

DESKGATE, INC. · SCHEDULE CH

Vereinbarung über die Auftragsbearbeitung (AVV)

gemäss Art. 9 des Bundesgesetzes über den Datenschutz (Datenschutzgesetz, DSG; SR 235.1) und Art. 1–4 der Datenschutzverordnung (DSV; SR 235.11)

Version 2.2 · Stand Oktober 2026

Gilt für DeskGate Operator ab Version 2.6.8 im Schweiz-Modus (§ 2.1).

ZWISCHEN

VERANTWORTLICHER

NAME DER ARZTPRAXIS / GRUPPENPRAXIS /
INSTITUTION

RECHTSFORM

STRASSE, NR.

PLZ, ORT

GLN

ZSR-NUMMER

KONTAKT FÜR DATENSCHUTZMELDUNGEN (E-MAIL)

– nachfolgend «Verantwortlicher» –

AUFTRAGSBEARBEITER

FIRMA

DeskGate, Inc.

RECHTSFORM

**Corporation nach dem Recht des US-
Bundesstaates Delaware (C-Corporation)**

REGISTERNUMMER · GRÜNDUNG

**Delaware Division of Corporations, File No.
10773474 · 17. September 2026**

EINGETRAGENER SITZ (REGISTERED OFFICE)

**131 Continental Dr, Suite 305, Newark, DE 19713,
USA**

Registered Agent: Legalinc Corporate Services Inc.

GESCHÄFTSADRESSE / OPERATIVER STANDORT

**Lauterbachstrasse 136a, CH-3068 Utzigen,
Schweiz**

PLATTFORM

deskgate.app

KONTAKT FÜR DATENSCHUTZMELDUNGEN (E-MAIL)

contact@deskgate.app

– nachfolgend «Auftragsbearbeiter» –

Verantwortlicher und Auftragsbearbeiter werden zusammen als «Parteien» bezeichnet.

Präambel

- A.** Der Verantwortliche erbringt medizinische Leistungen, insbesondere nach dem Bundesgesetz über die Krankenversicherung (KVG) und dem Bundesgesetz über die Unfallversicherung (UVG). Er bearbeitet dabei besonders schützenswerte Personendaten im Sinne von Art. 5 lit. c Ziff. 2 DSG (Daten über die Gesundheit) und untersteht dem Berufsgeheimnis nach Art. 321 StGB.
- B.** Der Auftragsbearbeiter stellt die Browser-Erweiterung «DeskGate Operator» bereit. Sie unterstützt Fachpersonen des Verantwortlichen bei Rechnungsbeanstandungen, TARDOC-Kürzungen und Auskunftsbegleichen von Versicherern nach Art. 42 Abs. 4 KVG, indem sie im Browser des Verantwortlichen Entwürfe für ärztliche Stellungnahmen vorbereitet.
- C.** Diese Vereinbarung regelt die datenschutzrechtlichen Rechte und Pflichten der Parteien nach Art. 9 DSG. Sie ist integrierender Bestandteil der DeskGate Master Terms einschliesslich der Schedules S, I und M (nachfolgend «Master Terms»).

§ 1 Gegenstand, Zweck, Art und Dauer der Bearbeitung

- 1.1 **Gegenstand.** Gegenstand dieser Vereinbarung ist die Bearbeitung von Personendaten durch den Auftragsbearbeiter im Auftrag des Verantwortlichen im Zusammenhang mit der Bereitstellung und dem Betrieb von DeskGate Operator.
- 1.2 **Zweck.** Die Bearbeitung dient ausschliesslich (a) der automatisierten Analyse von Auszügen aus der Krankengeschichte (KG), von Kürzungsbescheiden und von Anfragen der Kostenträger, (b) der Vorbereitung von Entwürfen für ärztliche Stellungnahmen und (c) der Lizenzverwaltung und Nutzungserfassung nach Anhang 3.
- 1.3 **Art der Bearbeitung.** Auslesen des Seitentexts im fokussierten Browser-Tab einschliesslich seiner Frames, Strukturierung und Analyse im Browser, Zuordnung zu Formularfeldern mittels Wortlisten im Browser, Vorbefüllen von Feldern und Erstellung von Entwürfen; Übermittlung der Lizenz-, Nutzungs- und Verbindungsdaten nach Anhang 3 Ziff. 5–7 an den Auftragsbearbeiter.
- 1.4 **Daten und betroffene Personen.** Die bearbeiteten Datenkategorien, die betroffenen Personen, die Bearbeitungsorte und die Speicherdauer ergeben sich aus Anhang 3.
- 1.5 **Dauer.** Diese Vereinbarung gilt für die Laufzeit der Master Terms. Die Bestimmungen über Geheimhaltung (§ 4), Haftung (§ 13) sowie Rückgabe und Löschung (§ 15) gelten über das Vertragsende hinaus.

