HCI solutions

Deutsch

Français

Italiano

English

September 2023

Auftragsdatenbearbeitungsvereinbarung

Vorbemerkungen

Die vorliegende Vereinbarung konkretisiert die Verpflichtungen der Auftraggeber und der Auftragsbearbeiter (die **Parteien**) in Bezug auf die Vorgaben aus dem Schweizer Datenschutzgesetz (DSG) und der Datenschutzgrundverordnung der EU (EU-DSGVO). Sie ergänzt diesbezüglich die vertraglichen Vereinbarungen zwischen HCI Solutions (Auftragsbearbeiter) und dem Kunden (Auftraggeber). Es kann sich dabei um einen einzelnen oder mehrere Verträge zwischen HCI Solutions und dem Kunden handeln. Genaue Details zu den "Verträgen" sind aus dem "Anhang" zu entnehmen.

Im Rahmen der Dienstleistungen stellt der Auftraggeber dem Auftragsbearbeiter Personendaten zur Bearbeitung im Auftrag zur Verfügung, er erhebt Personendaten im Auftrag vom Auftraggeber oder der Auftragsbearbeiter hat bei der Ausführung seines Auftrags Zugang zu Personendaten, für die der Auftraggeber verantwortlich ist. Um dabei die Einhaltung der Anforderungen des Schweizer Datenschutzgesetzes (DSG) wie auch der europäischen Datenschutzverordnung (EU-DSGVO) sicherzustellen, schliessen die Parteien die vorliegende Auftragsdatenbearbeitungsvereinbarung (die **Vereinbarung**).

1. Vertragsgegenstand

(a) Gegenstand: Die Parteien regeln in der Vereinbarung nur das datenschutzrechtliche Auftragsbearbeitungsverhältnis. Sie beabsichtigen nicht, den in der Leistungsvereinbarung vereinbarten Leistungskatalog auszuweiten oder einzuschränken.

(b) Konfliktregelungen: Bei Widersprüchen zwischen Vertragsbestimmungen gilt die folgende Reihenfolge: Die Anhänge dieser Vereinbarung gehen der Vereinbarung vor, und diese Vereinbarung geht insgesamt der Leistungsvereinbarung vor. Soweit die Parteien für eine Dienstleistung eine anderweitige Auftragsbearbeitungsvereinbarung schliessen oder geschlossen haben, gelten jeweils die strengeren Anforderungen.

(c) Definitionen: Fettgedruckte Begriffe werden in dieser Vereinbarung jeweils mit der ihnen zugewiesenen Bedeutung verwendet. Rechtsbegriffe wie „Personendaten“, „Bearbeitung“ usw. haben die im anwendbaren Datenschutzrecht festgelegte Bedeutung.

2. Gegenstand und Dauer der Auftragsbearbeitung

(a) Auftragsbearbeitung: Der Auftragsbearbeiter bearbeitet im Zusammenhang mit den Dienstleistungen Personendaten inklusive «Besonders Schützenswerte Daten» im Auftrag des Auftraggebers (gesamthaft **Auftragsdaten**). Der Gegenstand der Auftragsbearbeitung, ihre Art und ihr Zweck ergeben sich aus der Leistungsvereinbarung. Die Kategorien der von der Auftragsbearbeitung betroffenen Personen und die Kategorien der betroffenen Personendaten werden in Anhang 1 beschrieben.

(b) Weitere Dienstleistungen: Soweit der Auftragsbearbeiter im Lauf der weiteren Zusammenarbeit weitere Dienstleistungen für den Auftraggeber übernimmt, gilt diese Vereinbarung auch für diese Dienstleistungen.

(c) Dauer: Diese Vereinbarung beginnt mit ihrer Unterzeichnung oder, falls später, mit dem Inkrafttreten der Leistungsvereinbarung, spätestens aber mit dem ersten Zugriff des Auftragsbearbeiters auf Auftragsdaten. Sie endet mit Beendigung der Leistungsvereinbarung, frühestens aber mit der Löschung sämtlicher im Auftrag des Auftraggebers bearbeiteten Auftragsdaten.

(d) Stellung des Auftraggebers: Der Auftraggeber ist sich bewusst, dass die gesetzliche Verantwortung für die Zulässigkeit der Erhebung und Bearbeitung der Auftragsdaten und für die Erfüllung der Betroffenenrechte im Zusammenhang mit den Dienstleistungen bei ihm liegt.

3. Pflichten des Auftragsbearbeiters

(a) Befolgung von Weisungen:

(i) Der Auftragsbearbeiter ist verpflichtet, die Auftragsdaten ausschliesslich für die Dienstleistungen zu verwenden und bei ihrer Bearbeitung den Weisungen des Auftraggebers zu folgen. Vorbehalten sind abweichende Pflichten des anwendbaren Rechts (z.B. verbindliche Anordnungen zuständiger Behörden).

(ii) Das Weisungsrecht wird durch die Leistungsvereinbarung und durch diese Vereinbarung beschränkt. Die Weisungen sind in Textform zu erteilen. Der Auftraggeber ist verpflichtet, alle Weisungen angemessen zu dokumentieren.

(b) Ort der Datenbearbeitung. Grundsätzlich findet die Datenbearbeitung in der Schweiz statt. Jedwede Bekanntgabe von relevanten Daten durch HCI Solutions ins Ausland oder an eine internationale Organisation ist nur zulässig, wenn HCI Solutions die Bestimmungen von Art. 16 ff. DSG bzw. von Kapitel V EU-DSGVO einhält. Soweit hingegen eine solche Bekanntgabe von relevanten Daten vom Kunden gewünscht bzw. in seinem Auftrag erfolgt, obliegt die Einhaltung der entsprechenden Bestimmungen ausschliesslich dem Kunden.

(c) Rückgabe- und Löschpflicht: Auftragsdaten sind nach Vertragsende gemäss den vertraglichen Bestimmungen oder gemäss den Weisungen des Auftraggebers herauszugeben oder zu löschen. Der Auftragsbearbeiter setzt für die Löschung von Auftragsdaten branchenübliche Verfahren ein.

4. Unterstützungspflichten

(a) Datensicherheit: Der Auftragsbearbeiter unterstützt den Auftraggeber in angemessener Weise bei der Einhaltung seiner gesetzlichen Pflichten zur Gewährleistung einer angemessenen Datensicherheit und zur Meldung von Datenschutzverletzungen und bei der freiwilligen oder zwingenden Durchführung von Datenschutz-Folgenabschätzungen. Für Datenschutzverletzungen gilt Ziff. 5(b).

(b) Betroffenenrechte: Soweit sich eine betroffene Person im Zusammenhang mit datenschutzrechtlichen Ansprüchen (z.B. mit einem Auskunfts- oder Löschbegehren) an den Auftragsbearbeiter wendet, leitet der Auftragsbearbeiter das entsprechende Begehren unverzüglich dem Auftraggeber weiter. Er unterstützt den Auftraggeber angemessen bei der Bearbeitung solcher Begehren, ebenso wie bei Auskunftspflichten gegenüber von Behörden. Dazu gehört bei Bedarf die Unterstützung bei der Zusammenstellung der erforderlichen Daten und Informationen.

(c) Kontakt: Für datenschutzrechtliche Themen sind in erster Linie folgende Personen zu kontaktieren:

(i) **Auftraggeber**: Kontaktperson ersichtlich im Vertrag zwischen Auftraggeber und der HCI Solutions.

(ii) **Auftragsbearbeiter**: HCI Solutions AG, Untermattweg 8, Postfach, 3000 Bern 1
E-Mail: dataprotection@hcisolutions.ch, Telefon: +41 58 851 26 00

5. Datensicherheit

(a) Sicherheitsmassnahmen: Der Auftragsbearbeiter ergreift angemessene, in jedem Fall aber mindestens die in Anhang 2 umschriebenen technischen und organisatorischen Massnahmen zum Schutz der Auftragsdaten (**Sicherheitsmassnahmen**). Der Auftragsbearbeiter ist während der Dauer der Vereinbarung berechtigt, die Sicherheitsmassnahmen anzupassen, sofern dabei das Sicherheitsniveau nicht abgesenkt wird.

(b) Meldung von Verletzungen:

(i) Bei konkret vermuteten und bei festgestellten Sicherheitsverletzungen, die – ob rechts-, vertrags- oder weisungswidrig oder unbeabsichtigt – zur Vernichtung, zum Verlust, zur Veränderung oder zur Offenlegung von Personendaten führen, informiert der Auftragsbearbeiter den Auftraggeber so rasch als möglich und unter Angabe wenigstens der folgenden Informationen (wobei diese gestaffelt übermittelt werden können, wenn sie nicht sofort bekannt sind):

- eine Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und ungefähren Zahl der betroffenen Personen und der betroffenen Kategorien und ungefähren Zahl der betroffenen Datensätze und bei einer Offenlegung an unberechtigte Personen die betreffenden Personen oder Personenkreise

- Name und Kontaktdaten einer sonstigen Anlaufstelle des Auftragsbearbeiters für weitere Informationen;

- die wahrscheinlichen Folgen der Verletzung;

- die ergriffenen oder erwogenen Massnahmen zur Behebung der Verletzung bzw. die Behebung oder Mitigierung ihrer Folgen.

(ii) Der Auftragsbearbeiter ist verpflichtet, dem Auftraggeber auf Anfrage weitere sachdienliche Auskünfte zur Sicherheitsverletzung zu erteilen, soweit dies ohne Verletzung seiner vertraglichen und gesetzlichen Geheimhaltungspflichten möglich ist.

6. Unterauftragnehmer

(a) Zulässigkeit:

(i) Für die Erbringung der Dienstleistungen ist der Auftragsbearbeiter befugt, Unterauftragnehmern Auftragsdaten zur Verfügung zu stellen, sofern der Auftragsbearbeiter die Bestimmungen dieser Vereinbarung und insbesondere dieser Ziff. 6 einhält und mit dem Unterauftragnehmer eine Vereinbarung getroffen hat, die inhaltlich im Wesentlichen der vorliegenden Vereinbarung entspricht.

(ii) Als **Unterauftragnehmer** in diesem Sinne gilt jeder Dienstleister, dessen Leistungen sich unmittelbar auf die Bearbeitung von Auftragsdaten beziehen. Keine Unterauftragnehmer sind Anbieter von Nebenleistungen wie z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartungsleistungen oder der Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch auch bei ausgelagerten Nebenleistungen verpflichtet, angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen.

(b) Genehmigung:

(i) Eine Liste der bei Vertragsbeginn bestehenden und hiermit genehmigten Unterauftragnehmer mit Zugriff auf Auftragsdaten findet sich in Anhang 3. Der Auftragsbearbeiter informiert den Auftraggeber über beabsichtigte Änderungen der Unterauftragsnehmerverhältnisse innerhalb eines Monats. Nach der Benachrichtigung durch den Auftragsbearbeiter, kann der Auftraggeber Einspruch erheben, wenn wichtige datenschutzrechtliche Gründe gegen den Beizug des betroffenen Unterauftragnehmers sprechen. Der Einspruch durch den Auftraggeber muss schriftlich erfolgen und die Gründe für den Einspruch beinhalten.

