Technische und organisatorische Maßnahmen zum Datenschutz und Datensicherheit
PCV Systemhaus GmbH & Co. KG

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

1. Zutrittskontrolle
Sicherungsmaßnahmen des Gebäudes / Betriebsgeländes

Folgende technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle finden Anwendung:

Die PCV Systemhaus GmbH & Co. KG realisiert die Zutrittskontrolle, d. h. die Kontrolle über den physischen Zutritt zu den Datenverarbeitungsanlagen, im Rahmen des §9 BDSG durch folgendes Konzept:

Technisches Konzept:

1. Zutrittskontrolle Firmengebäude:
   Das Öffnen der Eingangstüren des Gebäudes kann mittels Schlüssel der Schließanlage erfolgen.
2. Überwachung des Gebäudes
   Das Gebäude ist darüber hinaus zu Nacht- und Wochenendzeiten mit einer Alarmanlage gesichert und mit einem Videoaufzeichnungssystem ausgerüstet. Das Gebäude wird durch einen externen Wachdienst bei Alarm überprüft. Bei Einbruch gibt es ein akustisches Signal.
3. Zutritt zu Räumen mit datenverarbeitenden Systemen (Serverräume):
   Der Serverraum ist permanent mit einer einbruchs- und feuerhemmenden Tür verschlossen. Zutritt ist nur für autorisierte Personen mittels Schlüssel möglich. Die tägliche Datensicherung wird schriftlich dokumentiert.

Organisatorisches Konzept:

1. **Zutrittskontrolle Firmengebäude:**
   Zutritt zum Gebäude ist nur den Mitarbeitern gestattet. Gäste müssen von den entsprechenden Mitarbeitern im Foyer in Empfang genommen werden und dürfen sich nicht frei im Gebäude bewegen.

2. **Zutritt zum Gebäude**
   Zutritt zum Gebäude erhalten nur Personen mit entsprechendem Schlüssel und Alarmanlagenfreischaltungschip.
3. **Verwaltung der Zutrittsmittel**
   Es existiert ein Schlüsselbuch in welchem die Dokumentation der Zutrittsmittel geregelt ist. Dies ist ein Schlüsselbuch/Schlüsselverzeichnis.
   Maßnahmen/Regelungen bei Verlust eines Zutrittsmittels werden ebenfalls im Schlüsselbuch festgehalten.
4. **Sicherungsmaßnahmen innerhalb der Geschäftsräume**
   Die Räume der Datenverarbeitung verfügen über einen separaten Schließkreis.
5. **Zutritt sonstiger Personen in die Geschäftsräume**
   Dritte haben die Möglichkeit von 7:30 bis 19:00 Uhr über dem Empfang (begleitet) in die Geschäftsräume zu gelangen.
6. **Reinigung der Geschäftsräume**
   Die Geschäftsräume werden durch einen externen Dienstleister gereinigt. Räume, in denen die Datenverarbeitungsserver aufgestellt sind, werden durch interne Kräfte gereinigt.
7. **Sicherungsmaßnahmen in den Räumlichkeiten**
   Geschäftsräume im EG sind mit Isolierverglasung versehen. Räume mit Datenverarbeitungsanlagen (Serverraum) besitzen keine Fenster.

2. Zugangskontrolle

Mit der Zugangskontrolle soll die Benutzung der Datenverarbeitungsanlagen gesichert werden. Zunächst betrifft dies den lokalen Zugangsschutz, wie z.B. passwortgesicherter Zugang auf Betriebssystemebene. Bei vernetzten Systemen muss der Zugang zusätzlich gegen Zugriffe über das Netz geschützt werden. Insbesondere bei Anschluss an das Internet sind erhöhte Anforderungen an den Schutz zu stellen. Eine Sicherung hat i.d.R. über eine Firewall zu erfolgen. Die unbefugte Nutzung der Datenverarbeitungsanlage wird unterbunden durch folgende,

technische Maßnahmen:

- Zugang zu Netzwerkdiensten nur über zentrales Benutzerregister (Active Directory Domain Services) mit Benutzername und Passwort
- Notwendigkeit einer zusätzlichen Einrichtung zur Authentifizierung an sensiblen Systemen
- Konzern-Vorgaben für Passwortkomplexität und -haltbarkeit

organisatorische Maßnahmen:

- Datensicherungen werden verschlüsselt extern gelagert

3. Zugriffskontrolle

Einsichtnahme und Verarbeitung personenbezogener Daten ist nur denjenigen Personen erlaubt und möglich, denen entsprechende Zugriffsrechte erteilt wurden, oder die zwingend für die Erbringung von Auftragsleistungen durch den Auftraggeber beauftragt wurden.