§ 2 Schweiz-Modus, Systemarchitektur und Datenminimierung

- 2.1 **Geltungsbereich: Schweiz-Modus.** Diese Vereinbarung gilt für den Einsatz von DeskGate Operator im Schweiz-Modus (Einstellung «Schweiz-Modus: 100 % lokale Ausführung»). Im Schweiz-Modus bearbeitet die Erweiterung Patientendaten ausschliesslich lokal in der Laufzeitumgebung des Browsers auf dem Arbeitsplatzrechner der Fachperson des Verantwortlichen. **Im Schweiz-Modus werden keine Personendaten von Patientinnen und Patienten an den Auftragsbearbeiter, an Unterauftragsbearbeiter oder an sonstige Dritte übermittelt.** Insbesondere wird kein Bildschirminhalt erfasst (§ 3.1), und die Zuordnung zu Formularfeldern erfolgt ohne KI-Modell ausserhalb des Browsers.
- 2.2 **Test- und Demonstrationsfunktionen.** Ausserhalb des Schweiz-Modus enthält die Erweiterung Test- und Demonstrationsfunktionen, insbesondere eine Bildschirmlesung und eine Feldzuordnung über Cloud-KI-Modelle. Diese Funktionen sind ausschliesslich für synthetische Testdaten bestimmt und nicht Gegenstand dieser Vereinbarung. Der Verantwortliche setzt sie nicht mit Personendaten ein (§ 6.5).
- 2.3 **Flüchtige Bearbeitung.** Patientendaten (insbesondere Namen, Geburtsdaten, AHV- und Versichertennummern, Befunde, Diagnosen und Freitexte) werden nur im Arbeitsspeicher der Erweiterung gehalten. Die Erweiterung schreibt keine Patientendaten in persistente Speicher, insbesondere nicht in den Erweiterungsspeicher (`chrome.storage`), `localStorage`, `IndexedDB`, den Cache-Speicher des Browsers oder das Dateisystem.
- 2.4 **Verwerfen von Falldaten.** Beim Auslösen der Funktion «Neuer Fall», beim Schliessen des Panels oder beim Beenden der Sitzung verwirft die Erweiterung sämtliche Referenzen auf Falldaten; diese werden damit zur Freigabe durch die Speicherverwaltung des Browsers bestimmt. Die Parteien halten fest, dass Zeitpunkt und Art des physischen Überschreibens des Arbeitsspeichers von Browser und Betriebssystem bestimmt werden und nicht von der Erweiterung gesteuert werden können. Die Sicherung des Arbeitsplatzes, auch gegen Auslagerungs- und Ruhezustandsdateien, regelt § 6.4.
- 2.5 **Keine serverseitige Speicherung von Patientendaten.** Die Systeme des Auftragsbearbeiters speichern, protokollieren oder cachen keine Patientendaten, insbesondere keine Klarnamen, Identifikatoren, medizinischen Inhalte, Dokumente oder Bildausschnitte. Serverseitig bearbeitet der Auftragsbearbeiter ausschliesslich die in Anhang 3 Ziff. 5–7 bezeichneten Daten.

- 2.6 Auslieferung und Nachprüfbarkeit.** Die Erweiterung wird als signierte CRX-Datei über den Update-Kanal `deskgate.app/ext/updates.xml` ausgeliefert und auf Google Chrome oder Microsoft Edge über eine Richtlinie des Verantwortlichen installiert; sie ist nicht im Chrome Web Store gelistet. Der Quellcode ist öffentlich einsehbar unter `github.com/deskgate-app/deskgate-operator-2.6.8-public` bzw. im Repository der jeweils ausgelieferten Version. Der Auftragsbearbeiter veröffentlicht zu jeder ausgelieferten Version die Versionsnummer und den SHA-256-Prüfwert der CRX-Datei, so dass der Verantwortliche oder ein beauftragter Prüfer nachvollziehen kann, dass die ausgelieferte Datei dem veröffentlichten Quellcode entspricht. Serverseitige Komponenten unterliegen den Prüfrechten nach § 14.

§ 3 Bildschirmlesung

- 3.1 Im Schweiz-Modus nicht verfügbar.** Im Schweiz-Modus ist die Bildschirmlesung (Erfassung von Bildausschnitten zur Texterkennung, z. B. bei PDF- oder Citrix-Darstellungen) deaktiviert und kann vom Verantwortlichen nicht aktiviert werden. Angaben, die nicht als Seitentext vorliegen, überträgt die Fachperson von Hand.
- 3.2 Voraussetzungen einer Einführung.** Der Auftragsbearbeiter kann die Bildschirmlesung im Schweiz-Modus nur einführen, wenn
- (a) er dies dem Verantwortlichen mindestens 30 Tage im Voraus in Textform mitteilt; § 8.3 gilt sinngemäss;
 - (b) die Funktion standardmässig deaktiviert bleibt und erst wirksam wird, wenn der Verantwortliche sie im Konfigurationsmenü ausdrücklich aktiviert;
 - (c) ausschliesslich der sichtbare Inhalt des aktiven Tabs erfasst wird und die Fachperson den Bildausschnitt nach Anzeige einer Vorschau auswählt und die Übermittlung bestätigt;
 - (d) Bildausschnitte verschlüsselt und ausschliesslich an Google Cloud Vertex AI im Projekt «deskgate-production» in der Region Zürich (europa-west6) übermittelt werden, ohne Weiterleitung über die Server von `deskgate.app`, und das Projekt dem Assured-Workloads-Kontrollpaket «Switzerland Data Boundary» zugeordnet ist;
 - (e) das Zwischenspeichern (Caching) von Modelleingaben deaktiviert ist, für die Protokollierung von Eingaben zur Missbrauchsüberwachung eine Ausnahme von Google erteilt wurde, soweit das Projekt einer solchen Protokollierung unterliegt, und keine Funktionen aktiviert sind, die Eingaben oder Ausgaben speichern oder protokollieren; und
 - (f) die Erweiterung vor jeder Übermittlung prüft, dass die Bearbeitung über diese Route und in dieser Region erfolgt, und andernfalls nichts übermittelt.

Entfällt eine dieser Voraussetzungen, deaktiviert der Auftragsbearbeiter die Funktion unverzüglich und informiert den Verantwortlichen.

- 3.3 Vertragsgrundlage mit Google.** Für eine Bearbeitung nach Einführung gelten im Verhältnis zu Google LLC (Anhang 2) das Google Cloud Data Processing Addendum (CDPA) und die jeweils geltenden Service Specific Terms von Google Cloud. Danach darf Google Kundendaten nicht ohne Zustimmung des Kunden zum Training von KI-Modellen verwenden; der Auftragsbearbeiter erteilt keine solche Zustimmung. Zusätzlich besteht zwischen Google LLC und dem Auftragsbearbeiter ein Google Cloud Platform HIPAA Business Associate Addendum.

