Checkliste **“Datenschutzprüfung in der Pflegeeinrichtung”**

Diese Premium-Checkliste richtet sich an Geschäftsführung, Pflegedienstleitung und interne Datenschutzverantwortliche. Sie basiert auf realen Prüferfahrungen, gesetzlichen Anforderungen wie DSGVO, BDSG, SGB V, SGB XI, SGB XII sowie § 203 StGB und berücksichtigt typische Risiken aus der pflegerischen Praxis. Jeder Punkt ist so formuliert, dass er unmittelbar überprüft werden kann und den Anforderungen einer tatsächlichen Datenschutzprüfung entspricht.

1. Datenschutzorganisation

- ○ Schriftliche Bestellung des Datenschutzbeauftragten liegt vor.
- ○ Meldung des Datenschutzbeauftragten an die Aufsichtsbehörde ist dokumentiert.
- ○ Qualifikation und pflegebezogene Fachkunde des Datenschutzbeauftragten sind nachweisbar.
- ○ Weisungsfreiheit des DSB ist dokumentiert und wird eingehalten.
- ○ Organigramm weist den DSB eindeutig aus.
- ○ Direkte Berichtslinie zur Geschäftsführung ist festgelegt.
- ○ Aktuelle Kontaktdaten des DSB sind intern hinterlegt.

2. Verzeichnis der Verarbeitungstätigkeiten (VVT)

- ○ Alle relevanten Prozesse erfasst: Pflegedokumentation, Bewohnerverwaltung, Abrechnung, Personalverwaltung, Dienstplanung, Hausnotruf, IT-Verwaltung, Schulungsverwaltung, Videoüberwachung.
- ○ Rechtsgrundlagen vollständig und korrekt: DSGVO, BDSG, SGB V, SGB XI, SGB XII, § 203 StGB.
- ○ Zwecke jeder Verarbeitung eindeutig formuliert.
- ○ Datenkategorien vollständig benannt, einschließlich Gesundheitsdaten.
- ○ Empfänger (intern und extern) klar definiert.
- ○ Drittlandübermittlungen explizit ausgeschlossen oder rechtlich begründet.
- ○ Technische und organisatorische Maßnahmen je Verarbeitung dargestellt.
- ○ Löschfristen vollständig, dokumentiert und mit SGB XI/XII abgestimmt.
- ○ Datum der letzten Aktualisierung eindeutig gekennzeichnet.

- ○ Verantwortliche Rollen pro Verarbeitung benannt.

3. Technische und organisatorische Maßnahmen (TOMs)

- ○ Rollen und Rechte in der Pflegesoftware nach dem Prinzip minimaler Rechte vergeben.
- ○ Rechtematrix vorhanden und aktuell.
- ○ Zugriffsprotokollierung aktiv und auswertbar.
- ○ Passwortkonzept dokumentiert und verbindlich.
- ○ Keine generischen Dienstkonten vorhanden.
- ○ Mobile Geräte vollständig verschlüsselt und zentral verwaltbar.
- ○ Fernlöschung über Mobile Device Management möglich.
- ○ Private Geräte für dienstliche Zwecke ausgeschlossen oder streng geregelt.
- ○ Firewalls, Virenschutz und Sicherheitsupdates aktiv und dokumentiert.
- ○ Backup-Konzept vorhanden und jährlich überprüft.
- ○ Backups regelmäßig getestet und Wiederherstellungen dokumentiert.
- ○ Papierakten verschlossen verwahrt, Zugriffskonzept vorhanden.
- ○ Stationszimmer und Computer gegen Einsicht geschützt.
- ○ Klare Regelungen zur Einsicht in Pflegedokumentationen vorhanden.

4. Auftragsverarbeitung (AVV)

- ○ Aktuelle Liste aller Dienstleister mit Zugriff auf personenbezogene Daten vorhanden.
- ○ Für jeden relevanten Dienstleister existiert ein vollständiger AV-Vertrag.
- ○ TOM-Dokumente der Dienstleister geprüft und abgelegt.
- ○ Fernwartungszugriffe eindeutig geregelt und protokolliert.
- ○ Kein Dienstleister ohne AV-Vertrag produktiv im Einsatz.

5. Besondere Risiken im Pflegealltag

- ○ Regelung zu Wundfotos dokumentiert: nur Dienstgeräte, zentrale Speicherung, Löschkonzept.
- ○ Einwilligungen zu Foto- und Videodokumentation korrekt dokumentiert.
- ○ Übergaben finden nicht in öffentlichen Bereichen statt.
- ○ Diagnosen werden nicht öffentlich ausgesprochen.
- ○ Telefonische Angehörigenkommunikation mit Identitätsprüfung geregelt.
- ○ Weitergabe von Informationen nur mit Einwilligung oder Vollmacht.

- ○ Arzt- und Klinikkommunikation dokumentiert und abgesichert.
- ○ Ambulante Tourenpläne geschützt und nicht in privaten Apps gespeichert.
- ○ Fahrzeuge mit sensiblen Unterlagen verschlossen.
- ○ Minimierung von Papier im Außendienst dokumentiert.

6. Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO

- ○ Prüfen Sie, ob Verarbeitungen mit hohem Risiko vorliegen (z. B. Gesundheitsdaten, systematische Beobachtung, mobile Pflegeprozesse).
- ○ DSFA-Vorprüfung durchgeführt (Dokumentation: „DSFA erforderlich ja/nein “).
- ○ Falls DSFA notwendig: vollständige Durchführung dokumentiert.
- ○ Risikoanalyse gemäß Art. 35 Abs. 7 DSGVO erstellt.
- ○ Maßnahmen zur Risikominimierung definiert und umgesetzt.
- ○ DSB in den Prozess einbezogen und Stellungnahme dokumentiert.
- ○ DSFA regelmäßig überprüft und bei wesentlichen Änderungen aktualisiert.

7. Bewohner- und Patientenrechte

- ○ Datenschutzhinweise nach Art. 13 DSGVO erstellt und nachweislich übergeben.
- ○ Auskunftsprozesse klar dokumentiert und technisch umsetzbar.
- ○ Identitätsprüfung vor Auskünften fest definiert.
- ○ Berichtigungsprozesse dokumentiert.
- ○ Löschprozesse dokumentiert und technisch umsetzbar.
- ○ Archivierungsregeln entsprechen SGB XI/XII.

8. Personalverwaltung

- ○ Sensibelste Gesundheitsdaten getrennt und geschützt abgelegt.
- ○ Arbeitsunfähigkeitsunterlagen gesichert verwahrt.
- ○ BEM-Verfahren dokumentiert.
- ○ Zugriffsrechte auf Personalakten klar geregelt.
- ○ Regelmäßige Datenschutzschulungen für alle Mitarbeitenden dokumentiert.
- ○ Teilnehmerlisten und Schulungsinhalte archiviert.
- ○ Neue Mitarbeitende bereits zum Arbeitsbeginn geschult.

9. IT-Systeme und Pflegesoftware

- ○ Rechtevergabe nach Funktion dokumentiert.
- ○ Administratorrechte klar definiert und eingeschränkt.
- ○ Logfiles vorhanden, gesichert und regelmäßig ausgewertet.
- ○ Backup-Konzept aktiv im Einsatz.
- ○ Wiederherstellungstests dokumentiert.
- ○ Updates und sicherheitsrelevante Patches dokumentiert.

10. Interne Prozesse und Kommunikation

- ○ Regelung für Faxkommunikation vorhanden.
- ○ E-Mail-Verschlüsselung aktiv und verpflichtend.
- ○ Vorlagen für sichere Arztkommunikation vorhanden.
- ○ Prozesse für kritische Ereignisse dokumentiert.
- ○ Prozesse für Datenschutzvorfälle nach Art. 33 DSGVO dokumentiert.
- ○ Erreichbarkeit des Datenschutzbeauftragten definiert.

11. Abschlussbewertung

- ○ Alle sicherheitsrelevanten Mängel dokumentiert.
- ○ Konkreter Maßnahmenplan erstellt.
- ○ Verantwortlichkeiten für Maßnahmen eindeutig festgelegt.
- ○ Bewertung der Prüfreife abgeschlossen.

Auswertung und nächste Schritte

Nach dem Durcharbeiten der Checkliste sollten Sie bewerten, wie viele Punkte Sie nicht eindeutig mit „erledigt“ markieren konnten. Jeder offene Punkt steht für ein konkretes Risiko. Wenn mehr als drei Punkte ungelöst bleiben, ist die Wahrscheinlichkeit hoch, dass Ihre Einrichtung im Rahmen einer Datenschutzprüfung negativ auffällt. Prüfer erkennen strukturelle Schwächen sehr schnell, insbesondere in Bereichen wie Pflegedokumentation, Wundfotografie, IT-Sicherheit und Auftragsverarbeitung.

In diesem Fall ist es sinnvoll, die offenen Punkte nicht weiter aufzuschieben. Pflegeeinrichtungen profitieren stark von einer fachlich spezialisierten Begleitung, da typische Fehler meist nicht im juristischen Bereich entstehen, sondern im Pflegealltag: Schichtdienst, mobile Pflege, unklar geregelte Übergaben, fehlende AV-Verträge, offene Monitore und organisatorische Lücken. Genau hier setzt eine professionelle Unterstützung an.

Als spezialisierter externer Datenschutzbeauftragter für Pflegeeinrichtungen begleite ich Sie dabei, sämtliche offenen Punkte vollständig, prüffest und alltagstauglich umzusetzen. Sie erhalten klar definierte Prozesse, vollständige und belastbare Dokumente, ein nachvollziehbares Löschkonzept sowie eine Struktur, die sowohl der Aufsicht als auch dem MDK standhält. Das Ziel ist nicht Papierkram, sondern Sicherheit im Alltag und ein verlässlicher Standard, der dauerhaft funktioniert.

Wenn Sie bei der Dokumentation Ihrer Verarbeitungstätigkeiten starten oder bestehende Unterlagen aktualisieren möchten, können Sie zusätzlich mein Muster für die Verarbeitung „Pflegedokumentation“ nutzen. Die Vorlage enthält alle typischen Anforderungen an ambulante und stationäre Pflegeeinrichtungen und ermöglicht einen schnellen Einstieg in eine rechtssichere VVT-Struktur.

➔ **VVT-Muster “Pflegedokumentation”** herunterladen:

https://datenschutzgerechte-pflege.de/vvt-muster-pflegedokumentation/

Bewerte diese Checkliste, folge mir auf Instagram und schreib mir dort eine kurze Nachricht – dann bekommst du die VVT-Vorlage „Mitarbeiterverwaltung“ gratis dazu.

https://www.instagram.com/datenschutzgerechtepflege/