(ii) Der Auftragsbearbeiter darf einen Unterauftragnehmer nur dann mit der Durchführung bestimmter Bearbeitungstätigkeiten beauftragen, wenn:

- Der Auftragsbearbeiter alle angemessenen und erforderlichen Überprüfungen und Bewertungen durchgeführt und sich von der Zuverlässigkeit und Fähigkeit des Unterauftragnehmers dahingehend überzeugt hat:

  (i) dass dieser das in den Datenschutzgesetzen geforderte Schutzniveau für Personendaten gewährleistet und

(ii) die Verpflichtungen des Auftragsbearbeiters gemäss diesem Vertrag erfüllt;

- der Auftragsbearbeiter dem Unterauftragnehmer durch einen Vertrag dieselben Verpflichtungen auferlegt, wie sie in diesem Vertrag festgelegt sind, und insbesondere ausreichende Garantien dafür bietet, dass geeignete technische und organisatorische Massnahmen getroffen werden;

- der Unterauftragnehmer seine Auftragsbearbeitungstätigkeiten beendet, sobald dieser Vertrag endet, und

(c) Dokumentation: Auf Anfrage übermittelt der Auftragsbearbeiter dem Auftraggeber eine Kopie seiner Vereinbarung(en) mit Unterauftragnehmern (ggf. einschliesslich der geeigneten Garantien), damit der Auftraggeber die Einhaltung dieser Vereinbarung durch den Auftragsbearbeiter prüfen kann. Dafür nicht relevante Teile der Vereinbarungen können geschwärzt werden.

(d) Haftung: Der Auftragsbearbeiter haftet dem Auftraggeber für die Einhaltung der Pflichten der Unterauftragnehmer.

7. Prüfrechte

(a) Prüfrecht: Der Auftragsbearbeiter ist verpflichtet, dem Auftraggeber auf Verlangen Informationen zur Verfügung zu stellen, um die Einhaltung der vereinbarten Pflichten zu dokumentieren. Der Auftraggeber hat das Recht, die Einhaltung der Pflichten gemäss dieser Vereinbarung durch den Auftragsbearbeiter zu prüfen. Der Auftragsbearbeiter ist verpflichtet, bei Prüfungen jeweils angemessen mitzuwirken. Der Auftraggeber nimmt bei der Planung und Durchführung der Prüfung Rücksicht auf die Bedürfnisse und Sicherheitsanforderungen des Auftragsbearbeiters und hat Vertraulichkeitspflichten des Auftragsbearbeiters zu respektieren. Für die im Rahmen der Prüfung wahrgenommenen Tatsachen gilt Ziff. 8(b).

(b) Externe Prüfstelle: Der Auftraggeber hat das Recht, die Prüfung nach Ziff. 7 durch eine externe, fachkundige und zur Vertraulichkeit verpflichtete Stelle durchführen zu lassen. Die beim Auftraggeber anfallenden Kosten der Prüfung trägt der Auftraggeber selbst.

8. Vertraulichkeit

(a) Auftragsdaten: Der Auftragsbearbeiter verpflichtet sich, Auftragsdaten strikt vertraulich zu behandeln und innerhalb seiner Organisation nur Personen zugänglich zu machen, die für die Erfüllung ihrer Pflichten auf Zugang zu den Auftragsdaten angewiesen sind. Er stellt sicher, dass alle Personen mit Zugang zu Auftragsdaten mit Bezug auf diese einer gesetzlichen oder vertraglichen Vertraulichkeitspflicht unterstehen.

(b) Sonstige Informationen: Beide Parteien unterstehen zudem mit Bezug auf im Rahmen dieser Vereinbarung wahrgenommene Tatsachen den auf sie anwendbaren gesetzlichen und zwischen ihnen in der Leistungsvereinbarung vereinbarten Vertraulichkeitspflichten.

9. Schlussbestimmungen

(a) Haftung: Für die Haftung aus Verletzungen dieser Vereinbarung gelten die für die Dienstleistungen vereinbarten oder von Gesetzes wegen geltenden Haftungsregelungen.

(b) Mitteilungen: In dieser Vereinbarung vorgesehene Mitteilungen müssen jeweils ausdrücklich und in Textform (z.B. per E-Mail oder Post) erfolgen, sofern nichts anderes vereinbart ist.

(c) Änderungen und Ergänzungen: Abweichend allfälliger Schriftformvorbehalte im Vertrag kann die vorliegende Vereinbarung auch auf elektronischem Weg zwischen den Parteien vereinbart oder geändert werden.

(d) Streitschlichtung: Das anwendbare Recht und der Gerichtsstand richten sich nach der Leistungsvereinbarung. Der Auftraggeber bleibt aber berechtigt, vor jedem zuständigen Gericht vorsorgliche Massnahmen zu verlangen und seine Ansprüche gegen den Auftragsbearbeiter im Fall einer Inanspruchnahme durch einen Dritten vor dem Gericht der Hauptklage geltend zu machen.

Anhang 1: Konkretisierung der ADV

Leistung	Kategorien von Personendaten	Betroffene Personen
Compendium.ch	Inkluiert: eMediplan, Documedis CDS.CE, Documedis PCA.CE und Documedis Vac	Patient:innen
Documedis eMediplan	Pflicht: Name, Vorname und Geburtsdatum Optional: Weitere Personalien und Gesundheitsinformationen	Patient:innen
Documedis eRezept	Pflicht: Name, Vorname, Geburtsdatum, Adresse und Medikation des Patienten Optional: Weitere Personalien	Patient:innen
Documedis CDS.CE	Pflicht: Medikation des Patienten Optional: Weitere Daten des Patienten (Personalien und Gesundheitsinformationen), abhängig vom Check, welcher durchgeführt werden möchte. Datenlogs: Um die Sicherheit des Patienten gewährleisten zu können, werden anonymisierte Daten gemäss Medizinprodukteverordnung (MepV) gefordert.	Patient:innen
Documedis PCA.CE	Pflicht: Name, Vorname und Geburtsdatum Optional: Weitere Daten des Patienten (Personalien, Gesundheitsinformationen und Medikation des Patienten). Datenlogs: Um die Sicherheit des Patienten gewährleisten zu können, werden anonymisierte Daten verwendet gemäss Medizinprodukteverordnung (MepV) gefordert.	Patient:innen
pharmaVISTA	Inkluiert: eMediplan, Documedis CDS.CE, Documedis PCA.CE, Einlösung Documedis eRezept und PMC Polymedications Check	Patient:innen
PMC Polymedications Check	Pflicht: Name, Vorname und Geburtsdatum Optional: Medikation des Patienten und weitere Personalien	Patient:innen
VAC Impferfassung / Dokumentation	Pflicht: Name, Vorname, und Geburtsdatum Optional: Impfungen des Patienten, Beantwortung der Fragen bezüglich des Gesundheitszustandes und weitere Personalien	Patient:innen

Anhang 2: Sicherheitsanforderungen

In diesem Anhang werden die technischen und organisatorischen Massnahmen beschrieben, welche der Auftragsbearbeiter bzw. die HCI Solutions AG als Unterauftragsnehmer des Auftragsbearbeiters ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(1) Pseudonymisierung und Verschlüsselung personenbezogener Daten

- Soweit möglich und mit dem Bearbeitungszweck vereinbar werden Personendaten pseudonymisiert oder verschlüsselt, unter sicherer Aufbewahrung der Zuordnungsinformationen bzw. des Schlüssels.

(2) Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen

Zugangskontrolle – *unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren* – und **Personendatenträgerkontrolle** – *unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen*:

- Der Zutritt zum Gebäude der Galenica AG in Bern und Niederbipp ist durch Badge gesichert. Das Verfahren zur Vergabe der Badges ist im Management System der Galenica AG in gelenkten Dokumenten beschrieben
- Der Zutritt zu den Rechenzentren der Galenica AG ist nur für berechtigte Badges freigeschaltet und erfordert zusätzlich die Eingabe eines persönlichen PIN-Codes. Die Türen der Rechenzentren sind über die EMA (Einbruchmeldeanlage) überwacht, und es ertönt ein Alarm, wenn eine Tür länger als 60 Sekunden geöffnet bleibt. Bleibt die Tür weitere 30 Sekunden geöffnet, geht ein Einbruchalarm an die Betriebstechnik
- Besucher müssen sich in einem Besucherbuch an- und abmelden. Im Gebäude werden Besucher durch einen Mitarbeitenden der Galenica AG begleitet
- Die Rechenzentren sind mit Video überwacht. Die Aufbewahrungsfrist und der Zugriff auf die Videodaten sind im Management System der Galenica AG in gelenkten Dokumenten festgeschrieben.

Zugriffskontrolle – *der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen* –, **Benutzerkontrolle** – *die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern* – und **Speicherkontrolle** – *unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern*:

- Der Zugriff auf die Personendaten beruht auf einem rollenbasierten Zugriffsberechtigungsmodell. Jeder Benutzer erhält eine individuelle User-ID
- Es bestehen Vorgaben zur Komplexität von Passwörtern, deren Einhaltung technisch durchgesetzt werden
- Das Netzwerk der Galenica Gruppe ist durch eine Firewall, durch ein Intrusion Detection System (IDS) sowie durch eine Netzwerksegmentierung geschützt
- Auf allen Server- und Client-Systemen, welche durch die Galenica AG betrieben werden, sind Virenscanner im Einsatz, welche regelmässig aktualisiert werden
- Die Server- und Client-Systeme, welche durch die Galenica AG betrieben werden, werden regelmässig gepatcht
- Bei mehr als 8-minütiger Inaktivität eines Clients wird ein kennwortgeschützter Bildschirmschoner aktiviert

- Es besteht eine interne Vorgabe, der zufolge Clients bei vorübergehendem Verlassen des Arbeitsplatzes betriebssystemseitig zu sperren sind
- Die Berechtigungen für IT-Basisdienste (Active Directory, VPN, FTP-Konten) sowie für ausgewählte Applikationen werden einmal jährlich durch den Data Governance Manager überprüft; dabei werden allfällig zu Unrecht bestehende Zutrittsberechtigungen entzogen

Transportkontrolle – *bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können* – und **Bekanntgabekontrolle** – *Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können*:

- Personendaten werden angemessen gegen unbefugte Zugriffe und Eingriffe geschützt, bspw. durch Transportverschlüsselung, durch Signierung, durch eine geschützte Schnittstelle oder auf andere Weise. Die Identifikation von Empfängern von Personendaten wird nach den jeweiligen Möglichkeiten sichergestellt.
- Sofern HCI für die Eingabe von Auftragsdaten verantwortlich ist, werden Massnahmen zu Gewährleistung von deren korrekter Erfassung ergriffen.

