Miet- und Hosting-Bestimmungen

MAQSIMA TMS

Version 5

der Firma

MAQSIMA GmbH
Am TÜV 1, 66280 Sulzbach

im Folgenden Auftragnehmer genannt

Inhaltsverzeichnis

§ 1 Allgemein

Die nachfolgenden Vereinbarungen regeln die Bereitstellung der Software MAQSIMA TMS durch die MAQSIMA GmbH in der MAQSIMA Cloud. Der Kunde erhält die technische Möglichkeit und Berechtigung, auf die Software MAQSIMA TMS, welche auf einem Server des Unterauftragnehmers inexio Informationstechnologie und Telekommunikation KGaA gehostet wird, mittels Internet zuzugreifen und die Funktionalitäten der Software im Rahmen dieser Bestimmungen zu nutzen.

§ 2 Leistungen, Preise

Die Preise für die Nutzung der MAQSIMA Cloud können bei der MAQSIMA individuell angefragt werden. Die Leistungen sind in Anlage A beschrieben.

§ 3 Datenschutz und Datensicherheit

3.1 Beide Parteien werden die jeweils anwendbaren, insbesondere die in Deutschland gültigen datenschutzrechtlichen Bestimmungen beachten und ihre eingesetzten Beschäftigten auf das Datengeheimnis nach § 5 BDSG verpflichten, soweit diese nicht bereits allgemein entsprechend verpflichtet sind.

3.2 Die technischen und organisatorischen Maßnahmen der MAQSIMA GmbH und des Unterauftragnehmers inexio Informationstechnologie und Telekommunikation KGaA sind in Anlage B beschrieben.

§ 4 Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit sich andere Personen (z.B. Kunden des Auftraggebers) unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer diesen Antrag unverzüglich an den Auftraggeber weitergeben.

§ 5 Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach § 62 BDSG folgende Pflichten:

5.1 Die Wahrung des Datengeheimnisses entsprechend § 53 BDSG. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem

Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

5.2 Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 64 BDSG und der Anlage zu § 64 BDSG.

5.3 Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 40 BDSG. Dies gilt auch, soweit eine zuständige Behörde nach §§ 42, 43 BDSG beim Auftragnehmer ermittelt.

5.4 Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Miet- und Hostingausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

§ 6 Pflichten und Obliegenheit des Auftraggebers

Der Auftraggeber wird die ihn zur Leistungserbringung und –abwicklung treffenden Pflichten erfüllen. Der Auftraggeber wird insbesondere

6.1 alle von ihm vorgesehene Nutzer schriftlich (z.B. per E-Mail) benennen. Der Auftraggeber verpflichtet sich ferner, jede durch Organisationsveränderungen, Mitarbeiterwechsel o.ä. hervorgerufene Veränderung in der Zuordnung der Nutzer, dem Auftragnehmer schriftlich mitzuteilen;

6.2 die ihm bzw. den Nutzern zugeordneten Nutzungs- und Zugangsberechtigungen sowie Identifikations- und Authentifikations-Sicherungen vor dem Zugriff durch Dritte schützen und nicht an unberechtigte Nutzer weitergeben;

6.3 dafür Sorge tragen, dass (z.B. bei der Übernahme von Texten und Daten Dritter auf Server vom Auftragnehmer) alle gewerblichen Schutz- und Urheberrechte beachtet werden;

6.4. die erforderliche Einwilligung des jeweils Betroffenen einholen, soweit er im Rahmen der Nutzung von MAQISMA TMS personenbezogene Daten erhebt, verarbeitet oder nutzt und kein gesetzlicher Erlaubnistatbestand eingreift;

6.5 MAQSIMA TMS nicht missbräuchlich nutzen oder nutzen lassen, insbesondere keine Informationsangebote mit rechts- oder sittenwidrigen Inhalten übermitteln oder auf solche Informationen hinweisen, die der Volksverhetzung dienen, zu Straftaten

anleiten oder Gewalt verherrlichen oder verharmlosen, sexuell anstößig bzw. pornographisch sind, geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden oder in ihrem Wohl zu beeinträchtigen oder das Ansehen vom Auftragnehmer schädigen können;

6.6 den Auftragnehmer von sämtlichen Ansprüchen Dritter freistellen, die auf einer rechtswidrigen Verwendung von MAQSIMA TMS durch ihn beruhen oder mit seiner Billigung erfolgen oder die sich insb. aus datenschutzrechtlichen, urheberrechtlichen oder sonstigen rechtlichen Streitigkeiten ergeben, die mit der Nutzung von MAQSIMA TMS verbunden sind. Erkennt der Auftraggeber oder muss er erkennen, dass ein solcher Verstoß droht, besteht die Pflicht zur unverzüglichen Unterrichtung des Auftragnehmers.

