Verfügung stellen, wenn AG konkret unter Zitat der entsprechenden gesetzlichen Formulierung benennt, für welche Pflicht von ISN gem. Art 28 DSGVO AG Informationen benötigt.

4.5 Wenn ISN erfährt, dass im Verantwortungsbereich von ISN gegen geltendes Datenschutzrecht oder gegen Regelungen aus dieser Zusatzvereinbarung verstoßen worden ist, wird die ISN den AG unverzüglich darauf hinweisen.

4.6 AG darf ISN Weisungen nur im Rahmen der vertraglichen Pflichten von ISN erteilen.

4.7 Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses im Sinne des § 5 BDSG bzw. ab dem 25.05.2018 zur Wahrung der Vertraulichkeit verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

4.8 Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese auf das Datengeheimnis i.S.d. § 5 BDSG verpflichtet wurden. Ab dem 25.5.2018 wird der Auftragnehmer stattdessen die in Satz 2 genannten Personen in einer dem Art. 28 Abs. 3 lit. b) genügenden Weise zur Vertraulichkeit verpflichten, sofern diese nicht schon anderweitig einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 5 Hinweispflicht, Pflichten bei Vertragsbeendigung

5.1 ISN wird AG unverzüglich darauf hinweisen, wenn ISN der Ansicht ist, dass eine Weisung von AG gegen geltendes Datenschutzrecht verstößt.

5.2 Spätestens einen Monat nach Beendigung des Vertrags wird ISN von AG übergebene Datenträger, die Nutzerdaten enthalten, an AG zurückgeben und die bei ISN gespeicherten Nutzerdaten nach Wahl von AG entweder löschen oder zurückgeben. Dies gilt nicht, soweit ISN aufgrund Unionsrecht oder dem Recht der Mitgliedstaaten der EU zur Speicherung der personenbezogenen Daten verpflichtet ist. Im Falle einer solchen längeren gesetzlichen Aufbewahrungs- bzw. Speicherungspflicht wird ISN die betreffenden Datenträger zurück- geben und die Nutzerdaten löschen, sobald das Gesetz dies zulässt. Für Datenträger gilt, dass dieses dem Auftraggeber auszuhändigen sind. Der Auftraggeber ist selber verpflichtet, die Datenträger zu vernichten, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist vom Auftraggeber auf die Sicherheitsstufe 3 gemäß DIN 66399 nachzuweisen.

§ 6 Schlussbestimmungen

6.1 Diese Zusatzvereinbarung bedarf der Schriftform, die elektronische Form ist ausgeschlossen. Änderungen bedürfen der Schriftform, die elektronische Form wahrt die Schriftform.

6.2 Sollten Bestimmungen dieser Zusatzvereinbarung rechtsunwirksam sein oder werden, so bleiben die übrigen Bestimmungen hiervon unberührt. Die rechtsunwirksamen Bestimmungen sind von den Vertragspartnern unverzüglich durch solche Bestimmungen zu ersetzen, die dem wirtschaftlich gewollten Zweck der Vertragspartner entsprechen. Das gilt entsprechend für Lücken im jeweiligen Vertrag.

6.3 Es gilt deutsches Recht. Gerichtsstand ist der Sitz der ISN Services KG.

Ort, Datum	Unterschrift Auftraggeber	Stempel Auftraggeber

Rödental, 12.02.2025

Oliver Lukas

ISN Services KG
IT-Solution & Consulting
Richard-Wagner-Str. 6
96472 Rödental
Telefon: 09563/54893-61
Fax: 09563/54893-67
www.isn-services.de
info@isn-services.de

Ort, Datum	Unterschrift Auftragnehmer Geschäftsführung ISN-Services KG

Anlage 1 Nutzerdaten

ISN kann Zugriff auf die nachfolgend genannten Nutzerdaten erhalten:

- Kategorie betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):
  - Auftraggeber
  - Kunden des Auftraggebers
  - Mitarbeiter des Auftraggebers
  - Dienstleister des Auftraggebers

- Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 3, 4, 13, 14 und 15 DSGVO):

  - allgemeine Personendaten (Name, Geburtsdaten, Anschrift, Telefonnummer, Familienstand, Staatsangehörigkeit, E-Mail-Adresse, Krankenkassen; Beruf, Arbeitgeberdaten)
  - Kennnummern (Kundennummer, Nummer bei den Krankenkassen, sonst. Versicherungsnr.)
  - Bankdaten
  - Administrative Daten (Betriebsstättenbezogene Daten)
  - physische Merkmale (Geschlecht)
  - Onlinedaten (IP-Adresse)
  - Software Lizenzdaten, Versionsdaten
  - Hard- und Softwareinformationen