Eine bedarfsorientierte Ausgestaltung des Berechtigungskonzepts kann detailliert auf Basis von Rollen erfolgen. Teilweise kann eine noch differenziertere Vergabe von Rechten zur Benutzung der Datenverarbeitungsanlage erteilt werden.

Arbeitsplatzgestaltung
Die eingerichteten Arbeitsplätze sind in den Bereichen, in denen Besucher Zugang haben, so gestaltet, dass Externen keinen Einblick (Bildschirm, Drucker, Fax, usw.) auf personenbezogene Daten geboten wird.

Identifikation und Authentifikation von Benutzern
Identifikation und Authentifikation von Benutzern erfolgt mit User-ID und Passwort am Client sowie an der Anwendung/Host (abhängig von der Applikation). Nach 15 min Inaktivität des Benutzers wird die Bildschirmsperrung des Arbeitsplatzrechners erzwungen. Die Bildschirmsperre ist nur durch Eingabe des Passwortes aufhebbar.

Passwortrichtlinien
Es existieren Vorgaben für die Mindestlänge und Komplexitätsanforderungen von Passwörtern. Passwörter sind mit einer Gültigkeitsdauer versehen.

Remotezugriff von Mitarbeitern
Remotezugriff von Mitarbeitern erfolgt über die Dienstrechner der Mitarbeiter sowie über verschlüsselte VPN-Verbindungen. Die Dienstrechner sind mit dem aktuellen Virenschutz versehen. Jeder Remotezugriff muss beantragt werden und unterliegt der Genehmigung. Die genehmigten Anträge werden dokumentiert. Die Einrichtung des Remotezugriffs erfolgt durch die hausinterne IT Abteilung.

Zugriffskontrolle zum Datenverarbeitungssystem
Zu verstehen ist hier insbesondere die Kontrolle der Berechtigung zum Zugriff auf die jeweiligen Daten. Nur die Person, die den Zugriff auf die jeweiligen Daten für die jeweilige Tätigkeit benötigt, darf die Zugriffsrechte erhalten. Es wird gewährleistet, dass die Nutzungsberechtigten ausschließlich auf ihre Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, verändert oder entfernt werden können.

Systemadministration
Die Administration der Datenverarbeitungssysteme wird von internen Mitarbeitern der PCV Systemhaus GmbH & Co. KG durchgeführt. Administratoren identifizieren sich mit User-ID und Passwort gegen den Client und ggf. die Anwendung/Host.

Trennungskontrolle
Es wird gewährleistet, dass die zu unterschiedlichen Zwecken erhobenen Daten getrennt verarbeitet werden und zwar durch eine logische sowie physikalische Trennung.

4. Weitergabekontrolle/Aufbewahrung/Vernichtung

Ziel ist die Gewährleistung, dass personenbezogene Daten bei der elektronischen Übertragung oder während eines Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen, eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
Die Datenweitergabe und der Datentransport beruht auf einheitlichen Systemen zur Authentifizierung von Benutzern durch Benutzerkennung, Zertifikat und Passwort. Alle Kanäle über unsichere Medien werden mittels kryptographischer Verschlüsselung (VPN) gesichert.
Datenträger, die aus Gründen der Betriebssicherheit angefertigt werden, werden an zentralen Stellen unter Verschluss gehalten (im Sicherheitsbereich + Tresor).

Datenträger werden aus Gründen der Betriebssicherheit zusätzlich an einem externen Standort ausgelagert.

Nicht mehr benötigte Dokumente in Papierform werden über einen zertifizierten externen Dienstleister datenschutzkonform entsorgt.

