Inhaltsverzeichnis

1. Einleitung

Dieses Dokument beschreibt unsere Informationssicherheitsphilosophie und die von uns angestrebten Ziele. Wo möglich, verzichten wir auf technische Details und das genaue Vorgehen. Das Dokument soll einen Gesamtüberblick ermöglichen – detaillierte Informationen sind den jeweiligen Richtlinien zu entnehmen.

Alle Regelungen sollen sich hieraus ableiten.

Der Geltungsbereich des ISMS wurde in Dokument ISMS 002 festgelegt. Alle Dokumente sind Vorgaben der ABT SE und gelten für die Firmen ABT SE, ABT Sportsline GmbH und ABT e-Line GmbH. (zur Vereinfachung wird in allen weiteren Dokumenten von der „ABT-Gruppe“ gesprochen) Firmeneigene Regelungen, Richtlinien oder Dokumente, die die Anforderungen der Vorgaben der ABT SE nicht verletzen oder umgehen sind in den einzelnen Tochterfirmen zugelassen. Diese Dokumente ergänzen im Bedarfsfall die allgemein gültigen Dokumente der ABT SE und gelten dann explizit für die jeweilige Tochterfirma.

1.1. Stellenwert der Informationssicherheit im Unternehmen

Unser Unternehmen ist auf IT-gestützte Prozesse im Unternehmen angewiesen. In dieser Situation ist es unerlässlich, Informationssicherheit zu gewährleisten, um die nötige Zuverlässigkeit im geschäftlichen Alltag zu schaffen. Informationssicherheit ist integraler Bestandteil aller Geschäftsprozesse in der ABT-Gruppe und hat wesentlichen Einfluss auf die Qualität, sowie die Effizienz und Wirtschaftlichkeit der Arbeitsergebnisse des Unternehmens. Wir verstehen Informationssicherheit als unerlässlichen Kundenservice, der die Vertraulichkeit von Informationen schützt und die Verfügbarkeit unserer Prozesse gewährleistet.
Wir leben eine aktive Sicherheitskultur und fördern Informationssicherheit, indem alle Mitarbeiter eingebunden, regelmäßig geschult und sensibilisiert werden. Der Mitarbeiter steht bei uns im Mittelpunkt der aktiven Sicherheitskultur.

1.2. Schutzziele

Das ISMS der ABT-Gruppe dient dem Schutz vor Gefahren, Bedrohungen und den damit verbundenen Schäden. Ziel ist es, in allen Kategorien Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Verbindlichkeit mit angemessenen Maßnahmen das Schutzziel „HOCH“ zu erreichen.
Die Ziele von Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Verbindlichkeit) können in verschiedenen Bereichen und Phasen eines Geschäftsprozesses durch die Bedarfsträger (z. B. „Informationseigentümer“) unterschiedlich priorisiert werden. Die Priorisierung wird entweder innerhalb von IT-Sicherheitskonzepten im Rahmen einer Risikobetrachtung vorgenommen und dokumentiert oder durch generelle Anforderungen (z. B. aus Gesetzen, Verordnungen und Verwaltungsvorschriften) festgelegt. Sie muss bei Bedarf im Rahmen von Revision und Audit entsprechend der aktuellen Sicherheitslage oder aufgrund anderer veränderlicher Bedürfnisse revisionssicher angepasst werden.
Die Priorisierung der Sicherheitsziele orientiert sich dabei an den bei einem IT-Sicherheitsvorfall zu erwartenden Schäden bei einem bestimmten Schadenszenario.
So kann z. B. bei einem Geschäftsprozess zu einem bestimmten Zeitpunkt die Vertraulichkeit von Informationen zum Schutz von Leib und Leben vor dem Ziel der Verfügbarkeit stehen, d. h. ein Fachverfahren wird nicht schnellstmöglich wieder in Betrieb gesetzt.

Im gleichen Geschäftsprozess bei einer anderen Sachlage oder in einem anderen Geschäftsprozess kann die Verfügbarkeit höher priorisiert werden als die Vertraulichkeit, um einen hohen finanziellen Schaden zu vermeiden, d. h. das betreffende Fachverfahren wird trotz zeitweisem Verlust der Vertraulichkeit schnellstmöglich mindestens in einen Notbetrieb überführt.

1.2.1. Schutz der Vertraulichkeit

In Abhängigkeit vom jeweiligen Schutzbedarf der Vertraulichkeit von Informationen sind angemessene organisatorische und technische Maßnahmen zu ergreifen und aufrecht zu erhalten. Eine Verletzung des für den Schutz der Vertraulichkeit jeweils definierten Schutzbedarfes ist durch entsprechende Maßnahmen zu unterbinden.
Dieses muss bei der längerfristigen Speicherung und revisionssicheren Vernichtung von Informationen, bei Aufbau und Anpassung der Infrastruktur der Informationsverarbeitung, bei der Nutzung von Informationen auf IT-Systemen, der Übertragung insbesondere über Datennetze außerhalb eigener Infrastrukturen und dem Transport mit mobilen Medien oder Systemen innerhalb und außerhalb des Geltungsbereiches dieser Richtlinie geschehen. Die gewählten Vorgehensweisen sind regelmäßig einer genauen Prüfung zu unterziehen und an die technologische Entwicklung sowie die Gefährdungslage anzupassen.
Der Zugriff auf Informationen ist unter besonderer Berücksichtigung des Rechtes auf informationelle Selbstbestimmung (Datenschutz) auf den mit ihrer Verarbeitung beauftragten Personenkreis zu beschränken ("need-to-know" Prinzip). Grundlage hierfür ist die Schutzbedarfsfeststellung.
Im Sinne einer Prävention sind Maßnahmen zur zentralen und dezentralen Schadsoftware- (z. B. Viren, Würmer, Trojaner, Rootkits) und Einbruchserkennung („Hacker“) flächendeckend zu etablieren. Der Nachweis der ordnungsgemäßen Funktion der gewählten Mechanismen muss möglich sein und erbracht werden.

1.2.2. Schutz der Integrität

Die Integrität von Informationen ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen.
In Abhängigkeit vom Schutzbedarf der Integrität von Informationen ist über eine angemessene Vorgehensweise zu entscheiden. Dieses muss bei der längerfristigen Speicherung von Informationen, bei Aufbau und Anpassung der Infrastruktur der Informationsverarbeitung, bei der Nutzung von Informationen auf IT-Systemen, bei der Übertragung über Datennetze und dem Transport mit mobilen Medien oder Systemen innerhalb und außerhalb des Geltungsbereichs dieser Richtlinie geschehen. Die gewählten Vorgehensweisen sind regelmäßig zu überprüfen und an die technologische Entwicklung sowie die Gefährdungslage anzupassen.
Die unbefugte Veränderung von Informationen ist durch den Einsatz entsprechender Mittel zu verhindern. Sicherung vor Schadsoftware und Einbruchserkennung sind hierbei wichtige, jedoch nicht ausschließliche Mechanismen. Der Nachweis der ordnungsgemäßen Funktion der gewählten Mechanismen muss möglich sein und mindestens stichprobenartig erbracht werden.

