ANLAGE · STAND 07.11.2026

Technische und organisatorische Maßnahmen (Anlage 2 zur Vereinbarung zur Auftragsverarbeitung)

> Keine Rechtsberatung. Nicht anwaltlich geprüft.

Muster als Arbeitshilfe, Stand 07.11.2026. Diese Anlage ist nicht anwaltlich geprüft und keine Rechtsberatung. Ob die Maßnahmen für Ihre Abläufe angemessen sind, bewerten Sie als Verantwortlicher, am besten mit Ihrem Datenschutzbeauftragten. Felder in eckigen Klammern füllen Sie vor der Unterschrift aus.

Gegenstand

Anlage 2 zur Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO vom [Datum] zwischen

- **[Firma]**, [Anschrift] – Verantwortlicher (im Folgenden „Sie“), und
- **Nick Illig, Prozessautomatisierung** (Einzelunternehmen, Marke „Illig Automatisierung“), Unterm Grasweg 57, 79379 Müllheim, Deutschland – Auftragsverarbeiter (im Folgenden „Illig“).

KI-PC: [PC oder VM, Bezeichnung, Standort] · Ansprechperson IT: [Name, Funktion]

Die KI-Mitarbeiterin ist Claude Code von Anthropic mit dem Regelwerk von Illig (im Folgenden „Kit“). Sie arbeitet auf einem eigenen PC oder einer VM Ihrer Firma (im Folgenden „KI-PC“) unter einem eigenen Windows-Benutzerkonto ohne Administratorrechte. Dort bedient sie Ihre Programme über Bildschirmfotos, Maus und Tastatur, zum Beispiel Outlook und Teams. Für jeden Arbeitsschritt gehen die nötigen Inhalte an das KI-Modell Claude von Anthropic.

Das Muster der Vereinbarung steht unter Vereinbarung zur Auftragsverarbeitung, die Unterauftragsverarbeiter in Anlage 3.

So ist die Anlage aufgebaut

Die Maßnahmen sind nach Art. 32 Abs. 1 DSGVO geordnet: lit. a Pseudonymisierung und Verschlüsselung, lit. b Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit, lit. c Wiederherstellbarkeit, lit. d regelmäßige Überprüfung. Getrennt ist danach, wer sie umsetzt:

- **A.** am KI-Arbeitsplatz bei Ihnen (vom Kit umgesetzt)
- **B.** bei Illig Automatisierung (Fernwartung, Geräte, Organisation)
- **C.** Ihre Mitwirkung (teils Pflichten nach § 4 der Vereinbarung, teils Empfehlungen)
- **D.** Anthropic (Verweis auf dessen Unterlagen)
- **E.** Grenzen der Maßnahmen, offen benannt

Die letzte Spalte der Tabellen nennt die Art der Maßnahme und, wo vorhanden, die Fundstelle im Kit-Ordner auf dem KI-PC. Dort kann Ihre IT sie nachprüfen.

Technik
: im Programm der KI-Mitarbeiterin umgesetzt

Einrichtung
: setzt Illig beim Einrichten um, gemeinsam mit Ihrer IT

Arbeitsanweisung
: Regel, die die KI befolgen soll und die protokolliert wird – keine technische Sperre

Zusage
: organisatorische Zusage von Illig

Kunde
: Ihre Mitwirkung, siehe Teil C

Für Kunden in der Schweiz dienen die Maßnahmen zugleich der Datensicherheit nach Art. 8 DSG (Hinweise zur Schweiz). Das Telefon-Modul (Annahme von Anrufen) ist nicht Gegenstand dieser Anlage; vor einem Einsatz wird es gesondert geregelt.

A. Am KI-Arbeitsplatz beim Kunden (vom Kit umgesetzt)

Teil A nennt nur, was das Kit nachweislich tut oder was bei der Einrichtung umgesetzt wird. Die Grenzen stehen jeweils dabei und gesammelt in Teil E. Was die KI sehen kann, bestimmen am Ende die Rechte ihres Windows-Kontos.

Vertraulichkeit: Zutritt, Zugang, Zugriff, Trennung (lit. b)

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A1	Zutritt: Arbeitsplatz bei Ihnen	Die KI-Mitarbeiterin läuft auf dem KI-PC in Ihren Räumen oder als VM in Ihrer IT. Illig betreibt für sie keine eigenen Server oder Speicher. Damit die KI den Bildschirm bedienen kann, ist die Bildschirmsperre ihres Kontos aus. Der KI-PC gehört deshalb in einen geschützten Raum (C3). Mit einer VM ist die KI-Mitarbeiterin bei Kunden noch nicht erprobt; Illig prüft sie vor dem Testtag.	Einrichtung · Kunde

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A2	Zugang: eigenes Windows-Konto	Eigenes Windows-Benutzerkonto nur für die KI-Mitarbeiterin, als Standardbenutzer ohne Administratorrechte; empfohlen auf eigenem PC oder eigener VM. Kein Zugriff auf Windows-Konten von Beschäftigten. Läuft das Einrichtungsskript mit Administratorrechten, warnt es; dass das Konto in keiner Administratorgruppe ist, prüft Ihre IT bei der Einrichtung (C1).	Technik + Einrichtung · Kunde
A3	Zugang: eigene Konten für Kommunikation	Eigene Zugänge für Microsoft 365 und Teams mit „(KI)“ im Anzeigenamen. Genutzt werden nur das KI-Konto und freigegebene Funktionspostfächer, keine persönlichen Postfächer oder Chats von Beschäftigten.	Einrichtung · Arbeitsanweisung
A4	Zugang: keine Passwörter bei der KI	Anmeldungen in Windows, Teams, Postfach und Fachprogrammen nimmt einmalig eine Person Ihrer Firma vor. Die KI gibt laut Arbeitsanweisung nie Passwörter ein. Die Bildschirmwerkzeuge verweigern technisch Eingaben in Windows-Anmelde- und Sicherheitsdialoge (UAC) und in Passwort-Manager. Kennwortfelder von Programmen erkennt nur ihr Werkzeug für die Bedienelemente; beim Tippen über das Maus- und Tastaturwerkzeug und im Browser-Werkzeug wird das nicht geprüft.	Arbeitsanweisung + Technik · `tools\screen\schutz.py`