- Komplettes Benutzer-Management (User anlegen/bearbeiten/löschen, Zugriffsberechtigung im Netzwerk vergeben), umfasst auch: Dateien von Usern transferieren (z.B. bei Benutzergruppen-Wechsel) oder -bei Bedarf- individuell aus Backup wiederherstellen
- Excel-Liste über vorgenanntes Benutzer-Management pflegen (Übersicht über die User, wann welche Veränderungen durchgeführt wurden, incl. von wem diese beauftragt wurden)
- Management des Mail-Server, umfasst: • Benutzer (Mail-Konten) anlegen/bearbeiten/löschen
- Verwaltung Mail-Server im Rechenzentrum der Serverdaten (White, Grey und Blacklisten, Protokolldaten) einsehen, anlegen, bearbeiten, löschen.
- Backup-Operationen: Sicherung der Server-Systeme,Sicherung der persönlichen Dateien der User, bei Bedarf Rücksicherung einzelner Dateien bis hin zu kompletten Systemen
- Hardware-Management: mittels Total Network Inventory-Software werden die Systeme (Server, Workstations, Switche, etc.) verwaltet/katalogisiert
  - Switch-Management: Konfiguration/Administration der Switche (incl. VLANs, etc.)
- Update-Operationen: mittels eigenem System wird neue Software ausgerollt (Updates für JAVA, Firefox, Chrome, etc.)
- Telefon-/Fernwartungs-Support für User: Problem-Lösungen und Hilfestellung in gemeinsamen Sitzungen (per Fernwartung eingewählt) mit den Usern für zahlreiche Anwendungen (Abrechnungssystem, Office- Programme, diverse Windows-Anwendungen)
- System-Wartung/Fehleranalyse: routinemäßige (und bei Bedarf angeforderte) Kontrolle/Wartung aller Systeme (Server, Workstations, Switche, NAS-Systeme, etc.), Behebung von Fehlern/Probleme
- Assistenz bei der Konfiguration der Zugangsprofile und Kommunikation mit den Herstellern bzw. Koordination der Vor-Ort-Einsätze der Hersteller
- Domaindaten einsehen und bearbeiten. Daten der Internetpräsentation zugreifen, einsehen und bearbeiten.

Anlage 2 Technische und organisatorische Maßnahmen

Generelle Beschreibung

- Vorhandensein von internem IT-Sicherheitskonzept und IT-Sicherheitsrichtlinien.
- Datenverarbeitung ist in Arbeits- und Prozessbeschreibungen schriftlich geregelt.
- Fremdfirmen haben keinen Zugriff auf die Datenverarbeitung.
- Vertretungsregelung für IT-Verantwortlichen bei Urlaub oder Krankheit.
- Keine Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DSGVO.
- Verpflichtung aller Mitarbeiter nachweislich auf das Datengeheimnis sowie ggf. § 88 TKG und ggf. § 35 SGB I, Belehrung über den § 203 StGB.
- Regelmäßige Kontrolle bzgl. Einhaltung von Datenschutz- und Datensicherheitsmaßnahmen.
- Vorhandensein von Verzeichnissen von Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DSGVO, soweit eine Verpflichtung gem. Art. 30 Abs. 5 DSGVO besteht.
- Namentliche Nennung der Ansprechpartner (IT/DV) zur Klärung fachlicher, technischer und organisatorischer Fragen.
- Rechenzentrum: Host Europe GmbH, Postfach 92 02 54, 51152 Köln
- Pseudonymisierung der Daten, soweit dies unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen in Anbetracht der Verarbeitungszwecke möglich ist.
- Verschlüsselung der Daten, soweit dies unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen in Anbetracht der Verarbeitungszwecke möglich ist.

In den folgenden Abschnitten sind einige technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO konkret beschrieben:

1. Zugangskontrolle

Die Zugangskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt (physikalische Sicherheit) zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen von ISN im Einzelnen:

- Die Geschäftsräume sind nur durch Personal mit entsprechenden Transpondern oder Schlüsseln zu betreten.
- Zusätzlich werden außerhalb der Bürozeiten die einbruch- und feuerhemmende Eingangstür verschlossen.
- Ausgabe und Rückgabe von Transpondern und Schlüsseln ist geregelt durch Systemdokumentation.
- Betriebsfremde Besucher werden am Empfang begrüßt, stets von Mitarbeitern von ISN im Büro begleitet und können sich nicht unkontrolliert im Bürobereich aufhalten.