§ 4 Berufsgeheimnis (Art. 321 StGB)

- 4.1 Hilfspersonen.** Der Auftragsbearbeiter und die von ihm eingesetzten Personen handeln als Hilfspersonen des Verantwortlichen im Sinne von Art. 321 Ziff. 1 StGB.
- 4.2 Geheimhaltung.** Der Auftragsbearbeiter behandelt alle ihm im Rahmen dieser Vereinbarung zugänglich werdenden Personendaten und Tatsachen streng vertraulich. Die Geheimhaltungspflicht gilt nach Beendigung dieser Vereinbarung zeitlich unbeschränkt fort.

- 4.3 Personal.** Alle beim Auftragsbearbeiter tätigen Personen mit Zugang zu Systemen, in denen Personendaten des Verantwortlichen bearbeitet werden, sind schriftlich zur Geheimhaltung verpflichtet und über die strafrechtlichen Folgen einer Verletzung des Berufsgeheimnisses belehrt. Administrative Zugriffe erfolgen nur durch namentlich bezeichnete Personen. Der Auftragsbearbeiter legt dem Verantwortlichen auf Anfrage die Liste dieser Personen einschliesslich des Landes offen, aus dem sie zugreifen.
- 4.4 Unterauftragsbearbeiter.** Unterauftragsbearbeiter nach Anhang 2 sind nach ihren Standardvertragsbedingungen verpflichtet, insbesondere zu Vertraulichkeit und Datensicherheit. Eine individuelle Verpflichtung als Hilfspersonen im Sinne von Art. 321 StGB wird mit ihnen nicht vereinbart. Im Schweiz-Modus erhalten sie keine Patientendaten (§ 2.1).

§ 5 Bearbeitung nach Weisung

- 5.1** Der Auftragsbearbeiter bearbeitet Personendaten ausschliesslich im Rahmen dieser Vereinbarung und nach dokumentierten Weisungen des Verantwortlichen. Die Einstellungen, die der Verantwortliche im Konfigurationsmenü vornimmt, gelten als Weisungen.
- 5.2** Ist der Auftragsbearbeiter der Ansicht, dass eine Weisung gegen das DSG oder andere Datenschutzvorschriften verstösst, teilt er dies dem Verantwortlichen unverzüglich mit.
- 5.3** Der Auftragsbearbeiter bearbeitet Personendaten des Verantwortlichen nicht für eigene Zwecke, ausgenommen die Vertragsabwicklung nach Anhang 3 Ziff. 5. Er unternimmt keine Versuche, pseudonymisierte Daten (Anhang 1 Ziff. 1.5) Personen oder Fällen zuzuordnen.

§ 6 Pflichten des Verantwortlichen

- 6.1 Rechtmässigkeit.** Der Verantwortliche ist für die Rechtmässigkeit der Bearbeitung verantwortlich, insbesondere für die Erhebung der Daten, die Information der betroffenen Personen (Art. 19 DSG) und die Bekanntgabe an Kostenträger.
- 6.2 Datenschutz-Folgenabschätzung.** Der Verantwortliche prüft, ob für den Einsatz von DeskGate eine Datenschutz-Folgenabschätzung nach Art. 22 DSG erforderlich ist. Der Auftragsbearbeiter unterstützt ihn dabei nach § 10.2.
- 6.3 Menschliche Freigabe (Human in the Loop).**
- (a) *WZW-Bestätigung (Art. 32 KVG):* Die Bestätigung von Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit erfolgt ausschliesslich durch die verantwortliche Ärztin oder den verantwortlichen Arzt. Die Erweiterung setzt entsprechende Bestätigungen nie automatisch.
 - (b) *Vertrauensärztlicher Dienst (Art. 42 Abs. 5 KVG):* Die Entscheidung, ob medizinische Angaben nur der Vertrauensärztin oder dem Vertrauensarzt des Versicherers bekanntgegeben werden, liegt ausschliesslich beim Verantwortlichen.
 - (c) *Einreichung:* Das Absenden auf dem Portal des Kostenträgers erfordert stets eine Handlung der Fachperson des Verantwortlichen; die Erweiterung reicht nichts selbständig ein.
 - (d) *Inhaltliche Verantwortung:* Von DeskGate erstellte Entwürfe sind Vorschläge. Die Fachperson prüft sie vor der Freigabe; der Verantwortliche trägt die Verantwortung für die eingereichten Inhalte.
- 6.4 Arbeitsplatzsicherheit.** Der Verantwortliche setzt DeskGate nur auf Arbeitsplatzrechnern mit aktuellem Betriebssystem und Browser, Festplattenverschlüsselung, automatischer Bildschirmsperre und persönlichen Benutzerkonten ein.

- 6.5 Einsatz im Schweiz-Modus.** Der Verantwortliche setzt DeskGate mit Personendaten von Patientinnen und Patienten ausschliesslich im Schweiz-Modus ein und prüft dies vor dem ersten Einsatz und nach jeder neuen Version anhand der Anzeige im Panel. Er verwendet die Funktionen nach § 2.2 nicht mit Personendaten, hinterlegt keine eigenen API-Schlüssel von KI-Anbietern und ändert die voreingestellte Server-Adresse <https://deskgate.app> nicht. Der Auftragsbearbeiter weist bei der Einrichtung auf diese Pflichten hin.

§ 7 Technische und organisatorische Massnahmen

- 7.1** Der Auftragsbearbeiter trifft die in Anhang 1 beschriebenen technischen und organisatorischen Massnahmen, um eine dem Risiko angemessene Datensicherheit nach Art. 8 DSG und Art. 1–4 DSV zu gewährleisten.
- 7.2** Der Auftragsbearbeiter überprüft die Massnahmen regelmässig und passt sie dem Stand der Technik an. Änderungen, die das Schutzniveau senken oder die Datenflüsse nach Anhang 3 erweitern, sind nur nach vorgängiger Mitteilung an den Verantwortlichen zulässig; § 8.2 und § 8.3 gelten sinngemäss.