1.2.3. Schutz der Verfügbarkeit

Die Verfügbarkeit von Informationen ist gemäß ihres Schutzbedarfes durch geeignete technische und organisatorische Maßnahmen sicherzustellen.
In Abhängigkeit der erforderlichen Verfügbarkeit von Informationen ist über eine angemessene Vorgehensweise zu entscheiden. Dieses muss bei der längerfristigen Speicherung und vor der Vernichtung von Informationen, bei Aufbau und Anpassung der Infrastruktur zur Informationsverarbeitung, bei der Nutzung von Informationen auf IT-Systemen, der Übertragung über Datennetze und dem Transport mit mobilen Medien oder Systemen innerhalb und außerhalb des Geltungsbereichs dieser Richtlinie geschehen.
Die gewählten Vorgehensweisen sind regelmäßig zu überprüfen und an die technologische Entwicklung sowie die Gefährdungslage anzupassen.

Durch den Einsatz entsprechender Sicherheitseinrichtungen ist eine Verminderung der Verfügbarkeit der IT und der verarbeiteten Informationen zu verhindern. Redundante IT-Infrastruktur, Datensicherung, Archivierung sowie die Absicherung gegen Schadsoftware und unbefugtes Eindringen in IT-Systeme und -Netze sind hierbei wichtige, jedoch nicht ausschließliche Mechanismen. Der Nachweis der Funktion der gewählten Mechanismen muss möglich sein und erbracht werden.
Im Interesse der Gesamtverfügbarkeit dürfen Teile der IT vom IT-Betrieb ausgeschlossen werden, wenn die IT-Sicherheitslage dieses erfordert. Dies gilt insbesondere auch für Systeme mit Informationen, deren Schutzbedarf größer als "*hoch*" eingestuft ist.

1.2.4. Gewährleistung der Authentizität

Die Authentizität von Informationen ist gemäß ihres Schutzbedarfes durch geeignete technische und organisatorische Maßnahmen sicherzustellen.
Hierzu muss die Echtheit von Informationen und ihrer Urheberschaft anhand charakteristischer Merkmale überprüfbar sein. Diese Überprüfung muss durch geeignete technische und organisatorische Maßnahmen vorgenommen werden. Ihre Anwendung und Einhaltung sind bei allen Schritten der Verarbeitung der Informationen ungeachtet der verwendeten Systeme, Kommunikationswege oder Übertragungsmedien einzuhalten. Der Nachweis der ordnungsgemäßen Funktion der gewählten Mechanismen muss möglich sein und erbracht werden.

1.2.5. Gewährleistung der Verbindlichkeit

Die Verbindlichkeit der Verarbeitung von Informationen muss in den Geschäftsprozessen bei allen Arbeitsschritten gewährleistet sein. Die Verarbeitungsvorgänge müssen hinsichtlich ihres Ablaufs nachvollziehbar und überprüfbar (revisionsfähig) sein. Hierbei ist das übergeordnete Ziel der Rechtsverbindlichkeit der Informationsverarbeitung einzuhalten.
Für Informationen mit "sehr hohem" Schutzbedarf müssen angemessene Maßnahmen zum Nachweis der Identität der Verarbeitung mit den vom Verarbeiter absichtlich vorgenommenen Aktionen ergriffen werden (z. B. Änderungshistorie). Die rechtlichen Rahmenbedingungen unter besonderer Berücksichtigung des Datenschutzes sind dabei besonders zu beachten.
Die verwendeten Verfahren zur Absicherung sind so weit wie möglich zu automatisieren, der Zugriff auf die gewonnenen Informationen ist besonders zu begrenzen.

2. Informationssicherheitsmanagement

2.1. ISMS

Die Organisation betreibt zur Erreichung der selbst gesteckten Sicherheitsziele ein ISMS auf Basis der ISO 27001 und des VDA-ISA Katalogs (TISAX).

2.2. Fortlaufende Verbesserung

- Das ISMS wird regelmäßig auf Aktualität und Wirksamkeit überprüft. Hierzu gehören regelmäßige Audits und die Wirksamkeitsüberprüfung von Maßnahmen.
- Alle Mitarbeiter sind dazu verpflichtet, den QM bei dieser Aufgabe zu unterstützen.
- Unser Unternehmen legt besonderen Wert darauf, technisch aktuelle Maßnahmen einzusetzen.
- Die Leitung des Unternehmens fördert und propagiert das ISMS im Unternehmen.
- Alle Abweichungen werden im Detail analysiert, um Verbesserungen zu erarbeiten.
- Alle Mitarbeiter sind in das ISMS in einem dem Maße eingebunden, dass Sie Fehler oder Verbesserungsmaßnahmen melden können.

2.3. Verantwortlichkeiten

Um das ISMS fachgerecht aufzubauen und zu pflegen, wurde das Thema Informationssicherheit dem leitenden Qualitätsmanager (QM) der Stabstelle HSEQ angegliedert. Es gelten folgende Rahmenbedingungen und Verantwortlichkeiten:

- Voraussetzungen
    - Der QM besitzt zur Wahrnehmung seiner Aufgabe eine hervorgehobene organisatorische Rolle, in der er direkt an die Unternehmensleitung berichtet.
    - Der QM verfügt über angemessenes Wissen und Qualifikationen im Bereich Informationssicherheit.
    - Die Verantwortung für das Thema Informationssicherheit wird schriftlich berufen.
- Verantwortlichkeiten
    - Aufbau eines Managementsystems gemäß den Anforderungen von TISAX
    - Regelmäßige Berichterstattung an das Management
    - Abstimmung der Informationssicherheitsziele mit der Unternehmensleitung
    - Koordination aller sich aus der Aufgabe heraus ergebenden Tätigkeiten
    - Analyse von Sicherheitsvorfällen
    - Der QM hat das Recht, die Belegschaft über Ereignisse oder aktuelle Themen zu unterrichten

Alle Mitarbeiter sind dazu angehalten den QM zu unterstützen. Dazu gehört:

- **Geschäftsführung**:
  - Trägt die Gesamtverantwortung für das ISMS
  - Bereitstellung der nötigen Ressourcen für das ISMS
  - Unterstützung des QM bei der Kommunikation gegenüber anderen Mitarbeitern
  - Förderung der fortlaufenden Verbesserung
  - Festlegung und Kommunikation der Informationssicherheitsziele gemeinsam mit dem QM
- **Führungskräfte**
  - Leben einer Vorbildrolle, um Informationssicherheit gegenüber Mitarbeitern förderlich zu kommunizieren
  - Weiterleiten von Verbesserungsvorschlägen an den QM
  - Einbeziehen des QM bei Veränderungen im Betriebsablauf, die die Informationssicherheit betreffen
- **IT-Leiter**
  - Besonders enge Zusammenarbeit mit QM zur Erreichung der Sicherheitsziele
  - Unterstützung des QM mit Ressourcen zur Umsetzung der Sicherheitsziele
- **Datenschutzbeauftragter**
  - Bezieht den QM bei Änderungen, die die Informationssicherheit betreffen, mit ein
  - Stimmt Sicherheitsmaßnahmen wo möglich mit dem QM ab
- **Alle Mitarbeiter**
  - Melden von Informationssicherheitsvorfällen und Unregelmäßigkeiten
  - Einhalten der vorgeschriebenen Richtlinien

2.4. Risikomanagement

Zur Identifikation von Risiken innerhalb des ISMS wird ein Risikomanagementsystem durch den QM betrieben. Das Risikomanagement dient zur Identifikation und Bewertung von Risiken. Der QM ist verpflichtet, bei Risiken, die vorher definierte Schwellwerte überschreiten, Gegenmaßnahmen einzuleiten.