(3) Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

- Die IT-Infrastruktur der Galenica AG ist in weiten Teilen redundant ausgelegt. Insbesondere werden die Serversysteme in zwei geografisch getrennten Rechenzentren je nach definierter Verfügbarkeitsanforderung gespiegelt betrieben werden
- Beide Rechenzentren der Galenica AG verfügen über eine doppelte (d.h. redundante) Stromversorgung, von denen eine ausserdem an USV und Notstromaggregat angeschlossen ist
- Beide Rechenzentren der Galenica AG verfügen ausserdem über zwei getrennte Internetanschlüsse über verschiedene Provider
- Beide Rechenzentren verfügen über voneinander unabhängige redundante Klimatisierungssysteme. Die Funktionsfähigkeit der Redundanzen wird wiederkehrend geprüft
- Beide Rechenzentren verfügen über ein dreistufiges Brandlöschkonzept, bestehend aus einer Detektion über ein Brandfrüherkennungssystem, einer Brandalarmanlage und einer aktiven Löschung.
- Es besteht ein Konzept zum Backup aller Server-Systeme, welches im Management System der Galenica AG in gelenkten Dokumenten beschrieben ist. Je nach System und definierter Backup-Gruppe erfolgen die Backups periodisch in unterschiedlichen Intervallen zwischen viertelstündlich und einmal täglich. Die Backups werden je nach Backup-Gruppe mindestens 5 Tage und, sofern für eine Applikation gefordert, langzeitaufbewahrt. Backups, welche auf Tape geschrieben werden, werden, sofern für eine Applikation gefordert, periodisch an einen anderen, geografisch getrennten Standort der Galenica Gruppe ausgelagert.
- Es besteht ein Notfall- und Krisenmanagement (N&K), welcher im Management System der Galenica AG in gelenkten Dokumenten beschrieben ist. Insbesondere besteht ein Notfall- und Krisenplan für das Szenario. Dieser regelt die Kommunikation und Information im Krisenfall, legt Sofort- und andere reaktive Massnahmen abhängig von verschiedenen Ausfallszenarien fest, beschreibt Szenarien des eingeschränkten IT-Betriebs, definiert die Prioritäten für die Wiederherstellung des Normalbetriebs und macht Vorgaben zu Tests und Schulung des Vorgehens im Krisenfall

(4) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

- Es besteht ein Risikoregister, in welchem alle identifizierten Risiken aufgeführt sind. Das Risikoregister wird regelmässig einem Review unterzogen, an welchem die Leitung HCI teilnimmt. Halbjährlich wird auch die Geschäftsleitung der Galenica AG über die wichtigsten Risiken aus dem IT-Risikoregister informiert
- Der Notfall- und Krisenplan wird einmal jährlich aktualisiert

Anhang 3: Genehmigte Unterauftragnehmer

Die folgenden Personen gelten als genehmigte Unterauftragnehmer i.S.v. Ziff. 6(b) der Vereinbarung:

Name und Sitz	Land der Bearbeitung	Betroffene Dienstleistungen	Aufgabe(n) des Unterauftragnehmers
Galenica AG, Bern	Schweiz	IT-Infrastruktur und Documedis Hosting	Vertrieb der IT-Infrastruktur und des Hostings der Applikationen Documedis eMediplan und CDS.CE
ISS	Schweiz	MepFlix für VacCheck	Vertrieb der IT-Infrastruktur und des Hostings der Applikation VacCheck

Convention de traitement des données en sous-traitance

Remarques préliminaires

La présente convention concrétise les obligations des donneurs d'ordre et des sous-traitants (les **parties**) en ce qui concerne les prescriptions de la loi suisse sur la protection des données (LPD) et du règlement général sur la protection des données (RGPD) de l'UE. Elle complète à cet égard les accords contractuels entre HCI Solutions SA (sous-traitant) et le client (donneur d'ordre). Il peut s'agir d'un ou de plusieurs contrats entre HCI Solutions SA et le client. Des détails précis sur les «contrats» figurent dans les annexes.

Dans le cadre des prestations, le donneur d'ordre met des données personnelles à la disposition du sous-traitant à des fins de traitement sur mandat; soit le sous-traitant collecte des données personnelles sur mandat du donneur d'ordre, soit il a accès, dans le cadre de l'exécution de son mandat, à des données personnelles dont le donneur d'ordre est responsable. Afin de garantir le respect des exigences de la loi suisse sur la protection des données (LPD) et du règlement général sur la protection des données (RGPD de l'UE), les parties concluent la présente convention de traitement des données en sous-traitance (l'**accord**).

1. Objet du contrat

(a) Objet: Dans la convention, les parties règlent uniquement la relation de sous-traitance en vertu de la législation sur la protection des données. Elles n'ont pas l'intention d'étendre ou de restreindre le catalogue de prestations convenu dans la convention de service.

(b) Règlement des conflits: En cas de contradictions entre des dispositions contractuelles, l'ordre suivant s'applique: les annexes de la présente convention prévalent sur la convention et cette dernière prime dans son ensemble la convention de service. Si les parties concluent ou ont conclu un autre contrat de sous-traitance pour une prestation, les exigences les plus strictes s'appliquent.

(c) Définitions: Dans la présente convention, les termes en gras sont utilisés avec la signification qui leur est attribuée. Les termes juridiques tels que «données personnelles», «traitement», etc. ont la signification définie dans le droit applicable en matière de protection des données.

2. Objet et durée du traitement des commandes

(a) Traitement des commandes: Le sous-traitant traite des données personnelles inclus «données sensibles»en rapport avec les prestations pour le compte du donneur d'ordre (ensemble **des données de commande**). L'objet du traitement des commandes, sa nature et sa finalité découlent de la convention de service. Les catégories de personnes concernées par le traitement des commandes et les catégories de données personnelles concernées sont décrites à l'annexe 1.

(b) Autres prestations: Dans la mesure où le sous-traitant assure d'autres prestations pour le donneur d'ordre au cours de la collaboration ultérieure, la présente convention s'applique également à ces prestations.

(c) Durée: La présente convention prend effet au moment de sa signature ou, si elle est postérieure, à l'entrée en vigueur de la convention de service, mais au plus tard au moment du premier accès du sous-traitant aux données de commande. Elle prend fin à la résiliation de la convention de service, mais au plus tôt avec la suppression de toutes les données de commande traitées pour le compte du donneur d'ordre.

(d) Position du donneur d'ordre: Le donneur d'ordre est conscient qu'il est responsable légalement de la licéité de la collecte et du traitement des données de commande et du respect des droits des personnes concernées en relation avec les prestations.

3. Obligations du sous-traitant

(a) Respect des instructions:

(i) Le sous-traitant est tenu d'utiliser les données de commande exclusivement aux fins des prestations et de suivre les instructions du donneur d'ordre lors de leur traitement. Sont réservées les obligations divergentes du droit applicable (p. ex. directives contraignantes des autorités compétentes).

(ii) Le droit d'émettre des instructions est limité par la convention de service et par la présente convention. Les instructions doivent être données sous forme de texte. Le donneur d'ordre est tenu de documenter toutes les instructions de manière appropriée.

(b) Lieu du traitement des données: Le traitement des données s'effectue en principe en Suisse. Toute communication de données pertinentes par HCI Solutions SA à l'étranger ou à une organisation internationale n'est autorisée que si HCI Solutions SA respecte les dispositions de l'art. 16 ss LPD ou du chapitre V RGPD de l'UE. En revanche, dans la mesure où une telle communication de données pertinentes est souhaitée par le client ou effectuée pour son compte, le respect des dispositions correspondantes incombe exclusivement au client.

(c) Obligation de restitution et de suppression: Les données de commande doivent être restituées ou supprimées à la fin du contrat, conformément aux dispositions contractuelles ou aux instructions du donneur d'ordre. Le sous-traitant utilise les procédures usuelles de la branche pour la suppression des données de commande.

4. Obligations d'assistance

(a) Sécurité des données: Le sous-traitant assiste le donneur d'ordre de manière appropriée pour satisfaire à ses obligations légales de garantir une sécurité appropriée des données et de signaler les violations de la protection des données, ainsi que pour la réalisation volontaire ou obligatoire d'analyses d'impact relatives à la protection des données. Le chapitre 5(b) s'applique en cas de violation de la protection des données.

(b) Droits des personnes concernées: Si une personne concernée s'adresse au sous-traitant dans le cadre de droits en matière de protection des données (p. ex. avec une demande d'information ou de suppression), ce dernier transmet immédiatement la demande correspondante au donneur d'ordre. Il soutient le donneur d'ordre de manière appropriée pour le traitement de telles demandes, ainsi que pour les obligations de renseigner vis-à-vis des autorités. Cela inclut, si nécessaire, l'assistance dans la compilation des données et informations nécessaires.

(c) Contact: Pour les questions relatives à la protection des données, il convient en premier lieu de contacter les personnes suivantes:

(i) **Donneur d'ordre**: Personne de contact indiquée dans le contrat entre le donneur d'ordre et HCI Solutions SA.

(ii) **Sous-traitant**: HCI Solutions SA, Untermattweg 8, case postale, 3000 Berne 1
E-mail: dataprotection@hcisolutions.ch, téléphone: +41 58 851 26 00

5. Sécurité des données

(a) Mesures de sécurité: Le sous-traitant prend des mesures techniques et organisationnelles appropriées, mais dans tous les cas au moins celles décrites à l'annexe 2, pour protéger les données de commande (**Mesures de sécurité**). Pendant la durée de la convention, le sous-traitant est autorisé à adapter les mesures de sécurité, pour autant que le niveau de sécurité ne soit pas abaissé.

(b) Signalement de violations:

(i) En cas de violations de la sécurité concrètement supposées ou constatées qui entraînent la destruction, la perte, l'altération ou la divulgation de données personnelles, qu'elles soient contraires à la loi, au contrat, aux instructions ou involontaires, le sous-traitant en informe le donneur d'ordre le plus rapidement possible, en fournissant au moins les informations suivantes (celles-ci pouvant être transmises de manière échelonnée si elles ne sont pas connues immédiatement):

- une description de la nature de la violation, en indiquant, si possible, les catégories et le nombre approximatif de personnes et de catégories concernées et le nombre approximatif d'ensembles de données concernés et, en cas de divulgation à des personnes non autorisées, les personnes ou les groupes de personnes concernés;
- le nom et les coordonnées d'un autre point de contact du sous-traitant pour toute information complémentaire;
- les conséquences probables de la violation;
- les mesures prises ou envisagées pour remédier à la violation ou pour éliminer ou atténuer ses conséquences.

