Datenschutz und Datensicherheit bei der Know How! AG Leinfelden-Echterdingen

Know How! AG

Magellanstraße 1
70771 Leinfelden-Echterdingen

Deutschland

Datum: März 2023

Anzahl der Seiten: 11

Inhaltsverzeichnis

1. Grundlagen

1.1. Vorbemerkung

Dieses Dokument wird bei Auftragsvergaben, in denen die Know How! AG als Dienstleister und damit als Auftragnehmer agiert, dem Auftraggeber zur Verfügung gestellt, um zum einen die von der Know How! AG angebotenen Leistungen im Hinblick auf die technisch-organisatorischen Maßnahmen gemäß Art. 32 DSGVO zu beschreiben, zum anderen um einen Prüfungsmaßstab in Bezug auf die technisch-organisatorischen Maßnahmen klar zu definieren. Die hierin enthaltenen Informationen sind als vertraulich klassifiziert und dürfen ohne die schriftliche Genehmigung der Know How! AG keinem Dritten zugänglich gemacht werden.

1.2. Ziel dieses Dokuments

Die vorliegenden Informationen zum Thema Datenschutz und Datensicherheit bei der Know How! AG geben einen Überblick über die Grundbausteine des Datenschutz- und Sicherheitskonzepts und erläutern die technischen und organisatorischen Maßnahmen sowie die Kontrollaktivitäten nach Art. 32 Abs. 1 DSGVO im Hinblick auf die von der Know How! AG angebotenen Services. Bei der Zurverfügungstellung dieser Dokumentation vor Auftragsvergabe an den Auftraggeber sollen diejenigen Services außen vor bleiben, die für das Auftragsverhältnis nicht relevant sind.

Detailliertere Beschreibungen einzelner Maßnahmen sind den entsprechenden Richtlinien und Verarbeitungsübersichten zu entnehmen. Besonderheiten und Abweichungen, die ein spezielles Auftragsverhältnis betreffen, sind als Abweichung der bereits bestehenden Maßnahmen individuell zu verhandeln und jeweils Bestandteil des Vertrages und eines ggf. zugehörigen Datenschutzrahmenvertrages.

1.3. Unternehmensbeschreibung

Die Know How! AG bietet ganzheitliche Weiterbildungslösungen für Unternehmen aus allen Branchen an. Die Learning Spezialisten betrachten dabei alle Stufen des Lernens und können durch ihre Konzepte die Produktivität und Leistungsfähigkeit der Mitarbeiter steigern. Unter dem Motto „we enable people“ befähigt die Know How! AG dazu, Wissen neu zu erlernen, effizient anzuwenden, zu erweitern und zu teilen. Dabei fest im Blick: die Bedürfnisse des Marktes und die Trends der Branche. So bietet die Know How! AG Lösungen mit Mehrwert an. Das Methodenspektrum von Lernsoftware über Performance Support und praxisorientierten Präsenzseminare bis hin zu Customized E-Learnings ist dafür die optimale Voraussetzung.

Die Know How! AG ist seit 1992 als inhabergeführtes Unternehmen am Markt und beschäftigt derzeit 100 Mitarbeiter.

1.4. Ansprechpartner

1.4.1. IT + Informationssicherheit

Herr Marcus Krupka, IT-Leiter

1.4.2. Datenschutzbeauftragte

Jens Kränke
c/o LEXDATA Consulting GmbH
Bösinghovener Str. 98
40668 Meerbusch

Telefon: +49 2159 / 922 53 74
E-Mail: post@lexdata.de

2. Organisationskontrolle

Werden Daten automatisiert verarbeitet oder genutzt, ist die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

2.1. Gesetzliche Grundlagen

Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gelten die Vorschriften des Bundesdatenschutzgesetzes (BDSG) gemäß § 1 Abs. 1. Insbesondere sind für die Datenverarbeitung im Auftrag durch die Know How! AG folgende Regelungen zu beachten:

- Art. 37 DSGVO Benennung eines Datenschutzbeauftragten
- Art. 38 DSGVO Stellung des Datenschutzbeauftragten
- Art. 39 DSGVO Aufgaben des Datenschutzbeauftragten
- Art. 29 DSGVO Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters
- Art. 32 DSGVO Sicherheit der Verarbeitung, technische und organisatorische Maßnahmen
- Art. 28 DSGVO Auftragsverarbeiter
- Art. 31 DSGVO Zusammenarbeit mit der Aufsichtsbehörde
- Art. 83 DSGVO Geldbußen
- Art. 84 DSGVO Sanktionen

2.2. Beauftragte/r für den Datenschutz

Gemäß Art. 37 DSGVO hat die Know How! AG eine/n betriebliche/n Datenschutzbeauftragte/n zu bestellen. Die Aufgabe des betrieblichen Datenschutzbeauftragten wird für die Know How! AG durch Jens Kränke wahrgenommen. Herr Kränke übt für die Know How! AG die Aufgaben des betrieblichen Datenschutzbeauftragten gemäß Art. 37-39 DSGVO aus und gewährleistet eine umfassende Unterstützung in allen rechtlichen, technischen und organisatorischen Fragen und Maßnahmen.

2.3. Formale Voraussetzungen und Maßnahmen

2.3.1. Interne Verarbeitungsübersicht

Im Rahmen der Verarbeitung personenbezogener Daten stellt die Know How! AG der Datenschutzbeauftragten eine Übersicht über die Verarbeitungen personenbezogener Daten sowie der zugriffsberechtigten Personen gemäß Art. 30 DSGVO (interne Verarbeitungsübersicht) zur Verfügung.

Der Inhalt dieser Angaben ergibt sich aus Art. 30 DSGVO:

1. Name der verantwortlichen Stelle,
2. Leiter der verantwortlichen Stelle und der Datenverarbeitung,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. Geplante Datenübermittlung an Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach Art. 32 DSGVO (i.V.m. der Anlage dazu) zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

Dabei dokumentiert die Know How! AG auf der Ebene der Verarbeitung bzw. des Verfahrens eine Reihe weiterer Umstände. Dies betrifft z.B. Zugriffsberechtigungen, die Meldepflicht, das Ergebnis der Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und den Grund des Verzichts auf die Benachrichtigung des Betroffenen.
Die für die Know How! AG vorliegende Übersicht wird im Rahmen regelmäßiger Statusgespräche bei Bedarf aktualisiert.
Die erforderlichen Unterlagen für den Auftraggeber werden diesem auf Anforderung zur Verfügung gestellt.

2.3.2. Öffentliches Verfahrensverzeichnis

Die Datenschutzbeauftragte hat auf Antrag die Angaben des öffentlichen Verfahrensverzeichnisses (Art. 30 DSGVO) jedermann in geeigneter Weise verfügbar zu machen.
Ein derartiges öffentliches Verfahrensverzeichnis für die Know How! AG liegt vor und wird auf Antrag jedermann zur Verfügung gestellt.

2.3.3. Auftragsverarbeitung

Die Know How! AG erbringt Dienstleistungen gegenüber ihren Kunden regelmäßig als Auftragsdatenverarbeitung gemäß Art. 28 DSGVO.

Dabei nimmt die Know How! AG ggf. wiederum selbst Dienstleistungen externer Unterauftragnehmer in Anspruch, die in den Bereich der Auftragsdatenverarbeitung fallen.

Die Unterauftragnehmer werden dabei unter besonderer Berücksichtigung der Eignung der getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt. Entsprechende Verträge zur Auftragsdatenverarbeitung mit den eingesetzten Unterauftragnehmern wurden von der Know How! AG geschlossen und werden dem Auftraggeber nach Aufforderung zur Verfügung gestellt. Dies bezieht sich ebenfalls auf die im Zusammenhang mit der Unterbeauftragung sichergestellte Verpflichtung auf das Datengeheimnis nach §53 BDSG. Dies beinhaltet ebenfalls die Ausgabe von Richtlinien und Merkblättern mit Informationen zum Datenschutz, aber auch zur Datensicherheit.

