



Vertrag

zur Auftragsbearbeitung gemäss Art. 10a DSG bzw. Art. 9 revDSG

zwischen

VITODATA-KUNDE

nachfolgend Auftraggeber

und

AUFTRAGSBEARBEITER

Vitodata AG
Deisrütistrasse 10
8472 Seuzach

nachfolgend Auftragnehmer

Der Auftragsbearbeiter verpflichtet sich, die im Folgenden beschriebenen Datenverarbeitungen im Sinne von Art. 5 lit. d rev DSG und Art. 9 revDSG bzw. Art. 10a DSG im Auftrag des Auftraggebers zu erbringen. Für die Zwecke dieses Vertrages gelten die Begriffsbestimmungen des Bundesgesetzes über den Datenschutz.

Stand: Juni 2022



1 Gegenstand und Dauer der Vereinbarung

1.1 Gegenstand des Vertrages

Der Gegenstand des Auftrags ergibt sich aus den Wartungsverträgen und den allgemeinen Vertragsbedingungen des Auftragsbearbeiters (im Folgenden Leistungsvereinbarung), welche mit dem Auftraggeber vereinbart sind.

1.2 Dauer der Vereinbarung

Die Dauer dieses Auftragsdatenbearbeitungsvertrages (im Folgenden ADV) entspricht der Laufzeit der Leistungsvereinbarung. Mit Kündigung der Leistungsvereinbarung erlischt gleichzeitig auch dieser Vertrag zur Auftragsdatenverarbeitung.

2 Konkretisierung des Auftragsinhalts

2.1 Verarbeitungszwecke

Die Einzelheiten der Bearbeitungstätigkeiten, insbesondere die Art und der Zweck der Bearbeitung von Personendaten, sind in der Leistungsvereinbarung beschrieben.

2.2 Ort der Durchführung der Datenverarbeitung

Die Erbringung der vertraglich vereinbarten Datenbearbeitung findet in der Schweiz statt.

2.3 Art der Daten/Betroffene Personengruppen

Die Art der Daten wird über die Module und gemäss Leistungsvereinbarung definiert:

Leistungsvereinbarung	Beschreibung	Personengruppen
Grundmodul vitomed (Softwarewartungsvertrag)	Personenstammdaten, Kommunikationsdaten, Kundenhistorie, medizinische Berichte und Korrespondenz, Arbeitsunfähigkeitszeugnisse, Bestellungen, Terminverwaltung	Patienten, Garanten, Lieferanten, Mitarbeiter, Dritte Dienstleistungserbringer
Patientendossier vitocase (Softwarewartungsvertrag)	Anamnesedaten, Problem-/ Diagnoseliste, Konsultationen-/Verlauf, Impfungen, Medikation, Objektive Befunde, Status, Messergebnisse Biologische Daten (Bspw. Blut, Urin etc.), Röntgenbilder, Ultraschallbilder	Patienten
Abrechnung vitomed (Softwarewartungsvertrag)	Fakturierung Patienten, Zahlungen, Buchhaltungsdaten	Patienten, Garanten
Schnittstellen	Keine zusätzliche Datenhaltung	Patienten, Garanten, Lieferanten, Mitarbeiter, Dritte Dienstleistungserbringer
Hosting (ITaaS) Online-Datensicherung (vitoManaged Backup)	Zusätzliche zu den obigen Datenkategorien: Geschäftsdaten der Praxis z.B. E-Mail, Rechnungen, Mitarbeiter, Lohn, usw.	Lieferanten, Mitarbeiter, Partner

2.4 Kategorien von Datenbearbeitung in Entsprechung von Art. 5 lit. d revDSG

Die übermittelten personenbezogenen Daten werden abhängig der Leistungsvereinbarung folgenden grundlegenden Verarbeitungsmassnahmen unterzogen:

Art der Bearbeitung	Leistungsvereinbarung
Erheben, Beschaffen	–
Erfassen	–
Organisieren	Hosting (ITaaS), Online-Datensicherung (vitoManaged Backup)
Ordnen	Hosting (ITaaS), Online-Datensicherung (vitoManaged Backup)
Speichern, Aufbewahren, Archivieren	Hosting (ITaaS), Online-Datensicherung (vitoManaged Backup)
Anpassen, Verändern	–
Auslesen (Einsicht)	Softwarewartungsvertrag Hosting (ITaaS), Online-Datensicherung (vitoManaged Backup)
Abfragen	Hosting (ITaaS), Online-Datensicherung (vitoManaged Backup)
Verwenden	–
Übermitteln, Bekanntgeben	–
Verbreiten oder eine andere Form des Bereitstellens	–
Abgleichen, Verknüpfen	–
Einschränken	–
Löschen	–
Vernichten	–