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A5	Zugriff: Schutzprüfung vor jedem Werkzeugaufruf	Ein Prüfprogramm prüft jeden Werkzeugaufruf der KI vor der Ausführung. Gesperrt sind unter anderem Installationen (in der Standardeinstellung) und Administratorrechte, Änderungen an System, Netzwerk, Konten und Schutzsoftware, geplante Aufgaben, Autostarts und Dienste, Zugriffe auf übliche Ablageorte von Zugangsdaten, darunter die Anmeldedatei von Claude Code und Umgebungsvariablen mit Schlüsseln von Anthropic, Änderungen an Kit- und Anweisungsdateien, Mailversand über eigene Skripte und Unteragenten. Startet die Prüfung nicht, wird gesperrt statt durchgelassen. Jede Sperre wird protokolliert. Grenze: Laut Programm ist das ein „Geländer gegen Fehler, keine Sicherheitsgrenze gegen Absicht“. Claude Code selbst fragt im Betriebsmodus des Kits (`bypassPermissions`) nicht nach.	Technik · `kit\hook_werkzeug.py`, `.claude\settings.json`
A6	Zugriff: Rechte nur für den Auftrag	Die KI sieht alles, was ihr Windows-Konto sieht: Bildschirm, Dateien und Laufwerke mit Rechten, Postfach und Chats des KI-Kontos, Windows-Benachrichtigungen. Deshalb bekommt das Konto nur die Ordner, Programme und Postfächer, die die vereinbarten Abläufe brauchen. In der Fachsoftware erhält es einen eigenen Benutzer „KI“ ohne Rechte für Zahlungen, Banking oder Unterschriften. Diese Rechte sind die harte Grenze.	Einrichtung · Kunde (C2)

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A7	Zugriff: Fotosperre bei sensiblen Fenstern	Das Foto-Werkzeug nimmt kein Bild auf, solange ein sichtbares Fenster mit sensiblem Titel im Aufnahmebereich liegt, zum Beispiel Passwort-Manager, Windows-Sicherheit, Authenticator oder TAN, AusweisApp, Elster, Online-Banking, PayPal. Die Liste ist erweiterbar. Programme für den Zahlungsverkehr bedienen die Werkzeuge nur lesend; PIN-, TAN- und Unterschriftsdialoge werden nicht fotografiert. Grenze: Erkannt wird nur am Fenstertitel oder Programmnamen, nicht am Inhalt; das Browser-Werkzeug prüft das nicht. Personal- oder Kundendaten in gewöhnlichen Fenstern werden fotografiert. Ein Schalter im Werkzeug hebt die Sperre auf; nutzen darf die KI ihn laut Arbeitsanweisung nur mit Freigabe eines Menschen.	Technik · `tools\screen\schutz.py`, `tools\screen\capture.py`
A8	Zugriff: keine Zusatzverbindungen	Die Connectoren des Kontos bei claude.ai (Team-Anmeldung) und die automatische Merkfunktion von Claude Code sind abgeschaltet. Zusätzliche Schnittstellen (MCP-Server) richtet nur Illig ein, nie mit Rechten für Zahlungen, Administration oder Schreiben im Internet.	Technik + Zusage · `.claude\settings.json`
A9	Trennung	Eigener KI-PC oder eigene VM und eigenes Konto nur für die KI-Mitarbeiterin. Das Kit wird je Kunde aus einer Vorlage eingerichtet, die vor der Auslieferung auf Namen und Daten anderer Kunden und Interessenten geprüft und bereinigt wird, nie aus dem Ordner eines anderen Kunden. Vorführungen laufen nur mit erfundenen Musterdaten. Journal, Protokolle und Verläufe liegen nur auf Ihrem KI-PC.	Einrichtung · Zusage

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A10	Zweckbindung der Protokolle	Protokolle und Bildschirmfotos dienen dazu, die Arbeit der KI nachzuvollziehen, nicht der Kontrolle von Beschäftigten. Die KI prüft Regeln, bewertet aber keine Personen.	Arbeitsanweisung · Zusage · Kunde (C15)

Konto bei Anthropic: Am Testtag nutzt die KI-Mitarbeiterin das Geschäftskonto von Illig; Illig bedient sie selbst, per Fernzugriff oder auf Wunsch vor Ort, und meldet sie am Ende des Testtags ab. Im Betrieb nutzt sie Ihr Abo „Claude Team“ und meldet sich mit ihrem Konto in Ihrer Team-Organisation an, ohne API-Schlüssel; über dieses Abo laufen keine Daten anderer Kunden von Illig.

Pseudonymisierung und Verschlüsselung (lit. a)

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A11	Verschlüsselte Übertragung zu Anthropic	Claude Code überträgt Eingaben und Antworten, also auch Bildschirmfotos und Dateiinhalte, verschlüsselt. Anthropic schreibt dazu: „encrypted in transit via TLS 1.2+“.	Technik (Claude Code) · Claude Code Docs, Data usage
A12	Datenträger des KI-PCs	Chatverläufe, Journal und Protokolle liegen auf dem KI-PC unverschlüsselt. Laut Anthropic sind bei den Verläufen die Dateirechte des Betriebssystems der einzige Schutz. Deshalb empfiehlt Illig eine Laufwerksverschlüsselung für den KI-PC oder die VM (C5).	Kunde
A13	Pseudonymisierung	Eine echte Pseudonymisierung gibt es nicht: Die KI muss die Daten lesen, um die Arbeit zu erledigen. Stattdessen gilt Datensparsamkeit. Das Aktionsprotokoll speichert getippten Text nur als Zeichenzahl. Auswertungen für Illig gibt es nur anonymisiert (B3).	Technik · `tools\screen\act.py`

Integrität: Weitergabe und Eingabe (lit. b)