Maßnahmen, die beim Transport, bei der elektronischen Übertragung und Übermittlung oder Speicherung auf Datenträger das unbefugte Lesen, Ändern, Kopieren oder Löschen verhindern:

Transport:
- Datenträger werden adäquat geschützt durch:
  a) Verschlüsselung der Daten mit geeigneten Verfahren
  b) ggf. Versand in geschützten Behältnissen

Elektronische Übertragung:
Verwendung verschlüsselter Verbindungen

Das Löschen und Ändern eigener, personenbezogener Daten erfolgt nach entsprechenden Berechtigungen (Unbefugten ist dies nicht möglich). Der Umgang mit fremden personenbezogenen Daten (Verarbeitung im Auftrag) ist nach Verfahrensanweisungen geregelt und jederzeit überprüfbar.

5. Eingabekontrolle

Alle Änderungen eigener personenbezogener Daten werden nachvollziehbar protokolliert (Protokolldateien mit folgenden Feldern: Zeitpunkt der Änderung, Benutzername des ändernden Mitarbeiters, alter Inhalt vor der Änderung und Art der Änderung).

Die Verarbeitung personenbezogener Daten im Rahmen von Auftragsdatenverarbeitung wird protokolliert oder gemäß Verfahrensanweisung gehandhabt.

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

6. Verfügbarkeitskontrolle

Datensicherung
Eigene personenbezogene Daten werden täglich gesichert;
fremde personenbezogene Daten werden in ebenfalls geeigneten Safes im Lager der PCV Systemhaus GmbH & Co. KG (Original des Auftraggebers) gelagert. Es erfolgt eine tägliche Prüfung der Protokollierung der Datensicherung.
Jeden Monat wird ein Einleseversuch der Datensicherung unternommen.
Jedes Jahr wird eine Wiederherstellung durchgeführt.

Unterbrechungsfreie Stromversorgung/Notstromaggregat
Alle systemrelevanten Datenverarbeitungsanlagen sind mit einer ausreichend dimensionierten USV versehen. Diese wird regelmäßig gewartet und einmal monatlich betrieben.

Wiederherstellbarkeit
Es findet mindestens einmal im Jahr ein Wiederherstellungstest statt. Die zeitliche Planung und die Einteilung der Wiederherstellungstests wird von der hausinternen IT Abteilung gesteuert. Die Ergebnisse der Wiederherstellungstest werden dokumentiert. Es gibt einen definierten Eskalationsprozess, welcher sicherstellen soll, dass Fehler und Probleme bei der Durchführung des Tests eingetreten sind, zeitnah behoben werden.

Richtlinien zur Datensicherheit
Vorliegende Richtlinien
- Datensicherungskonzept
- Sicherheits- und Notfallkonzept
- IT-Sicherheitsanforderung
- Förderung des Sicherheitsbewusstseins der Mitarbeiter
- Nutzung von E-Mail
- Nutzung von Internet
- Schutz, Bekanntgabe und Vernichtung von Daten
- Sicherheitsleitlinien für Mitarbeiter

Regelmäßige Aktivitäten
- Wartung von Sicherheitseinrichtungen
- administrativer Support
- Reaktion auf sicherheitsrelevante Ereignisse
- fortlaufende Überwachung der IT-Systeme
- Change Management
- Überprüfung von Maßnahmen auf die Übereinstimmung mit der Sicherheitspolitik
- Mitarbeiterschulungen

Weitergehende Maßnahmen
- Basis Benutzerpasswort
- Spam Filter
- Virtual Privat Network (VPN) für Datenverschlüsselung
- Secure Sockets Layer (SSL)
- Desktop Antiviren Software
- Gateway Antiviren Software
- Anwendungs-Firewalls
- Netzwerk-Firewalls
- VPN-Lösungen für Homeoffice-Anbindungen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. b DSGVO, Art. 25 Abs. 1 DSGVO)

7. Datenschutzmanagement

Das Datenschutzmanagementsystem ist ein Instrument zur Einhaltung von Datenschutzbestimmungen. Die PCV Systemhaus GmbH & Co. KG führte bereits in 2015 ein zentrales Datenschutzmanagement ein.
In das Datenschutzmanagement sind die Geschäftsleitung als Verantwortliche sowie beratend und regulatorisch der Datenschutzbeauftragte eingebunden. Die Aufgaben und die Pflichten des Datenschutzbeauftragten finden sich in Art. 39 DSGVO. Die Bestellung erfolgt formal und anhand einer standardisierten Vorlage.