§ 8 Unterauftragsbearbeiter

- 8.1 Genehmigung.** Der Verantwortliche genehmigt im Sinne von Art. 9 Abs. 3 DSG den Beizug der in Anhang 2 genannten Unterauftragsbearbeiter für die dort beschriebenen Leistungen.
- 8.2 Mitteilung von Änderungen.** Der Auftragsbearbeiter teilt dem Verantwortlichen jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsbearbeiters mindestens 30 Tage im Voraus in Textform mit. Die Mitteilung nennt Firma, Sitz, Bearbeitungsort, Zweck und vertragliche Garantien.
- 8.3 Widerspruchsrecht.** Der Verantwortliche kann innert dieser Frist aus datenschutzrechtlichen Gründen widersprechen. Bei einem Widerspruch verzichtet der Auftragsbearbeiter gegenüber diesem Verantwortlichen auf den Beizug oder bietet ihm die betroffene Funktion nicht mehr an. Ist beides nicht möglich, kann der Verantwortliche die Master Terms ohne Kostenfolge auf den Zeitpunkt des Wechsels kündigen; vorausbezahlte Gebühren werden anteilig zurückerstattet. Erhebt der Verantwortliche innert der Frist keinen Widerspruch, gilt die Genehmigung als erteilt.
- 8.4 Dringende Änderungen.** Ist ein Wechsel aus zwingenden Sicherheitsgründen kurzfristiger erforderlich, informiert der Auftragsbearbeiter den Verantwortlichen unverzüglich. Die betroffene Funktion bleibt bis zum Ablauf der Widerspruchsfrist deaktiviert, sofern der Verantwortliche dem Wechsel nicht vorher zustimmt.
- 8.5 Weiterverpflichtung und Haftung.** Der Auftragsbearbeiter verpflichtet Unterauftragsbearbeiter vertraglich auf Datenschutz- und Datensicherheitspflichten, die den Anforderungen des DSG und dieser Vereinbarung entsprechen, soweit diese für ihre Leistung massgeblich sind. Er haftet gegenüber dem Verantwortlichen für Unterauftragsbearbeiter im Rahmen von § 13.
- 8.6 Weitere Stufen.** Google und Flow Swiss setzen für ihre Leistungen eigene Unterauftragsbearbeiter ein. Google veröffentlicht sie unter cloud.google.com/terms/subprocessors, Flow Swiss in Anhang A ihres Auftragsbearbeitungsvertrags. Diese gelten als mitgenehmigt. Änderungen, die Google oder Flow Swiss dem Auftragsbearbeiter mitteilen und die die Bearbeitung von Personendaten des Verantwortlichen betreffen können, gibt der Auftragsbearbeiter unverzüglich an den Verantwortlichen weiter.

§ 9 Bekanntgabe ins Ausland und Anfragen von Behörden

- 9.1 Patientendaten.** Personendaten von Patientinnen und Patienten werden im Schweiz-Modus ausschliesslich im Browser des Verantwortlichen in der Schweiz bearbeitet und nicht übermittelt; eine Bekanntgabe ins Ausland findet nicht statt. Wird die Bildschirmlesung nach § 3.2 eingeführt, erfolgt die Bearbeitung in der Region europe-west6. Vertragspartnerin ist dann Google LLC mit Sitz in den USA; soweit ein Zugriff von Google aus dem Ausland als Bekanntgabe ins Ausland gilt, stützt sich diese auf die Zertifizierung von Google LLC nach dem Swiss-U.S. Data Privacy Framework (Art. 16 Abs. 1 DSG in Verbindung mit Anhang 1 DSV) sowie auf das CDPA.
- 9.2 Übrige Personendaten.** Der Auftragsbearbeiter ist eine nach dem Recht des US-Bundesstaates Delaware gegründete Gesellschaft mit operativem Standort in der Schweiz. Die Server von deskgate.app werden bei Flow Swiss AG, Baar, betrieben (Anhang 2). Die Daten nach Anhang 3 Ziff. 5–7 werden dort in Rechenzentren in der Schweiz gespeichert und bearbeitet. Eine Bekanntgabe ins Ausland, einschliesslich eines Fernzugriffs aus dem Ausland und einer Bekanntgabe durch Unterauftragsbearbeiter von Flow Swiss, erfolgt nur unter Einhaltung von Art. 16 und 17 DSG.
- 9.3 Anfragen von Behörden.** Erhält der Auftragsbearbeiter eine Anfrage oder Anordnung einer in- oder ausländischen Behörde auf Herausgabe von Personendaten des Verantwortlichen, einschliesslich Anordnungen nach US-Recht, so
- (a) informiert er den Verantwortlichen unverzüglich, soweit dies rechtlich zulässig ist,
 - (b) prüft er die Rechtmässigkeit der Anfrage und ergreift die zumutbaren Rechtsmittel, und
 - (c) gibt er nur die Daten heraus, zu deren Herausgabe er rechtlich verpflichtet ist.
- Die Parteien halten fest, dass der Auftragsbearbeiter nach § 2.4 keine Patientendaten speichert und solche deshalb nicht herausgeben kann.

