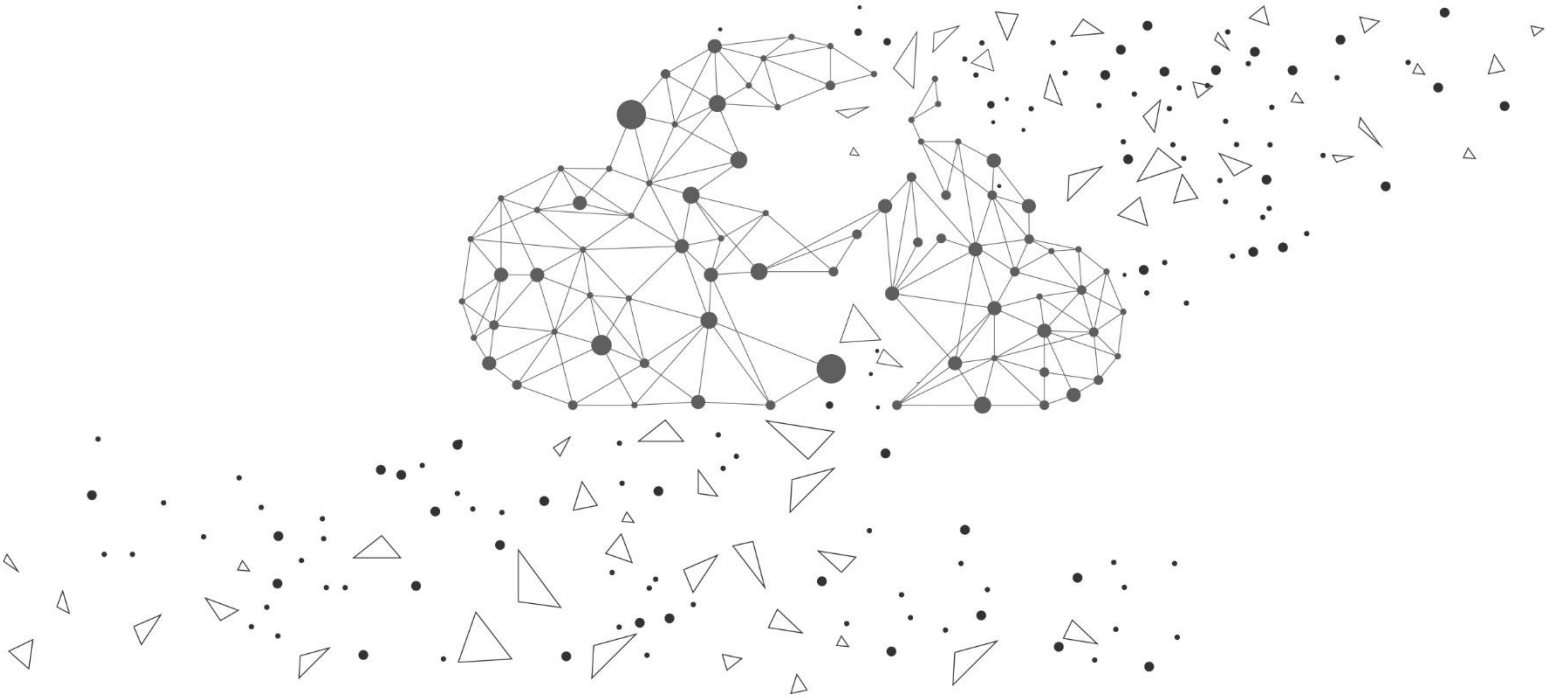

Technische und organisatorische Maßnahmen (TOMs)

nach DSGVO

DATASEC

Technische und organisatorische Maßnahmen (TOMs)

Impressum

Copyright: 2021 DATASEC information factory GmbH, Siegen
Ausgabedatum: September 2021
Autor: Steffen Billich
Version: 2.4

Inhalt

Präambel

DATASEC ist ein innovatives Unternehmen mit Schwerpunkt im Bereich des Informationsmanagements. Hierbei bietet DATASEC dem Kunden durch applikations-, standort- und plattformunabhängige Lösungen eine höchstmögliche Flexibilität. Das Leistungsportfolio reicht hierbei weit über die Entwicklung von Softwarelösungen hinaus und beinhaltet ein umfassendes Lösungsangebot, das es dem Kunden ermöglicht, Geschäftsprozesse durch modulare Serviceleistungen einfacher, effizienter und kostengünstiger zu gestalten. DATASEC hat insbesondere in den Bereichen revisionssichere Archivierung, Eingangsrechnungen, Dokumentenmanagement, Kundenmanagement, Portallösungen, Scandienstleistungen und Erfassungsdienstleistungen reichhaltige Erfahrung. DATASEC verfügt darüber hinaus über Branchenkenntnisse im Bereich der Wohnungswirtschaft.

Aus diesen Gründen ist für die DATASEC, sowohl als Auftragnehmer, als auch als Auftragsverarbeiter, der Datenschutz von besonderer Bedeutung. Daher hat die DATASEC Schutzmaßnahmen für jeglichen Umgang mit vertraulichen oder sicherungsbedürftigen Daten etabliert.

Beschreibung der technischen und organisatorischen Maßnahmen der DATASEC information factory GmbH

gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g DSGVO) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d DSGVO) gemäß Empfehlung der Aufsichtsbehörden

1. Gesetzesgrundlage

Art. 32 Abs. 1 DSGVO „Sicherheit der Verarbeitung“:

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“

Art. 30 DSGVO „Verzeichnis von Verarbeitungstätigkeiten“:

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

b) die Zwecke der Verarbeitung;

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(2) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der

Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

2. Pseudonymisierung

Die in Frage kommenden Personen können in folgende Gruppen unterteilt werden:

- Mitarbeiter des Unternehmens
- Kunden
- Lieferanten/Dienstleister

Die Pseudonymisierung der Daten ist für keine der genannten Gruppen umsetzbar. Die Daten der Personengruppen können nicht pseudonymisiert werden, da dies die Informationssicherheit und die dafür notwendigen Maßnahmen unmöglich machen würde. Allerdings findet auch für die o.g. Gruppen eine partiale Pseudonymisierung statt, da die Daten, die für eine Re-Identifikation notwendig sind, nur dem zugelassenen Personal zu Verfügung stehen.

3. Verschlüsselung

Im Unternehmen werden ausschließlich Verschlüsselungsverfahren eingesetzt, die dem aktuellen Stand der Technik entsprechen.

So ist DOKU@WEB ausschließlich über einen verschlüsselten VPN Tunnel (IPSEC, SSL) erreichbar, der in der jeweiligen Technik dem aktuellen Stand entspricht. Zusätzlich ist das Webfrontend nur über eine SSL verschlüsselte https Verbindung nach den aktuellen Standards erreichbar.

3.1 Weiterleitungskontrolle

DATASEC stellt sicher, dass personenbezogenen Daten keinesfalls bei der elektronischen Übertragung, beim Transport oder bei der Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Hierzu sind Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger sowie bei der nachträglichen Überprüfung etabliert.

Sicherung bei der elektronischen Übertragung:

- Bei der elektronischen Übertragung von Kundendaten in das DATASEC-Rechenzentrum sind alle Verbindungen über ein VPN verschlüsselt. Dies wird durch zertifizierte Linecrypts erreicht. Diese Linecrypts sind zertifiziert vom TÜV Informationstechnik und zugelassen vom Bundesamt für Sicherheit in der Informationstechnik.
- Einige Kunden haben eine eigene Leitung in das DATASEC-Rechenzentrum
- Die elektronische Übertragung von Kundendaten in das DATASEC Rechenzentrum wird protokolliert und ist laufend dokumentiert.
- Eine Übertragung von Datenbeständen des Auftraggebers (z. B. im Falle der beauftragten Datenexports erfolgt unter denselben Sicherheitsmaßnahmen und Protokollierungen wie die Datenübermittlung ins DATASEC-Rechenzentrum

- Bevor die elektronische Übertragung stattfindet, wird geprüft ob diese zulässig ist.
- Das DATASEC-Rechenzentrum wird durch ein redundantes Firewall-System, in dem nur bestimmte Ports freigeschaltet sind, geschützt.