§ 7 Höhere Gewalt

7.1 Der Auftragnehmer ist von der Verpflichtung zur Leistung dieser Bestimmungen befreit, wenn und soweit die Nichterfüllung von Leistungen auf das Eintreten von Umständen höherer Gewalt zurückzuführen ist.

7.2 Als Umstände höherer Gewalt gelten zum Beispiel Krieg, Streiks, Unruhen, Enteignungen, kardinale Rechtsänderungen, Sturm, Überschwemmungen und sonstige Naturkatastrophen sowie sonstige vom Auftragnehmer nicht zu vertretende Umstände, insbesondere Wassereinbrüche, Stromausfälle und Unterbrechungen oder Zerstörung datenführender Leitungen.

7.3 Auftragsnehmer und Auftraggeber haben sich wehcselseitig über den Eintritt eines Falles von höherer Gewalt unverzüglich und in schriftlicher Form in Kenntnis zu setzen.

§ 8 Laufzeit und Kündigungsfristen

8.1 Die Laufzeit der Nutzung durch den Auftraggeber beginnt mit Installation und Freischaltung von MAQSIMA TMS durch den Auftragnehmer.

8.2 Die Softwaremiete kann frühestens nach **12 Monaten Laufzeit** mit einer Frist von **drei Monaten** zum Ende eines Kalenderjahres gekündigt werden.
Der Kündigung muss zweifelsfrei zu entnehmen sein, dass die Unterzeichnung von einem – alleinvertretungsberechtigten oder zusammen mit einem weiteren gesamtvertretungsberechtigten - gesetzlichen Vertreter (z.B. Geschäftsführer, Vorstand

o.ä.), ebensolchen Prokuristen (im Sinne des § 48 HGB in Ermangelung eines die Prokura anzeigenden Zusatzes im Sinne des § 51 HGB) oder einem oder mehreren Handlungsbevollmächtigten (im Sinne des § 54 HGB in Ermangelung eines die Handlungsvollmacht anzeigenden Zusatzes im Sinne des § 57 HGB) erfolgte.

Sofern die Miete nicht fristgerecht gekündigt wird, verlängert sie sich um ein weiteres Kalenderjahr, ohne dass hierfür ein erneutes Angebot oder eine Bestellung erforderlich ist.
Die Erstellung eines formalen Angebots für die Verlängerung der Miete auf Kundenwunsch hat keinen Einfluss auf die Laufzeitverlängerung, es sei denn die Miete wurde fristgerecht gekündigt
8.3 Das Recht zur Kündigung aus wichtigem grund bleibt unberührt,

§ 9 Nutzungsrechte

Durch diese Bestimmungen werden keine Nutzungsrechte an den Betriebsdaten, die über die mit dem Auftrag definierten Zwecke hinausgehen, gewährt.

§ 10 Haftung und Schadensersatz

Im Falle von Ansprüchen Betroffener gegen den Auftraggeber wegen der Verletzung von Datenschutzbestimmungen übernimmt der Auftragnehmer die Beweislast dafür, dass der Schaden nicht Folge eines von ihm zu vertretenen Umstandes ist, soweit personenbezogene Daten des Betroffenen vom Auftragnehmer im Auftrag des Auftraggebers verarbeitet werden. Für sonstige Haftungs- und Schadensersatzansprüche gelten die gesetzlichen Bestimmungen, es sei denn, es werden gesondert vertragliche Vereinbarungen hierzu getroffen.

§ 11 Schlussbestimmungen

11.1 Der Auftraggeber kann die Rechte und Pflichten nur nach vorheriger schriftlicher Zustimmung des Auftragnehmers auf Dritte übertragen.

11.2 Den Miet- und Hostingbestimmungen liegt deutsches Recht zugrunde. Gerichtsstand ist Saarbrücken.

11.3 Im Falle der ganzen oder teilweisen Unwirksamkeit einzelner Klauseln der vorliegenden Bestimmungen sind eventuell unwirksame Bestimmungen so umzudeuten, zu ergänzen oder zu ersetzen, dass der mit der unwirksamen Bestimmung verfolgte wirtschaftliche Zweck erreicht wird. Dasselbe gilt für den Fall, dass Regelungslücken in dieser Vereinbarung vorhanden sein sollten.