§ 10 Unterstützung des Verantwortlichen

- 10.1 Rechte der betroffenen Personen.** Der Auftragsbearbeiter unterstützt den Verantwortlichen bei der Erfüllung von Begehren betroffener Personen nach Art. 25–32 DSG, insbesondere durch Auskunft über die bei ihm vorhandenen Daten. Richtet eine betroffene Person ein Begehren direkt an den Auftragsbearbeiter, leitet dieser es innert fünf Arbeitstagen an den Verantwortlichen weiter.
- 10.2 Datenschutz-Folgenabschätzung.** Der Auftragsbearbeiter stellt dem Verantwortlichen die Informationen über die Bearbeitung, ihre Risiken und die getroffenen Massnahmen zur Verfügung, die für eine Datenschutz-Folgenabschätzung (Art. 22 DSG) und eine allfällige Konsultation des EDÖB (Art. 23 DSG) erforderlich sind.
- 10.3 Verzeichnis.** Der Auftragsbearbeiter führt ein Verzeichnis seiner Bearbeitungstätigkeiten nach Art. 12 DSG.

§ 11 Verletzungen der Datensicherheit

- 11.1 Meldung.** Der Auftragsbearbeiter meldet dem Verantwortlichen jede Verletzung der Datensicherheit, die Personendaten des Verantwortlichen betrifft oder betreffen könnte, unverzüglich, spätestens innert 24 Stunden nach Kenntnisnahme (Art. 24 Abs. 3 DSG), an die vom Verantwortlichen bezeichnete Kontaktadresse.
- 11.2 Inhalt.** Die Meldung enthält, soweit bekannt, Art und Zeitpunkt der Verletzung, die betroffenen Datenkategorien und Personen, die möglichen Folgen sowie die ergriffenen und vorgeschlagenen Massnahmen. Spätestens innert 72 Stunden nach Kenntnisnahme liefert der Auftragsbearbeiter einen ausführlichen Bericht; noch nicht verfügbare Angaben werden laufend nachgereicht.

- 11.3 Unterstützung.** Der Auftragsbearbeiter unterstützt den Verantwortlichen bei einer allfälligen Meldung an den EDÖB und bei der Information der betroffenen Personen (Art. 24 DSG). Er informiert betroffene Personen oder die Öffentlichkeit nicht ohne vorgängige Absprache mit dem Verantwortlichen, es sei denn, er ist dazu gesetzlich verpflichtet.
- 11.4 Ereignisse bei Unterauftragsbearbeitern.** Sicherheitsrelevante Ereignisse, die ein Unterauftragsbearbeiter dem Auftragsbearbeiter meldet, gibt dieser nach § 11.1 weiter.

§ 12 Service Levels

- 12.1 Sicherheitsupdates.** Der Auftragsbearbeiter behebt Sicherheitslücken in der Erweiterung und in seinen serverseitigen Komponenten oder trifft wirksame Abhilfemassnahmen, einschliesslich der Deaktivierung betroffener Funktionen, innert folgender Fristen ab Kenntnisnahme:

SCHWEREGRAD	FRIST
Kritisch (CVSS $\geq$ 9.0)	72 Stunden
Hoch (CVSS 7.0–8.9)	14 Tage
Mittel und niedrig (CVSS < 7.0)	Nächstes reguläres Release, spätestens 90 Tage

- 12.2 Anpassung an Portaländerungen.** Beeinträchtigen Änderungen an den Portalen der Kostenträger die Funktion von DeskGate, stellt der Auftragsbearbeiter eine Anpassung innert fünf Arbeitstagen ab Kenntnisnahme bereit (Zielwert). Bis dahin informiert er die Nutzerinnen und Nutzer in der Erweiterung über die Einschränkung.
- 12.3 Versionshinweise.** Jede Version wird mit Versionshinweisen veröffentlicht. Sicherheitsrelevante Änderungen und Änderungen der Datenflüsse nach Anhang 3 teilt der Auftragsbearbeiter dem Verantwortlichen vorgängig in Textform mit; für Änderungen der Datenflüsse gilt § 7.2.
- 12.4 Weitere Service Levels.** Weitergehende Service Levels richten sich nach den Master Terms.

§ 13 Haftung und Freistellung

- 13.1 Haftungsobergrenze.** Die Gesamthaftung jeder Partei aus oder im Zusammenhang mit dieser Vereinbarung ist pro Vertragsjahr auf den Betrag der Abonnementgebühren begrenzt, die der Verantwortliche in den zwölf Monaten vor dem schadenstiftenden Ereignis bezahlt hat oder schuldet.
- 13.2 Freistellung.** Jede Partei hält die andere schadlos für Ansprüche Dritter, die auf einer schuldhaften Verletzung dieser Vereinbarung durch die freistellende Partei beruhen. Die Freistellung ist auf den Betrag nach § 13.1 begrenzt (Freistellungsmaximum) und wird auf diesen angerechnet. Bussen und andere strafrechtliche Sanktionen sind von der Freistellung ausgenommen.
- 13.3 Ausnahmen.** Die Begrenzungen nach § 13.1 und § 13.2 gelten nicht bei rechtswidriger Absicht oder grober Fahrlässigkeit (Art. 100 Abs. 1 OR) sowie, soweit gesetzlich zwingend, bei weiteren Haftungstatbeständen.
- 13.4 Inhalt von Stellungnahmen.** Der Auftragsbearbeiter haftet nicht für den Inhalt der vom Verantwortlichen freigegebenen Stellungnahmen und nicht für den Ausgang von Verfahren gegenüber Kostenträgern (§ 6.3 lit. d); § 13.3 bleibt vorbehalten.
- 13.5 Verhältnis zu den Master Terms.** Dieser § 13 geht in datenschutzrechtlichen Belangen abweichenden Haftungsbestimmungen der Master Terms vor.