Zu den Aufgaben des Datenschutzbeauftragten gehören

- Überwachung des Umfangs sowie der Verfahren, Methoden und Prozesse, mit deren Hilfe personenbezogene Daten verarbeitet werden.
- Erstellung, Pflege Verzeichnis für Verarbeitungstätigkeiten
- Einweisung der mit der Datenverarbeitung betrauten Personen und Unterrichtung über die datenschutzrechtlichen Grundlagen, sowie Verpflichtung der Mitarbeiter auf das Datengeheimnis.
- Überwachung und Koordinierung der technischen und organisatorischen Maßnahmen, die zur Sicherstellung des Datenschutzes gem. BDSG erforderlich sind.
- Die Einhaltung des Grundsatzes der Datenvermeidung und Datensparsamkeit in Bezug auf personenbezogene Daten sicherzustellen.
- Durchführung und Dokumentation von Vorabkontrollen, soweit notwendig bzw. vorgeschrieben.
- Vertretung des Unternehmens gegenüber Externen, in bzw. zu Fragen des Datenschutzes (z.B. gegenüber den Aufsichtsbehörden).
- Beratung der Unternehmensleitung sowie einzelner Fachabteilungen zu datenschutzrechtlichen Fragen.
- Erarbeitung betriebsinterner Richtlinien und Definition adäquater Prozesse zur praktischen Umsetzung der Datenschutzbestimmungen inkl. der Kontrolle auf Einhaltung.

Bei Datenverarbeitungsvorgaben, aus denen sich Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, wird der Beauftragte für den Datenschutz schon vor der Einführung der Verarbeitung beteiligt. Dies gilt insbesondere für besondere, schutzbedürftige und personenbezogene Daten.

Bei Datenschutzverletzungen und Beschwerden sind die verantwortlichen Führungskräfte durch definierte Prozesse verpflichtet, umgehend den Beauftragten für den Datenschutz zu unterrichten. Daneben kann sich jeder Betroffene jederzeit mit Anfragen an den Beauftragten für Datenschutz wenden. Die Anfragen und Beschwerden werden vertraulich behandelt. Die Entscheidungen des Beauftragten für den Datenschutz zur Abhilfe der Datenschutzverletzung sind durch die Geschäftsführung zu respektieren.

Der Datenschutzbeauftragte berichtet an die Geschäftsleitung in regelmäßigen Abständen in Schriftform.

Verantwortlichkeiten und Sanktionen
Die Verantwortlichkeiten sind intern geregelt. Eine missbräuchliche Verarbeitung von personenbezogenen Daten oder andere Verstöße gegen das Datenschutzrecht werden strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen.

Zuwiderhandlung, für die einzelner Mitarbeiter verantwortlich gemacht werden können, ziehen grundsätzlich arbeitsrechtliche Sanktionen entsprechend dem geltenden Recht bezogen auf diese Personen nach sich.

Datenschutzregelungen
Von der Richtline zum Datenschutz werden Verfahrensanweisungen abgeleitet. Sie regeln konkrete Vorgänge und Abläufe, definieren die Verantwortlichkeiten dafür und schreiben Dokumentationspflichten vor. Falls notwendig auch weitere verfahrensbezogene technische und organisatorische Maßnahmen. Folgende Vorgänge sind durch diese Regelungen abgedeckt:

- Informationspflichten des Unternehmens
- Wahrung der Rechte der Betroffenen
- Umgang mit Kunden und Patientendaten (inkl. Fernwartung und Datenimporte)
- Datenschutzfolgeabschätzung
- AV Verträge
- Datenpannen

Die Verfahrensanweisungen werden durch Hilfsmittel wie Checklisten und Vorlagen begleitet. Alle Dokumente sind zentral abgelegt.

