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 unter der Berücksichtigung des Datenschutz-gesetzes und insbesondere der Bestimmungen von Art. 16 ff. bzw. Kapitel V EU-DSGVO zulässig.. Soweit hingegen eine solche Bekanntgabe von relevanten Daten vom Kunden gewünscht bzw. in seinem Auftrag erfolgt, obliegt die Ein-haltung 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.

(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. 5(b)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 HCI Solutions AG ergreift, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Durch den gemeinsamen Standort mit der Galenica AG teilt sich HCI Solutions zum grossen Teil Sicherheitsvorschriften.

(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