Unterlage für Datenschutzbeauftragte (DSB) & IT-Abteilung

Vertrag zur Auftragsverarbeitung (AVV) gemäß Art. 28 DSGVO

inkl. Anlage 1 (Verarbeitungsdetails), Anlage 2 (TOM nach Art. 32 DSGVO) und Anlage 3 (Unterauftragsverarbeiter) · Version 1.0 (Stand: 11/2026)

Auftraggeber (Verantwortlicher):	Name / Einrichtung / Anschrift des Lizenznehmers (siehe Unterschriftsfeld unten)
Auftragnehmer (Auftragsverarbeiter):	**NurseCraft – Bastian Dieckhues**, Breilbusch 4, 59387 Ascheberg, Deutschland · E-Mail: info@nursecraft.de

§ 1 Gegenstand, Dauer und Weisungsgebundenheit

Der Auftragnehmer stellt dem Auftraggeber die Online-Plattform **NurseCraft** (`https://nursecraft.de`, `bedside.html`, `lms.nursecraft.de`) zur Planung, Durchführung und Dokumentation der gesetzlichen Praxisanleitung bereit. Die Verarbeitung personenbezogener Daten erfolgt ausschließlich im Auftrag und nach dokumentierten Weisungen des Auftraggebers. Die Laufzeit entspricht der jeweiligen Lizenzvereinbarung.

§ 2 Pflichten des Auftragnehmers & Vertraulichkeit

- Der Auftragnehmer gewährleistet die Vertraulichkeit der verarbeiteten Daten (Art. 28 Abs. 3 lit. b DSGVO) und trifft alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO (Anlage 2).
- Bei Störungen oder Datenschutzverletzungen (Art. 33, 34 DSGVO) informiert der Auftragnehmer den Auftraggeber unverzüglich (spätestens binnen 24 Stunden nach Bekanntwerden) unter Angabe aller relevanten Details.
- Der Auftragnehmer unterstützt den Auftraggeber bei Betroffenenrechten (Art. 15–22 DSGVO) sowie Datenschutz-Folgenabschätzungen (Art. 35 DSGVO) und löscht bzw. gibt sämtliche Daten nach Vertragsende auf Weisung heraus (spätestens nach 30 Tagen).
- Der Auftraggeber ist berechtigt, die Einhaltung der technischen und organisatorischen Maßnahmen nach vorheriger Ankündigung zu prüfen bzw. geeignete Nachweise anzufordern.

Anlage 1 – Gegenstand, Datenkategorien und betroffene Personen

Art & Zweck der Verarbeitung:	Digitale Planung von Praxisanleitungen, Erfassung von 10-%-Nachweisen gem. § 4 Abs. 3 PflAPrV, Gesprächsprotokolle, ALACT-Reflexionen, Azubi-Pool-Synchronisation innerhalb der Einrichtung sowie LMS-Teilnehmerzuordnung.
Datenkategorien:	Stammdaten der Praxisanleitenden (Name, dienstliche E-Mail, Einrichtung, Station/Funktion, Profilbild optional); Ausbildungsdaten der Lernenden (Name/Pseudonym, Ausbildungsjahr, Einsatzort, absolvierte Anleitungszeiten, Lernziele, Reflexionsnotizen). **Hinweis:** Patientenbezogene Gesundheitsdaten (Art. 9 DSGVO) dürfen gemäß Nutzungsbedingungen nicht mit Klarnamen eingegeben werden.
Betroffene Personen:	Praxisanleitende, Pflegepädagog*innen/PDL sowie Auszubildende / Lernende des Auftraggebers.

Anlage 2 – Technische und organisatorische Maßnahmen (TOM, Art. 32 DSGVO)

- **Zutritts- & Zugangskontrolle:** Dedizierte selbstgehostete Server-Hardware in Deutschland; SSH-Zugriff nur mit Authentifizierung; Admin-Zugang geschützt; Passwörter der Nutzer ausschließlich per **Bcrypt** gesalzen und gehasht gespeichert.
- **Zugriffskontrolle & Mandantentrennung:** Serverseitige PocketBase-Hooks erzwingen strikte Trennung nach Nutzerkonto (`@request.auth.id`) und Einrichtungs-Lizenzcode (`inst_pool_lic_*`). Unauthentifizierte Zugriffe auf Nutzerlisten, Lizenzen oder fremde Reflexionen sind technisch blockiert.
- **Übertragungs- & Eingabekontrolle:** Durchgehende Transportverschlüsselung via TLS/HTTPS inkl. HSTS, Content-Security-Policy (CSP), X-Frame-Options und serverseitige Filter-Maskierung.
- **Verfügbarkeit & Belastbarkeit:** Tägliche automatisierte Datenbank-Backups (`cron 02:00 Uhr`) plus verschlüsselte Off-Site-Snapshots; Offline-Resilienz der Web-App über Service Worker.

Anlage 3 – Unterauftragsverarbeiter

Dienstleister / Infrastruktur	Zweck	Standort / Garantie
Eigene Serverinfrastruktur (Synology DS725+)	Web-Hosting, PocketBase-Datenbank, Moodle LMS	**Deutschland (100 % Self-Hosted)**
IONOS SE (Elgendorfer Str. 57, Montabaur)	DNS-Routing & geschäftlicher E-Mail-Verkehr (`info@nursecraft.de`)	**Deutschland / EU (DSGVO)**
Google Ireland Limited / Google LLC *(optional, nur bei aktiver KI-Nutzung)*	KI-Didaktik-Coach & Pflegeplanungscheck über serverseitigen Proxy (ohne Patienten-Klarnamen)	EU / USA (EU-Standardvertragsklauseln & EU-US Data Privacy Framework)

Auftraggeber (Einrichtung / Schule)

Einrichtung, Ort, Datum

Unterschrift / Stempel Auftraggeber

Auftragnehmer (NurseCraft)

Ascheberg, den _____

Bastian Dieckhues, Inhaber NurseCraft