§ 14 Kontroll- und Auditrechte

- 14.1** Der Verantwortliche ist berechtigt, sich von der Einhaltung dieser Vereinbarung zu überzeugen (Art. 9 Abs. 2 DSG).
- 14.2 Nachweise.** Der Auftragsbearbeiter stellt dem Verantwortlichen auf Anfrage zur Verfügung:
- (a) den Zugang zum Quellcode und zu den Prüfwerten nach § 2.6;
 - (b) einen jährlich aktualisierten schriftlichen Bericht über die Umsetzung der Massnahmen nach Anhang 1;
 - (c) nach einer Einführung der Bildschirmlesung die schriftliche Bestätigung der Voraussetzungen nach § 3.2;
 - (d) die Beschreibung des Pseudonymisierungsverfahrens nach Anhang 1 Ziff. 1.5;
 - (e) nach einer Einführung der Bildschirmlesung die Drittzertifizierungen von Google Cloud, insbesondere ISO/IEC 27001, 27017 und 27018 sowie SOC 2 Type II. Die Parteien halten fest, dass diese Zertifizierungen die Infrastruktur von Google betreffen und keine Zertifizierung des Auftragsbearbeiters darstellen.
- 14.3 Prüfungen.** Der Verantwortliche kann die Einhaltung durch eine Prüfung vor Ort oder aus der Ferne überprüfen, selbst oder durch einen unabhängigen, zur Verschwiegenheit verpflichteten Prüfer. Prüfungen sind mit einer Frist von 30 Tagen anzukündigen und höchstens einmal pro Vertragsjahr zulässig, ausser bei begründetem Verdacht auf eine Verletzung dieser Vereinbarung oder nach einer Verletzung der Datensicherheit. Die Kosten trägt der Verantwortliche, es sei denn, die Prüfung ergibt eine wesentliche Verletzung dieser Vereinbarung.

§ 15 Beendigung, Rückgabe und Löschung

- 15.1 Patientendaten.** Da der Auftragsbearbeiter keine Patientendaten speichert (§ 2.4), sind bei Vertragsende keine Patientendaten zurückzugeben. Der Auftragsbearbeiter bestätigt dies dem Verantwortlichen schriftlich.
- 15.2 Lokale Daten.** Mit der Deinstallation der Erweiterung werden sämtliche lokal gespeicherten Daten der Erweiterung (Einstellungen nach Anhang 3 Ziff. 4) entfernt. Der Verantwortliche kann die Einstellungen zudem jederzeit im Konfigurationsmenü ändern oder leeren.
- 15.3 Serverseitige Daten.** Auf Verlangen des Verantwortlichen, das innert 30 Tagen nach Vertragsende zu stellen ist, übergibt der Auftragsbearbeiter die den Verantwortlichen betreffenden Lizenz- und Nutzungsdaten in einem gängigen maschinenlesbaren Format (CSV oder JSON). Er löscht diese Daten nach den Fristen von Anhang 3, ausgenommen Daten, die er aufgrund gesetzlicher Aufbewahrungspflichten aufbewahren muss.
- 15.4 Löschbestätigung.** Der Auftragsbearbeiter bestätigt die Löschung auf Verlangen schriftlich.

§ 16 Schlussbestimmungen

- 16.1 Rangfolge.** Bei Widersprüchen zwischen dieser Vereinbarung und den Master Terms oder anderen Lizenzvereinbarungen geht diese Vereinbarung in datenschutzrechtlichen Belangen vor.
- 16.2 Form.** Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Mitteilungen nach den §§ 7, 8, 11 und 12 können in Textform (E-Mail) erfolgen.
- 16.3 Teilnichtigkeit.** Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame Bestimmung, die ihrem wirtschaftlichen und datenschutzrechtlichen Zweck möglichst nahekommt.
- 16.4 Anwendbares Recht.** Diese Vereinbarung untersteht schweizerischem materiellem Recht unter Ausschluss der Kollisionsnormen des Bundesgesetzes über das Internationale Privatrecht (IPRG).

16.5 Gerichtsstand. Ausschliesslicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung ist der Sitz des Verantwortlichen.

16.6 Sprache. Massgebend ist die deutsche Fassung dieser Vereinbarung.

Unterschriften

FÜR DEN VERANTWORTLICHEN

Arztpraxis / Institution

ORT, DATUM

NAME (IN DRUCKBUCHSTABEN)

FUNKTION

RECHTSGÜLTIGE UNTERSCHRIFT

FÜR DEN AUFTRAGSBEARBEITER

DeskGate, Inc.

ORT, DATUM

Hans Johannes Schulte

NAME

CEO / Director

FUNKTION

RECHTSGÜLTIGE UNTERSCHRIFT

Anhänge: 1 Technische und organisatorische Massnahmen · 2 Genehmigte Unterauftragsbearbeiter · 3 Datenkategorien und Löschkonzept. Die Anhänge sind integrierende Bestandteile dieser Vereinbarung. Version 2.2 ersetzt alle früheren Fassungen von Schedule CH.

ANHANG 1

Technische und organisatorische Massnahmen

gemäss Art. 8 DSG und Art. 1–4 DSV, für den Einsatz im Schweiz-Modus. Die Gliederung folgt den Schutzzielen von Art. 2 DSV. Massnahmen auf den Arbeitsplatzrechnern des Verantwortlichen regelt § 6.4.