(ii) Le sous-traitant est tenu de fournir au donneur d'ordre, sur demande, d'autres renseignements pertinents concernant la violation de la sécurité, dans la mesure où cela est possible sans violer ses obligations contractuelles et légales de confidentialité.

6. Mandataires secondaires

(a) Admissibilité:

(i) Pour la fourniture des prestations, le sous-traitant est autorisé à mettre des données de commande à la disposition de mandataires secondaires dans la mesure où le sous-traitant respecte les dispositions de la présente convention, et en particulier du chapitre 6, et qu'il a conclu avec ces mandataires secondaires une convention dont le contenu correspond pour l'essentiel à la présente convention.

(ii) Par **mandataire secondaire**, on entend ici tout prestataire de services dont les prestations se rapportent directement au traitement de données de commande. Les fournisseurs de prestations annexes telles que les services de télécommunication, les services postaux / de transport, les prestations de maintenance ou l'élimination de supports de données ne sont pas des mandataires secondaires. Toutefois, même en cas de prestations annexes externalisées, le sous-traitant est tenu de conclure des accords contractuels appropriés et conformes à la loi.

(b) Approbation:

(i) Une liste des mandataires secondaires existants à la date du début du contrat et autorisés par la présente, ayant accès aux données de commande, se trouve à l'annexe 3. Le sous-traitant informe le donneur d'ordre des modifications envisagées des rapports avec les mandataires secondaires dans un délai d'un mois. Après notification par le sous-traitant, le donneur d'ordre peut faire opposition à l'implication du mandataire secondaire concerné pour des raisons importantes relevant du droit de la protection des données. L'opposition du donneur d'ordre doit être formulée par écrit et indiquer les motifs de l'opposition.

(ii) Le sous-traitant ne peut confier à un mandataire secondaire la réalisation de certaines activités de traitement que si:

- Le sous-traitant a effectué toutes les vérifications et évaluations appropriées et nécessaires et s'est assuré de la fiabilité et des capacités du mandataire secondaire à cet égard:

  (i) qu'il garantit le niveau de protection des données personnelles exigé par les lois sur la protection des données et

  (ii) qu'il remplit les obligations du sous-traitant en vertu du présent contrat;

- le sous-traitant impose contractuellement au mandataire secondaire les mêmes obligations que celles prévues par le présent contrat, et notamment offre des garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées;

- le mandataire secondaire met fin à ses activités de sous-traitance dès que le présent contrat prend fin, et

(c) Documentation: Sur demande, le sous-traitant transmet au donneur d'ordre une copie de sa/ses convention/s avec des mandataires secondaires (y compris, le cas échéant, les garanties appropriées), afin que le donneur d'ordre puisse vérifier le respect de la présente convention par le sous-traitant. Les parties des conventions qui ne sont pas pertinentes à cet égard peuvent être noircies.

(d) Responsabilité: Le sous-traitant est responsable envers le donneur d'ordre du respect des obligations des mandataires secondaires.

7. Droits de contrôle

(a) Droit de contrôle: Le sous-traitant est tenu de fournir au donneur d'ordre, sur demande, des informations afin de documenter le respect des obligations convenues. Le donneur d'ordre a le droit de vérifier le respect des obligations découlant de la présente convention par le sous-traitant. Le sous-traitant est tenu de participer de manière appropriée aux contrôles. Lors de la planification et de la réalisation du contrôle, le donneur d'ordre tient compte des besoins et des exigences de sécurité du sous-traitant et est tenu de respecter les obligations de confidentialité du sous-traitant. Le chapitre 8(b) s'applique aux faits constatés dans le cadre de l'audit.

(b) Organisme de contrôle externe: Le donneur d'ordre a le droit de faire effectuer le contrôle selon le chapitre 7 par un organisme externe compétent et soumis à la confidentialité. Les coûts du contrôle incombant au donneur d'ordre sont à la charge du donneur d'ordre.

8. Confidentialité

(a) Données de commande: Le sous-traitant s'engage à traiter les données de commande de manière strictement confidentielle et à ne les rendre accessibles qu'aux personnes au sein de son organisation qui ont besoin d'accéder aux données de commande pour remplir leurs obligations. Il s'assure que toutes les personnes ayant accès aux données de commande sont soumises à une obligation de confidentialité légale ou contractuelle les concernant.

(b) Autres informations: En ce qui concerne les faits dont elles ont connaissance dans le cadre de la présente convention, les deux parties sont en outre soumises aux obligations de confidentialité légales qui leur sont applicables et convenues entre elles dans la convention de service.

9. Dispositions finales

(a) Responsabilité: En cas de violation de la présente convention, les règles de responsabilité convenues pour les prestations ou en vigueur de par la loi s'appliquent.

(b) Communications: Sauf accord contraire, les communications prévues dans la présente convention doivent être faites expressément et sous forme de texte (p. ex. par e-mail ou par courrier postal).

(c) Modifications et compléments: Par dérogation à d'éventuelles réserves de forme écrite figurant dans le contrat, la présente convention peut également être convenue ou modifiée par voie électronique entre les parties.

(d) Règlement des litiges: Le droit applicable et le for sont déterminés par la convention de service. Le donneur d'ordre reste toutefois en droit d'exiger des mesures provisionnelles devant tout tribunal compétent et de faire valoir ses prétentions à l'encontre du sous-traitant devant le tribunal de l'action principale en cas de recours par un tiers.

Annexe 1 – Concrétisation de la Convention de traitement des données en sous-traitance

Prestation	Catégories de données personnelles	Personnes concernées
Compendium.ch	Inclus: eMediplan, Documedis CDS.CE, Documedis PCA.CE et Documedis Vac	Patientèle
Documedis eMediplan	Obligatoire: nom, prénom et date de naissance Facultatif: autres données personnelles et informations de santé	Patientèle
Documedis Ordonnance électronique	Obligatoire: nom, prénom, date de naissance, adresse et médication Facultatif: autres données personnelles	Patientèle
Documedis CDS.CE	Obligatoire: médication Facultatif: autres données patient (données personnelles et informations de santé), en fonction du contrôle qui doit être effectué. Journaux de données: afin de garantir la sécurité de la patientèle, des données anonymisées sont exigées conformément à l'ordonnance sur les dispositifs médicaux (ODim).	Patientèle
Documedis PCA.CE	Obligatoire: nom, prénom et date de naissance Facultatif: autres données patient (données personnelles, informations de santé et médication). Journaux de données: afin de garantir la sécurité de la patientèle, des données anonymisées sont utilisées conformément à l'ordonnance sur les dispositifs médicaux (ODim).	Patientèle
pharmaVISTA	Inclus: eMediplan, Documedis CDS.CE, Documedis PCA.CE, délivrance de l'ordonnance électronique Documedis et PMC Polymedications Check	Patientèle
CGP Contrôle de polymédication	Obligatoire: nom, prénom et date de naissance Facultatif: médicaments et autres données personnelles	Patientèle
VAC Saisie des vaccins / documentation	Obligatoire: nom, prénom et date de naissance Facultatif: vaccinations, réponse aux questions concernant l'état de santé et autres données personnelles	Patientèle

Annexe 2 – Exigences de sécurité

La présente annexe décrit les mesures techniques et organisationnelles prises par le sous-traitant ou par HCI Solutions SA en tant que mandataire secondaire du sous-traitant afin de garantir un niveau de protection adapté au risque.

(1) Pseudonymisation et cryptage des données à caractère personnel

- Dans la mesure du possible et en accord avec la finalité du traitement, les données personnelles sont pseudonymisées ou cryptées, avec conservation sécurisée des informations d'attribution ou de la clé.

(2) Capacité à garantir durablement la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services liés au traitement

Contrôle d'accès – *l'accès aux installations dans lesquelles des données personnelles sont traitées doit être interdit aux personnes non autorisées;* **contrôle des supports de données personnelles** – *la lecture, la copie, la modification ou la suppression de supports de données doit être rendue impossible par les personnes non autorisées*:

- L'accès aux bâtiments de Galenica SA à Berne et Niederbipp est sécurisé par un badge. La procédure d'attribution des badges est décrite dans les documents contrôlés dans le système de gestion de Galenica SA.
- L'accès aux centres de calcul de Galenica SA n'est autorisé que pour les badges autorisés et nécessite en outre la saisie d'un code PIN personnel. Les portes des centres de calcul sont surveillées par le système d'alarme anti-intrusion (EMA), et une alarme retentit lorsqu'une porte reste ouverte pendant plus de 60 secondes. Si la porte reste ouverte pendant 30 secondes de plus, une alarme anti-intrusion est transmise au service technique d'exploitation.
- Les visiteurs doivent s'inscrire et se désinscrire dans un registre des visiteurs. À l'intérieur du bâtiment, les visiteurs sont accompagnés par un collaborateur de Galenica SA.
- Les centres de calcul font l'objet d'une vidéosurveillance. Le délai de conservation et l'accès aux données vidéo sont consignés dans des documents contrôlés dans le système de gestion de Galenica SA.

Contrôle de l'accès – *l'accès des personnes autorisées doit être limité aux données personnelles dont elles ont besoin pour l'accomplissement de leur mission;* **contrôle des utilisateurs** – *l'utilisation de systèmes automatisés de traitement des données au moyen de dispositifs de transmission de données par des personnes non autorisées doit être empêchée;* **contrôle de l'enregistrement** – la *saisie non autorisée dans la mémoire ainsi que la consultation, la modification ou la suppression non autorisées de données personnelles enregistrées doivent être empêchées:*

- L'accès aux données personnelles repose sur un modèle de droit d'accès aux données basé sur les rôles. Chaque utilisateur reçoit un identifiant unique.
- Il existe des prescriptions relatives à la complexité des mots de passe, dont le respect est techniquement imposé.
- Le réseau du Groupe Galenica est protégé par un pare-feu, un système de détection d'intrusion (Intrusion Detection System, IDS) et une segmentation du réseau.
- Tous les systèmes serveurs et clients exploités par Galenica SA sont équipés de scanners antivirus mis à jour régulièrement.
- Les systèmes serveurs et clients exploités par Galenica SA sont régulièrement équipés de correctifs.

- En cas d'inactivité de plus de huit minutes d'un client, un économiseur d'écran protégé par mot de passe est activé.
- Il existe une directive interne selon laquelle les postes clients doivent être verrouillés par le système d'exploitation lorsqu'ils quittent temporairement leur poste de travail.
- Les autorisations pour les services informatiques de base (Active Directory, VPN, comptes FTP) ainsi que pour des applications sélectionnées sont vérifiées une fois par an par le Data Governance Manager; les autorisations d'accès éventuellement existantes à tort sont retirées.