3. Maßnahmen

3.1. Zugang zu Informationen und Systemen

Ziel: Steuerung und Einschränkung des Zugangs zu System und Informationen.

Die Verantwortlichkeiten für Informationssicherheit sind innerhalb der Organisation und relevanten Geschäftspartnern bekannt und für ihre Aufgaben qualifiziert.
Innerhalb der Organisation wird einem Informationssicherheitskonzept gefolgt, über welches alle Mitarbeiter informiert sind. Verantwortlich für die Umsetzung in den einzelnen Bereichen sind die jeweiligen Bereichsleiter. Notwendige Ressourcen zur Gewährleitung der Informationssicherheit sind ermittelt und werden den Mitarbeitern zur Verfügung gestellt.

3.1.1. Zugänge

- Wir fördern die Nutzung unserer Systeme und Dienste und verfolgen die Strategie, Zugänge wo nötig zur Erfüllung der Arbeit auch zu erteilen, wenn kein eklatanter Grund dagegenspricht.
- Die Vergabe von Rechten erfolgt, wenn möglich, in Bezug auf die organisatorische Rolle wie z.B. Bereichsleiter, Abteilungsleiter, etc., um eine konsistente Rechtevergabe zu ermöglichen.
- Erteilte Rechte werden dokumentiert und regelmäßig kontrolliert.
- Privilegierte Rechte werden nach besonders sorgfältiger Prüfung erteilt und ebenfalls regelmäßig auf Notwendigkeit überprüft.

3.1.2. Passwörter und Anmeldedaten

Alle Zugänge zu Systemen und Informationen werden mit personalisierten Anmeldedaten geschützt. Wir fördern die Erstellung sicherer Passwörter und die Nutzung eines Passwortmanagers für Zugänge, die nicht über Single-Sign-on (SSO) bereitgestellt werden können.

3.2. Personalsicherheit

Ziel: Vor, während und nach Beschäftigung sind sicherheitsrelevante Anforderungen an die Beschäftigung sichergestellt.

Es besteht eine Verpflichtung zur Geheimhaltung und Vertraulichkeit, welchen jeder Mitarbeiter mit Unterzeichnen seines Arbeitsvertrages zustimmt. Diese Verpflichtungen reichen über das Arbeitsverhältnis hinaus.
Außerdem verpflichten sich Mitarbeiter dazu, die Richtlinien zur Informationssicherheit einzuhalten. Aspekte der Informationssicherheit sind in den Arbeitsverträgen der Mitarbeiter berücksichtigt.
Verantwortlichkeiten und Pflichten für Umgang mit sensiblen Informationen sind im Arbeitsvertrag verankert.
Die Verpflichtungserklärung, die jeder Mitarbeiter vor Eintritt in die Organisation unterzeichnet, ergänzt bereits getroffene Vereinbarungen zu den Themen Datenschutz und Informationssicherheit
Eine Vorgehensweise bei Verstößen gegen vertragliche Inhalte mit Informationssicherheitsrelevanz ist im Arbeitsvertrag beschrieben und somit jedem Mitarbeiter bekannt.
Mitarbeiter werden von der QM-Abteilung über Änderungen der Richtlinien informiert.

3.2.1. Sensibilisierung und Schulung

Um Mitarbeiter in die Belange der Informationssicherheit einzubinden und zu sensibilisieren fördern wir die Schulung von Mitarbeitern. Dazu gehört:

- Regelmäßige (mindestens jährliche) Schulungen
- Zielgruppenorientierte Ausrichtung der Schulungen
- Bereitstellen von nötigen Informationen an einer zentralen Stelle in leicht verständlicher Form

3.2.2. Beschäftigungsänderungen

Bei Eintritt/Austritt von Personal oder der Änderung einer Beschäftigung ist wie folgt umzusetzen:

- Vor Eintritt:
  - Mitarbeiter werden auf eine Geheimhaltungsvereinbarung verpflichtet.
  - Die Zuteilung von Rechten erfolgt rechtzeitig vor Beginn der Beschäftigung.
- Bei Austritt:
  - Der verantwortliche Vorgesetzte stellt den Wissenstransfer sicher.
  - Der Mitarbeiter wird auf die Verpflichtungen, die sich aus der Geheimhaltungsvereinbarung ergeben, hingewiesen.
  - Die Deaktivierung von Zugängen und Rechten erfolgt innerhalb von 48 Stunden.
- Tätigkeitsänderungen:
  - Alte Rechte, die nicht mehr von Relevanz sind, werden entzogen.
  - Zugangsrechte werden angepasst.

Neue Mitarbeiter werden über sämtliche Richtlinien zur Informationssicherheit und über die Risiken beim Umgang mit Information und deren Verarbeitung geschult und sensibilisiert.

3.2.3. Sanktionen

Das mutwillige Verletzen von Sicherheitsrichtlinien führt zu Sanktionen:

- Die Maßnahmen sind mit dem Vorgesetzten abzusprechen.
- Strafrechtlich relevantes wird zur Anzeige gebracht.
- Sanktionen werden in den Schulungen kommuniziert und sind vertraglich verankert.

3.3. Lieferantenbeziehungen

Ziel: Lieferantenbeziehungen gewährleisten das gleiche Informationssicherheitsniveau wie bei internen Vorgängen.

Auftragnehmer, die folgende Bedingungen erfüllen:

- Verarbeitung sensibler Informationen
- Wartung, Bereitstellung oder Entwicklung sensibler IT-Systeme oder Dienste
- Zutrittsberechtigung zu Räumen, in denen sensible Informationen verarbeitet werden

Unterliegen unter anderem folgende Bedingungen:

- Vertragsbedingungen und Produkte werden im Sinne der Sicherheitsanforderungen geprüft.
- Je nach Tätigkeit wird der Lieferant auf eine Geheimhaltungsvereinbarung bzw. Sicherheitsrichtlinie verpflichtet.
- Der Lieferant kann regelmäßig auf die Einhaltung von getroffenen Vereinbarungen überprüft werden.
- Das Unternehmen unterstützt den Lieferanten bei der Umsetzung und Einhaltung der Sicherheitsmaßnahmen.
- Der Datenaustausch zwischen Dienstleistern und Lieferanten mit, der einer Firma der ABT-Gruppe ist nur über freigegebene Laufwerke (Cloud-Dienste) gestattet.
- Die Richtlinie zur Informationssicherheit für Lieferanten und Dienstleister ist zu beachten

3.4. Handhaben von Informationen

Ziel: Informationswerte sind über Ihren kompletten Lebenszyklus hinweg angemessen geschützt.

Verantwortlichkeiten für die Informationssicherheit in der Organisation sind definiert, dokumentiert und zugewiesen. Die verantwortlichen Mitarbeiter sind entsprechend für ihre Aufgabe qualifiziert. Ansprechpartner sind innerhalb der Organisation und relevanten Geschäftspartnern bekannt

- Das Unternehmen führt ein Asset-Inventar (Werte-Inventar), das aus einer übergeordneten Sichtweise relevante Informationswerte des Unternehmens klassifiziert.

- Informationen und Dokumente werden klassifiziert, um die Geheimhaltungsstufe sichtbar zu machen und den angemessenen Umgang zu ermöglichen. Informationen werden in folgendem System klassifiziert:
  - Öffentlich
    - Zugang zu diesen Informationen beeinträchtigt das Unternehmen keinesfalls. Diese Informationen unterliegen keinerlei Restriktionen und werden z.B. vom Unternehmen in Zeitungen oder im Internet veröffentlicht. Die Verwendung von Unternehmensinformationen in der Öffentlichkeit bedarf der Zustimmung der Presse-Abteilung.
  - Intern
    - Zugang durch Dritte oder nicht vertrauenswürdige Vertragspartner kann einen geringen Schaden oder Ansehensverlust zur Folge haben. Dazu zählen alle

Informationen, die nur für den internen Gebrauch und nicht für die Öffentlichkeit bestimmt sind.

- Vertraulich
  - Zugang zu Informationen durch Dritte oder unberechtigte Mitarbeiter kann einen erheblichen Schaden zur Folge haben. Personenbezogene Daten (Stammdaten) sind – wenn nicht als geheim gekennzeichnet – immer vertraulich zu behandeln.
- Geheim / Streng vertraulich
  - Zugang durch unbefugte und nicht berechtigte richtet einen unumkehrbaren Schaden an. Dazu zählen Informationen, deren Kenntnis durch Unbefugte oder deren missbräuchliche Weitergabe oder Verwendung das Erreichen von Unternehmensziele nachhaltig gefährden kann und die daher einem äußerst restriktiven Verteiler und strikten Kontrollen unterliegen müssen.

- Die Klassifizierungsstufe bestimmt ebenfalls den zulässigen Umgang (Verwendung) mit Dokumenten und Informationen über den Lebenszyklus hinweg.
- Informationen werden sicher vernichtet, um Einsicht durch Dritte zu verhindern. Näheres ist der zugehörigen Richtlinie zu entnehmen.

3.5. Mobile Geräte

Ziel: Die Arbeit an entfernten Standorten / mobil unterliegt dem gleichen Sicherheitsniveau.

- Alle Benutzer mobiler Geräte werden gesondert geschult und auf eine gesonderte Richtlinie verpflichtet, um den erhöhten Gefahren mobiler Geräte gerecht zu werden (Verlust, Einsicht durch Dritte).
- Mobile Geräte werden durch die IT bereitgestellt.
- Der Zugriff auf Unternehmensressourcen erfolgt stets verschlüsselt.

3.6. Definition der Verantwortlichkeiten zwischen IT und externen Dienstleistern

Ziel: Verhinderung von Missbrauch und Misskommunikation zwischen unterschiedlichen Gewerken durch fixe Ansprechpartner

- IT-Dienste und Dienstleistungen sind identifiziert, dokumentiert und erfüllen alle relevanten Sicherheitsanforderungen. Regelmäßig durchgeführte Audits, sowie Schulungen gewährleisten eine Einhaltung der Vorgaben.
- Die Liste unserer IT-Dienstleister mit allen relevanten Informationen zu Dienstkonfigurationen, relevanten Nachweisen der Dienstleister, etc. sind über die Dokumente „Sicherheitsanforderungen an IT-Dienstleister“ und „Liste IT-Dienstleister“ abrufbar

3.7. Kommunikationssicherheit

Ziel: Unternehmensnetze und Kommunikationsnetze sind angemessen geschützt.

Unternehmensnetze und Kommunikationsnetze innerhalb der Organisation sind angemessen geschützt. Dafür sind verschiedene Maßnahmen, wie z.B. Zugangsbeschränkungen, Verschlüsselung von Netzwerkverbindungen und Firewall-Systeme etabliert. Diese Sicherheitsmaßnahmen werden regelmäßig und sorgfältig von geschultem Personal überprüft.

3.7.1. Zugangsbeschränkungen

Alle Netzwerke werden im Zugang durch den Einsatz von Verfahren, die der Geräteautorisierung dienen, beschränkt, so dass nur unternehmensinterne Geräte Zugang zum Unternehmensnetzwerk erhalten.

3.7.2. Kryptografie

Alle kritischen internen Verbindungen werden kryptografisch gesichert.

- Wartungsverbindungen (SSH, RDP)
- Kabellose Netze (W-Lan mit WPA2)

Das Verschlüsselungskonzept bestimmt, dass sämtliche externe Verbindungen sowie externe Datenträger und Datenträger in mobilen Geräten verschlüsselt werden.
Ein Notfallprozess nicht benötigt, weil keine Verwendung eines MasterKey's gegeben ist, d.h. es findet keine Verschlüsselung von Datenspeichern statt.

3.8. Physische Sicherheit

Ziel: Steuerung und Einschränkung des Zutritts zu Räumlichkeiten. Erreichen eines Schutzes von schutzbedürftigen oder kritischen Informationen.

3.8.1. Zutrittssteuerung

- Die Vergabe von Zutrittsrechten erfolgt, wenn möglich, in Bezug auf die organisatorische Rolle wie z.B. Geschäftsleitung, Bereichsleitung, etc. um eine konsistente Rechtevergabe zu ermöglichen.
- Zutrittsrechte werden dokumentiert und regelmäßig überprüft.
- Sofern ein Mitarbeiter das Unternehmen verlässt oder sich sein Aufgabenbereich ändert, wird sichergestellt, dass die Zutrittsrechte entsprechend angepasst werden.

3.8.2. Sicherung von Infrastruktur und sensibler Bereiche

- Zentrale und sensible Infrastruktur wie z.B. der Serverraum wird besonders geschützt, so ist z.B. Zutritt für Gäste untersagt, ebenso Foto-, Video- und Tonaufnahmen.
- Der Zutritt zum Serverraum ist nur dem IT-Personal und weiteren, von der IT geschulten Personen möglich.
- Der Besuch durch Dritte in Sicherheitszonen wird dokumentiert und erfolgt begleitet durch einen befugten Mitarbeiter.
- Dieses Vorgehen ist auch auf weitere sensible Bereiche anzuwenden. Sicherheitsbereiche sind in den Bauplänen kenntlich gemacht (siehe Bauplan mit Sicherheitszonen).