Daneben unterhält die Know How! AG weitere Auftragsverhältnisse, so im Bereich der Datensicherung, der Datenentsorgung sowie im Rahmen der Software-Wartung. Hierbei legt die Know How! AG ebenfalls großen Wert darauf, dass gesetzeskonforme Verträge zur Auftragsdatenverarbeitung geschlossen werden und die Mitarbeiter des Dienstleisters auf das Datengeheimnis nach §53 BDSG verpflichtet sind.

2.4. Innerbetriebliche Organisation

2.4.1. Personelle Maßnahmen

2.4.1.1. Verpflichtung auf das Datengeheimnis

Alle Mitarbeiter der Know How! AG sind auf das Datengeheimnis nach § 53 BDSG verpflichtet. Neben einer allgemeinen Aufklärung über die Bedeutung des Datengeheimnisses enthält diese Verpflichtung auch Hinweise auf weitergehende Informationen zum Datenschutz sowie auf eventuelle Sanktionen.

2.4.1.2. Weitergehende Verpflichtungen

Soweit Mitarbeiter mit der Wartung der unternehmenseigenen EDV oder Telekommunikationsanlage betraut sind, werden diese auf die Wahrung des Fernmeldegeheimnisses nach § 88 TKG verpflichtet.

2.4.1.3. Information und Schulung

Die bei der Know How! AG geltenden Regelungen zu Datenschutz, IT-Sicherheit und Informationsschutz sind in der Richtlinie für den datenschutzkonformen Einsatz der Informations- und Kommunikationstechnik allen Mitarbeitern hinterlegt.
Erste Hinweise darauf erhalten die Mitarbeiter bereits bei Einstellung als Anlage zum Arbeitsvertrag. Weitergehende Informationen folgen im Zusammenhang mit der schriftlichen Verpflichtung auf das Datengeheimnis und auf die Einhaltung der Richtlinie sowie im Rahmen der arbeitsplatzbezogenen Einweisung durch die Mitarbeiter der EDV.

Hierdurch wird sichergestellt, dass jeder Mitarbeiter über folgende Punkte informiert ist:

- Grundlagen des Datenschutzes
- Interne Regelungen zum Datenschutz, IT-Sicherheit und Informationsschutz
- Grundzüge technischer und organisatorischer Maßnahmen zur Sicherstellung von Datenschutz, IT-Sicherheit und Informationsschutz
- Verantwortlichkeiten
- Informationsquellen

Ergänzend zu diesen grundsätzlichen Informationen werden die Mitarbeiter mindestens einmal jährlich tiefergehend im Hinblick auf spezielle Datenschutzfragen geschult.
Durch dieses Konzept wird sichergestellt, dass sowohl neu eingestellte Mitarbeiter in die Thematik des Datenschutzes eingeführt werden als auch die Kenntnisse der schon länger bei der Know How! AG beschäftigten Mitarbeiter regelmäßig aufgefrischt und aktualisiert werden.
Im Übrigen ist der eigentliche Verarbeitungsvorgang von Auftragsdaten durch rechtskonform zu gestaltende Weisungen des Auftraggebers vorgegeben, da der Umgang mit Daten regelmäßig weisungsgebunden im Rahmen eines Auftragsverhältnisses nach Art. 28 DSGVO erfolgt.

2.4.1.4. Regelmäßige Information

Die Know How! AG erhält über deren Datenschutzbeauftragen regelmäßig neueste Informationen über technische und rechtliche Entwicklungen auf den Gebieten des Datenschutzes und der Datensicherheit, so dass ständig eine entsprechende Sensibilisierung bei der Know How! AG gegeben ist.