Contrôle des transports – *lors de la communication de données personnelles ainsi que lors du transport de supports de données, il convient d'empêcher que les données puissent être lues, copiées, modifiées ou effacées sans autorisation;* **contrôle de la communication** – les *destinataires auxquels des données personnelles sont communiquées au moyen de dispositifs de transmission de données doivent pouvoir être identifiés:*

- Les données personnelles sont protégées de manière appropriée contre les accès et les interventions non autorisés, p. ex. au moyen d'un cryptage de transport, d'une signature, d'une interface protégée ou de toute autre manière. L'identification des destinataires des données personnelles est garantie dans la mesure du possible.
- Si HCI Solutions SA est responsable de la saisie des données de commande, des mesures sont prises pour garantir leur saisie correcte.

(3) Capacité à rétablir rapidement la disponibilité des données à caractère personnel et l'accès à celles-ci en cas d'incident physique ou technique

- L'infrastructure informatique de Galenica SA est en grande partie redondante. En particulier, les systèmes de serveurs seront exploités en miroir dans deux centres de données géographiquement séparés, selon les exigences de disponibilité définies.
- Les deux centres de calcul de Galenica SA disposent d'une alimentation électrique double (c.-à-d. redondante), dont l'un est en outre raccordé à ASI et au groupe électrogène de secours.
- Les deux centres de calcul de Galenica SA disposent en outre de deux connexions Internet séparées auprès de fournisseurs différents.
- Les deux centres de données disposent de systèmes de climatisation redondants indépendants l'un de l'autre. Le fonctionnement des redondances est contrôlé régulièrement.
- Les deux centres de calcul disposent d'un concept d'extinction d'incendie à trois niveaux, composé d'une détection par un système de détection précoce des incendies, d'un système d'alarme incendie et d'une extinction active.
- Il existe un concept de sauvegarde de tous les systèmes serveurs, qui est décrit dans les documents contrôlés dans le système de gestion de Galenica SA. Selon le système et le groupe de sauvegarde défini, les sauvegardes sont effectuées périodiquement à des intervalles différents, entre un quart d'heure et une fois par jour. Selon le groupe de sauvegarde, les sauvegardes sont conservées pendant au moins cinq jours et, si une application l'exige, à long terme. Si une application l'exige, les sauvegardes enregistrées sur bande sont périodiquement externalisées sur un autre site géographiquement séparé du Groupe Galenica.
- Il existe un système de gestion des urgences et des crises, qui est décrit dans les documents contrôlés dans le système de gestion de Galenica SA. Il existe notamment un plan d'urgence et de crise pour le scénario. Celui-ci régit la communication et l'information en cas de crise, définit les mesures immédiates et autres mesures réactives en fonction de différents scénarios de panne, décrit les scénarios d'exploitation informatique restreinte, définit les priorités pour le rétablissement du fonctionnement normal et donne des directives sur les tests et la formation à la procédure en cas de crise.

(4) Procédures permettant de réexaminer, d'évaluer et d'apprécier régulièrement l'efficacité des mesures techniques et organisationnelles visant à garantir la sécurité du traitement

- Il existe un registre des risques dans lequel sont répertoriés tous les risques identifiés. Le registre des risques est régulièrement soumis à une révision à laquelle participe la direction de HCI Solutions SA. Tous les six mois, la Direction de Galenica SA est également informée des principaux risques tirés du registre des risques informatiques.
- Le plan d'urgence et de crise est actualisé une fois par an.

Annexe 3 – Mandataires secondaires autorisés

Les personnes suivantes sont considérées comme des mandataires secondaires autorisés au sens du chiffre 6(b) de la convention:

Nom et siège	Pays de traitement	Personnes concernées Prestations	Tâche/s du mandataire secondaire
Galenica SA, Berne	Suisse	Infrastructure informatique et hébergement Documedis	Distribution de l'infrastructure informatique et de l'hébergement des applications Documedis eMediplan et CDS.CE
ISS	Suisse	MepFlix pour Vac Check	Distribution de l'infrastructure informatique et de l'hébergement de l'application Vac Check

Attention : ce document a été traduit de l'allemand. En cas d'ambiguïté ou de divergence d'interprétation, les formulations de la version originale allemande prévalent et doivent être considérées comme prépondérantes.

Accordo sull'affidamento del trattamento dei dati a un responsabile

Premesse

Il presente Accordo concretizza gli obblighi del committente e del responsabile del trattamento (le **parti**) in relazione alle disposizioni della Legge svizzera sulla protezione dei dati (LPD) e del Regolamento generale sulla protezione dei dati dell'UE (RGPD UE). A tal riguardo integra gli accordi contrattuali tra HCI Solutions (responsabile del trattamento) e il cliente (committente). A tale scopo si può trattare di uno o più contratti tra HCI Solutions e il cliente. Per maggiori dettagli sui «contratti» si rimanda all'«Appendice».

Nell'ambito dei servizi, il committente mette a disposizione del responsabile del trattamento dati personali per il loro trattamento, raccoglie dati personali per conto del committente oppure, nell'esecuzione del proprio incarico, il responsabile del trattamento ha accesso ai dati personali per i quali è responsabile il committente. Per garantire il rispetto dei requisiti della Legge svizzera sulla protezione dei dati (LPD) e del Regolamento europeo sulla protezione dei dati (RGPD UE), le parti stipulano il presente Accordo sull'affidamento del trattamento dei dati a un responsabile (l'**Accordo**).

1. Oggetto del contratto

(a) Oggetto: le parti disciplinano nell'Accordo solo il rapporto di trattamento dei dati ai sensi delle disposizioni in materia di protezione dei dati. Non intendono ampliare o limitare il catalogo delle prestazioni concordato nell'accordo sulle prestazioni.

(b) Risoluzione dei conflitti: in caso di contraddizioni tra le disposizioni contrattuali si applica l'ordine seguente: le appendici al presente Accordo hanno la priorità sull'accordo e il presente Accordo è prioritario rispetto all'accordo sulle prestazioni nel suo complesso. Se, per una prestazione, le parti stipulano o hanno stipulato un diverso accordo sull'affidamento del trattamento dei dati a un responsabile, si applicano di volta in volta i requisiti più severi.

(c) Definizioni: nel presente Accordo si utilizzano i termini in grassetto vengono utilizzati con il significato loro assegnato. Termini giuridici quali «dati personali», «trattamento» ecc. hanno il significato stabilito nel diritto applicabile in materia di protezione dei dati.

2. Oggetto e durata del trattamento dei dati

(a) Trattamento dei dati: in relazione alle prestazioni, il responsabile del trattamento tratta dati personali incluso dati personali degni per conto del committente (collettivamente **dati oggetto del trattamento**). L'oggetto del trattamento dei dati, la sua tipologia e il suo scopo sono indicati nell'accordo sulle prestazioni. Le categorie delle persone interessate dal trattamento dei dati e le categorie dei dati personali interessati sono descritte nell'Appendice 1.

(b) Ulteriori prestazioni: qualora, nel prosieguo della collaborazione, il responsabile del trattamento fornisca ulteriori prestazioni al committente, il presente Accordo si applica anche a esse.

(c) Durata: il presente Accordo ha decorrenza dalla sua firma o, se successivo, dall'entrata in vigore dell'accordo sulle prestazioni, al più tardi tuttavia con il primo accesso ai dati oggetto del trattamento da parte del responsabile del trattamento. Esso ha terme con la cessazione dell'accordo sulle prestazioni, al più presto tuttavia con la cancellazione di tutti i dati trattati per conto del committente.

(d) Posizione del committente: il committente è consapevole della propria responsabilità legale per l'ammissibilità della raccolta e del trattamento dei dati oggetto del trattamento e per l'adempimento dei diritti degli interessati in relazione alle prestazioni.

3. Obblighi del responsabile del trattamento

(a) Aderenza alle istruzioni:

(i) Il responsabile del trattamento è tenuto a utilizzare i dati oggetto del trattamento esclusivamente per le prestazioni e a seguire le istruzioni del committente per il loro trattamento. Sono fatti salvi gli obblighi divergenti dal diritto applicabile (come le disposizioni vincolanti delle autorità competenti).

(ii) Il diritto di impartire istruzioni è limitato dall'accordo sulle prestazioni e dal presente Accordo. Le istruzioni vanno impartite in forma scritta. Il committente è tenuto a documentare adeguatamente tutte le istruzioni.

(b) Luogo del trattamento dei dati. Il trattamento dei dati si svolge in linea di principio in Svizzera. Qualsiasi comunicazione di dati rilevanti da parte di HCI Solutions all'estero o a un'organizzazione internazionale è consentita solo se HCI Solutions rispetta le disposizioni dell'art. 16 e segg. LPD o del capitolo V RGPD UE. Qualora invece tale comunicazione di dati rilevanti sia richiesta del cliente o per suo incarico, il rispetto delle corrispondenti disposizioni spetta esclusivamente al cliente.

(c) Obbligo di restituzione e cancellazione: al termine del contratto, i dati oggetto del trattamento vanno restituiti o cancellati conformemente alle disposizioni contrattuali o alle istruzioni del committente. Il responsabile del trattamento applica le procedure abituali del settore per la cancellazione dei dati oggetto del trattamento.

4. Obblighi di assistenza

(a) Sicurezza dei dati: il responsabile del trattamento supporta adeguatamente il committente nell'adempimento dei suoi obblighi legali al fine di garantire un'adeguata sicurezza dei dati e di segnalare eventuali violazioni della protezione dei dati e per l'esecuzione volontaria o obbligatoria di valutazioni d'impatto sulla protezione dei dati. In caso di violazioni della protezione dei dati si applica il punto 5(b).

(b) Diritti degli interessati: se una persona interessata si rivolge al responsabile del trattamento in relazione a pretese in materia di protezione dei dati (ad esempio per richieste di informazioni o di cancellazione), il responsabile del trattamento inoltrerà immediatamente la relativa richiesta al committente. Assiste adeguatamente il committente nell'evasione di tali richieste nonché negli obblighi d'informazione nei confronti delle autorità. Ciò comprende, se necessario, l'assistenza nella raccolta dei dati e delle informazioni necessari.

(c) Contatto: per questioni relative alla protezione dei dati vanno contattate in primo luogo le seguenti persone:

(i) **Committente**: referente visibile nel contratto tra il committente e HCI Solutions.

(ii) **Responsabile del trattamento**:
HCI Solutions SA, Untermattweg 8, casella postale, 3000 Berna 1
E-mail: dataprotection@hcisolutions.ch, Telefono: +41 58 851 26 00

5. Sicurezza dei dati

(a) Misure di sicurezza: il responsabile del trattamento adotta misure tecniche e organizzative adeguate – in ogni caso almeno quelle descritte nell'Appendice 2 – al fine di proteggere i dati oggetto del trattamento (**misure di sicurezza**). Per la durata dell'Accordo, il responsabile del trattamento ha il diritto di adeguare le misure di sicurezza, a condizione che ciò non riduca il livello di sicurezza.