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A14	Freigabe vor Wirkung nach außen	Am Testtag soll nichts nach außen gehen (Arbeitsanweisung; technisch gesperrt nur, was A15 nennt; auf Wunsch zusätzlich Sperre in Exchange, C7). In der Anlaufphase legt die KI jede Mail nach außen als Sammelfreigabe vor. Eine laut Arbeitsanweisung berechtigte Person antwortet per Teams oder Mail („Ja“, „Ja, außer …“, „Nein“); geprüft wird an Name oder Kennung aus der Liste der Berechtigten, bei Unklarheit wird nachgefragt. Erst dann schaltet das Programm je Versand genau einen Klick auf „Senden“ für 10 Minuten frei. Feste Versandregeln ohne Einzelfreigabe („Hausregeln“) sind anfangs aus. Eingeschaltet werden sie nur auf Ihre Weisung, frühestens nach zwei Wochen Anlaufphase und 20 Sammelfreigaben, mit festen Grenzen.	Technik + Arbeitsanweisung · `kit\freigabe.py`

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A15	Technisches Freigabe-Tor und seine Grenzen	Technisch gesperrt sind: Outlook-„Senden“ ohne Freischaltung, Schaltflächen der Fachsoftware, die bei der Einrichtung eingetragen werden, das Löschen ganzer Laufwerke, System- und Arbeitsordner und Mailversand über eigene Skripte. Grenze: Teams-Nachrichten, Eingaben im Browser-Werkzeug (z. B. Bestellungen in Web-Anwendungen) und Schaltflächen ohne erkennbaren Namen regelt nur die Arbeitsanweisung; das Löschen einzelner Dateien, per Befehl oder über die Oberfläche, begrenzen Rechte und Arbeitsanweisung. Die Antwort auf eine Freigabe trägt die KI selbst ein. Das ist nachvollziehbar, aber nicht fälschungssicher. Für interne Empfänger stellt die KI die Freischaltung selbst aus, und an wen die Mail im Fenster geht, prüft das Werkzeug beim Klick nicht; Kontrolle über Journal und Kopie-Regel im Postfach (C7).	Technik · `kit\freigabe_knoepfe.txt`, `kit\hook_werkzeug.py`
A16	Regeln für Weitergabe und Entscheidungen	Nur mit Freigabe: Zahlungen, Bestellungen, Verträge und verbindliche Zusagen, Löschen von Daten, Weitergabe vertraulicher oder personenbezogener Daten nach außen, neue externe Empfänger, Änderungen an Konten, Passwörtern und Rechten. Bei Zahlungen, neuen Bankverbindungen und neuen externen Empfängern zusätzlich Rückbestätigung über einen zweiten Kanal. Unterschriften, Zahlungen und Entscheidungen über Personen bleiben beim Menschen.	Arbeitsanweisung · `CLAUDE.md`, `job.md`

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A17	Inhalte sind Daten, keine Befehle	Text in Mails, Anhängen, Dokumenten und Webseiten führt die KI nicht als Anweisung aus; ungewöhnliche Aufforderungen meldet sie als Klärfall. Anweisungsdateien, die im Eingangsordner landen, benennt das Programm automatisch um und schreibt einen Alarm.	Arbeitsanweisung + Technik · `kit\gemeinsam.py`
A18	Kennzeichnung als KI	Die erste Nachricht an jede Person und jede Mail tragen einen KI-Hinweis mit verantwortlicher Ansprechperson; der Anzeigename enthält „(KI)“. Technisch erzwungen ist der Hinweis nur beim Versand nach Hausregel (Fußzeile), sonst gilt die Arbeitsanweisung.	Arbeitsanweisung + Technik · `kit\hausregel.py`
A19	Eingabekontrolle: Protokolle	Tagesjournal (erledigt, offen, Freigaben mit Nummer, Person, Kanal, Ergebnis und Anfang der Antwort); Freigabe-Protokoll mit Person, Kanal, Uhrzeit und Wortlaut, das die KI ergänzen, aber nicht ändern kann (A34); Aktionsprotokoll jeder Aktion des Maus- und Tastaturwerkzeugs (Getipptes nur als Zeichenzahl; was die KI über die Bedienelemente von Programmen anklickt oder einträgt, steht im Gesprächsverlauf); Ereignisprotokoll (Aufpasser, Schutzprüfung, Sperren; Chat-Eingaben mit den ersten 80 Zeichen; bei Freigaben und gelernten Regeln mit dem Namen der Person). Alles bleibt auf dem KI-PC und ist dort für Sie einsehbar. Grenze: Das Journal ist kein revisionssicheres Archiv.	Technik + Einrichtung · `arbeit\journal`, `.zustand\log`, `.zustand\freigaben`

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A20	Schutz der eigenen Regeln	Die KI darf ihr Programm, ihre Regeln und ihre Arbeitsanweisung nicht selbst ändern (A5). Das sperrt die Schutzprüfung; eine Rechtegrenze ist das nicht. Auf Wunsch schützt Ihre IT Programmdateien, Regeln und Arbeitsanweisung zusätzlich per NTFS-Schreibschutz, sodass das KI-Konto sie nur lesen kann (C8); Pflicht ist das erst für den Versand nach Hausregel. Änderungen der Arbeitsanweisung dokumentiert Illig mit Datum, Inhalt und auslösender Weisung (B16).	Technik + Einrichtung + Zusage
A21	Kontrollierte Updates	Automatische Updates von VS Code und seinen Erweiterungen sind ausgeschaltet. Updates spielt Illig nur bei angehaltener KI-Mitarbeiterin und mit Abnahmetest ein.	Einrichtung + Zusage · `EINRICHTUNG.md`

Verfügbarkeit und Belastbarkeit (lit. b)