2.4.1.5. Richtlinien

Die Know How! AG verfügt über einen umfassenden Richtlinien-Katalog hinsichtlich der Regelung datenschutzrechtlicher sowie sicherheitsrelevanter Themen. Beispielhaft seien hierzu aufgeführt:

- Richtlinie für den datenschutzkonformen Einsatz der Informations- und Kommunikationstechnik (Datenschutzhandbuch)
- Richtlinien für die Nutzung von E-Mail und Internet
- Richtlinie Umgang mit mobilen Datenträgern
- Datenschutz-Richtlinie Schulungskonzept

2.4.2. Rechte der Betroffenen

In Fällen, in denen Betroffene anfragen, welche Informationen über sie verarbeitet werden, wird die Anfrage regelmäßig an den Datenschutzbeauftragten zur Prüfung und Koordination der Bearbeitung weitergegeben.

Ebenso verhält es sich bei der Geltendmachung von Rechten Betroffener auf Berichtigung, Löschung und Sperrung von Daten. Diese Anfragen werden durch den Datenschutzbeauftragten koordiniert und an den zuständigen Ansprechpartner bzw. die zuständige Abteilung beim Auftraggeber weitergeleitet. Der Auftraggeber ist im letzten Schritt allein verantwortlich für die Wahrung der Rechte der Betroffenen.

3. Allgemeine Sicherheitsgrundsätze bei der Know How! AG

Die nach Anlage zu Art. 32 DSGVO getroffenen Maßnahmen den Schutz personenbezogener Daten können wie nachfolgend, differenziert nach den jeweiligen Wirkungszielen, beschrieben werden:

3.1. Zutrittskontrolle

Ziel der **Zutrittskontrolle** ist es, mit Hilfe geeigneter Maßnahmen Unbefugten den Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen zu verwehren.

- Außensicherung:
  - Alle Türen sind geschlossen und der Zutritt ist nur mit Zutrittsberechtigung (manueller Schlüssel) bzw. am Empfang möglich.
  - Die Schlüsselübergabe wird von der HR protokolliert und kontrolliert.

- Serverraum:
  - Der Serverraum ist ständig geschlossen und der Zutritt mittels manuellen Schlüssels nur den Geschäftsführern sowie speziell autorisierten Mitarbeitern vorbehalten.
  - Der Serverraum ist klimatisiert.

- Besucherregelungen:
  - Während der Betriebszeiten haben Besucher nur nach Anmeldung und in Begleitung des besuchten Mitarbeiters Zugang zu den Betriebsräumen.
  - Besucher und Externe in Funktionsausübung (wie z.B. Wartungstechniker) werden im Serverraum begleitet.

3.2. Zugangskontrolle

Ziel der **Zugangskontrolle** ist es, mit Hilfe geeigneter Maßnahmen zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können.

Als Zugangskontrolle wird auf den PCs die Zugangskontrolle zu Windows verbunden mit der Zugangskontrolle zum Netz genutzt.

- Durch Zugangsregelungen, Benutzerkennungen, Passwörter und Zugriffsregelungen ist der Zugang auf Datenverarbeitungssysteme gesichert.
- Bildschirmschoner mit Kennworteingabe bei Reaktivierung, automatische Bildschirmsperre bei längerer Inaktivität.
- Regelmäßige technische Prüfungen der im Netzwerk angeschlossenen Geräte auf Schwachstellen und Sicherheitslücken.
- Aktive und zulässige Dienste sind dokumentiert und deren Verfügbarkeit begründet, dokumentiertes Update-Verfahren.
- Dokumentiertes Vorgehen bei Wartungs- und Reparaturarbeiten von IT- Systemen; Datenschutzverpflichtung und regelmäßige Datenschutzunterweisung aller Mitarbeiter, Unterzeichnung der Verpflichtungserklärung „Sicherheitspflichten“ durch alle Mitarbeiter.

3.3. Zugriffskontrolle

Mit der **Zugriffskontrolle** ist zu gewährleisten, dass die zur Benutzung eines DV-Systems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei Erhebung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden. Es ist sicherzustellen, dass nur auf die Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht.