- ISN verpflichtet auch Auftragnehmer, die keinen Kontakt zur Datenverarbeitung haben (beispielsweise den Gebäudereiniger), die eigenen Mitarbeiter über den Datenschutz aufzuklären und diese aufzufordern, sich vorsichtig zu verhalten, insbesondere Schlüssel sorgfältig zu verwahren.
- Der Zutritt zu den Servern ist durch eine separaten Raum abgesichert. Die Zutrittserlaubnis ist auf das unbedingt notwendige Personal (Systemadministratoren) beschränkt. Personen, die nicht für die Wartung und den Betrieb der Server zuständig sind, erhalten keinen Zutritt zu den Servern.

2. Datenträgerkontrolle

Die Datenträgerkontrolle umfasst Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen (logische Sicherheit) durch Unbefugte verhindert wird.

Maßnahmen von ISN im Einzelnen:

- Externer Zugriff von ISN Mitarbeitern auf ISN Servern ist nur via VPN und Authentifizierung am ISN LAN möglich.
- Trennung Gast-WLAN vom Firmennetzwerk.
- ISN-WLAN wird mit WPA2 betrieben.
- Anti-Viren-Software auf allen eingesetzten IT/DV-Anlagen.
- Akten unter Verschluss. Zugang nur für berechtigte Personen.
- Der Zugang zu den IT-Systemen ist durch Zugangsberechtigungen geregelt. Eine Firewall verhindert ungewollte Zugriffe von außen.
- Werden Passwörter mehrfach fehlerhaft eingegeben, erfolgt eine Sperrung. Diese kann nur durch einen Administrator rückgängig gemacht werden.
- Die Mitarbeiter sind gehalten, Notebooks vor unberechtigtem Zugriff zu schützen und so wenig Daten wie möglich aus dem Bereich des Auftraggebers auf dem Notebook zu speichern (sondern möglichst nur innerhalb der zentralen Server von ISN).
- Wenn ein Mitarbeiter ausscheidet, gibt er die ihm zur Verfügung gestellten Geräte an die ISN zurück.

3. Speicherkontrolle

Die Speicherkontrolle umfasst Maßnahmen, mit denen die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten verhindert wird.

Maßnahmen von ISN im Einzelnen:

- Zugriffe auf die Server von ISN erfolgen durch Authentifizierung (Benutzername/Passwort) mit entsprechenden Zugriffsberechtigungen. Bei Daten von Auftraggebern wird die Zugriffsberechtigung in der Vereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen gem. Art: 28 DSGVO (Auftragsdatenverarbeitung) geregelt.
- Über Zugriffsberechtigungen wird außerdem sichergestellt, dass die Mitarbeiter nur auf die Datenbanken, Anwendungen und Daten zugreifen können, die sie für ihre Aufgabenerfüllung benötigen.

- Wenn ein Mitarbeiter ausscheidet, werden ihm die Zugriffsrechte entzogen.
- Die Datenfernübertragungssysteme von ISN sind mit Datenverschlüsselung versehen und werden auf dem jeweils aktuellen technischen Stand gehalten.
- Aufgrund der aufgeführten Maßnahmen ist es Unbefugten nicht möglich, Daten aus dem Auftraggeberbereich zu lesen, zu kopieren, zu ändern oder zu entfernen.
- Wenn ISN die Daten aus dem Auftraggeberbereich nicht mehr benötigt, werden die Datenträger nach DIN 66399 und gemäß den Bestimmungen des Datenschutzes der AG zur Vernichtung zurückgegeben. Eventuell angefertigte Kopien der Daten, die zum Zweck der Aufgabenerfüllung erstellt wurden, werden gelöscht.
- siehe auch Datenträgerkontrolle (Punkt 2) und Zugriffskontrolle (Punkt 5).

4. Benutzerkontrolle

Die Benutzerkontrolle umfasst Maßnahmen, mit denen die Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte verhindert wird.

Maßnahmen von ISN im Einzelnen:

- siehe Datenträgerkontrolle (Punkt 2) und Zugriffskontrolle (Punkt 5).