(b) Notifica di violazioni:

(i) In caso di sospetti concreti o accertate violazioni della sicurezza – siano esse contrarie alla legge, al contratto, alle istruzioni o involontarie – che comportano la distruzione, la perdita, la modifica o la divulgazione di dati personali, il responsabile del trattamento informa il prima possibile il committente indicando almeno le seguenti informazioni (la cui trasmissione può avvenire per scaglioni, nel caso in cui non siano immediatamente note):

- una descrizione del tipo di violazione indicando, ove possibile, le categorie e il numero approssimativo di persone e categorie interessate nonché il numero approssimativo di record di dati interessati e, in caso di divulgazione a persone non autorizzate, le persone o i gruppi di persone interessati;
- il nome e i dati di contatto di un ulteriore referente del responsabile del trattamento per maggiori informazioni;
- le probabili conseguenze della violazione;
- le misure adottate o previste per porre rimedio alla violazione o risolverne o attenuarne le conseguenze.

(ii) Su richiesta, il responsabile del trattamento è tenuto a fornire al committente ulteriori e opportune informazioni relative alla violazione della sicurezza, nella misura in cui ciò sia possibile senza violare i propri obblighi di riservatezza contrattuali e legali.

6. Subappaltatori

(a) Ammissibilità:

(i) Per l'erogazione delle prestazioni, il responsabile del trattamento è autorizzato a mettere a disposizione dei subappaltatori i dati oggetto del trattamento, a condizione che rispetti le disposizioni del presente Accordo e, in particolare, il presente punto 6 e abbia stipulato con il subappaltatore un accordo sostanzialmente corrispondente al presente Accordo.

(ii) Per **subappaltatore** si intende in tal senso ogni fornitore di servizi le cui prestazioni si riferiscono direttamente al trattamento dei dati oggetto del trattamento. Non si considerano subappaltatori i fornitori di prestazioni accessorie – come ad esempio servizi di telecomunicazione, servizi postali e di trasporto, servizi di manutenzione o smaltimento di supporti dati. Anche nel caso di prestazioni accessorie in outsourcing, il contraente è tuttavia tenuto a stipulare accordi contrattuali adeguati e conformi alla legge.

(b) Autorizzazione:

(i) Un elenco dei subappaltatori esistenti all'inizio del contratto e con il presente approvati con accesso ai dati oggetto del trattamento è riportato nell'Appendice 3. Il responsabile del trattamento informa il committente in merito alle modifiche che intende apportare ai rapporti di subappalto entro un mese. In seguito alla notifica da parte del responsabile del trattamento, il committente può opporsi qualora sussistano importanti motivi di protezione dei dati che impediscano il coinvolgimento del subappaltatore interessato. L'obiezione da parte del committente va presentata per iscritto e deve contenere le ragioni di tale obiezione.

(ii) Il responsabile del trattamento può affidare a un subappaltatore l'esecuzione di determinate attività di trattamento solo qualora:

- Il responsabile del trattamento abbia effettuato tutte le opportune e necessarie verifiche e valutazioni e si sia accertato che l'affidabilità e la capacità del subappaltatore garantiscano:

  (i) il livello di protezione dei dati personali richiesto dalle leggi in materia di protezione dei dati e

  (ii) l'adempimento degli obblighi del responsabile del trattamento previsti dal presente contratto;

- l'imposizione, da parte del responsabile del trattamento impone con contratto al subappaltatore, dei medesimi obblighi stabiliti nel presente contratto e, in particolare, di garanzie sufficienti riguardo all'adozione di misure tecniche e organizzative adeguate;

- la cessazione delle attività di trattamento da parte del subappaltatore alla cessazione del presente contratto; e

(c) Documentazione: su richiesta, il responsabile del trattamento trasmette al committente una copia del proprio accordo o dei propri accordi con i subappaltatori (comprese le eventuali garanzie adeguate) affinché il committente possa verificare il rispetto del presente Accordo da parte del responsabile del trattamento. Le parti degli accordi irrilevanti possono essere oscurate.

(d) Responsabilità: il responsabile del trattamento è responsabile, nei confronti del committente, del rispetto degli obblighi da parte dei subappaltatori.

7. Diritti di verifica

(a) Diritto di verifica: su richiesta, il responsabile del trattamento è tenuto a mettere a disposizione del committente informazioni al fine di documentare il rispetto degli obblighi concordati. Il committente ha il diritto di verificare il rispetto degli obblighi previsti dal presente Accordo da parte del responsabile del trattamento. Il responsabile del trattamento è opportunamente tenuto a collaborare a tali verifiche. Nella pianificazione e nello svolgimento della verifica, il committente tiene conto delle esigenze e dei requisiti di sicurezza del responsabile del trattamento ed è tenuto a rispettare gli obblighi di riservatezza di quest'ultimo. Per i fatti rilevati nell'ambito della verifica si applica il punto 8(b).

(b) Organo di verifica esterno: il committente ha il diritto di far eseguire la verifica ai sensi del punto 7 da un organo di competenza esterno e tenuto alla riservatezza. I costi sostenuti dal committente per la verifica sono a carico del committente stesso.

8. Riservatezza

(a) Dati oggetto del trattamento: il responsabile del trattamento si impegna a trattare i dati con la massima riservatezza e a renderli accessibili all'interno della propria organizzazione solo alle persone che lo necessitano al fine di adempiere ai propri obblighi. Garantisce che tutte le persone che hanno accesso ai dati oggetto del trattamento siano soggette a un obbligo di riservatezza legale o contrattuale.

(b) Ulteriori informazioni: entrambe le parti sono inoltre soggette agli obblighi di riservatezza legali a loro applicabili e tra loro concordati nell'ambito dell'accordo sulle prestazioni in relazione ai fatti percepiti nell'ambito del presente Accordo.

9. Disposizioni finali

(a) Responsabilità: per la responsabilità derivante da violazioni al presente Accordo si applicano le norme sulla responsabilità concordate per le prestazioni o vigenti per legge.

(b) Comunicazioni: salvo se diversamente concordato, le comunicazioni previste nel presente Accordo devono avvenire in modo esplicito e in forma scritta (ad esempio via e-mail o posta).

(c) Modifiche e integrazioni: in deroga a eventuali riserve della forma scritta contenute nel contratto, il presente Accordo può essere stipulato tra le parti o da esse modificato anche per via elettronica.

(d) Risoluzione delle controversie: il diritto applicabile e il foro competente sono disciplinati dall'accordo sulle prestazioni. Il committente rimane tuttavia autorizzato a richiedere misure cautelari dinanzi a qualsiasi tribunale competente e a far valere i propri diritti nei confronti del responsabile del trattamento in caso di rivendicazione da parte di terzi dinanzi al tribunale competente per l'azione principale.

Appendice 1: Concretizzazione del contratto relativo al trattamento dei dati

Prestazione	Categorie di dati personali	Persone interessate
Compendium.ch	Include: eMediplan, Documedis CDS.CE, Documedis PCA.CE e Documedis Vac	Pazienti
Documedis eMediplan	Obbligatori: cognome, nome e data di nascita Facoltativi: ulteriori dati personali e informazioni sulla salute	Pazienti
Documedis Ricetta elettronica	Obbligatori: cognome, nome, data di nascita, indirizzo e terapia farmacologica del paziente Facoltativi: ulteriori dati personali	Pazienti
Documedis CDS.CE	Obbligatori: terapia farmacologica del paziente Facoltativi: ulteriori dati sul paziente (dati personali e informazioni sanitarie), a seconda del controllo che si desidera effettuare. Log dati: per poter garantire la sicurezza del paziente sono richiesti dati anonimizzati conformemente all'Ordinanza relativa ai dispositivi medici (ODmed).	Pazienti
Documedis PCA.CE	Obbligatori: cognome, nome e data di nascita Facoltativi: ulteriori dati sul paziente (dati personali, informazioni sanitarie e terapia farmacologica del paziente). Log dati: per poter garantire la sicurezza del paziente si impiegano dati anonimizzati conformemente a quanto richiesto dall'Ordinanza relativa ai dispositivi medici (ODmed).	Pazienti
pharmaVISTA	Inclusi: eMediplan, Documedis CDS.CE, Documedis PCA.CE, utilizzo della ricetta elettronica Documedis e PMC Polymedications Check	Pazienti
PMC Polymedications Check	Obbligatori: cognome, nome e data di nascita Facoltativi: terapia farmacologica del paziente e ulteriori dati personali	Pazienti
VAC Registrazione / documentazione delle vaccinazioni	Obbligatori: cognome, nome e data di nascita Facoltativi: vaccinazioni del paziente, risposta alle domande sullo stato di salute e ulteriori dati personali	Pazienti

Appendice 2: Requisiti di sicurezza

Nella presente Appendice sono descritte le misure tecniche e organizzative che il responsabile del trattamento o l'azienda subappaltatrice del responsabile del trattamento HCI Solutions SA adottano al fine di garantire un livello di protezione adeguato al rischio.

(1) Pseudonimizzazione e crittografia dei dati personali

- Per quanto possibile e compatibile con le finalità del trattamento, i dati personali vengono pseudonimizzati o crittografati, archiviando in sicurezza le informazioni relative all'attribuzione o la chiave.

(2) Capacità di garanzia a lungo termine di riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi correlati al trattamento

Controllo degli accessi – *alle persone non autorizzate va vietato l'accesso alle strutture in cui vengono trattati dati personali* – e **controllo dei supporti di dati personali** – *alle persone non autorizzate vanno impedite la lettura, la copia, la modifica o l'eliminazione di supporti di dati*:

- L'accesso agli edifici di Galenica SA a Berna e Niederbipp è protetto da badge. La procedura di assegnazione dei badge è descritta all'interno del Management System di Galenica SA nei documenti controllati.
- L'accesso ai centri di calcolo di Galenica SA è consentito solo ai badge autorizzati e richiede inoltre l'inserimento di un codice PIN personale. Le porte dei centri di calcolo sono sorvegliate tramite sistema antieffrazione e viene emesso un allarme se una porta rimane aperta per più di 60 secondi. Se la porta rimane aperta per altri 30 secondi viene inviato un allarme antieffrazione alla centrale operativa.
- I visitatori sono tenuti a registrarsi su un apposito registro visitatori sia all'entrata sia all'uscita. All'interno dell'edificio, i visitatori vengono accompagnati dal personale di Galenica SA.
- I centri di calcolo sono videosorvegliati. Il termine di conservazione e l'accesso ai dati video sono definiti nei documenti controllati all'interno del sistema di gestione di Galenica SA.