- Zur Sicherung der Organisation wird der Außenbereich einschließlich Kundenparkplatz und Einfahrt, sowie der komplette Werkstattbereich inkl. Entwicklung, Karosserie videoüberwacht
- Außerdem wird täglich automatisch die Alarmanlage zwischen 21:30 bis 05:30 Uhr aktiviert
- Mehr Information zu weiteren Sicherheitsbereichen ist im Dokument „Richtlinie zur Arbeit in Sicherheitsbereichen“ hinterlegt.

3.8.3. Clean-Desk-Policy

Um die Einsicht unberechtigter Personen in sensible Informationen vorzubeugen, fördern wir eine Clean-Desk-Policy. Detaillierte Informationen sind aus dem entsprechenden Dokument zu entnehmen

3.8.4. Entsorgung von Geräten und Datenträgern (Punkt 8.1. – 8.4.)

Ziel: Kontrollierte Entsorgung von Firmeneigentum und ordnungsgemäße Vernichtung von vorhandenen Daten

- Alle Datenträger, Geräte und Dokumente, die interne oder vertrauliche Informationen haben, werden ordnungsgemäß vernichtet oder gelöscht, bevor diese entsorgt oder weiterverkauft werden oder in anderer Form den Kontrollbereich des Unternehmens verlassen (siehe Dokument ISMS_08.V02 Entsorgungsrichtlinie).
- Es obliegt der Verantwortung des Bereichs- oder Abteilungsleiters, die sachgemäße Löschung bzw. Vernichtung beim IT-Leiter zu beauftragen

3.8.5. Entsorgung von Akten und Dokumenten

Ziel: Kontrollierte Vernichtung von Akten und Dokumenten, die interne Daten und Informationen enthalten

- Alle Dokumente und Akten, die firmeninterne Daten (z.B. Namen, Kundendaten, technische Unterlagen, Finanzen etc.) enthalten, müssen nach der Klassifizierung S2 / P4 vernichtet werden.
- Aktenvernichter, die Dokumente nach dem Standard vernichten sind in den Stockwerken vorhanden
- Größere Mengen von Dokumenten können in der Aktenvernichtungstonne in der Buchhaltung entsorgt werden. Diese wird zentral vernichtet

3.8.6. Naturkatastrophen, vorsätzliche Angriffe und Unfälle

Maßnahmen, die die Sicherheit, Vertraulichkeit, Verfügbarkeit und Integrität des Unternehmens auch im Falle von Naturkatastrophen, Unfällen oder vorsätzlichen Angriffen sind im Dokument „Richtlinie zu Naturkatastrophen, Unfällen und vorsätzlichen Angriffen“ festgehalten. Um z.B. einem Feuer vorzubeugen, sind in allen Bereichen Brandmeldeanlagen installiert, welche regelmäßig durch geschultes Personal auf ihre Funktionsfähigkeit geprüft werden. Ebenso sind Brandschutztüren in Sicherheitsbereichen, sowie Fluchtwegpläne an entsprechenden Orten im Firmengebäude platziert (siehe Gebäudeplan / Fluchtwegplan). Weitere Schutzmaßnahmen, wie z.B. im Falle einer Pandemie, Wasserschaden, Hagelschaden sind in den folgenden Dokumenten festgehalten und Mitarbeiter darauf hingewiesen worden (siehe Corona Maßnahmenplan, Versicherung bei Gebäudeschäden / Hagel-, Wasserschaden). Für die Prävention solcher Umstände besteht eine Risikobewertung für die

einzelnen Punkte. Diese Bewertung richtet sich nach der RPZ bzw. der Wahrscheinlichkeit eines möglichen Auftretens (siehe Dokument Risikobewertung?).

3.8.7. Schutz der Anlieferungs- und Versandbereiche vor unbefugtem Zutritt

Es ist sichergestellt, dass alle Zugänge zu geschützten Zonen, darunter der Anlieferungs- und Versandbereich vor unbefugtem Zutritt geschützt wird. Dazu zählt z.B. die Trennung des Bereichs von anderen Bereichen. Zutritt nur für identifiziertes und berechtigtes Personal. Bereich ist über Sicherheitstüren mit Chip-Eingang von anderen Bereichen getrennt. Zugangsbeschränkung nur für befugtes Personal.

3.9. Betriebssicherheit

3.9.1. Aktualisierungen

Das regelmäßige Aktualisieren von Systemen ist in der heutigen Zeit üblich und wird gefördert.

- Aktualisierungen werden zeitnah eingespielt.
- Die Priorisierung erfolgt auf Grund von Dringlichkeit, Risiko durch Sicherheitslücken und Testbedarf.

3.9.2. Schwachstellen

Werden Sicherheitslücken, für die keine Behebung in Form einer Aktualisierung vorhanden ist, identifiziert, kann der Zugang zu Diensten oder Systemen eingeschränkt werden, bis das Problem behebbar ist.

3.9.3. Änderungen an Systemen

- Änderungen an Systemen, insbesondere wenn Sie der Erhöhung der Sicherheit, Beschleunigung oder Vereinfachung von Arbeitsvorgängen dienen, können bei der IT-Abteilung beantragt werden.
- Änderungen werden kommuniziert und dokumentiert

3.9.4. Backups

Alle Systeme werden regelmäßig gesichert. Die Datensicherung erfolgt unter folgenden Gesichtspunkten:

- Datensicherungen erfolgen automatisch und an zwei getrennten Standorten.
- Datensicherungen sind in besonderem Maße vor Verlust, Änderung oder unberechtigten Zugriff geschützt.
- Datensicherungen müssen mindestens einmal am Tag erfolgen, die Wiederherstellung ebenfalls innerhalb von 24 Stunden möglich sein.
- Datensicherungen und die Wiederherstellungsprozedur werden regelmäßig getestet

- Gesetzliche Anforderungen werden eingehalten (z.B. werden Logs von Backups überprüft, etc.)
- Definition Ereignis-Logs

Regelmäßige Durchführungen von Audits durch den entsprechend qualifizierten Informationssicherheitsbeauftragten bzw. Auditor erfolgen rechtzeitig und nach Abstimmung mit Betreiber und Nutzer der entsprechenden IT-Systeme. Zu den Anforderungen an die Auditierung von IT-Systemen zählt die regelmäßige und nachvollziehbare Überprüfung. Die Audit-Planung erfolgt im Rahmen der ISO-Audit-Planung. Termine sind rechtzeitig mit den Beteiligten festgelegt. Die Überprüfung der ISMS-Anforderungen erfolgt mit den internen Audits zur ISO-9001. Folgende Punkte sollen mit abgeprüft werden:

- aus den Ergebnissen werden Maßnahmen abgeleitet,
- es erfolgt eine Nachverfolgung der abgeleiteten Maßnahmen
- für Abweichungen werden weitere Maßnahmen definiert, deren Änderung im Rahmen der regelmäßigen ISO-9001 Überprüfung kontrolliert werden
- Ergebnisse werden nachvollziehbar in einem Audit- bzw. Management-Bericht gespeichert
- Die Leistungserbringung durch Dienstleister wird regelmäßig überwacht und überprüft. Dies findet analog zu Punkt 12.8. statt. Interne und externe Audits folgen demselben Prozess. Zusätzlich wird bei externen Dienstleistern auch die Einhaltung vertraglicher Vereinbarungen überprüft.