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A22	Not-Aus	Eine leere Datei `STOP` im Kit-Ordner hält die KI-Mitarbeiterin an: Die Schutzprüfung sperrt alle Werkzeuge außer Lesen, Bildschirm- und Browser-Werkzeuge brechen ab, und der Aufpasser startet nichts neu. Die KI-Mitarbeiterin kann die Datei weder anlegen noch entfernen. Anlegen kann sie jeder, der am KI-PC sitzt; weiter geht es erst, wenn ein Mensch sie löscht. Weitere Wege: PC herunterfahren, Windows-Konto sperren und die Sitzung abmelden, Internetzugang sperren, Zugang bei Anthropic sperren. Der Not-Aus wird bei der Einrichtung einmal vorgeführt. Grenze: Die Esc-Taste oder das Schließen von VS Code halten nicht an.	Technik · Kunde · `kit\hook_werkzeug.py`

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A23	Aufpasser und Wiederanlauf	Eine Windows-Aufgabe prüft alle 5 Minuten, solange das KI-Konto angemeldet ist, ob die KI-Mitarbeiterin läuft, und startet sie nach Absturz oder Neustart wieder. Klappt das nach 3 Versuchen in 2 Stunden nicht, entstehen die Datei `ALARM.txt` und ein Hinweisfenster am KI-PC. Grenze: Ohne automatische Anmeldung läuft nach einem Neustart nichts, auch kein Alarm. Im Dauerbetrieb bei einem Kunden ist der Wiederanlauf noch nicht erprobt.	Technik · Einrichtung
A24	Rückfallebene	Fällt die KI-Mitarbeiterin aus oder ist sie angehalten, arbeitet der Fachbereich wie bisher von Hand weiter.	Kunde

Am Testtag meldet Illig die KI-Mitarbeiterin am Ende des Tages bei seinem Geschäftskonto ab. Für einen sofortigen Halt genügen `STOP`, das Herunterfahren oder das Sperren des Windows-Kontos mit Abmelden der Sitzung. Im Betrieb entfernen Sie ihr Konto aus Ihrer Claude-Organisation (laut Anthropic verliert sie damit sofort den Zugang) und melden sie am KI-PC mit „Claude Code: Logout“ ab.

Wiederherstellbarkeit (lit. c)

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A25	Daten in Ihren Systemen	Arbeitsergebnisse legt die KI in Ihren Programmen und Ablagen ab; sie fallen unter Ihre Datensicherung (C12). Die KI-Mitarbeiterin selbst lässt sich aus der sauberen Vorlage mit der freigegebenen Arbeitsanweisung neu einrichten. Eine Kopie mit Ihren Daten bei Illig gibt es nicht.	Einrichtung · Kunde

Regelmäßige Überprüfung (lit. d)

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A26	Diagnose	Ein Diagnoseprogramm des Kits warnt unter anderem, wenn die Datenschutz-Einstellungen des Kits nicht wirken, weil der Kit-Ordner nicht als vertrauenswürdig eingetragen ist.	Technik · `kit\diagnose.py`
A27	Protokolle für Ihre Kontrolle	Journal, Freigabe-Datensätze und Protokolle liegen auf dem KI-PC. Ihre Berechtigten können sie jederzeit einsehen; die Prüfung durch Illig steht in B20.	Technik · Kunde

Ergänzend: Datensparsamkeit und Löschfristen auf dem KI-PC

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A28	Feedback und Telemetrie aus	In Claude Code sind Feedback-Befehl, Sitzungsumfragen, Nutzungsmetriken und Fehlerberichte abgeschaltet. Feedback-Transkripte würde Anthropic laut eigener Angabe 5 Jahre speichern. Die Einstellungen wirken, sobald der Kit-Ordner als vertrauenswürdig eingetragen ist; das erledigt die Einrichtung. Grenze: Nicht vom Kit geregelt sind die Telemetrie von VS Code an Microsoft (auf Wunsch stellt Ihre IT sie ab) und die Prüfung von Web-Adressen vor dem Abruf; dabei geht der Name der Website an Anthropic.	Technik · `.claude\settings.json`
A29	Bildschirmfoto-Dateien	Fotos im Ordner `.zustand\shots` löscht das Foto-Werkzeug nach 3 Tagen von selbst, jeweils beim nächsten Foto. Grenze: Angesehene Bilder stecken zusätzlich im Chatverlauf (A30).	Technik · `tools\screen\capture.py`
A30	Chatverläufe von Claude Code	Verläufe, die 14 Tage nicht benutzt wurden, löscht Claude Code samt Bildschirmfotos von selbst (Einstellung `cleanupPeriodDays`). Die KI-Mitarbeiterin arbeitet in einem fortlaufenden Verlauf; ihn löscht Illig nach Absprache, spätestens beim Abbau. Grenze: Die KI kann ihre gespeicherten Verläufe lesen.	Technik · `.claude\settings.json`
A31	Übrige Protokolle und Ablagen	Journal, Aktions-, Freigabe- und Ereignisprotokoll und der Eingabeverlauf von Claude Code werden nach Ihrer Frist gelöscht (C13; Vorschlag von Illig: 3 Monate), heute von Hand: Illig löscht sie monatlich per Fernwartung oder vor Ort und vermerkt das im Löschprotokoll (Anlage 1 der Vereinbarung); Ihre IT kann jederzeit selbst löschen. Auf Ihre Weisung löscht Illig auch früher. Keine automatische Löschung gibt es für Versandprotokolle, das Browserprofil der KI sowie Ein- und Ausgangsordner; ihre Fristen legen Sie fest (C13).	Zusage · Kunde

Nr.	Maßnahme	Umsetzung	Art · Fundstelle
A32	Dateien statt Bildschirm	Wo möglich, liest die KI Dateien und Exporte direkt, statt Bildschirme zu fotografieren. Am KI-PC sind nur die nötigen Fenster offen.	Einrichtung
A33	Kamera und Mikrofon	Ein Werkzeug für Kamera, Mikrofon oder Aufzeichnung hat die KI nicht. Auf Wunsch schaltet Ihre IT Kamera und Mikrofon des KI-PCs ab.	Technik · Kunde
A34	Ablage der Freigabe-Protokolle	Das Freigabe-Protokoll liegt auf dem KI-PC im Ordner `.zustand\freigaben`. Die Schutzprüfung sperrt der KI das Ändern; lesen können es das KI-Konto und Ihre Administratoren. Wer sonst Zugriff auf den KI-PC hat, legen Sie fest (C15).	Technik · Kunde

B. Bei Illig Automatisierung (Fernwartung, Geräte, Organisation)

Illig ist ein Einzelunternehmen ohne Beschäftigte. Zugriff auf Ihre Daten hat Illig nur bei Einrichtung, Betreuung und Fernwartung, und nur auf dem KI-PC.