Controllo degli accessi – *l'accesso delle persone autorizzate va limitato ai dati personali di cui necessitano per l'adempimento dei loro compiti* – **controllo degli utenti** – *va impedito l'uso di sistemi automatizzati di trattamento dei dati tramite dispositivi per la trasmissione di dati da parte di persone non autorizzate* – e **controllo della memoria** – *vanno impediti l'inserimento non autorizzato nella memoria nonché la consultazione, la modifica o la cancellazione non autorizzate dei dati personali memorizzati*:

- L'accesso ai dati personali si basa su un modello di autorizzazione di accesso basato sui ruoli. Ogni utente riceve un ID utente individuale.
- Esistono direttive sulla complessità delle password, il cui rispetto viene imposto tecnicamente.
- La rete del Gruppo Galenica è protetta da un firewall, da un Intrusion Detection System (IDS) e da una segmentazione della rete.
- Su tutti i sistemi server e client gestiti da Galenica SA si utilizzano antivirus che vengono regolarmente aggiornati.
- I sistemi server e client gestiti da Galenica SA vengono regolarmente patchati.
- In caso di inattività di un client per più di 8 minuti viene attivato un salvaschermo protetto da password.
- Esiste una disposizione interna che comporta il blocco dei client dal sistema operativo in caso di abbandono temporaneo della postazione di lavoro.

- Le autorizzazioni per i servizi di base IT (Active Directory, VPN, account FTP) e per applicazioni selezionate vengono verificate a cadenza annuale dal Data Governance Manager; in tale occasione vengono revocate eventuali autorizzazioni di accesso indebitamente esistenti.

Controllo del trasporto – *nella comunicazione di dati personali e nel trasporto di supporti dati occorre evitare che i dati possano essere indebitamente letti, copiati, modificati o cancellati* – e **controllo della comunicazione** – *i destinatari di dati personali comunicati tramite dispositivi per la trasmissione di dati devono poter essere identificati*:

- I dati personali sono adeguatamente protetti da accessi e interventi non autorizzati – ad esempio tramite crittografia di trasporto, firma, interfaccia protetta o altre misure. L'identificazione dei destinatari dei dati personali viene garantita secondo le rispettive possibilità.
- Nella misura in cui HCI è responsabile dell'inserimento dei dati oggetto del trattamento vengono adottate misure per garantirne la corretta registrazione.

(3) Capacità di rapido ripristino della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico

- L'infrastruttura IT di Galenica SA è configurata in modo perlopiù ridondante. In particolare, la gestione dei sistemi server avviene a specchio in due centri di calcolo geograficamente separati in base a requisiti di disponibilità definiti.
- Entrambi i centri di calcolo di Galenica SA dispongono di un'alimentazione elettrica doppia (vale a dire ridondante), di cui una è inoltre collegata all'UPS e al gruppo elettrogeno d'emergenza.
- Entrambi i centri di calcolo di Galenica SA dispongono inoltre di due connessioni Internet separate tramite provider diversi.
- Entrambi i centri di calcolo sono dotati di sistemi di climatizzazione ridondanti e indipendenti l'uno dall'altro. La funzionalità delle ridondanze viene verificata periodicamente.
- Entrambi i centri di calcolo dispongono di un piano di estinzione di incendi su tre livelli, composto da una rivelazione tramite un sistema di rilevamento precoce di incendi, un impianto di allarme antincendio e un sistema di estinzione attiva.
- Esiste un piano per il backup di tutti i sistemi server descritto nei documenti controllati all'interno del sistema di gestione di Galenica SA. A seconda del sistema e del gruppo di backup definito, i backup avvengono periodicamente a intervalli diversi compresi tra un quarto d'ora e una volta al giorno. A seconda del gruppo di backup, i backup vengono conservati per almeno 5 giorni e, se richiesto per un'applicazione, per un periodo di tempo prolungato. Se richiesto per un'applicazione, i backup scritti su nastro vengono periodicamente trasferiti in un'altra sede del Gruppo Galenica geograficamente separata.
- Esiste una gestione delle emergenze e delle crisi descritta nei documenti controllati all'interno del sistema di gestione di Galenica SA. In particolare esiste un piano di emergenza e di crisi per il scenario. Esso regola la comunicazione e l'informazione in caso di crisi, stabilisce misure immediate e reattive a seconda dei diversi scenari di guasto, descrive scenari di funzionamento limitato dell'IT, definisce le priorità per il ripristino del normale esercizio e prescrive direttive sui test e sulla formazione in merito alle procedure da seguire in caso di crisi.

(4) Procedure per le periodiche verifiche e valutazioni dell'efficacia delle misure tecniche e organizzative volte a garantire la sicurezza del trattamento

- Esiste un registro dei rischi in cui sono riportati tutti i rischi identificati. Il registro dei rischi viene periodicamente sottoposto a una revisione alla quale partecipa la Direzione HCI. A cadenza semestrale, anche la Direzione di Galenica SA viene informata in merito ai principali rischi del registro dei rischi informatici.
- Il piano di emergenza e di crisi viene aggiornato su base annuale.

Appendice 3: Subappaltatori autorizzati

Le seguenti persone sono considerate subappaltatori autorizzati ai sensi del punto 6(b) dell’Accordo:

Nome e sede	Paese in cui avviene il trattamento	Interessati Prestazioni	Mansione/i del subappaltatore
Galenica SA, Berna	Svizzera	Infrastruttura IT e hosting Documedis	Distribuzione dell’infrastruttura IT e dell’hosting delle applicazioni Documedis eMediplan e CDS.CE
ISS	Svizzera	MepFlix per VacCheck	Distribuzione dell’infrastruttura IT e dell’hosting dell’applicazione VacCheck

Attenzione: Il presente documento è una traduzione dal tedesco. In caso di ambiguità o di interpretazioni divergenti, il testo della versione originale tedesca avrà la precedenza e dovrà essere considerato autorevole.

Order Data Processing Agreement

Preliminary remarks

This Agreement specifies the obligations of the Client and the Order Processor (the **Parties**) with regard to the provisions of the Swiss Data Protection Act (FADP) and the EU General Data Protection Regulation (EU GDPR). In this regard, it supplements the contractual agreements between HCI Solutions (Order Processor) and the customer (Client). These may consist of one or more contracts between HCI Solutions and the customer. Precise details on the “Contracts” can be found in the “Appendix”.

As part of its services, the Client shall provide the Order Processor with personal data for processing on behalf of the Client, it shall collect personal data on behalf of the Client, or the Order Processor shall have access to personal data for which the Client is responsible when performing its mandate. In order to ensure compliance with the requirements of the Swiss Data Protection Act (FADP) as well as the European Data Protection Regulation (EU-GDPR), the Parties shall conclude this Order Data Processing Agreement (the **Agreement**).

1. Subject of the Contract

(a) Subject: In the Agreement, the Parties shall only regulate the order processing relationship under data protection law. They do not intend to expand or restrict the list of services agreed in the Service Level Agreement.

(b) Conflict settlement: In the event of contradictions between contractual provisions, the following order of precedence shall apply: The Appendices to this Agreement shall take precedence over the Agreement and this Agreement shall take precedence over the Service Level Agreement as a whole. If the Parties conclude or have concluded another order processing agreement for a service, the stricter requirements shall apply.

(c) Definitions: Terms in bold shall be used in this Agreement with the meaning assigned to them. Legal terms such as “personal data,” “processing,” etc. shall have the meanings defined in the applicable data protection law.

2. Subject and duration of order processing

(a) Order processing: The Order Processor processes personal data including sensitive personal data on behalf of the Client in connection with the services (combined **order data**). The subject matter of order processing, its nature and its purpose are set out in the Service Level Agreement. The categories of persons affected by the order processing and the categories of personal data concerned are described in Appendix 1.

(b) Other services: Insofar as the Order Processor assumes additional services for the Client in the course of further collaboration, this Agreement shall also apply to these services.

(c) Duration: This Agreement begins when it is signed or, if later, when the Service Level Agreement enters into force, but no later than when the Order Processor first accesses the order data. It shall end upon termination of the Service Level Agreement, but at the earliest with the deletion of all order data processed on behalf of the Client.

(d) Position of the Client: The Client is aware that it is legally responsible for the approval of the collection and processing of order data and for the fulfilment of the rights of persons affected in connection with the services.

3. Obligations of the Order Processor

(a) Compliance with instructions:

(i) The Order Processor is obliged to use the order data exclusively for the services and to follow the Client's instructions when processing the data. Obligations to the contrary under applicable law (such as binding orders from responsible authorities) are reserved.

(ii) The right to issue instructions is limited by the Service Level Agreement and by this Agreement. Instructions must be issued in text form. The Client is obliged to document all instructions appropriately.

(b) Place of data processing. Generally, data processing takes place in Switzerland. Any disclosure of relevant data by HCI Solutions abroad or to an international organisation is only permitted if HCI Solutions complies with the provisions of Art. 16 et seq. of the FADP or Chapter V of the EU GDPR. If, on the other hand, such disclosure of relevant data is requested by the Client or carried out on its behalf, compliance with the relevant provisions shall be the sole responsibility of the Client.

(c) Obligation to return and delete: Order data must be surrendered or deleted after the end of the Contract in accordance with the contractual provisions or the Client's instructions. The Order Processor shall use industry standard procedures to delete order data.

4. Support obligations

(a) Data security: The Order Processor shall provide the Client with reasonable support in complying with its statutory obligations to ensure appropriate data security as well as reporting data protection breaches and in carrying out data protection impact assessments on a voluntary or mandatory basis. Section 5(b) applies for breaches of data security.

(b) Rights of persons concerned: If a person concerned contacts the Order Processor in connection with data protection rights (such as with a request for information or deletion), the Order Processor shall immediately forward the corresponding request to the Client. It shall provide the Client with appropriate support in processing such requests, as well as in the case of duties to provide information to the authorities. If necessary, this includes support in compiling the necessary data and information.

(c) Contact: The following persons should be contacted in the first instance as regards data protection issues:

(i) **Client**: The contact person can be found in the Contract between the Client and HCI Solutions.

(ii) **Order Processor**: HCI Solutions AG, Untermattweg 8, P.O. Box, CH-3000 Bern 1 Email: dataprotection@hcisolutions.ch, Phone: +41 58 851 26 00

5. Data security

(a) Security measures: The Order Processor shall take appropriate, but in all cases at least those described in Appendix 2, technical and organisational measures to protect the order data (**security measures**). The Order Processor is entitled to adjust the security measures for the duration of the Agreement, provided that the security level is not reduced.

(b) Reporting injuries:

(i) For specifically assumed and ascertained security breaches which – whether contrary to law, contract or instructions or unintentional – lead to the destruction, loss, alteration or disclosure of personal data, the Order Processor shall inform the Client as quickly as possible and providing at least the following information (where this can be transmitted in stages if it is not immediately known):

- a description of the nature of the breach, indicating, where possible, the categories and approximate number of persons and categories concerned as well as the approximate number of data records concerned and, if disclosed to unauthorised persons, the persons or groups of persons concerned
- name and contact details of another point of contact of the Order Processor for further information;
- the probable consequences of the breach;
- the actions taken or contemplated to remedy the breach or to remedy or to mitigate its consequences.