3.9.5. Schutz vor Schadprogrammen

Alle Systeme sind vor Schadprogrammen und weiteren Gefahren zu schützen:

- Einsatz einer Software mit Endpunktschutz, die zentrale Verwaltung und Einsicht möglich.
- Einsatz einer netzwerkseitigen und clientseitigen Firewall.
- Regelmäßiger Scan aller Systeme und Analyse der Protokolle.
- Die Installation von Programmen wird eingeschränkt und ist nur der IT möglich.

3.9.6. Protokollierung und Überwachung

Sicherheitsrelevante Ereignisse wie fehlgeschlagene Log-Ins oder Einbruchversuche werden gesammelt, mit Zugriffsrechten besonders geschützt und wenn nötig analysiert, um sicherheitsrelevante Vorkommnisse aufzuklären.

3.9.7. Cloud-Dienste

Cloud-Dienste unterliegen dem gleichen Sicherheitsniveau wie andere Dienste oder Systeme des Unternehmens. Die Erfüllung des Sicherheitsniveaus kann durch vertragliche Zusicherung (siehe Lieferantenbeziehungen) gewährleistet werden.

3.9.8. Uhrensynchronisation

Alle Uhren von IT-Systemen werden zentral mit einem einzigen Zeitserver synchronisiert.

3.10. Anschaffung und Entwicklung von Systemen

Ziel: Neu entwickelte oder angeschaffte Systeme erfüllen unsere Anforderungen an Informationssicherheit.

3.10.1. Anschaffung von Komponenten

Hardware und andere Komponenten sind auf einen definierten Anforderungskatalog der IT zu überprüfen. Bei Anschaffung sind mindestens folgende Kriterien in Bezug auf Informationssicherheit zu berücksichtigen:

- Unterstützungszeitraum für Updates (Firmware, Micro-Kernel und andere Sicherheitsupdates)
- Erfüllung unserer Anforderungen an Netzwerksicherheitsfunktionen
- Anschaffungszeitraum

Eine Prüfung des IT-Systems auf Einhaltung der Vorgaben wird vor dem produktiven Einsatz durchgeführt.

3.10.2. Softwareentwicklung

Die Entwicklung von Software und Systemen, intern oder durch Dritte, berücksichtigt folgende Aspekte:

- Sicherheitsanforderungen an Quellcodeverwaltung und Entwicklungsumgebung
- Sicherheitsanforderungen an das Produkt
- Test der Sicherheitsanforderungen
- Umgang mit Testdaten

3.11. Kapazitätsplanung

Ziel: Es werden Ressourcen in Ihrer Auslastung überwacht und Prognosen erstellt, um die erforderlichen Ressourcen in Zukunft bereitzustellen.

IT-Systeme werden wie folgt überwacht, um Ressourcenknappheit vorzubeugen und rechtzeitig Planungen / Gegenmaßnahmen einzuleiten:

3.12. Reaktion auf Sicherheitsvorfälle

Ziel: Auf Sicherheitsvorfälle wird angemessen reagiert und die Erfahrungen genutzt, um das ISMS und den Angriffsschutz zu verbessern.

3.12.1. Computer Emergency Response Team

Um auf Vorfälle und Sicherheitsprobleme reagieren zu können, wird ein Computer Emergency Response Team berufen. Die Aufgaben sind unter anderem:

- Überwachen von Systemen und Datenströmen auf verdächtige Aktivitäten
- Koordination von Reaktionen auf Sicherheitsvorfälle
- Forensische Analyse zur Aufarbeitung von Vorfällen
- Erkenntnisse aus Vorfällen fließen in die laufende Verbesserung der Systemsicherheit ein
- Befugnis zum Aussetzen von Sicherheitsrichtlinien, um im Notfall Handlungsfähigkeit zur Wiederherstellung des Normalbetriebs sicherzustellen

Auf Informationssicherheitsvorfälle wird durch das CERT angemessen reagiert, Dienste wiederhergestellt und Erfahrungen fließen in Verbesserungsmaßnahmen ein. Zur Meldung von Informationssicherheitsereignissen besteht ein Meldeformular, das für alle Mitarbeiter zugänglich ist.

3.13. Business Continuity Management

Ziel: Sicherstellen der Handlungsfähigkeit in Ausnahmesituationen.

Das Unternehmen identifiziert mit Hilfe des Risikomanagements mögliche Gefahrensituationen für das Unternehmen und konstruiert Notfallpläne und Maßnahmen, die in diesen Fällen die Handlungsfähigkeit des Unternehmens aufrechterhalten. Dieser besteht aus dem ISB, EDV und QM. Bei Bedarf werden die betroffenen Bereiche mit einbezogen und die Geschäftsführung über Maßnahmen und Prozesse informiert.

3.14. Desaster Recovery Process

Wiederherstellungsprozess von Laufwerken
→ Virenscan, Einspielen von Backup
→ siehe Backup-Richtlinie

3.15. DSGVO

3.15.1. Prinzipien für die Verarbeitung von personenbezogenen Daten

Fairness und Rechtmäßigkeit
Bei der Verarbeitung personenbezogener Daten muss das informationelle Selbstbestimmungsrecht des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise erhoben und verarbeitet werden.

Zweckbindung
Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

Datenvermeidung und Datensparsamkeit
Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden. Personenbezogene Daten dürfen nicht auf

Vorrat für potenzielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

Löschung und Speicherbegrenzung
Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt ist.

Sachliche Richtigkeit und Datenaktualität
Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

Vertraulichkeit und Datensicherheit
Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

3.15.2. Zulässigkeit der Datenverarbeitung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der nachfolgenden Erlaubnistatbestände vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

3.15.3. Kunden-, Lieferanten- und Geschäftspartnerdaten

Datenverarbeitung für eine vertragliche Beziehung
Wenn die Datenverarbeitung personenbezogener Daten der Vertragserfüllung oder der Erfüllung vorvertraglicher Maßnahmen dient, so ist die Verarbeitung zulässig.

Einwilligung in die Datenverarbeitung
Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden.
Vor der Einwilligung muss der Betroffene gemäß dieser Datenschutz-Leitlinie informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z. B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Die Erteilung muss dokumentiert werden.

Datenverarbeitung aufgrund gesetzlicher Erlaubnis
Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

Datenverarbeitung aufgrund berechtigten Interesses
Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses unseres Unternehmens erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z. B. Durchsetzung von offenen Forderungen) oder wirtschaftliche (z. B. Vermeidung von Vertragsstörungen). Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen.

Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen.