Vertraulichkeit (lit. b)

Nr.	Maßnahme	Umsetzung	Art
B1	Persönliche Leistung	Nick Illig arbeitet selbst; es gibt keine Beschäftigten. Weitere Personen erhalten Zugriff nur nach Ihrer Zustimmung in Textform und nach Verpflichtung auf Vertraulichkeit.	Zusage
B3	Keine Daten bei Illig	Keine Kopien, Bildschirmfotos, Ausdrucke oder Datenträger mit Ihren Daten auf Geräten von Illig. Ausgenommen sind Kontaktdaten Ihrer Ansprechpersonen und Vertrags- und Nachweisunterlagen ohne Daten aus den Abläufen, etwa Sitzungs- und Löschprotokolle. Auswertungen nur anonymisiert.	Zusage
B4	Keine Daten über Mail, WhatsApp oder Teams	Personenbezogene Daten aus Ihren Abläufen schicken Sie Illig nicht per E-Mail, WhatsApp oder über ähnliche Dienste; für Fehlerbilder genügen anonymisierte Beschreibungen. Bildschirmfreigaben mit personenbezogenen Daten finden nur über das Fernwartungswerkzeug oder Ihre eigenen Besprechungen statt. Geht Illig so etwas doch zu, löscht er es unverzüglich und teilt Ihnen das mit.	Zusage

Nr.	Maßnahme	Umsetzung	Art
B5	Musterdaten bis zur Unterschrift	Vor der Unterschrift der Vereinbarung arbeitet Illig nur mit Musterdaten und leeren Vorlagen. Echte personenbezogene Daten verarbeitet die KI-Mitarbeiterin erst, wenn zusätzlich die Voraussetzungen nach § 4 Abs. 2 der Vereinbarung erfüllt sind.	Zusage

KI-Konto: Am Testtag läuft die KI-Mitarbeiterin über das Geschäftskonto von Illig bei Anthropic (gewerbliche Bedingungen mit Vereinbarung zur Auftragsverarbeitung); Anthropic ist dann Unterauftragsverarbeiter von Illig (Anlage 3). Illig bedient die KI-Mitarbeiterin am Testtag selbst, per Fernzugriff oder auf Wunsch vor Ort, schützt das Konto mit Zwei-Faktor-Anmeldung und meldet sie am Ende des Testtags ab. Im Betrieb läuft sie über Ihr Abo „Claude Team“: Sie meldet sich mit ihrem Konto in Ihrer Team-Organisation an, einen API-Schlüssel nutzt sie nicht. Dazu erhält Illig keine Zugangsdaten und wird nicht Mitglied Ihrer Organisation bei Anthropic, außer Sie laden ihn für eine bestimmte Aufgabe ein; das wird in Textform dokumentiert und danach wieder entzogen. Ein privates Claude-Abo (Verbrauchertarife wie Free, Pro, Max oder Ultra) nutzt Illig für Ihre Daten nie.

Fernwartung: Zugang und Weitergabe (lit. b)

Nr.	Maßnahme	Umsetzung	Art
B6	Nur der KI-PC	Das Fernwartungswerkzeug wird nur auf dem KI-PC eingerichtet. Ein Zugang zu anderen Rechnern, Laufwerken oder Ihrem Netzwerk wird weder eingerichtet noch genutzt; Ausnahmen nur, wenn vereinbart: beim Azure-Rechner ein Gastzugang nur für dessen Ressourcengruppe, eine VPN-Verbindung nur für die vereinbarten Programme (§ 10 Abs. 1 der Vereinbarung). Kein Windows-Remotedesktop (RDP) als Arbeitsweg, außer beim Azure-Rechner nur bei Bedarf und nur für die Adresse von Illig (§ 10 Abs. 4).	Zusage
B7	Werkzeug	Bevorzugt das Werkzeug Ihrer IT. Hat Ihre IT keins, nutzt Illig ein Werkzeug über ein eigenes Konto nur nach Ihrer vorherigen Genehmigung (Anlage 3). Derzeit ist kein solches Werkzeug im Einsatz; vorgesehen ist TeamViewer.	Zusage
B8	Freigabe nach Ihrer Wahl	Es gilt die Variante, die Sie in der Vereinbarung ankreuzen: **je Sitzung** (nur nach vorheriger Freigabe durch eine benannte Person), **Zeitfenster** (im vereinbarten Fenster ohne Einzelfreigabe) oder **Dauerzugang** (nur, wenn Sie ihn ausdrücklich ankreuzen; im Betreuungsabo empfohlen).	Zusage · Kunde

Nr.	Maßnahme	Umsetzung	Art
B9	Ankündigung und Protokoll	Jede Sitzung kündigt Illig vorher in Textform an (Zweck, voraussichtliche Dauer). Bei Zeitfenster oder Dauerzugang genügt eine Mitteilung unverzüglich danach; geplante Updates kündigt Illig vorher an. Kurzprotokoll je Sitzung: Datum, Beginn, Ende, Anlass, durchgeführte Arbeiten, ob personenbezogene Daten sichtbar waren, wer freigegeben hat. Dieses Protokoll erhält Ihre Ansprechperson nach jeder Sitzung automatisch per E-Mail.	Zusage
B10	Keine Daten mitnehmen	In der Sitzung keine Übertragung von Dateien auf Geräte von Illig, keine Zwischenablage nach außen, keine Aufnahmen oder Bildschirmfotos mit personenbezogenen Daten.	Zusage
B11	Entzug jederzeit	Sie können den Fernzugang jederzeit ohne Angabe von Gründen beenden: Dienst beenden, Konto von der Zugriffsliste nehmen oder Netzwerk trennen.	Kunde