Vor der Benutzung der PCs müssen sich die Mitarbeiter durch die Eingabe einer Benutzerkennung und eines Passwortes im Netzwerk identifizieren und authentifizieren. Jeder Mitarbeiter verfügt nur über die Anwendungen, die er für seinen Aufgabenbereich benötigt. Ferner ist für bestimmte Anwendungen ein zusätzlicher Login erforderlich. Eine Zugriffsberechtigung auf die bei der Know How! AG vorhandenen Datenbanken besteht nur für Serversysteme und die Datenbankadministratoren. Die Administrationspasswörter sind bei der Geschäftsführung hinterlegt.

Damit auch bei einer kürzeren Abwesenheit des IT-Benutzers ein Zugriffsschutz für das IT- System gewährleistet ist, wird bei Inaktivität automatisch eine Bildschirmsperre aktiv, welche nur durch eine erfolgreiche Authentifikation deaktiviert werden kann.

- Zugriffsberechtigungen werden aufgrund benutzerbezogener Konten erteilt.
- Durch Benutzerkennungen, Passwörter und Zugriffsregelungen ist der Zugriff auf entsprechende Datenbereiche gesichert.
- Alle Zugriffe auf gesicherte Datenbereiche werden protokolliert.
- Datenschutzverpflichtung und regelmäßige Datenschutzunterweisung aller Mitarbeiter.
- Unterzeichnung der Verpflichtungserklärung „Sicherheitspflichten“ durch alle Mitarbeiter.
- Sicherung der Netzwerke durch Firewall-Systeme.
- Dokumentiertes Vorgehen bei Wartungs- und Reparaturarbeiten von IT-Systemen.
- Löschen der personenbezogenen Daten der Produktionsaufträge, wenn die Daten für keine weitere Bearbeitung benötigt werden.
- Löschung der Auftrags-, Produktions- und Sicherungsdaten gemäß den Vereinbarungen mit den Auftraggebern.

3.4. Weitergabekontrolle

Unter dem Begriff der **Weitergabekontrolle** sind sämtliche Aspekte der Weitergabe personenbezogener Daten, also elektronische Übertragung, Datenträgertransport und Übermittlungskontrolle zusammengefasst.

Je nach Sensibilität der Daten sind ausreichende Maßnahmen zu ergreifen, damit ein Missbrauch verhindert wird. In den Besitz der Know How! AG gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, werden, basierend auf den Vereinbarungen mit dem Auftraggeber und auf dessen Weisungen hin, diesem nach Wegfall des Verarbeitungszwecks ausgehändigt oder datenschutzgerecht vernichtet.

Zum Empfang von personenbezogenen Daten der Auftraggeber stellt die Know How! AG die Wege über verschlüsselte E-Mail oder eine im Haus betriebene Datenaustausch-Software (Nextcloud) bereit.

Möchte ein Auftraggeber Daten per E-Mail an die Know How! AG schicken, hat er die Möglichkeit, diese verschlüsselt an eine hierfür eingerichtete Adresse bei der Know How! AG zu senden. Unverschlüsselte Übertragungen per E-Mail erfolgen wiederum nur auf expliziten Wunsch des Auftraggebers sowie auf dessen Verantwortung.

Sämtliche Datenbereitstellungen und -übertragungen werden umfassend protokolliert.

Die Entsorgung der nicht mehr benötigten Ausdrucke oder Listen auf Anweisung des Auftraggebers erfolgt in dafür vorgesehenen gesicherten Behältern. Die Behälter stehen für jeden Mitarbeiter zentral und dezentral zur Verfügung und werden einem externen, auf die Aktenvernichtung spezialisierten Dienstleister zur datenschutzkonformen und umweltgerechten Entsorgung übergeben.