Neben den verpflichtenden Datenschutzregelungen wurden bestimmte Prozesse zentral durch Automatismen geregelt. Dazu gehören:

- Verpflichtung aller Mitarbeiter auf das Datengeheimnis nach DSGVO sowie auf die Schweigepflicht nach §203 StGB (Verpflichtungen sind als Anlagen in die Arbeitsverträge integriert, jeder neue Mitarbeiter wird somit vor Beginn der Tätigkeit verpflichtet)

- Schulung neuer Mitarbeiter auf Datenschutz zeitnah der Einstellung (Pflicht zur Schulung neuer Mitarbeiter)

- Datenschutzprüfung neuer Software/Module bereits während der Planungsphase

Kontrollprozesse
Es werden regelmäßig Datenschutzaudits durchgeführt.

Es wird ein Protokoll zum Datenschutzaudit erstellt. Das Protokoll beinhaltet neben den Prüfergebnissen auch eine Risikoeinschätzung. Die Audits werden alle zwei Jahre durchgeführt und protokolliert. Die Audits werden mit der Geschäftsleitung besprochen.

Vor der Einführung neuer Verfahren werden die Prozesse umfangreich auf datenschutzrechtliche Anforderungen geprüft.

Auftragskontrolle
Den Kunden wird grundsätzlich empfohlen, die Fernwartungs-Zugänge geschlossen zu halten und nur bei Bedarf und nach telefonischer Anfrage den Zugang frei zu schalten. Dieses Vorgehen liegt im Interesse des Kunden.

In der Regel werden Fernwartungs-Werkzeuge verwendet, bei welchen der Kunde aktiv den Zugang freigeben muss und die Aktivitäten mitverfolgen kann (z.B. Teamviewer). Wenn die eingesetzte Fernwartungssoftware diese aktive Freigabe nicht voraussetzt, wird der Kunde über die Notwendigkeit des Zugriffs informiert und seine Zustimmung dafür angefordert. Die Zustimmung (wer und wann) wird dokumentiert.

Die Dokumentation des Fernwartungszugriffs und dessen Inhalt erfolgt immer in einem CRM System. Es ist nicht erlaubt, undokumentierte Fernwartungszugriffe durchzuführen. Sämtliche Aktivitäten auf dem Kundensystem sind nachvollziehbar für Dritte sachlich beschrieben.
Hierbei wird immer:

- der ausführende Mitarbeiter
- der Zeitpunkt (Datum/Uhrzeit) und die Dauer
- das Zielsystem (Test oder Produktivsystem, Remotedesktop, usw.)
- das Fernwartungsmedium (z.B. Teamviewer)
- die Tätigkeiten sachlich in Kurzform insbesondere, wenn Prozesse gestoppt/gestartet, Änderungen in Datenbanken, Änderungen in Konfigurationstabellen, Uploads und Downloads durchgeführt wurden
- bei kritischen Tätigkeiten als 4-Augenprinzip herangezogene Kollegen dokumentiert.

Die Aufzeichnung der durchgeführten Sitzung, falls die Fernwartungssoftware diese Funktion unterstützt, wird nicht durchgeführt. Falls in bestimmten Situationen diese Aufzeichnung notwendig wäre, muss sie vom Kunden selbst und nur auf seinem System durchgeführt werden.

Ein Sonderfall stellt die Aufzeichnung des Vorgangs dar, wo ausschließlich mit anonymisierten Testdaten gearbeitet wird. In diesem Fall wird nicht mit personenbezogenen Daten gearbeitet, die Aufzeichnung darf stattfinden.

Mit Kunden, die per Fernwartung betreut werden, müssen einmalig schriftliche Datenschutzvereinbarungen, sog. AV Verträge (AVV), abgeschlossen werden. Diese Vereinbarungen regeln die Fernwartungszugriffe sowie Datenverarbeitung auf den Kundensystemen.