Verschlüsselung (lit. a)

Nr.	Maßnahme	Umsetzung	Art
B12	Verschlüsselte Fernsitzung	Fernzugang nur über eine verschlüsselte Verbindung und nur aus der EU oder dem EWR; aus weiteren Ländern nur, wenn sie in Anlage 1 der Vereinbarung benannt sind und ein Angemessenheitsbeschluss besteht (§ 15 Abs. 1).	Zusage
B13	Gerät von Illig	Das Gerät, mit dem Illig Fernwartung leistet, hat eine Festplattenverschlüsselung, aktuelle Sicherheitsupdates, einen Virenschutz und eine automatische Bildschirmsperre. E-Mail-Konto und Zugang zum Fernwartungswerkzeug sind mit Zwei-Faktor-Anmeldung geschützt.	Zusage
B14	Datensicherung von Illig	Eigene Datensicherungen von Illig (Verträge, Nachweise, Kit-Vorlage; keine Daten aus Ihren Abläufen) liegen nur verschlüsselt vor.	Zusage

Integrität (lit. b)

Nr.	Maßnahme	Umsetzung	Art
B15	Dokumentierte Weisungen	Weisungen nimmt Illig in Textform entgegen und dokumentiert sie. Hält Illig eine Weisung für rechtswidrig, weist er Sie darauf hin.	Zusage
B16	Änderungen der Arbeitsanweisung	Jede Änderung wird mit Datum, Inhalt und auslösender Weisung dokumentiert und liegt auf dem KI-PC.	Zusage

Verfügbarkeit und Belastbarkeit (lit. b)

Nr.	Maßnahme	Umsetzung	Art
B17	Überwachung zwischen den Sitzungen	Ohne Blick auf den Bildschirm: Im Betreuungsabo richtet Illig ein Lebenszeichen vom KI-PC zu sich ein – erst nach Ihrer Genehmigung in Textform (§ 10 Abs. 7 der Vereinbarung): Der KI-PC ruft regelmäßig eine feste Adresse beim Überwachungsdienst healthchecks.io (`hc-ping.com`) auf; bleibt das aus oder meldet er eine Störung, bekommt Illig eine E-Mail. Übertragen wird nur dieses Signal, ohne Namen von Personen, Dateinamen oder Inhalte von Nachrichten. Zusätzlich meldet der KI-PC Störungen vor Ort (A23).	Zusage
B18	Abwesenheit	Urlaub kündigt Illig vorher an. Im Betrieb läuft die KI-Mitarbeiterin über Ihr Abo weiter; Sie können sie jederzeit selbst anhalten (A22).	Zusage

Wiederherstellbarkeit (lit. c)

Nr.	Maßnahme	Umsetzung	Art
B19	Saubere Vorlage	Bei Illig liegen keine Daten aus Ihren Abläufen, die wiederherzustellen wären. Illig hält die saubere Vorlage des Kits bereit, damit die KI-Mitarbeiterin bei Bedarf neu eingerichtet werden kann.	Zusage

Regelmäßige Überprüfung (lit. d)

Nr.	Maßnahme	Umsetzung	Art
B20	Prüfung alle drei Monate	Während der Betreuung prüft Illig alle drei Monate auf dem KI-PC: Rechte, Protokolle, Löschung (ob Journal und Protokolle nach Ihrer Frist gelöscht wurden; auf Ihre Weisung löscht Illig auch früher), Sperren und Vorfälle. Das Ergebnis erhalten Sie in Textform. Bekannt gewordene Änderungen bei Anthropic oder Claude Code, die den Einsatz betreffen, teilt Illig mit. Eine rechtliche Prüfung ist damit nicht verbunden.	Zusage
B21	Tests	Not-Aus-Test bei der Einrichtung, Abnahmetest nach jedem Update.	Zusage
B22	Datenpannen	Meldung an Ihre Meldestelle unverzüglich, möglichst binnen 24 Stunden nach Kenntnis, mit den Angaben, die Sie für eine Meldung nach Art. 33 DSGVO brauchen.	Zusage
B23	Verzeichnis	Illig führt ein Verzeichnis der Verarbeitungstätigkeiten als Auftragsverarbeiter (Art. 30 Abs. 2 DSGVO) und ergänzt es vor Beginn für Sie.	Zusage

Nr.	Maßnahme	Umsetzung	Art
B24	Einweisung	Kurze Einweisung der Beteiligten: was die KI-Mitarbeiterin darf, wie man sie anhält, wohin man Fehler meldet (Art. 4 KI-Verordnung); dokumentiert.	Zusage
B25	Ende und Nachweise	Beim Ende Abbau nach Liste und Löschprotokoll: nach Ende von Einrichtung und Betreuung binnen 10 Werktagen; nach einem Testtag ohne Folgeauftrag binnen 5 Werktagen, sobald Sie absagen oder 14 Tage nach dem Angebot vergangen sind (§ 13 der Vereinbarung). Kontrollen durch Sie oder einen beauftragten Prüfer nach der Vereinbarung. Illig hat als Einzelunternehmen keine eigenen Zertifikate oder Prüfberichte; Nachweise sind diese Anlage, die Protokolle auf dem KI-PC und Ihre Kontrollrechte.	Zusage

C. Mitwirkung des Kunden (C1-C4 und C12 Pflichten nach § 4 Abs. 3, C11 und C17 nach § 4 Abs. 2 und Anlage 4 der Vereinbarung; übrige Empfehlungen)

Diese Maßnahmen liegen bei Ihnen. Viele davon setzt Ihre IT bei der Einrichtung gemeinsam mit Illig um. Die Spalte „Erledigt“ hilft bei der Dokumentation.