Sicherung bei der Lagerung und Transport:

- Es besteht ausreichender Zugriffsschutz zwischen dem Speichern der Daten auf den Datenträgern und dem Transport. Die Datenträger verweilen in einem Safe, für den spezielle Zugangsberechtigungen gelten. Erst kurz vor dem Versand wird der Datenträger dem Empfang übergeben.
- Datenträger werden in Tresoren mit ausgewiesenen Berechtigungen gelagert
- Beauftragung zuverlässiger Transportunternehmen bzw. Datenabholung und Transport durch eigene Logistik.
- Verschlossene Transportboxen
- Dokumentation des Transportwegs
- Alle Datenexporte verlassen das Unternehmen (wenn möglich) verschlüsselt.
- Datenexporte werden immer durch das Vier-Augen-Prinzip geprüft

4. Gewährleistung der Vertraulichkeit

Der Zugang zu Daten im Unternehmen wird u. a. durch Gruppenrichtlinien reguliert, die dafür Sorge tragen, dass nur befugte Personen in bestimmte Bereiche zugelassen werden.

Programme und Systemkonfiguration, die für die technische Realisierung der Zuteilung der Zugänge zuständig sind, sind wiederum nur dem qualifizierten Personal zugänglich.

4.1 Zutrittskontrolle

Gemeint sind Maßnahmen, um zu verhindern, dass Unbefugte räumlichen Zutritt zu Datenverarbeitungsanlagen erhalten.

Gebäudesicherung:

- Das Gebäude ist durch eine Alarmanlage, die an einen Wachdienst gekoppelt ist, gesichert.
- Alle sich im Erdgeschoss befindlichen Fenster sind vergittert.
- Videoüberwachung erfolgt für Außen- und Eingangsbereiche sowie Flure und Datenräume
- Hochsicherheits-Schleusentür im DATASEC-Hauptrechenzentrum, die den höchsten normgerechten Sicherheitsanforderungen entspricht:
  - Einbruchhemmung bis WK 4, geprüft nach DIN V ENV 1627
  - Beschusshemmung bis FB 6 NS, geprüft nach DIN EN 1522
  - Feuerhemmung bis EI 30, geprüft nach DIN EN 1634
- Der Empfang ist wochentags durchgehend von 08.00Uhr – 17.00Uhr besetzt. Alle Personen müssen sich am Empfang anmelden. Vor Einlassgewährung wird Rücksprache mit dem Besuchten gehalten. Der Besucher wird am Empfang abgeholt. Zuvor muss der Besucher schriftlich in die DATASEC Datenschutzbestimmungen einwilligen und erhält dann einen Besucherausweis.
- Im gesamten Gebäude sind elektronische, per Chipkarte gesteuerte Türöffner verbaut. Die Chips werden per Software mit den benötigten, individuellen Berechtigungen ausgestattet. Die Berechtigungen können nur von einem zuständigen Mitarbeiter gesetzt werden. Es wird darauf geachtet, dass die jeweilige Chipkarte nur die notwendigsten Berechtigungen erhält. Die Berechtigungen sind alle elektronisch dokumentiert.

- Zusätzlich sind im gesamten Gebäude Sicherheitsschlösser verbaut. Die Schlüsselvergabe ist strikt geregelt und elektronisch dokumentiert. Schlüssel werden nur im besonderen Ausnahmefall vergeben.
- Außerhalb der Regelarbeitszeiten sind die Gebäude Innentüren per Sicherheitsschlüssel verschlossen.
- Der Zugang zum DATASEC-Rechenzentrum ist nur durch eine zusätzliche zweitürige Sicherheitsschleuse möglich. Diese wird videoüberwacht.
- Für die Datenverarbeitung von hochsensiblen Daten existieren besonders geschützte Sicherheitsräume. Diese haben zusätzliche Sicherheitsschleusen mit elektronischen Türöffnern und werden ebenfalls videoüberwacht.

4.2 Zugangskontrolle

Gemeint sind Maßnahmen, die verhindern, dass Datenverarbeitungsanlagen (PC) unbefugt genutzt werden können.

PC-Sicherung:

- Zunächst greifen alle Maßnahmen der oben beschriebenen Zutrittskontrolle
- Benutzerkennung mit Passwortvergabe. Jeder User bekommt eine eigene Benutzerkennung mit eigenem Passwort. (Netzwerk Authentifizierung)
- Automatische passwortgeschützte Bildschirm und PC-Sperre nach 5 Minuten
- Alle Mitarbeiter der DATASEC sind angewiesen worden, ihre PCs bei kurzzeitigem Verlassen des Arbeitsplatzes zu sperren. Die Einhaltung dieser Anweisung wird strengstens überwacht.
- Für die Passwortvergabe und -änderung gelten folgende Passwortrichtlinien der DATASEC:
  - Mindestens 8 Zeichen

- Das Kennwort darf nicht den Kontonamen des Benutzers oder mehr als zwei Zeichen enthalten, die nacheinander im vollständigen Namen des Benutzers vorkommen.
- Das Kennwort muss Zeichen aus drei folgenden Kategorien aufweisen:
  - Großbuchstaben (A-Z)
  - Kleinbuschstaben (a-z)
  - Zahlen (0-9)
  - Nicht alphabetische Zeichen (z.B. ! # %)
- Alle 90 Tage ein erzwungener Kennwortwechsel
- Die letzten beiden Kennwörter sind für die Verwendung gesperrt
- Sperrung des Users nach dreimaligen Fehlversuch des Anmeldens

4.3 Zugriffskontrolle

DATASEC gewährleistet, dass die zur Benutzung von DV-Anlagen berechtigten Mitarbeiter ausschließlich auf Inhalte zugreifen können, für die eine Zugriffsberechtigung besteht, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt kopiert, verändert oder gelöscht werden können.

- Innerhalb des hausinternen Firmennetzwerks werden für verschiedene User unterschiedliche Berechtigungsrollen vergeben. So wird gewährleistet, dass ein Nutzer nur auf solche Verzeichnisse Berechtigungen erhält, die er auch sehen darf.
- Zusätzlich ist das Hausnetz in differenzierte hausinterne Netzsegmente eingeteilt. User können folglich nicht auf bestimmte Server zugreifen.
- Jeder User erhält eine eindeutige Benutzerkennung in der Kombination aus Username und Passwort. Zudem ist an den Workstations standardmäßig der Bildschirmschoner mit Passworteingabe vorkonfiguriert.

- Auf jeder Workstation im Arbeitsprozess unserer Kunden ist ein Tool installiert. Darüber lassen sich alle Computerschnittstellen wie z.B. USB-Ports sowie CD-Brenner bei Bedarf sperren.
- Der Administrationsbereich der DATASEC ist durch eine weitere Sicherheitstür sowie durch die elektronische Schließanlage mit zusätzlichem elektronischem Zahlenschloss gesichert.

Das Storage System lagert in einem verschlossenen Raum. Da der Storage neben anderen Hardware-Komponenten überwacht wird, ist ein unbemerkter Zugriff auf die Medien nicht möglich. Zudem erfolgt auf täglicher Basis eine Datensynchronisation in einem Offsite Backup-Rechenzentrum mit Standort in Frankfurt.

5. Gewährleistung der Integrität

Die Integrität der Daten wird durch den Einsatz der Versionsverwaltung, Überwachung und einer Regelung der Zugänge anhand der Gruppenrichtlinien gewährleistet. Zusätzlich wird die Veränderbarkeit der Daten in bestimmten Bereichen eingeschränkt.

Die Möglichkeit der Verfälschung der im Unternehmen eingesetzten Programme wird durch eine interne, zentrale Installationsquelle, die administrativ verwaltet wird, unterbunden. Fremde Installationsquellen sind dabei administrativ sowie technisch verboten. Der Einsatz von Antivirus-Lösungen und Endpoint Protection sorgt für die zusätzliche Überprüfung der eigesetzten Programme.