- Nach Absprache mit den Auftraggebern können zur Sicherung elektronischer Übertragungen spezielle Software und Verschlüsselungsverfahren wie z.B. PGP und/oder gesicherte Übertragungswege wie VPN-Verbindungen verwendet werden.
- Administration der Hardware Security Module im 4-Augen-Prinzip und nur vom Serverraum aus möglich.
- Die Aufbewahrung von Datenträgern erfolgt gesichert.
- Dokumentierte Regelungen zur Datenträgerverwaltung (Berechtigung, Lagerung, Kennzeichnung eigener und fremder Datenträger, Bestandsführung).
- Dokumentierte Regelungen zum Versand von Datenträgern (Transportunternehmen, Transportfahrzeuge, Transportbehälter, Verpackungs- und Versandvorschriften, Begleitpapiere, Identitätsprüfung der Beauftragten Personen, Abgangs- und Ankunftsbestätigung).
- Datenschutzverpflichtung und regelmäßige Datenschutzunterweisung der Mitarbeiter.
- Dokumentierte Vernichtung von Datenträgern.
- Dokumentiertes Vorgehen bei Wartungs- und Reparaturarbeiten von IT-Systemen.

3.5. Eingabekontrolle

Bei der **Eingabekontrolle** geht es um die Nachprüfbarkeit eines Erhebungs- bzw. Verarbeitungsvorgangs. Urheber, Inhalt und Zeitpunkt von Dateneingabe, -veränderung oder -löschung sollen im Nachhinein ermittelt werden können. Die Protokollierung darf nicht allgemeiner Art sein, sondern muss erkennen lassen, wer wann welche Daten eingegeben, verändert oder entfernt hat.

Um die Nachvollziehbarkeit einzelner Benutzeraktivitäten im Nachhinein zu gewährleisten, werden Aktivitäten sämtlicher Nutzer auf den für die Bewältigung der Auftragsdatenverarbeitung eingesetzten Systemen (Rechner/Server) benutzerbezogen protokolliert. Dabei werden

Objektzugriffe registriert (wer/wann auf was zugegriffen hat) und sicherheitsrelevante Ereignisse in einem separaten Sicherheitsprotokoll festgehalten.

3.6. Auftragskontrolle

Die **Auftragskontrolle** schließt die Maßnahmen mit ein, die bei der Vergabe eines Unterauftrages durchgeführt werden.

- Es gibt nur Weiterverarbeitungsprogramme für Auftraggeber, mit denen eine vertragliche Regelung über die Verarbeitung existiert.
- Einsatz interner Auftragsnummern, Plausibilitätsprüfungen und Checklisten.
- Zusätzliche Vereinbarungen mit Auftraggebern werden in Datenschutzvereinbarungen sowie ggf. in Verfahrensbeschreibungen getroffen.
- Regelmäßige Datenschutzunterweisung der Mitarbeiter.
    - Verpflichtungserklärung Sicherheitspflichten durch die Mitarbeiter.
- Dokumentiertes Verfahren, um Auftraggeber auf nicht datenschutzgerechte Übertragungen hinzuweisen.

3.7. Verfügbarkeitskontrolle

Im Rahmen der **Verfügbarkeitskontrolle** sind Maßnahmen zu treffen, die je nach Art der zu schützenden Daten geeignet sind, die Gefahr des Verlustes, der Beschädigung oder der Zerstörung von Daten während der Verarbeitung und Speicherung, bei der Datenfernübertragung, im Falle eines Systemzusammenbruchs zu minimieren, zu gewährleisten, dass keine unvollständigen oder beschädigten Daten der Verarbeitung zugeführt werden, sicherzustellen, dass jeder Verlust, jede Beschädigung und jede Zerstörung von Daten automatisch und zweifelsfrei erkannt wird, zu gewährleisten, dass Daten nach Verlust, Beschädigung oder Zerstörung mit vertretbarem Aufwand einwandfrei rekonstruiert werden können.