§ 12 Weitere Bestimmungen

Wesentliche Bestandteile dieser Bestimmungen sind die folgenden ergänzend geltenden Anhänge:

Anhang A: Leistungspflichten des Auftragnehmers

Anhang B: Technische und organisatorische Maßnahmen des Auftragnehmers zur Einhaltung der Vorgaben des Bundesdatenschutzgesetzes

Anhang C: Technische und organisatorische Maßnahmen für eine Colocation i.S.d. Art. 25 EU-DSGVO

Anhang A:
Leistungspflichten des Auftragnehmers

1. Bereitstellung der Standardleistungen

Der Auftragnehmer stellt dem Auftraggeber die Software MAQSIMA TMS mit in Punkt 2 beschriebenen Leistungs- und Softwareumfang betriebsfähig bereit. Die Software MAQSIMA ist betriebsfähig bereitgestellt, wenn der Auftragnehmer dem Auftraggeber die Freischaltung (Zugang zur funktionsfähigen Software MAQSIMA TMS) mitgeteilt hat. Der Zugriff auf die Software MAQSIMA TMS erfolgt über Citrix Access Gateway unter https://login.die-cloud.saarland bzw. über den MAQSIMA TMS/ Web Explorer.

2. Serviceleistungs- und Funktionsumfang von MAQSIMA TMS

Funktionsumfang Software MAQSIMA TMS und Fremdprodukte:

- MS Word Viewer zur Erstellung von Ausdrucken
- Adobe Reader XI

Serviceleistungsumfang Auftragnehmer:

- Installation und Update der Software MAQSIMA TMS
- Installation und Update der Fremdprodukte
- Regelmäßig Datensicherung (s. Punkt 4)
- Bereitstellung einer Hotline bei Problemen und Fehlern (s. Punkt 8)
- Einrichtung neuer Nutzer in der Citrix Umgebung
- Versenden von E-Mails über SMTP
- Lizenzen MAQSIMA TMS (siehe gesonderten Softwarelizenzbestimmungen)

3. Zugangsberechtigung

Zugangsberechtigt zum Citrix Access Gateway unter https://login.die-cloud.saarland sind die vom Auftraggeber schriftlich gemeldeten Nutzer.
Login und Benutzerrechte der Nutzer des Citrix Access Gateway werden durch die MAQSIMA verwaltet.

Die Verwaltung der Nutzer und Berechtigungen innerhalb von MAQSIMA TMS obliegt dem Auftraggeber. Der Auftraggeber wird durch geeignete Verfahren sicherstellen, dass nur so viele Nutzer in MAQSIMA TMS angelegt werden, wie entsprechende Softwarelizenzen von MAQSIMA TMS (s. Punkt 2) vorhanden sind.

4. Datensicherung

4.1 Datensicherungskonzept

- Die für TMS relevanten Datenbanken werden nachts im Zeitraum von 01:00-03:00 Uhr gesichert.
- Die Produktivdatenbank wird täglich gesichert. Die Datensicherung liegt auf einem gesicherten Netzwerkspeicher in einem separaten Brandabschnitt des Rechenzentrums.
- Die gesicherten Daten können 14 Tage rückwirkend wieder hergestellt werden, ältere Sicherungen werden gelöscht.

4.2 Vom Leistungsumfang nicht erfasst, ist die der Einhaltung von Archivierungspflichten, z.B. handelsrechtlicher oder steuerlicher Art, dienende längerfristige Datensicherung, für die der Auftraggeber verantwortlich ist.

5. Kundenseitige Voraussetzungen für die Leistungserbringung

5.1 Der Zugriff auf MAQSIMA TMS erfolgt über Citrix Access Gateway. Es gelten die Systemvoraussetzungen in der zum Zeitpunkt der Beauftragung gültigen Revision der Systemanforderungen „QMD_PRI_Systemanforderungen_TMS_Hosting“. Die MAQSIMA passt die Systemvorraussetzungen regelmäßig aufgrund von Sicherheitsupdates oder neuen Versionen der Fremdprodukte an. Diesbezüglich informiert die MAQSIMA den Auftraggeber rechtzeitig, um den reibungslosen Zugriff zu gewährleisten.