Die Unveränderbarkeit der Daten wird durch strukturierte und definierte Systemrechte sichergestellt. Der Verfälschung von Hardware und sonstigen notwendigen Mitteln wird durch regemäßige Wartung, Kontrolle, permanentes Monitoring, Inventarisierung und Versionierung seitens qualifizierten Personals entgegengewirkt.

5.1 Eingabekontrolle

Maßnahmen zur Gewährleistung der nachträglichen Überprüfung und Nachvollziehbarkeit der Datenverwaltung und -pflege, insbesondere hinsichtlich Eingabe, Veränderung oder Löschung von Daten:

- Im Scanprozess wird protokolliert welcher Mitarbeiter ein Dokument bearbeitet hat.
- Sobald ein Dokument archiviert wurde, ist es nicht mehr änderbar.
- Protokollierungs- und Protokollauswertungssysteme befinden sich im Einsatz.

6. Gewährleistung der Verfügbarkeit

DATASEC stellt sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

Alle Alarmierungspläne, Handlungsanweisungen, Notfallregelungen sowie Wiederanlaufpläne sind sämtlich in einem Notfallhandbuch festgehalten. Daher werden hier nur einige wichtige Maßnahmen stichpunktartig genannt:

- Klimaanlagen im Rechenzentrum
- Sicherheitsschleuse im Rechenzentrum
- Unterbrechungsfreie Stromversorgung (USV) im Rechenzentrum
- Zugangskonzept für das Gebäude
- Backupkonzept sowie RAID Verfahren
- Datenübertragung und Datenspiegelung im gesicherten Backup-Rechenzentrum in Frankfurt am Main.
- Cluster-Betrieb und redundante Systeme
- Alle Server werden live überwacht. Zusätzlich wird per E-Mail-Benachrichtigung auf Fehler hingewiesen.

- Live-Überwachung von Feuchtigkeit, Temperatur, Wassereinbruch und Rauchentwicklung im DATASEC-Rechenzentrum
- Dieselbetriebenes Notstromaggregat (100 kVA) zur Gewährleistung einer durchgängigen Stromversorgung des gesamten Gebäudes im Falle eines Stromausfalls. Die Autonomie-Zeit des Aggregats ohne Nachtanken beträgt über 10 Stunden bei Vollauslastung.

7. Gewährleistung der Belastbarkeit der Systeme/Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Die für unternehmenskritische Prozesse eingesetzten IT-Systeme sind hochredundant ausgelegt. Der Einsatz der skalierbaren Architektur ermöglicht eine zügige Reaktion auf die Veränderung der Bedingungen. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall sind in einem internen Notfallhandbuch dokumentiert und werden regelmäßig in Testszenarien (Wiederanlauftests) überprüft.

Die regelmäßige, geografisch verteilte, redundante Datensicherung ermöglicht dem qualifizierten internen Personal eine Wiederherstellung der Daten. Die Prozedur der Wiederherstellung entspricht der üblichen in der IT-Branche Vorgehensweise.

An dieser Stelle sei auf den Notfallplan der DATASEC verwiesen.

Sämtliche Maßnahmen werden durch permanentes Monitoring überwacht und dokumentiert. Zusätzlich prüft DATASEC durch regelmäßige Wiederanlauf-Tests die ordentliche Funktionsweise der Maßnahmen.

8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Der externe Datenschutzbeauftrage Michael Letter (siehe unten) hat sich bei seiner Unternehmensdatenschutzanalyse von den oben beschriebenen Maßnahmen überzeugt. Im Zuge der Umstellung auf die EU-DSVGO wird ein regelmäßiges Datenschutzaudit durch den Datenschutzbeauftragten durchgeführt und dokumentiert.