Nr.	Maßnahme	Schutzziel	Erledigt
C1	**Eigener KI-PC, eigenes Konto ohne Admin:** PC oder VM nur für die KI-Mitarbeiterin bereitstellen, mit eigenem Windows-Konto als Standardbenutzer. Prüfen, dass das Konto in keiner Administratorgruppe ist.	Zugang, Trennung	☐
C2	**Rechte knapp halten:** nur die nötigen Ordner, Programme und Funktionspostfächer. In der Fachsoftware ein eigener Benutzer „KI“ ohne Rechte für Zahlungen, Banking oder Unterschriften.	Zugriff	☐
C3	**Raum schützen:** KI-PC in einem abschließbaren oder nur Befugten zugänglichen Raum, Bildschirm nicht für Unbefugte einsehbar. Die Bildschirmsperre des KI-Kontos ist aus (A1).	Zutritt	☐
C4	**Anmeldungen selbst vornehmen:** einmalig durch eine Person Ihrer Firma. Passwörter nie im Kit-Ordner, in Notizen oder Chats ablegen.	Zugang	☐
C5	**Laufwerksverschlüsselung** (z. B. BitLocker) für den KI-PC oder die VM einschalten.	Verschlüsselung	☐

Nr.	Maßnahme	Schutzziel	Erledigt
C6	**Netzwerkfreigaben und Domain-Freigabeliste:** keine Netzlaufwerke oder Freigaben anderer Bereiche. Internetzugang des KI-PCs möglichst auf eine Liste beschränken: api.anthropic.com, platform.claude.com (Erneuern der Anmeldung), für die Anmeldung im Browser claude.ai und claude.com, Microsoft 365 und Teams, Ihre Fachprogramme und, falls genutzt, das Fernwartungswerkzeug. Für Anthropic genügt ausgehend HTTPS (Port 443); ein eingehender Port ist nicht nötig. Anthropic selbst empfiehlt für KI, die einen Computer bedient, eine solche Liste.	Zugriff, Integrität	☐
C7	**Senden nach außen sperren oder kontrollieren:** Am Testtag auf Wunsch das Senden nach außen für das KI-Konto per Regel in Exchange bzw. Microsoft 365 sperren. Im Betrieb eine Regel „Mail vom KI-Konto an Empfänger außerhalb der Firma → Kopie (Bcc) an die Fachabteilung“.	Integrität (Weitergabe)	☐
C8	**Schreibschutz der Kit-Dateien** (auf Wunsch; Pflicht erst für den Versand nach Hausregel): Ihre IT schützt Programmdateien, Regeln und Arbeitsanweisung per NTFS, sodass das KI-Konto sie nur lesen kann (A20).	Integrität	☐
C9	**Fernwartungswerkzeug Ihrer IT:** nur auf dem KI-PC, nur genehmigte Konten auf der Zugriffsliste, Weg zum Entzug bekannt. Kein Windows-Remotedesktop (RDP), außer beim Azure-Rechner nur bei Bedarf für die Adresse von Illig.	Zugang	☐
C10	**Claude Team für den Betrieb:** eigenes Abo „Claude Team“ zu den gewerblichen Bedingungen mit Vertrag zur Auftragsverarbeitung (DPA), mindestens zwei Plätze (einer für die KI-Mitarbeiterin, einer für eine Person Ihrer Firma), Nutzungsguthaben mit Ausgabenlimit für Organisation und Konto der KI-Mitarbeiterin; kein API-Schlüssel in der Umgebung. Die Anmeldung nimmt eine Person Ihrer Firma vor; das Konto können Sie jederzeit selbst aus der Organisation entfernen.	Zugang, Verfügbarkeit	☐
C11	**Personen benennen:** Weisungsberechtigte, Freigabeberechtigte (mit Kennung), Not-Aus-Verantwortliche und Vertretung, Meldestelle für Datenpannen. Den Not-Aus einmal selbst testen.	Integrität, Verfügbarkeit	☐
C12	**Datensicherung** der Systeme, in denen die KI arbeitet; vor dem Testtag eine aktuelle Sicherung bestätigen.	Wiederherstellbarkeit	☐

Nr.	Maßnahme	Schutzziel	Erledigt
C13	**Löschfristen festlegen** für Journal und Protokolle (danach werden sie gelöscht, heute von Hand, monatlich durch Illig; Anlage 1 der Vereinbarung), Versandprotokolle sowie Ein- und Ausgangsordner (A31); unbenutzte Chatverläufe löscht Claude Code nach 14 Tagen, den laufenden Verlauf Illig nach Absprache (A30). Vorschlag von Illig für Journal und Protokolle: 3 Monate, sofern keine Aufbewahrungspflicht greift.	Datensparsamkeit	☐
C14	**Rückfallebene:** Der Fachbereich kann jederzeit von Hand weiterarbeiten.	Verfügbarkeit	☐
C15	**Zweckbindung:** Protokolle nur nutzen, um die Arbeit der KI nachzuvollziehen, nicht zur Leistungs- oder Verhaltenskontrolle von Beschäftigten. Betriebsrat beteiligen, falls vorhanden (Hinweise zum Betriebsrat).	Vertraulichkeit	☐
C16	**Stichproben:** Journal und Prüfergebnisse von Illig gelegentlich sichten, z. B. Journal mit den Kopien aus C7 abgleichen.	Überprüfung	☐
C17	**Vor echten Daten:** Vereinbarung unterschrieben, Datenschutzbeauftragter eingebunden, Bedarf einer Datenschutz-Folgenabschätzung geprüft, Beschäftigte informiert, Betriebsrat beteiligt (falls vorhanden), Übermittlung in die USA bewertet (Checkliste für Datenschutzbeauftragte).	Organisation	☐

D. Anthropic

Am Testtag ergeben sich die Maßnahmen von Anthropic aus dem Vertrag von Illig mit der Anthropic Ireland, Limited, im Betrieb aus Ihrem eigenen Vertrag. In beiden Fällen sind das die gewerblichen Bedingungen (Commercial Terms) mit dem Data Processing Addendum (DPA). Die Sicherheitsmaßnahmen stehen im Anhang des DPA (Schedule 2) und werden hier nicht wiederholt.