1 Vertraulichkeit (Art. 2 lit. a DSV)

- 1.1 **Physischer Zugang.** Auf Servern des Auftragsbearbeiters werden keine Patientendaten gespeichert. Die Server von deskgate.app werden bei Flow Swiss AG in Rechenzentren in der Schweiz betrieben, deren physische Sicherheit Flow Swiss verantwortet.
- 1.2 **Benutzer- und Sitzungskontrolle.** DeskGate arbeitet ausschliesslich innerhalb der vom Verantwortlichen bereits authentifizierten Browser-Sitzung (z. B. HIN- oder Portal-Sitzung). DeskGate speichert keine Passwörter oder Anmeldetoken für Praxis- oder Kostenträgersysteme.
- 1.3 **Zugriffskontrolle im Browser.** Die Erweiterung ist auf allen Seiten geladen. Sie liest Inhalte nur in dem Tab, in dem die Fachperson einen Vorgang auslöst, einschliesslich seiner Frames, und nur im Rahmen dieses Vorgangs: beim Lesen, beim Vorbefüllen und danach während höchstens 90 Sekunden zur Erkennung der Einreichungsbestätigung des Portals. Ändert die Fachperson ein vorbefülltes Feld, erfasst die Erweiterung nur Länge und Kennzeichen der Änderung, nie den Text. Die Erweiterung greift nicht auf das Dateisystem des Rechners zu und öffnet keine von der Fachperson zum Hochladen gewählten Dateien.
- 1.4 **Zugriffskontrolle im Betrieb.** Administrative Zugriffe auf die Konten des Auftragsbearbeiters bei Flow Swiss und Google Cloud erfolgen nur durch namentlich bezeichnete Personen mit persönlichen Konten, Zwei-Faktor-Authentisierung und minimalen Berechtigungen (Least Privilege). Zugriffe auf die Server von deskgate.app erfolgen nur mit persönlichen kryptografischen Schlüsseln.
- 1.5 **Pseudonymisierung der Nutzungserfassung.** Nach einer Einreichung übermittelt die Erweiterung eine Zählzeile ohne Klardaten (Anhang 3 Ziff. 6). Die Eingangsnummer des Kostenträgers wird noch im Browser mit SHA-256 gehasht:

```
Payload = SHA-256( Eingangsnummer )
```

Aus dem Hashwert lässt sich die Eingangsnummer nicht direkt berechnen. Wer die Eingangsnummer kennt, kann den Hashwert jedoch nachrechnen, und bei kurzen oder strukturierten Nummern ist eine Zuordnung durch systematisches Durchprobieren nicht ausgeschlossen. Es handelt sich deshalb um eine Pseudonymisierung, nicht um eine Anonymisierung. Der Auftragsbearbeiter verwendet den Hashwert nur zur Zählung und zur Erkennung doppelter Einträge und unternimmt keine Zuordnungsversuche (§ 5.3).

2 Verfügbarkeit (Art. 2 lit. b DSV)

- 2.1 **Primärdaten.** DeskGate führt keine Datenbank mit Patientendaten. Datenhaltung, Datensicherung und Aufbewahrung der Krankengeschichte nach den anwendbaren kantonalen Bestimmungen verbleiben vollständig im Primärsystem (KIS bzw. Praxissoftware) des Verantwortlichen.
- 2.2 **Abhängigkeit vom Server.** Ein Ausfall von deskgate.app kann die Nutzung der Erweiterung einschränken, insbesondere die Lizenzprüfung. Patientendaten sind davon nicht betroffen.

3 Integrität (Art. 2 lit. c DSV)

- 3.1 **Transport.** Sämtliche Verbindungen der Erweiterung zu deskgate.app erfolgen verschlüsselt über HTTPS (mindestens TLS 1.2).
- 3.2 **Integrität des Codes.** Auslieferung als signierte CRX-Datei mit gleichbleibendem Signaturschlüssel über den Update-Kanal nach § 2.6; Veröffentlichung von Versionsnummer und SHA-256-Prüfwert jeder Version.

- 3.3 Vorbefüllen und Kontrolle.** Die Erweiterung überschreibt keine Textfelder, die bereits ausgefüllt sind. Sie hebt jedes befüllte Feld kurz hervor, liest es zurück und zeigt im Panel an, welche Felder befüllt wurden und welche Angaben fehlen ([MISS]). Sie setzt keine Häkchen, wählt keine Optionsfelder an und betätigt keine Schaltflächen, insbesondere nicht «Absenden» (§ 6.3).

4 Nachvollziehbarkeit (Art. 2 lit. d DSV)

- 4.1 Administrative Zugriffe.** Administrative Zugriffe erfolgen nur über persönliche Konten (Ziff. 1.4). Die Zugriffsprotokolle der Plattformen Flow Swiss und Google Cloud werden genutzt, soweit die Plattformen sie bereitstellen; Anmeldungen auf den Servern von deskgate.app werden protokolliert.
- 4.2 Nutzungserfassung.** Einreichungen werden pseudonymisiert nach Ziff. 1.5 erfasst; Änderungen der Fachperson an vorbefüllten Feldern nur als Länge und Kennzeichen (Ziff. 1.3).

5 Überprüfung und Organisation (Art. 1 DSV)

- 5.1 Prüfung vor jedem Release.** Vor jedem Release prüft der Auftragsbearbeiter den Code, insbesondere darauf, dass die Erweiterung im Schweiz-Modus keine Verbindungen zu anderen Servern als deskgate.app aufbaut und keine Patientendaten übermittelt.
- 5.2 Überprüfung der Massnahmen.** Die Massnahmen dieses Anhangs werden mindestens jährlich überprüft; das Ergebnis wird dokumentiert (§ 14.2 lit. b).
- 5.3 Organisation.** Geheimhaltungsverpflichtung und Belehrung des Personals (§ 4.3), Zugriffe nach dem Need-to-know-Prinzip und ein dokumentierter Prozess zur Behandlung von Sicherheitsvorfällen (§ 11).