Feuerlöscher sind in zentraler Lage vorhanden. Im Serverraum wird zudem darauf geachtet, keine leicht brennbaren Materialien zu lagern. Um bei Überspannung, Unterspannung oder Stromausfall die Versorgung der Server sicherzustellen, ist eine unterbrechungsfreie Stromversorgung vorhanden, die in den Serverschrank integriert ist. Der Server-Raum verfügt zudem über eine Klimaanlage, die den Raum auf konstanter Betriebstemperatur hält.

Ein Datensicherungsplan legt fest, welche Daten/Systeme in welchen Abständen und zu welchem Zeitpunkt auf welche Medien bzw. anderen Systeme gesichert werden und wie die Verantwortlichkeiten hierfür geregelt sind.

Sämtliche Systeme (Arbeitsplatzrechner und Server) sind durch eine aktuelle Virenschutzlösung gesichert. Hierzu überprüft der Verwaltungsserver jede Antiviren-Software im Hinblick auf ihre Viren-Signaturen automatisch bei der Bereitstellung neuer Updates und aktualisiert diese bei Bedarf.

Auf den Mailservern der Know How! AG werden eingehende E-Mails automatisch auf Viren überprüft. Infizierte E-Mails werden dem Empfänger nicht zugestellt, sondern verbleiben zur Löschung durch den Administrator in einem geschützten Speicherbereich.

- Server und wichtige Teile der DV sind an eine zentrale USV angeschlossen.
- Einsatz von redundant ausgelegten DV-Systemen wie z.B. mit Plattenspiegelung in einer gesicherten IT-Umgebung.
- Es ist ein firmenweiter Virenschutz im Einsatz, der das Einschleusen von schadhafter Software verhindert.
- Tägliche Datensicherung auf Band und Aufbewahrung der Archivierungsbänder.
- Gesicherte Aufbewahrung der Backup-Kennwörter.
- Arbeitsanweisungen und Sicherheitsrichtlinien.
- Unterzeichnung der Verpflichtungserklärung „Sicherheitspflichten“ durch alle Mitarbeiter.

- Regelmäßige Schulung aller Mitarbeiter.
- Vorgaben für Verfahrens- und Softwaredokumentation.
- Regelmäßige Prüfung der getroffenen Maßnahmen.

3.8. Trennungsgebot

Ziel des **Trennungsgebots** ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten grundsätzlich auch getrennt verarbeitet werden können.

Eine Zusammenführung dieser Daten ist unzulässig, soweit dies nicht für die Erfüllung einer gesetzlichen Aufgabe erforderlich ist. Das Trennungsgebot stellt in technischer Sicht klar, was das materielle Recht bei den Vorschriften über die Zweckbindung bereits vorsieht. Im Rahmen der Datenverarbeitung im Auftrag schließt das Trennungsgebot die Trennung der Daten unterschiedlicher Auftraggeber (Mandantentrennung) mit ein.

Die Daten verschiedener Auftraggeber werden in relationalen Datenbanken, je nach in Anspruch genommener Dienstleistung, gespeichert. Eine Trennung der Daten der unterschiedlichen Auftraggeber innerhalb einer Service-Datenbank erfolgt mittels eindeutiger Markierungen, so dass jedem Datensatz eindeutig der Datenlieferant zugeordnet werden kann (logische Trennung).

- Es bestehen nur Weiterverarbeitungsprogramme für Kunden, mit denen vertragliche Regelungen über die Verarbeitung existieren.
- Einsatz interner Auftragsnummern, Plausibilitätsprüfungen und Checklisten.
- Es wird sichergestellt, dass Daten eines Produktionsauftrages nicht kopiert oder mehrfach verarbeitet werden können.
- Die temporäre Speicherung der Verarbeitungsdateien erfolgt mindestens in einer logischen Trennung zur weiteren Datenverarbeitung.
- Eine dauerhafte Datenhaltung erfolgt nur nach vertraglicher Regelung mit dem Auftraggeber.
- Datenschutzverpflichtung und regelmäßige Datenschutzunterweisungen aller Mitarbeiter.