Technische und organisatorische Maßnahmen (TOM)

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

1. Verantwortliche Stelle

Firma	PCV Systemhaus GmbH & Co. KG
Straße	Auf den Hundert Morgen 15
PLZ/Ort	41516 Grevenbroich
Telefon	02182 8268 123
Fax	02182826888
E-Mail	datenschutz@pcv.de
Internet Adresse (URL)	www.pcv.de
Fachverantwortlicher für dieses Verfahren	Carsten Priebs
Organisationseinheit	Datenschutzmanagement

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

• Zutrittskontrolle:

Abgeschlossene Serverräume
Alarmanlage
Personenkontrolle beim Pförtner/Empfang
Regelmäßige Überprüfung der Schutzmaßnahmen für Serverräume.
Schließsystem mit Codesperre
Regelungen für Zutritt zu Serverräumen externer Personen
Schlüsselregelung/Schlüsselbuch
Videoüberwachung der Zugänge
Der Zugang zum Serverraum ist nur für berechtigte Personen gestattet

• Zugangskontrolle:

Authentifikation mit Benutzer und Passwort
Autorisierte Geräte bekommen logischen Zugang zum Netzwerk.
Benutzerberechtigungen verwalten

Technische und organisatorische Maßnahmen (TOM)

Einsatz von Anti-Viren-Software
Einsatz von Firewalls
Einsatz von VPN-Technologie
Erstellen von Benutzerprofilen
Formale Benutzerregistrierung für Informationssysteme
Passwortvergabe/Passwortregeln
Regelung für den Umgang mit Passwörtern
Schlüsselregelung/Schlüsselbuch
Sorgfältige Auswahl von Reinigungspersonal
Verschlüsselung von Datenträgern
W-LAN ist gesichert

• Zugriffskontrolle:

Anzahl der Administratoren auf das Mindeste begrenzt
Clean Desk
Einsatz von Aktenvernichtern
Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat)
Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399-1, DIN 66399-2 und DIN-SPEC 66399-3)
Passwortrichtlinie inkl. Länge und Wechsel
Protokollierung der Vernichtung von Daten
Verschlüsselung von Datenträgern
Verwaltung der Benutzerrechte durch Systemadministratoren

• Trennungskontrolle:

"Interne Mandantenfähigkeit" ist hergestellt.
Logische Mandantentrennung (softwareseitig).
Physikalisch getrennte Speicherung auf gesonderten Systemen und Datenträgern.
Trennung von Produktiv- und Testsystem.

• Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO):

Eine Pseudonymisierung findet nicht statt.

3. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Technische und organisatorische Maßnahmen (TOM)

• Weitergabekontrolle:

Angemessene Verschlüsselungstechniken
Datenübergabe nur gegen Nachweis
Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
Einrichtung von VPN-Tunneln
Mitarbeiterunterweisung
Prüfung der Rechtmäßigkeit der Weitergabe von Daten
Regelungen bei Ausscheiden von Mitarbeitern
Regelungen zum datenschutzkonformen Vernichten von Datenträgern
Verpflichtung der Mitarbeiter auf das Datengeheimnis
Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

• Eingabekontrolle:

Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
Protokollierung der Eingabe, Änderung und Löschung von Daten
Protokollierung genutzter Dienste
Schutz gegen Manipulation
Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

• Verfügbarkeitskontrolle:

Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
Erstellen eines Notfallplans
Feste Prozesse zur Datensicherung
Feuer- und Rauchmeldeanlagen
Feuerlöschgeräte in Serverräumen
IT- Risiken sind über Versicherungen abgedeckt
Kapazitätsplanung für die Datensicherung

Technische und organisatorische Maßnahmen (TOM)

Mitarbeiterschulungen für Sicherheitsanweisungen
Serverräume nicht unter sanitären Anlagen
Testen von Datenwiederherstellung
Unterbrechungsfreie Stromversorgung (USV)

• Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO):

Notfallmanagement inkl. Notfallpläne.
Testen der Wiederherstellungssysteme.
Backup Konzept (Offline/Online in der Cloud).

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

• Datenschutz-Management:

Die Datenschutz-Folgenabschätzung (DSFA wird bei Bedarf durchgeführt)
Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
Interner / externer Datenschutzbeauftragter
meinDatenschutz.de wird bei uns als Datenschutzmanagement Lösung eingesetzt und in regelmäßigen Abständen auf Aktualität geprüft.
Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet

Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach
Bedarf / Berechtigung (z.B. Wiki, Intranet ?)

• Incident-Response-Management:

Datenschutz-Management
Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
Dokumentierte Vorgehensweise zum
Umgang mit Sicherheitsvorfällen
Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)

Technische und organisatorische Maßnahmen (TOM)

Einbindung von DSB und/oder ISB in Sicherheitsvorfälle und Datenpannen
Einsatz von Firewall und regelmäßige Aktualisierung
Einsatz von Spamfilter und regelmäßige Aktualisierung
Einsatz von Virenscanner und regelmäßige Aktualisierung
Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
Regelmäßige Datenschutzschulungen

• Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO):

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO).
Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

• Auftragskontrolle:

Ausreichende Ressourcen für Datenschutzmanagementsystem
Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
Auszusondernde Hardware wird sicher zerstört
Datenschutz-/ Datensicherheitskonzepte
Datenschutzbeauftragter
Datenschutzmanagement-Audits und Maßnahmenplan
Datenschutzreport
Dokumente werden aktuell gehalten
Hard- und Softwareprodukte aus seriösen Quellen
Prozesse für Betroffenenrechte
Schriftliche Weisungen an den Auftragnehmer (z. B. durch Auftragsverarbeitungsvertrag) i.S.d. Art. 28 DS-GVO
Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
Unterauftragnehmer haben die gleichen Anforderungen wie Auftraggeber zu erfüllen
Verpflichtung der Mitarbeiter des Auftragnehmers auf die Vertraulichkeit
Vertragliche Verpflichtung der Auftragnehmer
Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation
Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbaren