MUSTER · STAND 07.11.2026

Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO – Muster

> Keine Rechtsberatung. Nicht anwaltlich geprüft.

Muster, keine Rechtsberatung. Nicht anwaltlich geprüft. Eine Arbeitshilfe für Sie und Ihre Datenschutzbeauftragte bzw. Ihren Datenschutzbeauftragten; die Bewertung liegt bei Ihnen als Verantwortlichem. Geschlossen wird die Vereinbarung je Hauptvertrag: für den Testtag und, bei einem Folgeauftrag, für Einrichtung und Betreuung; ausgefüllt wird sie nach der Prozessaufnahme. Stand: 07.11.2026.

Kontomodell dieser Fassung: Der Testtag läuft über das Geschäftskonto von Illig bei Anthropic; Anthropic ist dann nur für diesen Tag Unterauftragsverarbeiter von Illig. Der Betrieb läuft über das Abo „Claude Team“ Ihrer Firma bei Anthropic; Anthropic ist dann Ihr eigener Auftragsverarbeiter.

Zwischen [Firma, Rechtsform], [Anschrift], [Registergericht, Registernummer], vertreten durch [Name, Funktion] – nachfolgend **„Kunde“**, Verantwortlicher –

und Nick Illig, Prozessautomatisierung (Einzelunternehmen, Marke „Illig Automatisierung“), Unterm Grasweg 57, 79379 Müllheim, Deutschland, nick@illig-automatisierung.com – nachfolgend **„Illig“**, Auftragsverarbeiter –

Vorbemerkung

(1) Der Kunde setzt eine KI-Mitarbeiterin ein (nachfolgend **„System“**): ein Software-Kit von Illig auf Basis von Claude Code (Anthropic). Es arbeitet auf einem eigenen PC oder einer eigenen virtuellen Maschine des Kunden (nachfolgend **„KI-PC“**) unter einem eigenen Windows-Benutzerkonto ohne Administratorrechte und bedient dort Programme über Bildschirmfotos, Maus und Tastatur, einschließlich Microsoft Teams und Outlook. Für jeden Arbeitsschritt nutzt es das KI-Modell Claude (§ 8).

(2) Der Kunde ist **Verantwortlicher**. Illig ist **Auftragsverarbeiter**, soweit er bei Testtag, Einrichtung, Betreuung und Fernwartung auf personenbezogene Daten zugreift oder zugreifen kann; schon die Zugriffsmöglichkeit bei Fernwartung ist nach Auffassung der Datenschutzkonferenz Auftragsverarbeitung (Kurzpapier Nr. 13). Überblick: Rollen.

(3) Die Verarbeitung durch Anthropic regelt am Testtag diese Vereinbarung (§ 8 Abs. 4), im Betrieb der eigene Vertrag des Kunden mit Anthropic (§ 8 Abs. 3).

---

§ 1 Gegenstand und Dauer

(1) **Hauptvertrag** (ankreuzen):

- ☐ Vereinbarung zum Testtag vom [Datum], ein Testtag mit genau einem Ablauf: [Bezeichnung]
- ☐ Vertrag über Einrichtung und Betreuung vom [Datum]

(2) **Gegenstand** sind die Tätigkeiten von Illig, bei denen er auf personenbezogene Daten zugreift oder zugreifen kann:

1. **Testtag:** Vorbereitung bei Illig nur mit Musterdaten; am Testtag Installation auf dem KI-PC, Einweisung, Begleitung der vereinbarten Fälle, Vergleich der Ergebnisse, Anhalten des Systems.
2. **Einrichtung:** Installation und Konfiguration, Anbindung an freigegebene Ordner, Postfächer, Teams und Programme, Arbeitsanweisung mit den Hausregeln des Kunden, Abnahmetest.
3. **Betreuung:** Fehlerbehebung, Anpassungen nach Weisung, Updates und Prüfungen, vor Ort oder per Fernwartung (§ 10). Dabei sieht Illig Protokolle, Arbeitsdateien und Bildschirminhalte des KI-PCs.
4. **Beendigung:** Abbau und Löschung (§ 13).

(3) **Ort.** Die Daten liegen auf den Systemen des Kunden; ausgenommen sind die Inhalte, die für jeden Arbeitsschritt an Anthropic gehen (§ 8). Illig greift vor Ort oder per Fernwartung zu, nur aus Deutschland oder einem anderen Staat der EU bzw. des EWR (weitere Länder nur nach § 15 Abs. 1). Auf eigenen Geräten oder in eigenen Diensten speichert er keine personenbezogenen Daten des Kunden, außer Kontaktdaten der Ansprechpersonen und Nachweisunterlagen (§ 13 Abs. 5).

(4) **Echte Daten erst nach Unterschrift.** Vorher arbeitet Illig nur mit Musterdaten und leeren Vorlagen. Echte personenbezogene Daten verarbeitet das System erst, wenn die Voraussetzungen nach § 4 Abs. 2 erfüllt sind; bis dahin nur Muster- oder Testdaten ohne Personenbezug.

(5) **Dauer.** Die Vereinbarung gilt ab Unterschrift, solange Illig Tätigkeiten nach Abs. 2 erbringt, und bis die Löschung nach § 13 abgeschlossen ist. Endet der Hauptvertrag, endet auch sie; § 13 gilt weiter. Die außerordentliche Kündigung bei schweren Verstößen bleibt unberührt.

(6) **Folgeauftrag.** Ein Folgeauftrag erhält eine eigene Vereinbarung nach diesem Muster; sie ersetzt ab ihrer Unterschrift die für den Testtag geschlossene Vereinbarung zur Auftragsverarbeitung.

Ab dann läuft das System nur noch über das Abo „Claude Team“ des Kunden bei Anthropic (§ 8 Abs. 3).

---

§ 2 Art und Zweck der Verarbeitung

(1) **Zweck** ist es, das System für die Abläufe nach Anlage 1 einzurichten, am Testtag zu erproben und auszuwerten und im Betrieb zu betreuen.

(2) **Art der Verarbeitung durch Illig:** Einrichten und Konfigurieren, Ansehen von Bildschirminhalten, Arbeitsdateien und Protokollen, Fehlersuche und -behebung, Anpassen der Arbeitsanweisung nach Weisung, Berichte für den Kunden, Löschen. Eigene Auswertungen nur anonymisiert und mit Zustimmung im Hauptvertrag.

(3) **Was das System tut.** Es liest Eingänge, bedient die freigegebenen Programme, legt Ergebnisse in den Systemen des Kunden ab und schreibt mit berechtigten Personen; dabei macht es Bildschirmfotos und führt Journal und Protokolle. Nach seiner Arbeitsanweisung wirkt es nur nach Freigabe einer eingetragenen Person nach außen und gibt sich gegenüber Menschen als KI zu erkennen. **Am Testtag soll es nicht nach außen wirken:** Nach seiner Arbeitsanweisung versendet es nichts nach außen, bucht nichts und ändert keine Stammdaten, sondern bereitet solche Schritte nur als Entwurf vor. Technisch gesperrt sind davon nur Outlook-„Senden“ ohne Freischaltung und bei der Einrichtung eingetragene Schaltflächen der Fachsoftware; die Freischaltung für interne Empfänger stellt das System selbst aus, und beim Klick prüft das Werkzeug den Empfänger nicht; Teams-Nachrichten, Eingaben im Browser und das Löschen einzelner Dateien begrenzen nur Arbeitsanweisung und Rechte. Auf Wunsch sperrt der Kunde zusätzlich das Senden nach außen in Exchange bzw. Microsoft 365 (Anlage 2, C7).

(4) **Ausdrücklich nicht Zweck** sind Entscheidungen über Personen mit rechtlicher oder ähnlich erheblicher Wirkung (Art. 22 DSGVO) – sie trifft ein Mensch des Kunden –, Leistungs- oder Verhaltenskontrolle von Beschäftigten, Profiling, die Auswertung von Protokollen zur Kontrolle einzelner Beschäftigter und jede Verarbeitung für eigene Zwecke von Illig (z. B. Training von KI-Modellen, Werbung, Referenzen mit echten Daten).

(5) **Freigaben im Betrieb.** Verzichtet der Kunde per Weisung in Textform für bestimmte Schritte auf Freigaben, gilt das nie für Fälle nach Abs. 4 und nicht, soweit die Nutzungsrichtlinie von Anthropic (Fassung ab 12.11.2026) eine Prüfung durch eine qualifizierte Person verlangt, z. B. bei Empfehlungen zu Schichten, Arbeitszeit, Lohn oder zur Bewertung einzelner Beschäftigter.

---

§ 3 Art der Daten und betroffene Personen

(1) Art der Daten und Kategorien betroffener Personen ergeben sich aus **Anlage 1**. In jedem Einsatz kommen außerdem vor: Nachrichten zwischen dem System und berechtigten Personen, Freigaben mit Name, Kanal und Uhrzeit, E-Mails des vereinbarten Postfachs, Bildschirmfotos (sie können alles zeigen, was auf dem KI-PC sichtbar ist), Journal, Protokolle und lokale Chatverläufe. Betroffen sind dabei immer die Beschäftigten, die mit dem System arbeiten.

(2) **Besondere Kategorien** (Art. 9 DSGVO) und Daten über Straftaten (Art. 10 DSGVO) gehören nur zum Ablauf, wenn Anlage 1 sie nennt. Gehen sie unaufgefordert ein, liest das System sie zwangsläufig mit, und der Inhalt geht für diesen Arbeitsschritt an Anthropic; nach seiner Arbeitsanweisung übernimmt es sie nicht in Journal oder Übergaben und meldet den Eingang einer berechtigten Person. **Hinweis:** Im Anhang des DPA von Anthropic (Schedule 1) steht bei „Special categories of personal data“ der Eintrag „None“. Sollen Daten nach Art. 9 DSGVO zum Ablauf gehören, klären Sie das bitte vorher mit Ihrem DSB.

(3) **Nicht Gegenstand** sind Zugangsdaten mit Zahlungsberechtigung (z. B. TAN, PIN) und Passwörter. Anmeldungen nimmt einmalig eine Person des Kunden vor.

---

§ 4 Pflichten und Rechte des Kunden

(1) **Verantwortung.** Der Kunde verantwortet die Zulässigkeit der Verarbeitung: die Rechtsgrundlage (Art. 6, ggf. Art. 9 Abs. 2 DSGVO); die Information der Betroffenen, auch über Anthropic als Empfänger und die Übermittlung in die USA (Art. 13, 14 DSGVO; Vorlage für Beschäftigte); sein Verzeichnis (Art. 30 Abs. 1 DSGVO); die Prüfung und ggf. Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO; Angaben dafür); die Bewertung der Drittlandübermittlung (§ 15); die Einbindung seines Datenschutzbeauftragten; falls vorhanden die Beteiligung des Betriebsrats: rechtzeitige Unterrichtung über den Einsatz von KI (§ 90 Abs. 1 Nr. 3 BetrVG) und Klärung der Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG, weil das System Freigaben und Nachrichten mit Namen und Uhrzeit protokolliert.

(2) **Voraussetzungen vor echten Daten:** Die Vereinbarung ist unterschrieben, und die vor dem Start nötigen Punkte aus Abs. 1 sind erledigt (Datenschutzbeauftragter eingebunden, Folgenabschätzung geprüft, Beschäftigte informiert, Betriebsrat beteiligt, Bewertung der Übermittlung in die USA dokumentiert).

Außerdem hat der Kunde die gewerblichen Bedingungen, das DPA und die Liste der Unterauftragsverarbeiter von Anthropic mit Abrufdatum erhalten (§ 8 Abs. 4).

Fehlt etwas davon, wird nur mit Muster- oder Testdaten ohne Personenbezug gearbeitet.

(3) **Mitwirkung.** Der Kunde stellt den KI-PC mit einem eigenen Windows-Konto für das System ohne Administratorrechte bereit, vergibt Rechte nur nach Anlage 1 – keine Zahlungs-, Banking- oder Unterschriftsrechte, keine persönlichen Postfächer oder Chats von Beschäftigten –, nimmt die Anmeldungen selbst vor, schützt den Raum des KI-PCs und sichert die Daten der Systeme, in die das System schreibt (Einzelheiten: Anlage 2).

(4) **Rechte.** Der Kunde kann jederzeit Weisungen erteilen (§ 5), Nachweise verlangen und prüfen (§ 14), den Fernzugang entziehen (§ 10 Abs. 6) und das System anhalten: Datei `STOP` im Kit-Ordner anlegen, das Windows-Konto des Systems sperren oder den Zugang bei Anthropic sperren (§ 8 Abs. 6).

(5) Der Kunde informiert Illig unverzüglich über Fehler oder Unregelmäßigkeiten. Rechtsberatung leistet Illig nicht; er unterstützt mit einer Beschreibung des Systems, seiner Datenflüsse und Maßnahmen.

---

§ 5 Weisungen

(1) Illig verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Kunden, auch hinsichtlich der Übermittlung in ein Drittland (Art. 28 Abs. 3 lit. a DSGVO). Ausnahme: Illig ist nach dem Recht der EU oder eines Mitgliedstaats dazu verpflichtet; dann teilt er dem Kunden diese Pflicht vorher mit, soweit das Recht das nicht verbietet.

(2) **Dokumentierte Weisungen** sind diese Vereinbarung mit Anlagen, der Hauptvertrag mit seiner Ablaufbeschreibung, die vom Kunden freigegebene Arbeitsanweisung des Systems und Einzelweisungen in Textform einer weisungsberechtigten Person nach Anlage 4. Mündliche Weisungen bestätigt der Kunde unverzüglich in Textform. Jede Änderung der Arbeitsanweisung dokumentiert Illig mit Datum, Inhalt und Weisung.

(3) Weisungsempfänger ist Nick Illig. Hält er eine Weisung für rechtswidrig, weist er den Kunden unverzüglich darauf hin und darf sie bis zur Bestätigung oder Änderung aussetzen (Art. 28 Abs. 3 UAbs. 2 DSGVO).

---

§ 6 Vertraulichkeit

(1) Illig erbringt die Leistungen persönlich und beschäftigt keine Mitarbeitenden. Er ist zur Vertraulichkeit verpflichtet, auch nach Ende dieser Vereinbarung (Art. 28 Abs. 3 lit. b DSGVO). Weitere Personen setzt er nur nach vorheriger Zustimmung des Kunden in Textform ein, nachdem er sie schriftlich auf Vertraulichkeit verpflichtet hat. Personenbezogene Daten gibt er nicht an Dritte weiter.

(2) **Keine Daten über die Dienste von Illig.** Personenbezogene Daten werden Illig nicht per E-Mail, WhatsApp oder über ähnliche Dienste geschickt; für Fehlerbilder genügen anonymisierte Beschreibungen. Bildschirmfreigaben mit personenbezogenen Daten finden nur über das Werkzeug nach § 10 oder in Besprechungen des Kunden statt. Geht Illig solches doch zu, löscht er es unverzüglich und teilt das mit. E-Mail, WhatsApp und Teams von Illig dienen nur der Abstimmung.

---

§ 7 Sicherheit der Verarbeitung

(1) Die Parteien treffen die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO in **Anlage 2** (TOM-Anlage), getrennt nach KI-Arbeitsplatz (Teil A), Illig (Teil B), Kunde (Teil C) und Anthropic (Teil D), mit Grenzen (Teil E). Den Schutzbedarf legt der Kunde in Anlage 1 fest.

(2) **Änderungen** sind zulässig, wenn das Schutzniveau gleichwertig oder besser bleibt. Wesentliche Änderungen teilt Illig vorher in Textform mit. Ein geringeres Schutzniveau erfordert eine Änderung dieser Vereinbarung.

(3) **Grenzen, offen benannt.** Die Regeln des Systems (z. B. Freigaben, Datensparsamkeit) sind Arbeitsanweisung und Protokoll, keine technische Sperre. Ein Sprachmodell hält sie in aller Regel ein, aber nicht in jedem Fall. Die harte Grenze sind die Rechte, die der Kunde dem System gibt. Weitere Grenzen: Anlage 2 und Grenzen des Kits.

(4) Verfügbarkeit und Reaktionszeiten regelt allein der Hauptvertrag. Illig ist Einzelunternehmer und hat keine Zertifikate oder Prüfsiegel. Die Rückfallebene bei einem Ausfall ist die Arbeit von Hand im Fachbereich.

---

§ 8 Rolle von Anthropic

(1) **Was an Anthropic geht.** Für jeden Arbeitsschritt gehen die nötigen Inhalte – Text, Dateiinhalte und Bildschirmfotos – verschlüsselt an das KI-Modell Claude, mit den darin enthaltenen personenbezogenen Daten. Vertragspartner für Kunden im EWR und in der Schweiz ist die **Anthropic Ireland, Limited** (Dublin). Laut Anthropic werden die Daten in den USA gespeichert und können auch in Europa, Asien und Australien verarbeitet werden. Grundlage sind die gewerblichen Bedingungen (Commercial Terms, Fassung vom 17.06.2025) mit dem Vertrag zur Auftragsverarbeitung von Anthropic (Data Processing Addendum, „DPA“, Fassung vom 24.02.2025) samt EU-Standardvertragsklauseln (Modul 2 und 3) und Schweizer Zusatz.

(2) **Laut diesen Bedingungen** trainiert Anthropic nicht mit den Inhalten, meldet Sicherheitsverletzungen spätestens binnen 48 Stunden, kündigt neue Unterauftragsverarbeiter mit 15 Tagen Widerspruchsfrist an und löscht nach Vertragsende binnen 30 Tagen. **Laut den Hilfeseiten von Anthropic** (Privacy Center, Claude Code „Data usage“; nicht Teil des Vertrags) werden Ein- und Ausgaben standardmäßig binnen 30 Tagen gelöscht, länger bei gesetzlichen Pflichten oder bei Markierung als Verstoß gegen die Nutzungsrichtlinie (Ein- und Ausgaben bis zu 2 Jahre, Klassifizierungswerte bis zu 7 Jahre); eine Speicherung von null Tagen ist nicht vereinbart. Zertifikate und Prüfberichte laut Trust Center von Anthropic (für „Claude via Anthropic's API“ und „Claude Team“): SOC 2 Typ II (Prüfbericht), ISO/IEC 27001:2022, ISO/IEC 42001:2023 und CSA STAR. Einzelheiten: Unterauftragsverarbeiter.

(3) **Betrieb über das Abo des Kunden.** Der Betrieb sowie Einrichtung und Betreuung laufen immer über ein eigenes Abo „Claude Team“ des Kunden bei Anthropic zu den gewerblichen Bedingungen mit DPA; Verbrauchertarife (z. B. Free, Pro, Max, Ultra) sind ausgeschlossen. Das Abo hat mindestens zwei Plätze: einen für das System, einen für eine Person des Kunden. Das System meldet sich mit seinem Konto in der Team-Organisation des Kunden an; einen API-Schlüssel nutzt es nicht. Was über das Kontingent seines Platzes hinausgeht, deckt vorab gekauftes Nutzungsguthaben, gedeckelt durch ein Ausgabenlimit des Kunden für die Organisation und für das Konto des Systems. Der Kunde zahlt Anthropic direkt; Illig reicht keine Claude-Kosten durch. Anthropic ist damit unmittelbar Auftragsverarbeiter des Kunden und **kein Unterauftragsverarbeiter von Illig**; Unterauftragsverarbeiter von Anthropic, Drittlandübermittlung, Meldungen und Kontrollen regelt allein dieser direkte Vertrag. Illig erhält keine Zugangsdaten zu dem Konto und wird nicht Mitglied der Organisation des Kunden bei Anthropic, außer der Kunde lädt ihn für eine bestimmte Aufgabe ein; das wird in Textform dokumentiert und danach wieder entzogen.

(4) **Testtag über das Konto von Illig.** Am Testtag läuft das System über das Geschäftskonto von Illig bei Anthropic zu den gewerblichen Bedingungen mit DPA. Der Kunde genehmigt hiermit die Anthropic Ireland, Limited als Unterauftragsverarbeiter von Illig, nur für den Testtag. Illig legt Bedingungen, DPA und Liste der Unterauftragsverarbeiter vorher mit Abrufdatum vor. Dazu gilt:

- **Bedienung durch Illig:** Illig bedient das System am Testtag selbst, per Fernzugriff oder auf Wunsch vor Ort, und meldet es am Ende des Testtags bei seinem Geschäftskonto ab, auf Bitte des Kunden sofort.
- **Unterauftragsverarbeiter von Anthropic:** allgemeine Genehmigung, bezogen auf die veröffentlichte Liste in der Fassung, die Illig vor der Unterschrift mit Abrufdatum vorlegt (Anlage 3). Über Ankündigungen informiert Illig unverzüglich in Textform. Widerspricht der Kunde binnen 10 Tagen, widerspricht Illig innerhalb der Frist von Anthropic (15 Tage) oder stellt die Verarbeitung über sein Konto ein.
- **Offen benannte Abweichungen:** Für Anthropic gilt dessen Standard-DPA, u. a. Meldung binnen 48 Stunden (statt möglichst 24), Kontrollen vorrangig über Prüfberichte, Löschung der Ein- und Ausgaben des Testtags standardmäßig binnen 30 Tagen nach Eingang (bei Markierung als Verstoß gegen die Nutzungsrichtlinie bis zu 2 Jahre); eine Rückgabe oder vorzeitige Löschung nach DPA H.1 gibt es nicht, weil der Vertrag von Illig mit Anthropic nach dem Testtag weiterläuft.
- **Haftung:** Für Anthropic haftet Illig dem Kunden nach Art. 28 Abs. 4 Satz 2 DSGVO; im Verhältnis der Parteien gilt die Haftungsregel des Hauptvertrags.

(5) **Sonst kein KI-Konto von Illig.** Außer am Testtag verarbeitet Illig Daten des Kunden nie über ein eigenes KI-Konto (Abo oder API-Schlüssel), auch nicht zur Fehlersuche oder in Fernsitzungen.

(6) **Zugang auf dem KI-PC.** Die Anmeldung des Systems bei Anthropic liegt im Windows-Konto des Systems (Datei `.credentials.json` im Profil) und ist für das System technisch lesbar. Sie gilt nur für das Konto des Systems in der Team-Organisation des Kunden, mit Ausgabenlimit, und lässt sich dort jederzeit sperren (Mitglied entfernen). Ein API-Schlüssel darf nicht gesetzt sein. Läuft die Anmeldung ab, meldet eine Person des Kunden das System neu an.

(7) Beim Tarif Claude Team (ebenso Enterprise) verlangen die Bedingungen von Anthropic zusätzlich, dass der Kunde seine Nutzer über den administrierten Dienst und die geltenden Richtlinien von Anthropic informiert.

---

§ 9 Unterauftragsverarbeiter

(1) Illig setzt nur die Unterauftragsverarbeiter nach **Anlage 3** ein.

Derzeit ist das nur Anthropic, und nur am Testtag (§ 8 Abs. 4).

(2) **Einzelgenehmigung.** Weitere oder andere Unterauftragsverarbeiter setzt Illig nur nach vorheriger gesonderter Genehmigung des Kunden in Textform ein (Art. 28 Abs. 2 Satz 1 DSGVO). Vorher teilt er Name, Sitz, Leistung, Ort der Verarbeitung, Vertragsgrundlage und bei Drittländern die Garantien mit. Das gilt auch für ein Fernwartungswerkzeug über ein Konto von Illig.

Für die Unterauftragsverarbeiter von Anthropic gilt am Testtag die allgemeine Genehmigung nach § 8 Abs. 4.

(3) Illig verpflichtet jeden Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten wie in dieser Vereinbarung (Art. 28 Abs. 4 DSGVO) und haftet dem Kunden für ihn.

Soweit Anthropic am Testtag verarbeitet, legen die Parteien für Meldung von Verletzungen, Kontrollen und Löschung die Pflichten aus dem DPA von Anthropic fest (§ 8 Abs. 4); insoweit sind die Pflichten dieser Vereinbarung und die von Anthropic dieselben (Art. 28 Abs. 4 Satz 1 DSGVO).

(4) **Keine** Unterauftragsverarbeiter von Illig sind Dienste, die der Kunde selbst beauftragt (sein Abo bei Anthropic, sein Fernwartungswerkzeug, Microsoft 365, Microsoft Azure für den KI-PC, seine VPN-

Verbindung, Fachsoftware), und E-Mail, WhatsApp und Teams von Illig, die nur der Abstimmung dienen, sowie der Alarmweg im Betreuungsabo, der nur ein Lebenszeichen ohne personenbezogene Daten sendet (§ 10 Abs. 7).

---

§ 10 Fernwartung und Überwachung

(1) **Nur der KI-PC.** Fernwartung findet nur auf dem KI-PC statt; ein Zugang zu anderen Rechnern, Laufwerken oder zum Netzwerk des Kunden wird weder eingerichtet noch genutzt. Werkzeug (ankreuzen):

- ☐ Keine Fernwartung; Illig arbeitet nur vor Ort.
- ☐ Werkzeug des Kunden (bevorzugt), auch ein gemeinsam ausgesuchtes, das der Kunde bereitstellt und verwaltet: [Name].
- ☐ Werkzeug über ein Konto von Illig: [Name, Anbieter, Sitz, Serverstandort] – nur nach Genehmigung nach § 9 Abs. 2. Stand 07.11.2026: vorgesehen ist TeamViewer, noch nicht im Einsatz (Anlage 3).

Ausnahmen, nur soweit im Hauptvertrag vereinbart: (a) Ist der KI-PC ein virtueller Rechner im Azure-Konto des Kunden, erhält Illig dort einen Gastzugang nur für die Ressourcengruppe dieses Rechners (Einrichtung des Rechners und, falls vereinbart, der Azure-Seite einer VPN-Verbindung in Abstimmung mit der IT des Kunden; Größe, Zeitplan, Start, Stopp, Neustart); jeder Eingriff über Azure (Befehl, Neustart, Öffnen des Remotedesktops) steht als Vorgang im Azure-Aktivitätsprotokoll des Kunden; was Illig dabei auf dem KI-PC tut, steht im Protokoll nach Abs. 3. Der Gastzugang gilt als Fernzugang nach diesem Paragrafen, der Kunde kann ihn jederzeit entziehen (Abs. 6). Zugriffe auf den KI-PC selbst (Anmeldung, Remotedesktop, Befehle über Azure) gibt es nur nach der Freigabe-Variante nach Abs. 2 und mit Protokoll nach Abs. 3; die reine Verwaltung des Rechners (Größe, Zeitplan, Start, Stopp, Neustart) braucht keine Einzelfreigabe. (b) Erreicht der KI-PC Programme im Netz des Kunden über eine VPN-Verbindung, wird sie mit der IT des Kunden eingerichtet und auf die vereinbarten Programme und Laufwerke beschränkt; Illig nutzt sie nur vom KI-PC aus und nur dafür.

(2) **Freigabe** (ankreuzen; ohne Kreuz gilt „je Sitzung“, am Testtag in jedem Fall):

- ☐ **Je Sitzung:** jede Sitzung nur nach vorheriger Freigabe durch eine Person nach Anlage 4.
- ☐ **Zeitfenster:** [Tage, Uhrzeit] ohne Einzelfreigabe; außerhalb nur je Sitzung.
- ☐ **Dauerzugang** (im Betreuungsabo empfohlen): jederzeit ohne Einzelfreigabe, bis der Kunde ihn entzieht; gilt nur, wenn ausdrücklich angekreuzt.

Die angekreuzte Variante gilt als dokumentierte Weisung nach § 5. Bei „Je Sitzung“ und außerhalb eines Zeitfensters laufen die Reaktionszeiten der Betreuung erst ab der Freigabe.

(3) **Ankündigung und Protokoll.** Jede Sitzung wird vorher in Textform angekündigt (Zweck, Dauer); bei Zeitfenster oder Dauerzugang genügt die Mitteilung unverzüglich danach; geplante Updates kündigt Illig vorher an. Illig protokolliert Beginn, Ende, Anlass, Arbeiten, ob personenbezogene Daten sichtbar waren und wer freigab; nach jeder Sitzung erhält die Ansprechperson nach Anlage 4 dieses Protokoll automatisch per E-Mail (wann, Anlass, was gemacht wurde und was sich geändert hat).

(4) **Sicherheit.** Die Verbindung ist verschlüsselt; auf der Zugriffsliste stehen nur vom Kunden genehmigte Konten; Illig nutzt ein persönliches Konto mit Zwei-Faktor-Anmeldung, soweit das Werkzeug sie anbietet, und greift nur aus den Ländern nach § 1 Abs. 3 zu. Windows-Remotedesktop (RDP) ist kein Arbeitsweg, weil das Trennen die Windows-Sitzung des Systems gesperrt zurücklässt und das System dann nicht weiterarbeiten kann. Ausnahme Azure-Rechner: Dort ist RDP von außen gesperrt und wird nur bei Bedarf für die Wartung (Freigabe nach Abs. 2, Protokoll nach Abs. 3) und nur für die

Internetadresse von Illig geöffnet und danach wieder geschlossen; eine geplante Aufgabe auf dem KI-PC hängt die Sitzung des Systems nach dem Trennen wieder an die Konsole. Illig speichert keine Kennwörter von Beschäftigten des Kunden; er nutzt nur eigene Zugänge (Gastzugang, Konto im Fernwartungswerkzeug) und das Windows-Konto des Systems.

(5) **Nichts mitnehmen.** Keine Dateien auf Geräte von Illig, keine Zwischenablage nach außen, keine Aufnahmen oder Bildschirmfotos mit personenbezogenen Daten, außer im Einzelfall in Textform vereinbart.

(6) **Entzug jederzeit.** Der Kunde kann den Fernzugang ohne Angabe von Gründen beenden: Dienst beenden, Konto von der Zugriffsliste nehmen, beim Azure-Rechner den Gastzugang von Illig entfernen oder den KI-PC vom Netz trennen. Leistungen, die ohne Fernzugang nicht möglich sind, ruhen dann.

(7) **Zwischen den Sitzungen** sieht Illig den Bildschirm nicht. Im Betreuungsabo richtet Illig einen Alarmweg vom KI-PC zu sich ein, erst nach Genehmigung des Kunden in Textform; Anbieter und Inhalt teilt Illig vorher mit; vorgesehen ist ein Überwachungsdienst für das Lebenszeichen (derzeit healthchecks.io: der KI-PC ruft regelmäßig eine feste Adresse auf; bleibt der Aufruf aus oder meldet er eine Störung, benachrichtigt der Dienst Illig per E-Mail; der Dienst sieht dabei nur technische Verbindungsdaten wie die Internetadresse des KI-PCs). Der Alarmweg überträgt nur dieses Signal, ohne Namen von Personen, Dateinamen oder Inhalte von Nachrichten; der Anbieter ist dafür kein Unterauftragsverarbeiter (§ 9 Abs. 4). Bei einer Störung erhält auch die Ansprechperson nach Anlage 4 eine kurze E-Mail (Art der Störung, Uhrzeit, ohne personenbezogene Daten): vom Postfach des Systems, solange es noch arbeitet, sonst von Illig, sobald er die Störung bemerkt. Zusätzlich zeigt der KI-PC Störungen vor Ort an (Datei `ALARM.txt`, Hinweisfenster). Vor Ort arbeitet Illig nur mit Wissen der Ansprechperson.

---

§ 11 Rechte betroffener Personen

Illig unterstützt den Kunden bei Anträgen nach Art. 12 bis 22 DSGVO (Art. 28 Abs. 3 lit. e DSGVO): Er zeigt, wo das System Daten zu einer Person ablegt und protokolliert, und berichtigt oder löscht sie dort auf Weisung. Anträge, die ihn direkt erreichen, leitet er unverzüglich an den Kunden weiter und beantwortet sie nicht selbst. Erreicht ein Antrag das System, gibt es ihn nach seiner Arbeitsanweisung an die zuständige Person weiter.

---

§ 12 Datenschutzverletzungen und weitere Unterstützung

(1) **Meldung.** Illig meldet dem Kunden eine Verletzung des Schutzes personenbezogener Daten **unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis**, an die Meldestelle nach Anlage 4, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit bekannt; Fehlendes reicht er nach. Beispiele: Nachricht an eine falsche Person, unbefugter Zugriff auf den KI-PC, Daten auf einem Gerät von Illig. Die Meldung an die Aufsichtsbehörde (möglichst binnen 72 Stunden, Art. 33 Abs. 1 DSGVO) und die Benachrichtigung Betroffener sind Sache des Kunden.

(2) **Vorfälle bei Anthropic** meldet Anthropic am Testtag an Illig (laut DPA spätestens binnen 48 Stunden); Illig gibt Meldungen, die Daten des Kunden betreffen können, unverzüglich weiter. Im Betrieb meldet Anthropic direkt dem Kunden.

(3) **Weitere Unterstützung** (Art. 28 Abs. 3 lit. f DSGVO): bei der Sicherheit der Verarbeitung (Art. 32), bei Meldungen und Benachrichtigungen (Art. 33, 34), bei der Datenschutz-Folgenabschätzung mit einer

Beschreibung von System, Datenflüssen und Maßnahmen (Art. 35) und bei einer vorherigen Konsultation (Art. 36 DSGVO).

(4) Ob Unterstützung nach §§ 11 und 12 vergütet wird, regelt der Hauptvertrag; für Fälle, die Illig zu vertreten hat, berechnet er nichts.

---

§ 13 Löschung und Rückgabe

(1) **Speicherorte.** Arbeitsergebnisse legt das System in den Systemen des Kunden ab; ihre Aufbewahrung verantwortet der Kunde. Auf dem KI-PC entstehen im Kit-Ordner Arbeitsdateien, Tagesjournal (Freigaben mit Nummer, Person, Kanal, Ergebnis und Anfang der Antwort), Aktionsprotokoll (Klicks und Tastatureingaben des Maus- und Tastaturwerkzeugs, Getipptes nur als Zeichenzahl), Ereignisprotokoll (u. a. Chat-Eingaben mit den ersten 80 Zeichen, Namen bei Freigaben und gelernten Regeln, bei freigeschalteten Mails Empfänger und Fenstertitel), Hinweise am KI-PC (`ALARM.txt`), Bildschirmfotos und im Ordner `.zustand\freigaben` die Freigabe-Protokolle mit Namen, die das System ergänzen, aber nicht ändern kann; im Windows-Konto des Systems unter `%USERPROFILE%\.claude\` die Chatverläufe von Claude Code im Klartext samt angesehenen Bildschirmfotos, Vorher-Kopien geänderter Dateien und der Eingabeverlauf.

(2) **Fristen.** Von selbst gelöscht werden nur Bildschirmfoto-Dateien nach drei Tagen, jeweils wenn das System das nächste Foto aufnimmt, und Chatverläufe samt Bildschirmfotos, die 14 Tage nicht benutzt wurden (Claude Code). Das System arbeitet in einem fortlaufenden Chatverlauf; ihn löscht Illig nach Absprache, spätestens beim Abbau. Tagesjournal, Aktions-, Ereignis- und Freigabe-Protokoll, Eingabeverlauf, Arbeitsdateien, Versand- und Regelprotokolle und `ALARM.txt` löscht das System nicht von selbst: Ihre Fristen legt der Kunde in Anlage 1 fest (Vorschlag für Journal und Protokolle: drei Monate). Nach Ablauf löscht Illig sie von Hand, monatlich per Fernwartung oder vor Ort, und vermerkt das im Löschprotokoll; ist in Anlage 1 stattdessen die IT des Kunden angekreuzt, löscht diese. Auf Weisung löscht Illig auch früher; die IT des Kunden kann jederzeit selbst löschen. Illig prüft bei seinen Prüfungen (alle drei Monate, Anlage 2 B20), ob gelöscht wurde. Bei Anthropic gelten dessen Fristen (§ 8 Abs. 2).

(3) **Nach dem Testtag** hält Illig das System an (Not-Aus). Es arbeitet nicht unbeaufsichtigt weiter und bleibt angehalten, bis der Kunde über das Angebot entschieden hat. Sagt er ab, verlangt er den Abbau oder kommt binnen 14 Tagen nach dem Angebot kein Folgeauftrag zustande, baut Illig das System binnen fünf Werktagen ab. Bis dahin gilt diese Vereinbarung weiter.

(4) **Abbau.** Der Kunde wählt, ob er Ergebnisse zurückerhält oder ob nur sichergestellt wird, dass sie in seinen Systemen liegen. Dann entfernt Illig mit dem Kunden, vor Ort oder per Fernwartung: den Kit-Ordner mit allen Inhalten nach Abs. 1 (die Freigabe-Protokolle vorher auf Wunsch an den Kunden übergeben), die Daten von Claude Code unter `%USERPROFILE%\.claude\`, die geplante Aufgabe des Aufpassers, die Anmeldung bei Anthropic auf dem KI-PC („Claude Code: Logout“) und alle Zugänge von Illig (Fernwartung, Azure-Gastzugang) samt seinem Alarmweg. Windows-Konto und Zugänge des Systems zu Programmen, Postfach und Teams sperrt oder löscht der Kunde. Frist nach Ende von Einrichtung und Betreuung: 10 Werktage. Gesetzliche Aufbewahrungspflichten bleiben unberührt. **Ausnahme Weiterbetrieb:** Betreibt der Kunde das System nach dem Hauptvertrag selbst weiter (dauerhaftes Nutzungsrecht), gilt dieser Absatz nur so: Illig entfernt seine eigenen Zugänge, schaltet seinen Alarmweg auf dem KI-PC ab und löscht Daten in seinem eigenen Zugriff; Kit-Ordner, Protokolle, Chatverläufe, die Anmeldung bei Anthropic sowie Windows-Konto und Zugänge des Systems bleiben in der alleinigen Verantwortung des Kunden auf dessen KI-PC.

Am Ende des Testtags meldet Illig das System bei seinem Geschäftskonto ab; dort gespeicherte Inhalte löscht Anthropic nach seinen Fristen. Im Betrieb entfernt der Kunde das Konto des Systems selbst aus seiner Claude-Organisation.

(5) **Nachweis.** Illig bestätigt die Löschung in Textform mit einem Löschprotokoll (was, wann, von wem). Nachweisunterlagen (Vereinbarung, Weisungen, Löschprotokoll, Fernwartungsprotokolle) darf er bis zum Ablauf der Verjährung aufbewahren; sie enthalten nur Namen und Kontaktdaten. Versehentlich erhaltene Daten löscht Illig unverzüglich und bestätigt das.

---

§ 14 Nachweise und Kontrollen

(1) Illig stellt alle Informationen zum Nachweis der Pflichten nach Art. 28 DSGVO zur Verfügung, insbesondere die aktuelle Anlage 2 und die Fernwartungsprotokolle (Art. 28 Abs. 3 lit. h DSGVO). Er führt ein Verzeichnis der Verarbeitungstätigkeiten als Auftragsverarbeiter (Art. 30 Abs. 2 DSGVO).

(2) Der Kunde oder ein beauftragter, zur Verschwiegenheit verpflichteter Prüfer (kein Wettbewerber von Illig) kann nach Anmeldung mit angemessener Frist, in der Regel 14 Tage, Überprüfungen einschließlich Inspektionen durchführen; Illig wirkt mit. Geprüft wird vorrangig beim Kunden, wo die Daten liegen, und anhand von Nachweisen. Die Protokolle des Systems kann der Kunde auf dem KI-PC jederzeit einsehen.

(3) Für den Testtag gibt Illig die Nachweise von Anthropic weiter (Zertifikate und Prüfberichte laut Trust Center von Anthropic), soweit Anthropic das erlaubt; Prüfungen bei Anthropic richten sich nach dessen DPA. Im Betrieb erhält der Kunde die Nachweise direkt.

---

§ 15 Übermittlungen in Drittländer

(1) Illig übermittelt selbst keine personenbezogenen Daten in Drittländer. Aus anderen Ländern als Deutschland, der EU oder dem EWR greift er nur zu, wenn sie in Anlage 1 benannt sind und ein Angemessenheitsbeschluss der EU-Kommission besteht.

(2) **Anthropic** speichert laut eigenen Angaben in den USA. Grundlage sind die EU-Standardvertragsklauseln im DPA (Durchführungsbeschluss (EU) 2021/914). Ob Anthropic in der Liste des EU-US Data Privacy Framework geführt wird, war bei Erstellung dieses Musters nicht belegt; das Muster stützt sich nicht darauf. Informationen für eine Transfer-Folgenabschätzung stellt Anthropic laut DPA auf Anfrage bereit.

(3) Am Testtag ist die Übermittlung an Anthropic Teil der Verarbeitung durch Illig; diese Vereinbarung gilt als dokumentierte Weisung dazu (Art. 28 Abs. 3 lit. a DSGVO). Im Betrieb ist sie eine Verarbeitung des Kunden nach seinem eigenen Vertrag. Die Bewertung dokumentiert der Kunde.

---

§ 16 Haftung

Gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Verhältnis der Parteien gilt die Haftungsregelung des Hauptvertrags, auch für Ansprüche aus dieser Vereinbarung; darüber hinaus begründet diese Vereinbarung keine Garantien, Vertragsstrafen oder Freistellungen.

§ 17 Zusatz für Kunden in der Schweiz

Gilt, wenn der Kunde seinen Sitz in der Schweiz hat oder die Bearbeitung dem Schweizer Datenschutzgesetz (DSG) unterliegt; die Kundenfassung verwendet dann Schweizer Begriffe und „ss“. Mehr: Schweiz.

(1) Illig bearbeitet Personendaten im Auftrag nach Art. 9 DSG; weil er in Deutschland sitzt, gilt für ihn zusätzlich Art. 28 DSGVO. Unteraufträge sind nur mit vorgängiger Genehmigung des Kunden zulässig (Art. 9 Abs. 3 DSG); die Einzelgenehmigung nach § 9 Abs. 2 erfüllt das.

Für Anthropic und dessen Unterauftragsverarbeiter am Testtag erteilt der Kunde die Genehmigung mit dieser Vereinbarung vorgängig (§ 8 Abs. 4).

(2) Anlage 2 dient auch Art. 8 DSG und der Prüfung nach Art. 9 Abs. 2 DSG, ob Illig die Datensicherheit gewährleisten kann. Verletzungen der Datensicherheit meldet Illig so rasch als möglich (Art. 24 Abs. 3 DSG), mit der Frist nach § 12 Abs. 1. Für den Kunden gelten statt der DSGVO-Artikel insbesondere Art. 19, 21, 22 bis 24, 25 ff. und 12 DSG; Aufsicht ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB).

(3) Für die USA gilt ein angemessenes Schutzniveau nur für Organisationen, die im Swiss-U.S. Data Privacy Framework gelistet sind (Anhang 1 DSV); ob Anthropic dazu gehört, war nicht belegt. Sonst kommen vom EDÖB anerkannte Standarddatenschutzklauseln in Betracht (Art. 16 Abs. 2 Bst. d DSG); das DPA von Anthropic enthält dafür einen Schweizer Zusatz mit dem EDÖB als Aufsicht.

(4) Der Kunde informiert und hört die Arbeitnehmenden oder ihre Vertretung vor dem Einsatz an (Art. 5 und 6 ArGV 3, Art. 48 ArG; ohne Vertretung direkt, Art. 4 Mitwirkungsgesetz). Systeme, die das Verhalten am Arbeitsplatz überwachen sollen, sind nach Art. 26 ArGV 3 unzulässig; die Protokolle des Systems werden dafür nicht verwendet. Neben dem deutschen Recht bleiben zwingende Vorschriften des Schweizer Datenschutzrechts unberührt.

§ 18 Schlussbestimmungen

(1) Bei Widersprüchen geht in Fragen des Datenschutzes diese Vereinbarung dem Hauptvertrag vor, in Fragen der Haftung der Hauptvertrag.

(2) Diese Vereinbarung und Änderungen werden schriftlich geschlossen; ein elektronisches Format genügt (Art. 28 Abs. 9 DSGVO). Einzelweisungen und von beiden Parteien bestätigte Änderungen der Anlagen 1 und 4 genügen in Textform.

(3) Es gilt das Recht der Bundesrepublik Deutschland; für den Gerichtsstand gelten die gesetzlichen Regeln. Ist eine Bestimmung unwirksam, bleibt die Vereinbarung im Übrigen wirksam.

(4) **Anlagen:** 1 – Ablauf, Daten, betroffene Personen, Löschfristen · 2 – Technische und organisatorische Maßnahmen · 3 – Unterauftragsverarbeiter · 4 – Weisungsberechtigte und Ansprechpersonen.

Für den Kunden: [Firma], [Name, Funktion] · Für Illig: Nick Illig, Illig Automatisierung

Ort, Datum, Unterschrift Verantwortlicher	Ort, Datum, Unterschrift Auftragsverarbeiter

Anlage 1 – Ablauf, Daten, betroffene Personen, Löschfristen

Zum Ausfüllen nach der Prozessaufnahme; nur ankreuzen, was im Ablauf wirklich vorkommt.

Angabe	Eintrag
Bereich und Ablauf	[Bezeichnung; bestätigte Zusammenfassung mit Testfällen und Erfolgskriterium vom …]
Programme und Zugänge des Systems	[Programme, Ordner, Funktionspostfach, Teams-Konto mit „(KI)“ im Namen]
Schritte ohne Freigabe (nur Betrieb, § 2 Abs. 5)	☐ keine · ☐ [Beschreibung, Grenzen]
Am Testtag mit echten Daten?	☐ ja, Voraussetzungen nach § 4 Abs. 2 erfüllt · ☐ nein, nur Muster- oder Testdaten
Fernzugriff aus weiteren Ländern (§ 15 Abs. 1)	☐ keine · ☐ [Land, Angemessenheitsbeschluss]
Schutzbedarf (legt der Kunde fest)	☐ normal · ☐ hoch · ☐ sehr hoch – [Begründung]

Art der Daten

- ☐ Geschäftliche Kontaktdaten · ☐ Kunden- und Lieferantenstammdaten (Nummern, Anschrift, Steuernummer bei Einzelunternehmen) · ☐ Vorgangsdaten (Anfragen, Aufträge, Lieferscheine, Rechnungen, Beträge, Fristen) · ☐ Buchungs- und Zahlungsdaten · ☐ Bankverbindungen (nur lesen und abgleichen) · ☐ Korrespondenz mit Anhängen (Fotos können Personen zeigen)
- ☐ Beschäftigte: Stammdaten, Arbeitszeiten, Dienstplan, Abwesenheiten ohne Grund und Diagnose · ☐ Beschäftigte: Lohn-, Steuer- und Sozialversicherungsdaten
- ☐ Besondere Kategorien (Art. 9 DSGVO), z. B. Zeiten der Arbeitsunfähigkeit, Schwerbehinderung, Kirchensteuermerkmal – nur nach Klärung mit dem DSB (§ 3 Abs. 2) · ☐ Sonstige: [Beschreibung]

Immer dabei: die Kommunikations- und Protokolldaten nach § 3 Abs. 1. Ausgeschlossen: Zugangsdaten mit Zahlungsberechtigung, Passwörter, [weitere Ausschlüsse, z. B. Diagnosen, Bewerbungsunterlagen zur Auswahl].

Betroffene Personen

- ☐ Ansprechpersonen bei Kunden, Lieferanten und Dienstleistern · ☐ Kundinnen und Kunden, die Verbraucher sind · ☐ Lieferanten als Einzelunternehmen · ☐ Interessentinnen und Interessenten
- ☐ Beschäftigte, deren Daten im Ablauf vorkommen, auch ehemalige · ☐ Angehörige in Steuer- oder Sozialversicherungsdaten · ☐ Ansprechpersonen bei Behörden, Krankenkassen und Banken · ☐ Sonstige: [Beschreibung]
- Immer: Beschäftigte des Kunden, die mit dem System arbeiten (Fachbereich, Freigabeberechtigte, IT)

Löschfristen auf dem KI-PC (legt der Kunde fest; Vorschlag von Illig für Journal und Protokolle: 3 Monate)

- Tagesjournal mit Freigaben und Freigabe-Datensätze: 3 Monate (Vorschlag) oder [Frist] · Aktionsprotokoll (rotiert nicht): 3 Monate (Vorschlag) oder [Frist] · Ereignisprotokoll: 3 Monate (Vorschlag) oder [Frist] · Versand- und Regelprotokolle: 3 Monate (Vorschlag, sofern keine Aufbewahrungspflicht greift) oder [Frist] · Arbeitsdateien in Ein- und Ausgangsordnern: [Frist] · Browserprofil des Systems: [Frist] · Eingabe-Historie von Claude Code: [Frist]
- Von selbst gelöscht (§ 13 Abs. 2) werden nur Bildschirmfoto-Dateien nach 3 Tagen, jeweils beim nächsten Foto, und Chatverläufe, die 14 Tage nicht benutzt wurden; den fortlaufenden Chatverlauf löscht Illig nach Absprache, spätestens beim Abbau
- Alles Übrige wird nach der Frist oben von Hand gelöscht durch: ☐ Illig, monatlich per Fernwartung oder vor Ort, mit Löschprotokoll (Standard; gilt, wenn nichts angekreuzt ist) · ☐ IT des Kunden nach Anleitung von Illig, [Turnus]

Nicht Teil dieses Musters ist die Annahme von Telefonaten durch das System; sie bräuchte eine eigene Regelung (Telefon).

Anlage 2 – Technische und organisatorische Maßnahmen

Die Maßnahmen stehen in der Unterlage **TOM-Anlage**. Sie ist in der bei Unterschrift geltenden Fassung (zu diesem Muster gehört die Fassung vom 07.11.2026) Anlage 2 dieser Vereinbarung; Änderungen nach § 7 Abs. 2.

Anlage 3 – Unterauftragsverarbeiter

Die aktuelle Übersicht steht in der Unterlage **Unterauftragsverarbeiter**. Für diese Vereinbarung gilt:

Anthropic Ireland, Limited, Dublin (Irland) – nur am Testtag: KI-Modell Claude, Verarbeitung der Inhalte je Arbeitsschritt über das Geschäftskonto von Illig. Vertragspartner in Irland; laut Anthropic Speicherung in den USA, Verarbeitung auch in Europa, Asien und Australien. Grundlage: Commercial Terms mit DPA und EU-Standardvertragsklauseln. Liste der Unterauftragsverarbeiter von Anthropic (Trust Center): in der Fassung, die Illig vor der Unterschrift mit Abrufdatum vorlegt (§ 8 Abs. 4); Stand bei Erstellung dieses Musters: abgerufen am 01.11.2026, 22 Einträge, letzte Änderung laut Trust Center 15.10.2026. Im Betrieb ist Anthropic Auftragsverarbeiter des Kunden über dessen eigenes Konto (§ 8 Abs. 3).

Fernwartungswerkzeug über ein Konto von Illig: Stand 07.11.2026 keines im Einsatz; vorgesehen ist TeamViewer (TeamViewer Germany GmbH, Göppingen), falls der Kunde kein eigenes Werkzeug hat. Eingesetzt wird es nur, wenn es nach § 10 Abs. 1 angekreuzt und nach § 9 Abs. 2 genehmigt ist; dann hier eintragen: [Anbieter, Sitz, Serverstandort, Genehmigung vom]

Anlage 4 – Weisungsberechtigte und Ansprechpersonen

Je Rolle Name, Funktion, Kontakt (E-Mail, Telefon) und bei Freigaben die eindeutige Kennung (Teams-Anmeldename oder E-Mail):

- **Weisungsberechtigt (Kunde) und Vertretung:** [Name, Funktion, Kontakt]
- **Freigabeberechtigte für das System:** [Name, Funktion, Kontakt, Kennung]
- **Freigabe von Fernwartungssitzungen:** [Name, Funktion, Kontakt, Kennung]
- **Not-Aus und Vertretung:** [Name, Telefon]

- **IT (KI-PC, Rechte, Fernwartungswerkzeug):** [Name, Funktion, Kontakt]
- **Datenschutzbeauftragte/r des Kunden (falls benannt):** [Name, Kontakt]
- **Meldestelle für Datenschutzverletzungen:** [Name oder Funktion, Kontakt]
- **Illig (Weisungsempfänger):** Nick Illig, nick@illig-automatisierung.com – nur Abstimmung, keine personenbezogenen Daten (§ 6 Abs. 2)

Für Datenschutzbeauftragte: Pflichtinhalte und Quellen

Wo die Pflichtinhalte nach Art. 28 DSGVO stehen (nicht Teil der Vereinbarung): Gegenstand, Dauer, Art und Zweck, Daten, Betroffene (Abs. 3 Satz 1) – §§ 1 bis 3, Anlage 1 · Pflichten und Rechte des Verantwortlichen – §§ 4, 5, 10 Abs. 6, 14 · lit. a Weisungen, auch Drittland – §§ 5, 10 Abs. 2, 15 · lit. b Vertraulichkeit – § 6 · lit. c Maßnahmen nach Art. 32 – § 7, Anlage 2 · lit. d Unterauftragsverarbeiter (Abs. 2 und 4) – §§ 8, 9, Anlage 3 · lit. e Betroffenenrechte – § 11 · lit. f Art. 32 bis 36 – § 12 · lit. g Löschung oder Rückgabe – § 13 · lit. h Nachweise und Inspektionen – § 14 · UAbs. 2 Hinweis bei rechtswidriger Weisung – § 5 Abs. 3 · Abs. 9 Form – § 18 Abs. 2 · Schweiz, Art. 9 DSG – § 17.

Weitere Unterlagen: alle Unterlagen · Kontakt für Datenschutzfragen.

Quellen – alle Webquellen abgerufen am 01.11.2026; zu Anthropic gilt die jeweils aktuelle Fassung:

- Recht: DSGVO · Standardvertragsklauseln, Beschluss (EU) 2021/914 · DSK-Kurzpapier Nr. 13 (Stand 17.12.2018), jeweils abgerufen am 01.11.2026
- Anthropic: Commercial Terms („Effective Jun 17, 2025“) · Data Processing Addendum („Effective Feb 24, 2025“) · Service Specific Terms („Effective Aug 31, 2026“) · Usage Policy („Effective Nov 12, 2026“; bis 11.11.2026 gilt die Fassung vom 15.09.2025) · Privacy Center Serverstandorte (Stand 15.06.2026) und Aufbewahrung (Stand 01.07.2026), jeweils abgerufen am 01.11.2026
- Claude Code Docs ohne Datum: Data usage · Legal and compliance · cleanupPeriodDays; Trust Center: Zertifikate und Prüfberichte · Unterauftragsverarbeiter (letzte Änderung laut Trust Center 15.10.2026), jeweils abgerufen am 01.11.2026
- Schweiz: DSG (Stand 7.7.2025) · DSV mit Anhang 1 (Stand 1.12.2025) · ArGV 3 (Stand 1.9.2024) · EDÖB, Bekanntgabe ins Ausland, jeweils abgerufen am 01.11.2026