(ii) Upon request, the Order Processor is obliged to provide the Client with further relevant information about the security breach, insofar as this is possible without breaching its contractual and statutory confidentiality obligations.

6. Subcontractors

(a) Admissibility:

(i) For the provision of services, the Order Processor is authorised to provide subcontractors with order data, insofar as the Order Processor complies with the provisions of this Agreement and in particular this section 6 and has reached an agreement with the Subcontractor which essentially corresponds to the content of this Agreement.

(ii) A **subcontractor** in this sense is any service provider whose services relate directly to the processing of order data. Providers of ancillary services such as telecommunications services, postal/transport services, maintenance services or services for the disposal of data storage devices are not subcontractors. However, even in the case of outsourced ancillary services, the Contractor is obliged to make appropriate and legally compliant contractual arrangements.

(b) Approval:

(i) A list of subcontractors with access to order data existing at the start of the Contract and hereby authorised can be found in Appendix 3. The Order Processor informs the Client about intended changes to the subcontractor relationship within one month. After notification by the Order Processor, the Client may raise an objection if important data protection reasons speak against the involvement of the Subcontractor concerned. Any objection by the Client must be made in writing and must state the reasons for the objection.

(ii) The Order Processor may only engage a subcontractor to carry out certain processing activities if:

- the Order Processor has carried out all appropriate and necessary inspections and evaluations and has satisfied itself of the reliability and ability of the Subcontractor:

  (i) that the latter guarantees the level of protection for personal data required by data protection laws and

  (ii) fulfils the obligations of the Order Processor in accordance with this Contract;

- the Order Processor imposes on the Subcontractor by means of a contract the same obligations as set out in this contract and, in particular, offers sufficient guarantees that suitable technical and organisational measures will be taken;

- the Subcontractor shall terminate its order processing activities as soon as this contract ends, and

(c) Documentation: Upon request, the Order Processor shall provide the Client with a copy of its subcontractor Agreement(s) (including, if applicable, the appropriate guarantees) so that the Client can verify the Order Processor's compliance with this Agreement. Non-relevant parts of the agreements may be blackened.

(d) Liability: The Order Processor shall be liable to the Client for compliance with the obligations of the subcontractors.

7. Rights of inspection

(a) Right of inspection: The Order Processor is obliged to provide the Client with information upon request in order to document compliance with the agreed obligations. The Client shall have the right to check that the Order Processor is complying with the obligations under this Agreement. The Order Processor is obliged to cooperate appropriately in each inspection. When planning and carrying out the inspection, the Client shall take the needs and security requirements of the Order Processor into consideration and shall respect the Order Processor's confidentiality obligations. Section 8(b) applies for the facts identified during the course of the inspection.

(b) External inspection body: The Client has the right to have the inspection in accordance with section 7 carried out by an external, expert body bound to confidentiality. The costs incurred by the Client for the inspection shall be borne by the Client itself.

8. Confidentiality

(a) Order data: The Order Processor undertakes to treat order data as strictly confidential and to only make it accessible to persons within its organisation who need access to the order data in order to meet their obligations. It shall ensure that all persons with

access to order data are subject to a statutory or contractual obligation of confidentiality with regard to such data.

(b) Additional information: In addition, both Parties are subject to the statutory obligations of confidentiality applicable to them and agreed between them in the Service Agreement with respect to facts learned under this Agreement.

9. Final provisions

(a) Liability: Liability arising from breaches of this Agreement shall be subject to the liability regulations agreed for the services or applicable by law.

(b) Notices: The notices provided for in this Agreement must be made expressly and in text form (for example, by email or post), unless otherwise agreed.

(c) Changes and additions: Notwithstanding any written form requirements in the Contract, this Agreement may also be agreed or amended electronically between the Parties.

(d) Dispute resolution: The applicable law and place of jurisdiction are governed by the Service Level Agreement. However, the Client shall remain entitled to demand precautionary measures before any competent court and to assert its claims against the Order Processor before the court of the principal claim in the event of a claim made by a third party.

Appendix 1: Specification of the ODPA

Service	Categories of personal data	Persons concerned
Compendium.ch	Includes: eMediplan, Documedis CDS.CE, Documedis PCA.CE and Documedis Vac	Patients
Documedis eMediplan	Mandatory: Surname, first name and date of birth Optional: Further personal details and health information	Patients
Documedis ePrescription	Mandatory: Surname, first name, date of birth, address and patient's medication Optional: Other personal details	Patients
Documedis CDS.CE	Mandatory: Patient's medications Optional: Further patient data (personal details and health information), depending on the check to be carried out. Data logs: In order to guarantee patient security, anonymised data is required in accordance with the Medical Devices Ordinance (MedDO).	Patients
Documedis PCA.CE	Mandatory: Surname, first name and date of birth Optional: Other patient data (personal details, health information and medication of the patient). Data logs: In order to guarantee patient security, anonymised data is required in accordance with the Medical Devices Ordinance (MedDO).	Patients
pharmaVISTA	Includes: eMediplan, Documedis CDS.CE, Documedis PCA.CE, dispensing of Documedis ePrescription and PMC Polymedications Check	Patients
PMC Polymedications Check	Mandatory: Surname, first name and date of birth Optional: Patient's medication and other personal details	Patients
VAC Vaccination recording/documentation	Mandatory: Surname, first name and date of birth Optional: Vaccinations of the patient, answers to questions regarding the patient's state of health and other personal details	Patients

Appendix 2: Security requirements

This Appendix describes the technical and organisational measures which the Order Processor or HCI Solutions AG as subcontractor of the Order Processor take to ensure a level of protection appropriate to the risk.

(1) Pseudonymisation and encryption of personal data

- Where possible and compatible with the processing purpose, personal data is pseudonymised or encrypted, with assignment information or the key stored securely.

(2) Ability to ensure the long-term confidentiality, integrity, availability and resilience of systems and services in connection with processing

Access control – *unauthorised persons must be denied access to the facilities in which personal data is processed* – and **personal data carrier control** – *unauthorised persons must be prevented from reading, copying, changing or removing data carriers*:

- Access to the Galenica Ltd. buildings in Bern and Niederbipp is secured by badges. The procedure for issuing badges is described in controlled documents in the Galenica Ltd. management system.
- Access to the data centres of Galenica Ltd. is only granted for authorised badges and also requires a personal PIN code to be entered. The doors of the data centres are monitored by the IAS (intrusion alarm system) and an alarm sounds if a door remains open for more than 60 seconds. If the door remains open for a further 30 seconds, an intruder alarm is sent to Operations Technology.
- Visitors must log in and log out of a visitor book. Visitors to the building will be accompanied by an employee of Galenica Ltd.
- The data centres are monitored by video. The retention period and access to video data are defined in the management system of Galenica Ltd. in controlled documents.

Access control – *access by authorised persons is to be limited to the personal data they need to perform their tasks* –, **user control** – *the use of automated data processing systems by means of data transmission equipment by unauthorised persons is to be prevented* – and **storage control** – *unauthorised entry into storage and unauthorised inspection, modification or deletion of stored personal data must be prevented*:

- Access to personal data is based on a role-based access authorisation model. Each user receives an individual user ID.
- Rules on password complexity exist, compliance with which is technically enforced.
- The Galenica Group network is protected by a firewall, an intrusion detection system (IDS) as well as network segmentation.
- Virus scanners are used on all server and client systems operated by Galenica Ltd. and are regularly updated.
- The server and client systems operated by Galenica Ltd. are regularly patched
- If a client is inactive for more than 8 minutes, a password-protected screen-saver is activated.
- According to an internal guideline, clients are to be blocked by the operating system when they temporarily leave the workstation.
- The authorisations for basic IT services (Active Directory, VPN, FTP accounts) and for selected applications are reviewed once a year by the Data Governance Manager; any incorrectly existing access authorisations are withdrawn.

Transport control – *when disclosing personal data and transporting data carriers, unauthorised reading, copying, modification or deletion of the data must be prevented* – and **disclosure control** – *it must be possible to identify data recipients to whom personal data is disclosed using data transmission equipment*:

- Personal data is adequately protected against unauthorised access and intervention, for example, by means of transport encryption, signature, protected interface or other means. The identification of recipients of personal data is ensured as far as possible.
- If HCI is responsible for entering order data, measures are taken to ensure that it is entered correctly.

(3) Ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident

- Large parts of the IT infrastructure of Galenica Ltd. are designed as redundant. In particular, the server systems are mirrored in two geographically separate data centres depending on the defined availability requirements.
- Both data centres of Galenica Ltd. have a double (i.e. redundant) power supply, one of which is also connected to the UPS and emergency generator.
- Both data centres of Galenica Ltd. also have two separate Internet connections from different providers.
- Both data centres have redundant air conditioning systems independent of each other. The functionality of the redundancies is checked regularly.
- Both data centres have a three-stage fire extinguishing concept consisting of detection via an early fire detection system, a fire alarm system and active extinguishing.
- A backup concept for all server systems is in place and is described in the management system of Galenica Ltd. in controlled documents. Depending on the system and defined backup group, backups are carried out periodically at different intervals, ranging from quarter-hourly to once a day. Depending on the backup group, backups are retained for at least 5 days and, if required for an application, stored for the long-term. Backups written to tape are periodically outsourced to another, geographically separate location of the Galenica Group if they are required for an application.
- An emergency and crisis management system (E&C) is in place and is described in the management system of Galenica Ltd. in controlled documents. In particular, an emergency and crisis plan exists for the scenario. This manages communication and information in the event of a crisis, defines immediate and other reactive measures depending on various failure scenarios, describes scenarios of restricted IT operations, defines the priorities for restoring normal operations, and specifies requirements for testing and training of the procedure in the event of a crisis.

(4) Procedures for regularly reviewing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of processing

- All identified risks are listed in a risk register. This risk register is regularly reviewed, in a process in which the Head of HCI is involved. The Executive Committee of Galenica Ltd. is also informed every six months about the most important risks from the IT risk register.
- The emergency and crisis plan is updated once a year.

Appendix 3: Approved subcontractors

The following persons are deemed to be approved subcontractors in terms of section 6(b) of the Agreement:

Name and registered office	Country of processing	Services concerned	Task(s) of the Subcontractor
Galenica Ltd., Bern	Switzerland	IT infrastructure and Documedis hosting	Sales of the IT infrastructure and hosting of the Documedis eMediplan and CDS.CE applications
ISS	Switzerland	MepFlix for VacCheck	Sales of the IT infrastructure and hosting of the VacCheck application

Disclaimer: This document is a translation from German. In the event of ambiguities or differing interpretations, the wording in the original German version shall take precedence and should be regarded as authoritative.