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 / Betriebsgelände

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 erhalten nur Personen mit entsprechendem Schlüssel und Alarmanlagenfreischaltungschip.

3. Verwaltung der Zutrittsmittel
   Es existiert ein Schlüsselbuch in welchen die Dokumentation der Zutrittsmittel geregelt ist. Dies ist ein Schlüsselbuch/Schlüsselverzeichnis. Maßnahmen/Regellungen bei Verlust eines Zutrittsmittels ist 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

Smartphones / mobile E-Mail

Einige Mitarbeiter (Techniker / GF) haben mit ihrem Mobiltelefon /Smartphone die Möglichkeit, unterwegs Emails zu empfangen/versenden. Daher ist das Mobiltelefon mit einem Passwort/PIN Code geschützt, um vertrauliche Informationen nicht unbefugten Dritten verfügbar zu machen.

Home-Office / Telearbeitsplatz

Emails können über Outlook Web Access nur über eine verschlüsselte Verbindung (https) von jedem beliebigen PC aus abgerufen werden. Hierzu sind Benutzername und Passwort des User-Accounts erforderlich, analog der Authentifizierung im Netzwerk. Fernverbindungen auf den Firmenserver / Telearbeitsplätze sind nur über die Firewall und nur über zertifikatsbasierte SSL-VPN Verbindungen mit Passwortabfrage möglich, dies entspricht den aktuellen Sicherheitsstandards.

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 kein 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 zu 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 personenbezogenen 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.

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

4. Weitergabekontrolle/Aufbewahrung/Vernichtung

Ziel ist die Gewährleistung, dass personenbezogene Daten bei der elektronischen Übertragung oder während eines Transport 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 -transport 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, dass 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, das 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 Datenschutznestimmungen. 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 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 oder 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 einzelnen Mitarbeiter verantwortlich gemacht werden können, ziehen grundsätzlich arbeitsrechtliche Sanktionen entsprechend dem geltenden Recht bezogen auf diese Personen an 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
- Gewährung 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 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.