3 Technische und organisatorische Massnahmen

- Der Auftragsbearbeiter ergreift alle erforderlichen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 7 DSG bzw. Art. 7 und 8 revDSG. Die Massnahmen gewährleisten ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Art und der Umfang der Datenbearbeitung sowie das Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt im Sinne von Art. 7 Abs. 2 revDSG zu berücksichtigen.
- Die erforderlichen technischen und organisatorischen Massnahmen sind im Anhang zu diesem Vertrag dokumentiert. Wesentliche Änderungen sind ebenfalls umgehend zu dokumentieren.
- Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden.
- Soweit die getroffenen Sicherheitsmassnahmen den Anforderungen des Verantwortlichen nicht oder nicht mehr genügen, benachrichtigt Letzterer den Auftragsbearbeiter.

4 Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Bearbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5 Pflichten des Auftragnehmers

Der Auftragnehmer gewährleistet insbesondere aufgrund der gesetzlichen Pflichten des DSG die Einhaltung folgender Vorgaben:

- a) Gemäss Art. 10 revDSG hat der Auftragnehmer einen Datenschutzberater bestellt. Sofern der Auftragnehmer keinen Datenschutzberater bzw. Datenschutzbeauftragten bestellt hat, ist eine andere Person als Ansprechpartner für den Datenschutz bzw. diesen Vertrag ernannt. In beiden Fällen ist der Datenschutzberater resp. Ansprechpartner über die E-Mail-Adresse datenschutz@vitodata.ch oder über die Hauptnummer 52 320 55 55 erreichbar.
- b) Der Auftragnehmer verpflichtet sich sämtliche vertraulichen Informationen, Unterlagen etc., die er im Rahmen des Abschlusses und der Abwicklung der Leistungsvereinbarung erhält oder sonst wie wahrnimmt, geheim zu halten und Dritten weder direkt noch indirekt zugänglich zu machen. Diese Verpflichtung gilt unbeschränkt, auch nach Auflösung der Leistungsvereinbarung.
- c) Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu Personendaten hat, dürfen diese Daten ausschliesslich entsprechend der Weisung des Auftraggebers verarbeiten einschliesslich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Bearbeitung verpflichtet sind.
- d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Massnahmen gemäss Art. 7 DSG bzw. Art. 7 und 8 revDSG [Einzelheiten in Anhang 1].
- e) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit dem EDÖB bzw. der zuständigen Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- f) Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Massnahmen des EDÖB bzw. der Aufsichtsbehörde informieren, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Gerichtsverfahrens in Bezug auf die Bearbeitung von Personendaten bei der Auftragsbearbeitung beim Auftragnehmer ermittelt.
- g) Soweit der Auftraggeber seinerseits einer Kontrolle des EDÖB bzw. der Aufsichtsbehörde, einem Gerichtsverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsbearbeitung beim Auftragnehmer ausgesetzt ist, wird ihn der Auftragnehmer nach besten Kräften unterstützen.
- h) Der Auftragnehmer kontrolliert regelmässig die internen Prozesse sowie die technischen und organisatorischen Massnahmen, um zu gewährleisten, dass die Bearbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.



- i) Der Auftragnehmer stellt die Nachweisbarkeit der getroffenen technischen und organisatorischen Massnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages sicher.
- j) Der Auftragnehmer verpflichtet sich, den Auftraggeber angemessen bei der Erfüllung der Betroffenenrechte und dem allfälligen Recht auf Datenportabilität zu unterstützen.

6 Unterauftragsbearbeiter

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmassnahmen zu ergreifen.

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu:

Unterauftragnehmer	Dienstleistung	Kontaktangabe/Land
Wortmann	Onsite Hardware Garantieleistungen	Schweiz
VADIAN.NET AG	SMS-Versand	Schweiz

Ein Wechsel der bestehenden Unterauftragnehmer oder das Zuziehen eines neuen Unterauftragnehmers ist zulässig, soweit

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab per E-Mail anzeigt;
- eine vertragliche Vereinbarung nach Massgabe des DSG (sog. Auftragsbearbeitungsvertrag) zugrunde gelegt wird und
- im Falle der Übermittlung in ein Land, welches nicht über einen angemessenen Datenschutz verfügt, zusätzlich die besonderen Garantien des DSG (Kapitel 2.2) erfüllt sind.