5.2 Die Bereitstellung dieser Voraussetzungen sowie der Telekommunikationsdienste einschließlich der Übermittlungsleistungen vom Leistungsübergabepunkt bis zu den vom Auftraggeber eingesetzten Geräten sind nicht Gegenstand dieser Bestimmungen, sondern obliegen dem Auftraggeber.

5.3 Schutz vor Viren

Der Auftraggeber ist verpflichtet, vor der Versendung von Daten und Informationen diese auf Viren zu prüfen und dem Stand der Technik entsprechende Virenschutzprogramme einzusetzen.

6. Verfügbarkeit

Das System steht (sofern keine technischen Probleme oder Wartungsarbeiten anstehen) 24 Stunden tägl. zur Verfügung. Wartungsarbeiten und dadurch verursachte Ausfallzeiten, werden mit dem Kunden wie in Punkt 7 angegeben vor der Durchführung abgesprochen.

7. Geplante Nichtverfügbarkeit

Geplante Nichtverfügbarkeiten zum Zweck der Wartung, Systemaktualisierung sind mit dem Auftraggeber in Textform zu vereinbaren. Bei wichtigen Gründen wird der Auftraggeber seine Zustimmung nicht unbillig verweigern.

8. Technische Unterstützung

Bei Problemen steht dem Auftraggeber die Hotline der MAQSIMA GmbH zu den im Softwarepflegebestimmungen genannten Zeiten als Ansprechpartner zur Verfügung, außerhalb der Hotlinezeiten behalten wir uns eine Reaktionszeit von bis zu 48 Stunden vor.

Anhang B:

Technische und organisatorische Maßnahmen des Auftragnehmers zur Einhaltung der Vorgaben des Bundesdatenschutzgesetzes

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1. Zutrittskontrolle (Räume und Gebäude)

Ziel: Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.

- Zaunanlagen
- Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- Wachdienst
- Spezielle Schutzvorkehrungen und Zutrittskontrolle des Serverraums
- Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups
- Telefone, Datenverarbeitungsanlagen und Personalcomputer befinden sich in einem abgeschlossenen Bereich mit beschränktem Zugang
- Alle mobilen EDV-Geräte, die den abgeschlossenen Bereich verlassen können und auf denen Kunden-, bzw. Firmendaten gespeichert sind, sind verschlüsselt.
- Festlegung von Zugangsberechtigungen für einzelne Firmenbereiche.
- Besucherregelung (Bspw. Abholung am Eingang, Begleitung nach dem Besuch bis zum Ausgang)
- Zutrittsberechtigung für das Firmengebäude erfolgt über einen personalisierten PIN-Code.

2. Zugangskontrolle (IT-Systeme u. Anwendungen)

Ziel: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- Begrenzung der befugten Benutzer
- Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
- Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
- Zusätzlicher System-Log-In für bestimmte Anwendungen
- Firewall
- Virenscanner
- Externe Verbindung zum Firmennetzwerk ist nur über VPN möglich

- Datenverschlüsselung von kritischen Bereichen
- Höhere Schutzmaßnahmen für den Zugang zu bestimmten Bereichen

3. Zugriffskontrolle (Auf Daten und Informationen)

Ziel: Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

- Verwaltung und Dokumentation von differenzierten Berechtigungen (Profile-/Rollenkonzept)
- Funktionstrennung
- Verschiedene Netzwerksegmente
- Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
- Identifikation mit eindeutigem Benutzernamen und komplexen Passwort
- Alle mobilen EDV-Geräte und Datenträger, die den abgeschlossenen Bereich verlassen können und auf denen Kunden-, bzw. Firmendaten gespeichert sind, sind verschlüsselt
- Eine externe Verbindung zum Firmennetzwerk ist nur mit personalisiertem VPN-Zugang möglich

4. Trennbarkeit

Ziel: Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können.

- Trennung von Entwicklungs- und Produktionsumgebungen
- Trennung von Firmen- und Kundendaten
- Funktionstrennung
- Verschiedene Netzwerksegmente
- Zugriffsberechtigungen nach funktioneller Zuständigkeit
- Getrennte Datenverarbeitung durch differenzierte Zugriffsregelungen

5. Pseudonymisierung

Ziel: die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

- Personenbezogene Daten, werden an bestimmten Stellen, an denen sie nicht zur Auftragserfüllung benötigt werden, pseudonymisiert
- Von extern übermittelten Daten werden verschlüsselt übertragen und gespeichert
- Die Softwareprodukte der Fa. MAQSIMA GmbH können mit entsprechend eingestellten Systemeinstellungen Benutzerdaten in der Historie nach einer vorgegebenen Zeit ausblenden

II. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

6. Weitergabekontrolle

Ziel: Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

- Alle mobilen EDV-Geräte und Datenträger, die den abgeschlossenen Bereich verlassen können und auf denen Kunden-, bzw. Firmendaten gespeichert sind, sind verschlüsselt
- Gesicherte Datenübertragung
- Gesicherter Datentransport (z.B. SSL)
- Protokollierung von Datenübertragung oder Datentransport
- Verpackungs- und Versandvorkehrungen
- Gesichertes WLAN
- Regelung zum Umgang mit mobilen Speichermedien (z.B. Laptop)
- Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)

7. Eingabekontrolle

Ziel: Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

- Systemseitige Protokollierungen bei bestimmten Systemen vorhanden
- Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

8. Verfügbarkeitskontrolle

Ziel: Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

- Sicherheitskonzept für Software- und IT-Anwendungen
- Back-Up Verfahren
- Aufbewahrungsprozess für Back-Ups
- Redundante, örtlich getrennte Datenaufbewahrung (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
- Gewährleistung der Datenspeicherung im gesicherten Netzwerk
- Bedarfsgerechtes Einspielen von Sicherheits-Updates
- Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
- Klimatisierter Serverraum
- Virenschutz
- Firewall

- Notfallplan
- Erfolgreiche Notfallübungen

9. Wiederherstellbarkeit

Ziel: Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

- Wiederherstellungsprozess der Serverlandschaft ist etabliert und wird regelmäßig überprüft

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

10. Leitlinie(n), Richtlinien, Arbeitsanweisungen und Sicherheitskonzepte

- Firmeninterne Vorgaben entsprechend dem QM-System. Bspw.:
  - QMD_HB_DV_Organisation
  - QMD_VA_Datensicherung
  - QMD_VA_Desaster_Recovery
  - QMD_VA_Support

11. Regelmäßige Kontrollen, Dokumentation und ggf. Optimierung

- Das gesamte QM-System der MAQSIMA GmbH unterliegt einem ständigen Überwachungs- und Verbesserungsprocedere

Anhang C:

Technische und organisatorische Maßnahmen für eine Colocation i.S.d. Art. 25 EU-DSGVO

von der

inexio GmbH
Am Saaraltarm 1
66740 Saarlouis

und der

MAQSIMA GmbH
Am TÜV 1
66280 Sulzbach

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Alarmanlage
- Automatisches Zugangskontrollsystem
    - Lichtschranken / Bewegungsmelder
    - Schlüsselregelung (Schlüsselausgabe etc.)
    - Protokollierung der Besucher
    - Sorgfältige Auswahl von Wachpersonal
    - Chipkarten-/Transponder-Schließsystem
    - Manuelles Schließsystem
    - Videoüberwachung der Zugänge
    - Sorgfältige Auswahl von Reinigungspersonal
    - Schließsystem mit Codesperre

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Zuordnung von Benutzerrechten
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Schlüsselregelung (Schlüsselausgabe etc.)
- Protokollierung der Besucher
- Sorgfältige Auswahl von Wachpersonal
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Sicherheitsschlösser
- Sorgfältige Auswahl von Reinigungspersonal
- Einsatz einer Software-Firewall
- Zuordnung von Benutzerprofilen zu IT- Systemen
- Erstellen von Benutzerprofilen

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, 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.

Anzahl der Administratoren auf das „Notwendigste“ reduziert

Erstellen eines Berechtigungskonzepts Verwaltung der Rechte durch Systemadministrator

Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

Ausblenden von unbefugten Funktionen

Einsatz von Aktenvernichtern bzw. datenschutzzertifizierten Dienstleistern zur Aktenvernichtung

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger 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.

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Verschlüsselte Übermittlung von personenbezogenen Daten
- beim physischen Transport: sichere Transportbehälter/-verpackung

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle
- Benutzernamen (nicht Benutzergruppen)
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines

  Berechtigungskonzepts

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

7. Verfügbarkeitskontrolle

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

- Unterbrechungsfreie Stromversorgung (USV)
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- in Hochwassergebieten Serverräume über der Wassergrenze
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- redundante Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Notfallplans
- Serverräume nicht unter sanitären Anlagen

8. Trennungsgebot

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

- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem
- Festlegung von Datenbankrechten
- Berechtigungskonzept gem. Minimalprinzip