Auftragskontrolle und Datenimport
Für den Import von Kundendaten gilt ein generelles Verbot mit Erlaubnisvorbehalt. Der Import der Kundendaten ist somit nur in Ausnahmefällen, nur im Auftrag des Kunden und nur unter bestimmten Voraussetzungen erlaubt:

- Es besteht keine andere Möglichkeit als nur mit Echtdaten des Kunden ein Problem zu beheben oder einen Kundenauftrag zu erfüllen.
- Es liegt eine schriftliche Vereinbarung (befristeter AV Vertrag) zwischen dem Kunden und der PCV Systemhaus GmbH & Co. KG vor, die den Import selbst, Umfang der Daten, Art und Zweck der Verarbeitung sowie den vorgesehenen Zeitraum regelt.
- Vor dem Import wird eine schriftliche Vereinbarung mit dem Kunden getroffen. Dies erfolgt ausschließlich in Form eines befristeten AV Vertrages. In dem Vertrag werden immer: Zweck des Imports, Art und Umfang der Daten, Zeitraum der Nutzung und Löschfristen eingegeben. Andere Formen der Vereinbarung sind nicht erlaubt. Die Übermittlung der Daten erfolgt nur in schriftlicher Form.

Die Kundendaten werden nur auf den dafür vorgesehenen geschützten Serverbereichen importiert. Die Datenhaltung von nicht anonymisierten Kundendaten auf Arbeitsplatzrechner, Notebooks oder externen portablen Speichermedien ist strengstens untersagt.

Während des Analysevorgangs wird der Original-Datenträger des Kunden in einem Safe aufbewahrt. Alle Datenträger mit Kundendaten sind für die Aufbewahrung explizit als solche gekennzeichnet und erkennbar.

Jeder am Analyseprozess beteiligte Mitarbeiter dokumentiert seine Tätigkeiten und Abläufe mit den Kundendaten im CRM System an dem initialen Eintrag, und ohne Personenbezüge.

Der Vorgang im CRM System wird so lange „offen gehalten“, bis die Daten vernichtet oder an den Kunden zurückgesandt worden sind.

Am Ende des Vorgangs werden alle Datenbestände gelöscht. Für die Einhaltung der mit den Kunden vereinbarten Löschfristen, ist der jeweilige Vorgesetzte der für den Import verantwortlichen Person zuständig.

Die Originaldatenträger werden entsprechend der getroffenen Vereinbarungen vernichtet oder zurückgeschickt.

Sicherheitsbuch Datenimporte
Neben der Dokumentation der durchgeführten Tätigkeiten in einem CRM System werden bei jedem Datenimport bestimmte Angaben in einem zu diesem Zweck geführtem Sicherheitsbuch eingetragen. Das Sicherheitsbuch wird in Papierform geführt und muss eine festgebundene Form haben.

Folgende Angaben werden zu jedem Import in dem Buch eingetragen:

- Kunde: Name, Kundennummer, Ort und Ansprechpartner
- Grund des Imports
- Bearbeiter: Name
- AV Vertrag (befristet): Datum des Abschlusses
- Eingang: Datum, Empfänger
- Kopie auf Server: Servername und Verzeichnis
- Aufbewahrungsort des Originaldatenträgers (nur falls Import mittels Datenträger)
- Bearbeitung Beginn: Datum
- Bearbeitung Ende: Datum
- Löschung der Kopie vom Server: Datum, Name Mitarbeiter
- Originaldaten nach Abschluss der Arbeiten: Datenträger vernichtet oder zurückgeschickt, Datum, Name Mitarbeiter, Art der Vernichtung

Risikomanagement
Mit den Richtlinien zum Notfallplan bei Verletzungen des Schutzes personenbezogener Daten soll sichergestellt werden, dass:

- Sicherheitsvorfälle frühzeitig erkannt und deren Auswirkung minimiert oder begrenzt werden können
- Sicherheitsvorfälle einheitlich zentralisiert werden
- bei Eintreten eines Vorfalls strukturierte und zeitsparende Vorgehensmodelle in Verbindung mit klaren Verantwortlichkeiten existieren wie z.B.: Erste Maßnahmen, Vorgehensweisen bei Notfällen u. Ausfällen, Reihenfolge der Alarmierung der Verantwortlichen, Wiederanlaufverfahren, hierarchische aufgebaute Eskalationsketten innerhalb der PCV Systemhaus GmbH & Co. KG
- Vorfälle nachvollziehbar dokumentiert, begutachtet und analysiert werden können
- die Wiederholung des Vorfalls durch Ergreifen nachhaltiger Maßnahmen vermieden werden kann