Der Auftraggeber hat die Möglichkeit, diesen Änderungen aus wichtigen Gründen innerhalb von 14 Tagen ab Erhalt der Mitteilung zu widersprechen. In diesem Fall hat er das Recht, die Leistungsvereinbarung sowie die vorliegende Vereinbarung mit einer Kündigungsfrist von 4 Wochen zum Quartalsende zu kündigen.

Kündigt der Auftraggeber die Leistungsvereinbarung nicht, dann gilt dies als Rückzug seines Widerspruchs und der Auftragnehmer ist berechtigt, die vertraglich vereinbarten Leistungen mit dem neuen bzw. dem gewechselten Unterauftragnehmer zu erbringen.



7 Rechte und Pflichten des Auftraggebers

Der Auftraggeber ist berechtigt,

- a) die Einhaltung der vom Auftragnehmer getroffenen technischen und organisatorischen Massnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu kontrollieren. Der Nachweis solcher Massnahmen erfolgt in der Regel dadurch, dass der Auftragnehmer dem Auftraggeber eine Kopie des aktuellen Zertifikats zur Qualitätssicherung zustellt resp. dieses auf der Webseite des Auditors zur Verfügung stellt.
- b) Der Auftraggeber hat zudem das Recht, in Absprache mit dem Auftragnehmer zusätzliche Überprüfungen in dessen Geschäftsbetrieb durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.
- c) Kontrollen beim Auftragnehmer erfolgen ohne vermeidbare Störungen seines Geschäftsbetriebs und ausser bei dringlichen Gründen nach angemessener Vorankündigung und während der Geschäftszeiten des Auftragnehmers.

Der Auftraggeber ist verpflichtet,

- d) sicherzustellen, dass die Rechtmässigkeit der Verarbeitung gegeben ist;
- e) zu gewährleisten, dass die Rechte der betroffenen Personen gewahrt werden. Wenn allerdings nur der Auftragnehmer die Kompetenz hat, den Anfragen nachzukommen, leitet der Auftraggeber ihm die betreffenden Anfragen umgehend weiter;
- f) dem Auftragnehmer Aufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format zu übermitteln. Mündliche Weisungen sind schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen;
- g) den Auftragnehmer unverzüglich über Fehler oder Unregelmässigkeiten bei der Prüfung der Auftragsergebnisse zu informieren;
- h) alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmassnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

8 Mitteilung bei Verstössen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung seiner Pflichten zur Sicherheit von Personendaten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u. a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Massnahmen, die die Umstände und Zwecke der Bearbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- b) die Verpflichtung, Verletzungen von Personendaten (Datensicherheits- oder Informationssicherheitsvorfälle) unverzüglich an den Auftraggeber zu melden
- c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen sowie den zuständigen Behörden zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen



- d) die Unterstützung des Auftraggebers bei der Durchführung einer Datenschutz-Folgenabschätzung, soweit sie sich auf den Gegenstand der Leistungsvereinbarung bezieht
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit dem EDÖB oder mit der Aufsichtsbehörde

Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung oder im vorliegenden ADV enthalten sind, kann der Auftragnehmer eine Vergütung beanspruchen, sofern sie nicht auf ein Fehlverhalten vom Auftragnehmer zurückzuführen sind.

9 Weisungsbefugnis des Auftraggebers

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mindestens in Textform wie beispielsweise per E-Mail).

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstosse gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10 Löschung und Rückgabe von Personendaten

Der Auftragnehmer ist nach Beendigung der Auftragsbearbeitung verpflichtet, alle Verarbeitungsergebnisse und übermittelten personenbezogenen Daten und deren Kopien, dem Auftraggeber zurückzugeben bzw. in dessen Auftrag zu vernichten, sofern nicht gesetzlich eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

Die Löschung erfolgt innerhalb von 3 Monaten nach Beendigung der Auftragsbearbeitung. Von der Löschung ausgenommen sind Backups auf Langzeitspeichermedien. Auf diese Backups ist kein operativer Zugriff ohne vorangegangenes Zurücklesen möglich und wird ein Backup zurückgelesen, werden Daten einer beendeten Auftragsbearbeitung explizit ausgenommen.

Der Auftragnehmer wird die Daten in demjenigen technischen Format übergeben, in welchem dieser es verarbeitet. In der Regel ist dies ein Dump aus der Datenbank z. B. MS SQL-Server Dump und/oder Files aus Fileshare.

11 Anhang – Technisch-organisatorische Massnahmen

11.1 Zutrittskontrolle

Massnahmen zur Verhinderung von Zutritten Unberechtigter zu Datenverarbeitungsanlagen.