5. Zugriffskontrolle

Die Zugriffskontrolle umfasst Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Maßnahmen von ISN im Einzelnen:

- Vorhandensein eines Berechtigungskonzepts.
- Datenträgerverwaltung, Datensicherung, Verschlüsselung.
- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.
- Dokumentation von Datenträgerwechseln und Aufbewahrungsorten.
- Verbot der Nutzung privater Datenträger.
- Zugriff auf Notebooks, PC und Server von ISN nur mit Username und Passwort möglich.
- Passwörter unterliegen definierten Passwortrichtlinien (hohen Anforderungen).
- Administratoren sind für Vergabe und regelmäßige Änderung von Passwörtern verantwortlich.
- Betrieb von Arbeitsplatz-PC und Servern nur nach Anmeldung mit Benutzername und Passwort.
- Automatische Bildschirmsperre mit Passwort-Aktivierung.
- Sperrung nach mehrmaligen fehlerhaften Anmeldeversuchen.
- Löschung und Zwischenlagerung defekter Datenträger bis zur datenschutzkonformen Vernichtung.
- Vernichtung ausgedruckter Daten im Aktenvernichter.
- Umgang mit Datenträgern sowie Verwendung von USB-Sticks, PDAs, externen Festplatten, Tablets und Smartphones und anderer externer Geräte durch Arbeitsanweisung geregelt.

6. Transportkontrolle

Die Transportkontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen von ISN im Einzelnen:

- Firewall.
- Versendung personenbezogener Daten mit verschlüsselter elektronischer Verbindung.

7. Wiederherstellbarkeit

Die Wiederherstellbarkeit umfasst Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Maßnahmen von ISN im Einzelnen:

- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.
- Datenträgerverwaltung, Datensicherung.
- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.
- Dokumentation von Datenträgerwechseln und Aufbewahrungsorten.

8. Zuverlässigkeit

Die Zuverlässigkeit umfasst Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Maßnahmen von ISN im Einzelnen:

- siehe Verfügbarkeitskontrolle (Punkt 10).

9. Auftragskontrolle

Die Auftragskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen verarbeitet werden können.

Maßnahmen von ISN im Einzelnen:

- Alle ISN-Mitarbeiter sind angewiesen, nur nach den vereinbarten Vertragsinhalten zu arbeiten.
- Alle vom Auftraggeber bereit gestellten Daten verbleiben ausschließlich in der Verfügungsmacht von ISN.
- Weitergabe personenbezogener Daten erfolgt nur nach schriftlicher Einwilligung vom Auftraggeber.
- Die ISN führt Arbeiten, bei denen sie Kontakt zu personenbezogenen Daten aus dem Bereich des Auftraggebers bekommen kann oder bekommen soll, nur durch, wenn dieser diese im Einzelfall anfordert. Dies ist beispielsweise dann der Fall, wenn der Auftraggeber an die ISN einen Fehler oder ein Problem meldet. Die Mitarbeiter von ISN sind angewiesen, solche Maßnahmen vorsorglich mit dem Auftraggeber abzustimmen.
- Alle Mitarbeiter von ISN, die mit personenbezogenen Daten aus dem Bereich des Auftraggebers in Kontakt kommen können, sind schriftlich auf die Einhaltung des Datenschutzes verpflichtet. Sie sind entsprechend belehrt und angewiesen, dass sie Arbeiten gemäß dem vorstehenden Absatz nur auf Anforderung des Auftraggebers durchführen dürfen.

10. Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen von ISN im Einzelnen:

- Tägliche Datensicherung.
- Rauchverbot im Serverraum.
- Serverraum mit unterbrechungsfreier Stromversorgung, Überspannungsschutz.
- Back-Up-Verfahren für Server und Arbeitsplatz-PCs.
- Alle betroffenen Server verfügen über RAID-Systeme, welche das Verlustrisiko minimieren.
- Von einem Auftraggeber übergebene Datenträger werden unter Verschluss verwahrt.
- Virenschutzprogramme auf allen Computersystemen.
- Intrusion Detection System.
- ISN setzt eine Firewall und aktuelle Virenscanner zur Absicherung sowohl des zentralen Datenbankservers als auch des E-Mail-Servers ein. Die Virensignaturen des verwendeten Virenscanners werden täglich mehrmals aktualisiert.
- Arbeitsplatzrechner werden laufend durch aktuelle Scannerprogramme auf schadhafte Software überprüft. E-Mail-Anhänge werden auf Infizierung überwacht.
- Die Mitarbeiter sind angehalten, personenbezogene Daten, die sie auf ihren Notebooks gespeichert haben, möglichst bald auf ein zentrales System von ISN zu überspielen.

11. Trennbarkeit

Das Trennungsgebot umfasst Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen von ISN im Einzelnen:

- Es ist nicht vorgesehen, dass ISN personenbezogene Daten aus dem Bereich des Auftraggebers verarbeitet.
- Wenn Daten aus dem Bereich des Auftraggebers zum Zwecke der Fehlersuche oder deren Wiederherstellung übertragen werden, werden diese gesondert von Daten anderer Auftraggeber gespeichert.

Anlage 3 Unterauftragnehmer

Allgemein

Softwarearchitekt Mario Morgenthum	Rießberg 51	96472 Rödental