Michael Letter
Zertifizierter externer betrieblicher Datenschutzbeauftragter (GDD)
5medical-management GmbH
Geschäftsführerin Karin Letter
HRB Nr. 15323, Amtsgericht Neuss
www.5medical-management.de
Matthiasstraße 33a
41468 Neuss

Die Einsicht der Protokolle der Hard- und Software-Komponenten der Infrastruktur gehört zu täglichen Aufgaben des zuständigen Personals. Darüber hinaus ist ein System der Benachrichtigung bzw. Alarmierung bei automatisierten Vorgängen eingerichtet. Die regelmäßigen Besprechungen und Informationsaustausch sind ein integraler Bestandteil des Arbeitsprozesses im Unternehmen.

9. Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten lediglich entsprechend den Weisungen des jeweiligen Auftraggebers verarbeitet werden.

- Schriftliche Vereinbarungen und Verträge
- Klare Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber
- Sanktionen bei Vertragsverletzung
- Festlegung der Sicherheitsmaßnahmen
- Weisungsbefugnisse eindeutig definiert
- Vor-Ort-Kontrollen
- Datenschutzvertrag gemäß den Vorgaben nach DSGVO

10. Trennungskontrolle

Es ist sicher zu stellen, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden getrennt verarbeitet werden können.

DOKU@WEB® ist von der KPMG zertifiziert worden. In diesem Zertifikat ist die getrennte Mandantenfähigkeit bescheinigt worden. Stichpunktartig hier die wichtigsten Maßnahmen:

- Trennung von Produktiv- und Testsystem
- Getrennte Ordnerstrukturen (Mandantenfähigkeit)
- Getrennte Tables in der Datenbank
- Getrennte Datenbanken
- Getrennte Server

11. Mobiles Arbeiten

Auch für das mobile Arbeiten gelten grundsätzlich die oben genannten Maßnahmen in Bezug auf die Nutzung der IT-Infrastruktur. Für abteilungsspezifische Mitarbeiter/-innen der DATASEC ist die Arbeit außerhalt der Geschäftsräume ausdrücklich gestattet bzw. zwingend erforderlich. Dies trifft nicht auf Mitarbeiter/-innen der Produktion (Scannen, Erfassen, Datenverarbeitung) zu. Das mobile Arbeiten erfolgt ausschließlich auf von DATASEC zur Verfügung gestelltem Equipment und beinhaltet lediglich Zugänge zum System. Persönliche Daten werden hingegen ausschließlich in den Räumen und auf den Servern der DATASEC verarbeitet.

Für das mobile Arbeiten gelten folgende Maßnahmen und Regelungen:

Arbeitsumgebung:

- Der Arbeitsplatz ist so zu wählen, dass keine firmenfremden Personen (Passanten, Familienmitglieder, andere Personen desselben Haushalts sowie Besucher) einen Blick auf das Endgerät (Notebook, Mobiltelefon) oder in die Papierunterlagen werfen können
- Es gilt eine Clean-Desk-Policy am Ende des Arbeitstages
- Es werden Sichtschutzfolien angeboten, wenn dies erforderlich ist
- Fenster werden in Erdgeschossräumen bei Verlassen des mobilen Arbeitsplatzes immer geschlossen.
- Sperrung des Notebooks bei Verlassen des mobilen Arbeitsplatzes
- Es ist darauf zu achten, dass Telefongespräche nicht von unbefugten Personen mitgehört werden.

Genutzte Hardware:

- Der Einsatz von Privatgeräten zur Datenverarbeitung ist grundsätzlich untersagt.
- Dienstliche Notebooks und Smartphones werden gestellt.
- Dienstlich zur Verfügung gestellte Geräte werden auch beim mobilen Arbeiten nicht für private Zwecke genutzt
- Für die Nutzung der dienstlichen Endgeräte kommen verschlüsselte Remoteverbindungen (VPN-Tunnel) zu Terminalservern im firmeneigenen Rechenzentrum zum Einsatz.
- Die lokale Speicherung von Daten auf den dienstlichen Notebooks ist nicht gestattet.
- Eine Weiterleitung von dienstlichen E-Mails an private E-Mail-Konten ist untersagt.

Umgang mit Papierdokumenten:

- In der Regel wird beim mobilen Arbeiten nicht mit Papierdokumenten gearbeitet.