Automatisierte Einzelentscheidungen
Automatisierte Verarbeitungen personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale (z.B. Kreditwürdigkeit) bewertet werden, dürfen nicht die ausschließliche Grundlage für Entscheidungen mit negativen rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen sein. Dem Betroffenen muss die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit zu einer Stellungnahme gegeben werden. Zur Vermeidung von Fehlentscheidungen muss eine Kontrolle und eine Plausibilitätsprüfung durch einen Mitarbeiter gewährleistet werden.

Nutzerdaten und Internet
Wenn auf Webseiten oder in Apps personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber in Datenschutzerklärungen und ggf. Cookie Hinweisen zu informieren. Die Datenschutzhinweise und ggf. Cookie-Hinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind.
Werden zur Auswertung des Nutzungsverhaltens von Webseiten und Apps Nutzungsprofile erstellt (Tracking), so müssen die Betroffenen darüber in jedem Fall in den Datenschutzerklärungen informiert werden. Erfolgt das Tracking unter einem Pseudonym, so soll dem Betroffenen in den Datenschutzerklärungen eine Widerspruchsmöglichkeit eröffnet werden (Opt-out).

3.15.4. Mitarbeiterdaten

Datenverarbeitung für das Arbeitsverhältnis
Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind.

Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt. Eine Einwilligung ist auch für eine Verwendung der Daten für weitere Bewerbungsverfahren oder vor der Weitergabe der Bewerbung an andere Unternehmensteile erforderlich.

Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift.

Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den Bewerber bei einem Dritten erforderlich, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des Betroffenen einzuholen.

Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

Datenverarbeitung aufgrund gesetzlicher Erlaubnis
Die Verarbeitung personenbezogener Mitarbeiterdaten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften. Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des Mitarbeiters berücksichtigt werden.

Kollektivregelungen für Datenverarbeitungen
Geht eine Verarbeitung über den Zweck der Vertragsabwicklung hinaus, so ist sie auch dann zulässig, wenn sie durch eine Kollektivregelung gestattet wird. Kollektivregelungen sind Tarifverträge oder Vereinbarungen

zwischen Arbeitgeber und Arbeitnehmervertretungen im Rahmen der Möglichkeiten des jeweiligen Arbeitsrechts. Die Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken und sind im Rahmen des staatlichen Datenschutzrechts gestaltbar.

Einwilligung in die Datenverarbeitung
Eine Verarbeitung von Mitarbeiterdaten kann aufgrund einer Einwilligung des Betroffenen stattfinden.
Einwilligungserklärungen müssen freiwillig abgegeben werden. Unfreiwillige Einwilligungen sind unwirksam. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Erlauben die Umstände dies ausnahmsweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung muss in jedem Fall ordnungsgemäß dokumentiert werden. Bei einer informierten freiwilligen Angabe von Daten durch den Betroffenen kann eine Einwilligung angenommen werden, wenn nationales Recht keine explizite Einwilligung vorschreibt. Vor der Einwilligung muss der Betroffene gemäß dieser Datenschutz-Leitlinie informiert werden.

Datenverarbeitung aufgrund berechtigten Interesses
Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses unseres Unternehmens erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z. B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftlich begründet.

Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen. Das Vorliegen schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen.

Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmaßnahme (z. B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Maßnahme betroffenen Mitarbeiters am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das berechtigte Interesse des Unternehmens und die möglichen schutzwürdigen Interessen der Mitarbeiter müssen vor jeder Maßnahme festgestellt und dokumentiert werden. Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen
(z. B. Mitbestimmungsrechte der Arbeitnehmervertretung und Informationsrechte der Betroffenen) berücksichtigt werden.

Verarbeitung besonders schutzwürdiger Daten
Besonders schutzwürdige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten, über die Gesundheit oder das Sexualleben des Betroffenen.
Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden.
Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die verantwortliche Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann.
Der Mitarbeiter kann freiwillig auch ausdrücklich in die Verarbeitung einwilligen.

Automatisierte Entscheidungen
Soweit im Beschäftigungsverhältnis personenbezogene Daten automatisiert verarbeitet werden, durch welche einzelne Persönlichkeitsmerkmale bewertet werden (z. B. im Rahmen der Personalauswahl oder der Auswertung von Fähigkeitsprofilen), darf eine solche automatisierte Verarbeitung nicht die ausschließliche Grundlage für Entscheidungen mit negativen Folgen oder erheblichen Beeinträchtigungen für die betroffenen Mitarbeiter sein.

Um Fehlentscheidungen zu vermeiden, muss in automatisierten Verfahren gewährleistet sein, dass eine inhaltliche Bewertung des Sachverhalts durch eine natürliche Person erfolgt und diese Bewertung Grundlage für die Entscheidung ist. Dem betroffenen Mitarbeiter muss außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben werden.

Telekommunikation und Internet
Telefonanlagen, E-Mail-Adressen, Intranet und Internet sowie interne soziale Netzwerke werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und Unternehmensressource. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der unternehmensinternen Richtlinien genutzt werden.

Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Intranet- und Internet-Nutzung findet statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer sind Schutzmaßnahmen an den Übergängen in das Netzwerk implementiert worden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit und Nachvollziehbarkeit wird die Nutzung der Telefonanlagen, der E-Mail-Adressen, des Intranets und Internets sowie der internen sozialen Netzwerke protokolliert.

Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien unseres Unternehmens erfolgen. Diese Kontrollen dürfen nur unter Wahrung des Verhältnismäßigkeitsprinzips erfolgen. Die jeweiligen nationalen Gesetze sind ebenso zu beachten wie die hierzu bestehenden Konzernregelungen. Die Auswertungen dienen nicht der Leistungserfassung.

3.15.5. Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb oder innerhalb unseres Unternehmens unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten.

Der Empfänger der Daten muss darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden.

Im Falle einer Datenübermittlung an einen externen Empfänger in einem Drittstaat muss dieser ein zu dieser Datenschutz-Leitlinie gleichwertiges Datenschutzniveau gewährleisten.

Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt.
Im Falle einer Datenübermittlung von Dritten an unser Unternehmen muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

3.15.6. Auftragsdatenverarbeitung

Eine Auftragsdatenverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. In diesen Fällen ist mit externen Auftragnehmern eine Vereinbarung über eine Auftragsdatenverarbeitung abzuschließen.

Dabei behält das beauftragende Unternehmen die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der Erteilung des Auftrags sind die nachfolgenden Vorgaben einzuhalten; der beauftragende Fachbereich muss ihre Umsetzung sicherstellen.

1. Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.

2. Der Auftrag ist in Textform zu erteilen.
Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des

Auftragnehmers zu dokumentieren.

3. Der Auftraggeber muss sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung nachweisen.

4. Je nach Risiko der Datenverarbeitung ist die Kontrolle gegebenenfalls während der Vertragslaufzeit regelmäßig zu wiederholen.