- DV-Anlagen befinden sich in Sicherheitsbereichen mit eingeschränktem Zugang
- Es ist gewährleistet, dass keine betriebsfremden Personen Zutritt zu den DV-Anlagen haben
- Alarmsystem
- Sicherheitsschlösser und Schlüsselverwaltung
- Überwachungseinrichtungen, (Video/CCTV-Monitor, Alarmanlage etc.)

11.2 Zugangskontrolle

Massnahmen zur Verhinderung von unbefugtem Zugang zu Datenverarbeitungsanlagen.

- Benutzerautorisierung und -authentifizierung
- automatische Sperrung (z. B. Bildschirmsperre bei Auszeiten und Aufforderung zur Eingabe des Passworts)
- Einsatz von Anti-Viren-Software
- Einsatz von Firewall
- Einsatz von VPN-Technologien
- Berechtigungskonzept und Verwaltung der Benutzerberechtigungen durch Administratoren
- Sicherheitsmassnahmen hinsichtlich Nutzer-IDs/Passwörtern (z.B. Sonderzeichen, Mindestlänge, Pflicht zur Änderung von Passwörtern)

11.3 Zugriffskontrolle

Berechtigte dürfen ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

- Erstellen von Benutzerprofilen
- Verschlüsselter Zugriff (z. B. https, SSL etc.)
- Verfahren zur Sicherstellung für die Vernichtung von gebrauchten Medien
- Fernwartungen der IT-Systeme sind gesichert (Verschlüsselung etc.)
- Interne Richtlinien und Verfahren

11.4 Trennungskontrolle

Zu unterschiedlichen Zwecken erhobene Personendaten müssen getrennt verarbeitet werden können.

- Trennung von aktiven und Testdaten
- Die für die Verarbeitung genutzten IT-Systeme sind mandantenfähig und werden entsprechend betrieben
- Berechtigungskonzept

11.5 Weitergabekontrolle

Massnahmen, die gewährleisten, dass Daten nicht unbefugt gelesen, kopiert, verteilt, verändert oder entfernt werden können.

- Verschlüsselte Übertragungswege (SSL, HTTPS, SFTP etc.)
- Einrichtung von VPN-Tunneln
- Verschlüsselung von E-Mail (HIN)
- IPS / IDS (Systems zur Erkennung/ Verhinderung von Einbrüchen)



11.6 Eingabekontrolle

Massnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem die Daten eingegeben, geändert oder gelöscht worden sind.

- Protokollierung von Eingaben, Änderungen und Löschungen
- Jeder Benutzer hat ein personalisiertes Konto
- Die Verwaltung von Nutzerkonten und Zugriffsberechtigungen ist organisiert und dokumentiert

11.7 Auftragskontrolle

Massnahmen, die gewährleisten, dass personenbezogene Daten nur entsprechend den Weisungen des Datenverantwortlichen verarbeitet werden.

- Sorgfältige Auswahl und Instruktion des Auftragnehmers
- Definierte Prozesse für die Beauftragung von Vertragspartnern
- Auftragnehmer ist weisungsgebunden

11.8 Verfügbarkeitskontrolle

Massnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust (physisch und logisch) geschützt werden.

- Unterbrechungsfreie Stromversorgung
- Schutz gegen Feuer, Rauch, Überflutungen, Feuchtigkeit etc.
- Backups
- Backupkonzept
- Notfall-/Notfallwiederherstellungsplan

11.9 Datenschutz-Management

Massnahmen die ein effektives Datenschutzmanagement gewährleisten.

- Zugriff der Mitarbeiter auf interne Regelungen betr. Datenschutz (z.B. Intranet)
- Überprüfung der Wirksamkeit der Technischen Schutzmassnahmen
- Datenschutzberater (intern und extern)
- Schulung der Mitarbeiter auf: Vertraulichkeit, Geheimhaltung, Datenschutz
- Sensibilisierung der Mitarbeiter
- Durchführung Datenschutzfolgenabschätzung (DSFA)
- Organisation kommt Informationspflichten nach
- Prozess zur Bearbeitung von Auskunftsanfragen der Betroffenen
- Incident-Response-Management
- Erhebung von Personendaten nur sofern für Zweck erforderlich

11.10 Weitere Massnahmen

- Jeder Mitarbeiter hat eine Geheimhaltungserklärung mit Hinweis auf Art. 321 StGB unterzeichnet (besonderer Schutz des ärztlichen Berufsgeheimnisses)