Zur Orientierung, nur mit Angaben, die Anthropic selbst veröffentlicht:

Angabe	Laut Anthropic	Quelle
Bereiche der Maßnahmen	Sicherheitsprogramm und Richtlinien, Zugriffskontrollen, Personal, Audits und Zertifikate, Verschlüsselung, Schutz der Endgeräte, Umgang mit Schwachstellen, Datenverwaltung, Protokollierung und Umgang mit Vorfällen, Drittanbieter	DPA, Schedule 2, Abschnitte A bis J

Angabe	Laut Anthropic	Quelle
Verschlüsselung	ruhende Daten mindestens AES-256, Übertragung über öffentliche Netze mit TLS 1.2 oder höher („a minimum of AES-256 for data at rest, and TLS1.2+ for data in transit over public networks“)	DPA, Schedule 2, Abschnitt E
Zertifikate und Prüfberichte	laut Trust Center von Anthropic: SOC 2 Typ II (Prüfbericht), ISO/IEC 27001:2022, ISO/IEC 42001:2023 und CSA STAR, in der Übersicht ausgewiesen für „Claude via Anthropic's API“ und „Claude Team“	Trust Center, abgerufen am 01.11.2026
Berichte anfordern	Laut DPA lässt sich Anthropic jährlich von externen Prüfern prüfen und stellt Prüfberichte (z. B. SOC 2) auf schriftliche Anfrage bereit. Im Trust Center gibt es die Dokumente nur auf Anfrage („Request access“).	DPA, Abschnitt F.1; Trust Center

Wo Anthropic die Daten speichert, wie lange und ob trainiert wird, steht auf der Seite unter Anthropic.

E. Grenzen der Maßnahmen (offen benannt)

- **Arbeitsanweisung ist keine Sperre.** Regeln zu Freigaben, Weitergabe, Datensparsamkeit und KI-Hinweis befolgt die KI in aller Regel, aber nicht in jedem Fall; sie werden protokolliert. Die harte Grenze sind die Rechte, die Sie vergeben (A6, C2). Deshalb erhält die KI-Mitarbeiterin keine Rechte für Zahlungen, Banking oder Unterschriften.
- **Die Schutzprüfung ist ein Geländer.** Sie fängt Fehler ab, ist aber keine Sicherheitsgrenze gegen Absicht. Anthropic weist selbst darauf hin, dass Claude unter Umständen Anweisungen aus Inhalten folgt, etwa aus einer Mail. Claude Code fragt im Betriebsmodus des Kits nicht selbst nach. Kein Programm erkennt jeden gefährlichen Befehl.
- **Daten an Anthropic.** Inhalte auf Bildschirmfotos und in Dateien gehen für jeden Arbeitsschritt an Anthropic; gespeichert wird laut Anthropic in den USA. Das bewerten Sie in der Prüfung zur Datenschutz-Folgenabschätzung.
- **Fotosperre:** Sie erkennt sensible Fenster nur an Titel und Programmname. Ein Schalter hebt sie auf; nutzen darf die KI ihn laut Arbeitsanweisung nur mit Freigabe eines Menschen.
- **Anmeldung bei Anthropic:** Die KI kann die Anmeldedaten technisch lesen, weil sie im selben Windows-Konto liegen. Die Schutzprüfung sperrt nur die üblichen Zugriffswege. Deshalb gilt die Anmeldung nur mit Ausgabenlimit und wird beim Ende entzogen. Sie kann ablaufen; dann meldet ein Mensch die KI-Mitarbeiterin neu an.
- **Ohne technisches Tor:** Teams-Nachrichten, Eingaben im Browser-Werkzeug, Schaltflächen ohne erkennbaren Namen und das Löschen einzelner Dateien (per Befehl oder über die Oberfläche). Hier schützen Arbeitsanweisung und Rechte. Freigabe-Antworten trägt die KI selbst ein; sie sind nicht fälschungssicher.
- **Klartext auf dem KI-PC:** Verläufe und Protokolle liegen bis zur Löschung unverschlüsselt im Profil des KI-Kontos. Schutz bieten Konto, Laufwerksverschlüsselung und Raum.
- **Versand:** Eine verschickte Mail lässt sich nicht zurückholen. Freigaben und Kennzeichnung begrenzen das Risiko, schließen es aber nicht aus.

- **Betrieb:** Der Wiederanlauf ist im Dauerbetrieb bei einem Kunden noch nicht erprobt. Ohne automatische Anmeldung läuft nach einem Neustart nichts, auch kein Alarm.
- **Noch nicht im Einsatz:** ein Fernwartungswerkzeug über das Konto von Illig (vorgesehen: TeamViewer, B7).

Mehr dazu auf der Seite unter Grenzen der KI-Mitarbeiterin und Fernzugriff.

Quellen

Alle Webquellen abgerufen am 01.11.2026.

- Art. 32 DSGVO, Verordnung (EU) 2016/679: https://eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- Anthropic, Data Processing Addendum, Stand 24.02.2025 („Effective Feb 24, 2025“): https://www.anthropic.com/legal/data-processing-addendum
- Anthropic Trust Center (Seite ohne Stand-Datum): https://trust.anthropic.com
- Anthropic Privacy Center, „What Certifications has Anthropic obtained?“, Stand 30.10.2026: https://privacy.claude.com/en/articles/10015870-what-certifications-has-anthropic-obtained
- Claude Code Docs, „Data usage“ (ohne Stand-Datum): https://code.claude.com/docs/en/data-usage
- Claude Code Docs, „Explore the .claude directory“ (ohne Stand-Datum): https://code.claude.com/docs/en/claude-directory
- Claude Platform Docs, „Computer use tool“, Empfehlung einer Domain-Freigabeliste (ohne Stand-Datum): https://platform.claude.com/docs/en/agents-and-tools/tool-use/computer-use-tool
- Fundstellen im Kit: Dateien im Kit-Ordner auf dem KI-PC, Pfade wie in den Tabellen angegeben.