5. Bei einer grenzüberschreitenden Auftragsdatenverarbeitung sind die jeweiligen nationalen Anforderungen für eine Weitergabe personenbezogener Daten ins Ausland zu erfüllen. Insbesondere darf die Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum in einem Drittstaat nur stattfinden, wenn der Auftragnehmer ein zu dieser Datenschutz-Leitlinie gleichwertiges Datenschutzniveau nachweist.

6. Anerkennung verbindlicher Unternehmensregeln des Auftragnehmers zur Schaffung eines angemessenen Datenschutzniveaus durch die zuständigen Datenschutz Aufsichtsbehörden.

3.15.7. Rechte des Betroffenen

Jeder Betroffene kann die folgenden Rechte wahrnehmen.
Ihre Geltendmachung ist umgehend durch den verantwortlichen Bereich zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen.

1. Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind. Falls im Arbeitsverhältnis nach dem jeweiligen Arbeitsrecht weitergehende Einsichtsrechte in Unterlagen des Arbeitgebers
(z. B. Personalakte) vorgesehen sind, so bleiben diese unberührt.

2. Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.

3. Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.

4. Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung widersprechen. Für diese Zwecke müssen die Daten gesperrt werden.

5. Der Betroffene ist berechtigt, die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.

6. Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt.
Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

3.15.8. Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern untersagt.

Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner

Aufgaben betraut und entsprechend berechtigt zu sein. Es gilt das Need-to-know-Prinzip:

Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist.

Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten.

Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen.

3.15.9. Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen.

Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen.

Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten (ermittelt durch den Prozess zur Informationsklassifizierung) zu orientieren.

Die technisch organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des unternehmensweiten Informationssicherheits- und Datenschutz-Managements und müssen kontinuierlich an die technischen Entwicklungen und organisatorische Änderungen angepasst werden.

3.15.10. Datenschutzvorfälle

Jeder Mitarbeiter muss der Geschäftsleitung oder dem Datenschutzbeauftragten unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle) melden.

In Fällen von
- unrechtmäßiger Übermittlung personenbezogener Daten an Dritte,
- unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten oder
- bei Verlust personenbezogener Daten

sind die im Unternehmen vorgesehenen Meldungen unverzüglich vorzunehmen, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen erfüllt werden können.

3.15.11. Verantwortlichkeiten und Sanktionen

Die Geschäftsleitung ist für die verordnungskonforme Datenverarbeitung personenbezogener Daten verantwortlich.

Damit ist sie verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutzrichtlinie enthaltenen Anforderungen des Datenschutzes eingehalten werden (z. B. nationale Meldepflichten).

Es ist eine Managementaufgabe der Geschäftsleitung, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen.

Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter.
Bei Datenschutzkontrollen durch Behörden ist der Datenschutzbeauftragte umgehend zu informieren. Der

Datenschutzbeauftragte ist Ansprechpartner für den Datenschutz.
Er kann Kontrollen durchführen und die Mitarbeiter mit den Inhalten der Datenschutz-Leitlinie vertraut machen.

Die Geschäftsleitung ist verpflichtet, den Datenschutzbeauftragten in seiner Tätigkeit zu unterstützen.
Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen müssen der Datenschutzbeauftragten rechtzeitig über neue Verarbeitungen personenbezogener Daten informieren.

Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Datenschutzbeauftragte schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten.

Die Geschäftsleitung hat sicherzustellen, dass ihre Mitarbeiter im erforderlichen Umfang zum Datenschutz geschult werden. Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht werden in vielen Staaten auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen.

Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.

3.15.12. Datenschutzbeauftragter

Der Datenschutzbeauftragte als fachlich weisungsunabhängiges Organ wirkt auf die Einhaltung der Datenschutzvorschriften hin. Der Datenschutzbeauftragte ist berechtigt:
- auf die Beachtung der Datenschutzvorschriften und deren Einhaltung hinzuwirken,
- Büroräume aus datenschutzrechtlichen Gesichtspunkten zu besichtigen und zu bewerten,
- Stellungnahmen innerhalb der Abteilungen einzuholen,
- Mitarbeiter über die Einhaltung des Datenschutzes zu belehren,
- grob fahrlässige Zuwiderhandlungen gegen datenschutzrechtliche Bestimmungen unverzüglich der Geschäftsführung anzuzeigen. Der Datenschutzbeauftragte unterrichtet die Geschäftsleitung zeitnah über Datenschutzrisiken.

Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Datenschutzbeauftragten wenden.

Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt.

Der Datenschutzbeauftragte:

Johannes Landerer
PCK IT Consulting GmbH
Telefon: 0831 / 56400 500
e-Mail: johannes.landerer@pck-consulting.de
https://www.pck-consulting.de

3.16. Compliance

Ziel: Einhaltung gesetzlicher und vertraglicher Vorgaben.

Personenbezogene Daten dürfen nur erhoben, genutzt oder verarbeitet werden, soweit dies für festgelegte, eindeutige und rechtmäßige Zwecke erforderlich ist. Es ist Mitarbeitern untersagt, neue Erkenntnisse, sowie Patente und Erfindungen in irgendeiner Form an Dritte weiterzugeben. Weitere Informationen können im Dokument „ISMS_18.V01 Verhaltensrichtlinien der ABT-Gruppe“ gefunden werden.

Mitarbeiter sind dazu angehalten sich an die internen Verhaltensrichtlinien zum Thema Compliance zu halten. Nationale und internationale Bestimmungen regeln, wie Produkte und Technologien verkauft werden sollen oder Informationsaustausch mit Wettbewerbern betrieben werden darf. Die jeweiligen Bestimmungen sind für Mitarbeiter bindend. Deshalb gilt im Wettbewerb um Marktanteile das Gebot der Integrität. Insbesondere dürfen Mitarbeiter mit Wettbewerbern keine Gespräche führen, bei denen Preise oder Kapazitäten abgesprochen werden.

Unser Unternehmen setzt sich zum Ziel, vertragliche und gesetzliche Vorgaben stets zu erfüllen. Hierzu setzen wir wie folgt um:

- Regelmäßige Identifikation von Compliance-Anforderungen
- Überprüfung und Umsetzung dieser Anforderungen
- Zusammenarbeit mit externen Parteien wie Behörden, um Compliance sicherzustellen
- Offene Kultur, die das Melden von Missständen fördert

Änderungshistorie:

Datum	*Version*	*Autor*	*Beschreibung*
01.11.2019	001	CDI	Erste Version der Dokumentvorlage mit Kopf- und Fußzeile.
12.05.2020	002	M. Frik	Erste Ausarbeitung der Punkte 6 - 11
15.05.2020	003	M. Frik	Ausarbeitung Punkte 7 - 11
03.09.2020	004	CDI	Kopf- und Fußzeile auf neues Format angepasst
06.10.2020	005	CDI	Geltungsbereich der Dokumente in der Einleitung erfasst
25.11.2020	006	SaSc	Punkt 3.15 DSGVO hinzugefügt
29.01.2021	007	CDI	Entsorgung von Akten und Dokumenten eingefügt
20.07.2022	008	PBA	Review und Überarbeitung mit PCK
05.09.2023	009	CDI	Review und Aktualisierung ABT SE