ANHANG 2

Genehmigte Unterauftragsbearbeiter

gemäss Art. 9 Abs. 3 DSGVO und § 8 dieser Vereinbarung

UNTERAUFTRAGSBEARBEITER 1 · SERVER VON DESKGATE.APP · IM EINSATZ

Unternehmen	Flow Swiss AG, Baarermattstrasse 10, 6340 Baar, Schweiz (UID CHE-284.156.502)
Eingesetzter Dienst	Cloud-Infrastruktur für die Server von deskgate.app, einschliesslich des Update-Kanals
Bearbeitungsort	Rechenzentren von Flow Swiss in der Schweiz (§ 9.2)
Zweck	Lizenzprüfung, Nutzungserfassung, Auslieferung von Updates und Vertragsabwicklung
Datenkategorien	Vertrags- und Lizenzdaten, pseudonymisierte Nutzungserfassung und technische Verbindungsdaten (Anhang 3 Ziff. 5–7). Keine Patientendaten.
Speicherung	Gemäss Anhang 3 Ziff. 5–7
Vertragsgrundlage und Garantien	Auftragsbearbeitungsvertrag von Flow Swiss als Bestandteil ihrer Allgemeinen Geschäftsbedingungen, gestützt auf das DSGVO; Speicherung der gehosteten Daten in der Schweiz (§ 9.2)
Weitere Unterauftragsbearbeiter	Unterauftragsbearbeiter von Flow Swiss gemäss Anhang A ihres Auftragsbearbeitungsvertrags (§ 8.6)

UNTERAUFTRAGSBEARBEITER 2 · BILDSCHIRMLESUNG · DERZEIT NICHT IM EINSATZ

Status	Vorab bezeichnet für eine Einführung der Bildschirmlesung nach § 3.2. Derzeit findet keine Bearbeitung von Personendaten des Verantwortlichen statt.
Unternehmen	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
Eingesetzter Dienst	Google Cloud Vertex AI (Gemini-Modelle)
Bearbeitungsort	Region Zürich, Schweiz (europa-west6); Projekt «deskgate-production»; Assured Workloads «Switzerland Data Boundary»
Zweck	Texterkennung aus vom Verantwortlichen ausgewählten Bildausschnitten (§ 3.2)
Datenkategorien	Nach Einführung: Bildausschnitte, die Identifikatoren und klinische Daten enthalten können
Speicherung	Keine; ausschliesslich flüchtige Bearbeitung (§ 3.2 lit. e)
Vertragsgrundlage und Garantien	Google Cloud Data Processing Addendum (CDPA) und Service Specific Terms; Zertifizierung nach dem Swiss-U.S. Data Privacy Framework (§ 9.1); Ausschluss der Nutzung zum Modelltraining (§ 3.3); zusätzlich Google Cloud Platform HIPAA Business Associate Addendum
Weitere Unterauftragsbearbeiter	Unterauftragsbearbeiter von Google gemäss cloud.google.com/terms/subprocessors (§ 8.6)

Im Schweiz-Modus (§ 2.1) erhält kein Unterauftragsbearbeiter Patientendaten.

ANHANG 3

Datenkategorien und Löschkonzept

gemäß § 1.4 und § 15 dieser Vereinbarung, für den Einsatz im Schweiz-Modus

NR.	DATENKATEGORIE	BETROFFENE PERSONEN	BEARBEITUNGSORT	SPEICHERDAUER / LÖSCHUNG
1	Identifikatoren Name, Geburtsdatum, AHV-Nummer, Versichertennummer, Rechnungsnummer	Patientinnen und Patienten	Arbeitsspeicher der Erweiterung (lokal)	Keine persistente Speicherung. Verwerfen bei «Neuer Fall», Schliessen des Panels oder Sitzungsende (§ 2.4).
2	Klinische Daten Diagnosen, Befunde, Konsultationsdauer, TARDOC-Positionen, Freitexte	Patientinnen und Patienten	Arbeitsspeicher der Erweiterung (lokal)	Wie Ziff. 1.
3	Angaben zum Leistungserbringer aus Dokumenten Name der Ärztin oder des Arztes, GLN, ZSR-Nummer	Leistungserbringer	Arbeitsspeicher der Erweiterung (lokal)	Wie Ziff. 1.
4	Einstellungen Desk-Code, Zugangsschlüssel, Server-Adresse, Modusschalter, Angaben zur Pilotorganisation (Bezeichnung, verantwortliche Person, Anzahl Bearbeitende, Ausgangswert), Checkliste	Praxispersonal, Ansprechpersonen	Lokaler Speicher der Erweiterung	Bis zur Änderung oder Leerung im Konfigurationsmenü oder zur Deinstallation.
5	Vertrags- und Lizenzdaten Firma, Ansprechperson, E-Mail-Adresse, Desk-Code, Rechnungsdaten	Vertragspartner, Ansprechpersonen	Server deskgate.app bei Flow Swiss, Schweiz (§ 9.2)	Vertragsdauer; danach Löschung innert 12 Monaten, soweit keine gesetzliche Aufbewahrungspflicht für Geschäftsunterlagen besteht.
6	Nutzungserfassung Desk-Code, Lane, Hostname des Kostenträgerportals, zufällige Fall-ID, Build, Statuskennzeichen (vorbefüllt, geändert, eingereicht, abgebrochen), SHA-256-Wert der Eingangsnummer, Bearbeitungsminuten, Zähler (z. B. fehlende oder von Hand ergänzte Felder)	Leistungserbringer, Praxispersonal; Fälle nur pseudonymisiert (Anhang 1 Ziff. 1.5)	Server deskgate.app bei Flow Swiss, Schweiz (§ 9.2)	Vertragsdauer zuzüglich 12 Monate, danach Löschung. Abrechnungsrelevante Summenwerte ohne Hashwerte nach den gesetzlichen Aufbewahrungsfristen.
7	Technische Verbindungsdaten IP-Adresse, Zeitpunkt, aufgerufene Schnittstelle, Hostname des Kostenträgerportals bei der Lizenzprüfung	Praxispersonal	Server deskgate.app bei Flow Swiss, Schweiz (§ 9.2)	Höchstens 30 Tage, danach Löschung; keine weitergehende Auswertung.

Daten nach Ziff. 5 bearbeitet der Auftragsbearbeiter für die eigene Vertragsabwicklung als Verantwortlicher; sie sind hier zur Vollständigkeit aufgeführt. Daten nach Ziff. 6 und 7 können trotz Pseudonymisierung Personendaten der Leistungserbringer und ihres Personals sein und werden entsprechend geschützt.