Auftragsverarbeitungsvereinbarung

1 Einleitung

Die vorliegende Auftragsverarbeitungsvereinbarung (nachstehend «**AVV**») ergänzt den Hauptvertrag hinsichtlich der Verarbeitung personenbezogener Daten in Bezug auf die Vorgaben insbesondere aus dem Schweizer Datenschutzgesetz (DSG) und der Datenschutzgrundverordnung der EU (EU-DSGVO) zur Verarbeitung von personenbezogenen Daten durch die bbv Software Services AG, Blumenrain 10, 6002 Luzern (nachstehend «**bbv**» oder «**Service-Anbieter**»). Es kann sich dabei um einen einzelnen oder mehrere Verträge zwischen bbv als dem Service-Anbieter und dem Kunden oder Auftraggeber handeln, sofern die bbv als Leistungserbringerin gegenüber dem Auftraggeber auftritt. Dabei gelten Offerten und Rechnungen als vertragliche Dokumente. Im Falle von Widersprüchen zwischen den Bestimmungen dieser AVV und den übrigen vertraglichen Regelungen zwischen den Parteien gehen die Regelungen dieser AVVs in Bezug auf die Verarbeitung von personenbezogenen Daten den anderen Verträgen vor. Diese AVV gilt für alle Verarbeitungen personenbezogener Daten, die bbv im Auftrag des Kunden als Auftragsverarbeiter durchführt.

In dieser AVV wird die Terminologie der EU-DSGVO verwendet, wobei die Verwendung der Terminologie der EU-DSGVO lediglich der Vereinheitlichung und Vereinfachung dienen soll. Die entsprechenden Begriffe umfassen, soweit anwendbar, zugleich die inhaltlich gleichwertigen oder vergleichbaren Begriffe des DSG, auch wenn diese dort abweichend bezeichnet werden. Verweise auf Begriffe der EU-DSGVO sind daher so auszulegen, dass sie die entsprechenden Konzepte des DSG miteinschliessen.

2 Gegenstand und Gültigkeit

Der Auftraggeber handelt als Verantwortlicher im Sinne der Datenschutzgesetze. Der Service-Anbieter handelt als Auftragsverarbeiter.

Der Gegenstand der Datenverarbeitung ergibt sich aus dem Hauptvertrag. Die Laufzeit dieser AVV entspricht der Laufzeit des Hauptvertrags, sofern sich aus den nachfolgenden Bestimmungen keine weitergehenden Verpflichtungen ergeben.

Die Kategorien der verarbeiteten personenbezogenen Daten, die Kategorien betroffener Personen sowie die zutreffenden technischen und organisatorischen Massnahmen sind Gegenstand dieser AVV.

3 Anwendungsbereich und Verantwortlichkeit

3.1 Rechtmässigkeit der Datenverarbeitung

Die Parteien bearbeiten personenbezogene Daten ausschliesslich rechtmässig und halten sich an die anwendbaren Datenschutzvorschriften und Grundsätze.

Der Service-Anbieter verarbeitet die personenbezogenen Daten ausschliesslich zum Zweck der Vertragserfüllung beziehungsweise zu den im Hauptvertrag genannten Zwecken, gemäss dieser AVV und den dokumentierten Weisungen und Instruktionen des Auftraggebers. Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen der anwendbaren Datenschutzgesetze, insbesondere der Rechtmässigkeit der Datenweitergabe, die Datenverarbeitung durch die bbv an sich, inklusive der Zulässigkeit der Auftrags- respektive Unterauftragsverarbeitung, allein verantwortlich.

Die Verarbeitung erfolgt grundsätzlich innerhalb der Schweiz oder des EWR. Sofern eine Verarbeitung in Drittländern erfolgt, stellt der Service-Anbieter sicher, dass hierfür ein angemessenes Datenschutzniveau gemäss DSG bzw. DSGVO besteht.

3.2 Zusätzliche Aufträge

Der Auftraggeber hat das Recht, dem Service-Anbieter jederzeit schriftlich zusätzliche Aufträge in Bezug auf die Verarbeitung der personenbezogenen Daten zu erteilen. Der Service-Anbieter kommt diesen Aufträgen nach, soweit diese im Rahmen der vertraglich vereinbarten Leistungen durch den Service-Anbieter umsetzbar und objektiv zumutbar sind. Führen solche Aufträge zu Mehrkosten für den Service-Anbieter oder einem geänderten Leistungsumfang, so ist das vertraglich vereinbarte Vertragsänderungsverfahren anwendbar.

3.3 Konformität der Aufträge

Der Service-Anbieter informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass ein Auftrag gegen das DSG oder die EU-DSGVO verstösst. Der Service-Anbieter darf in diesem Fall die Umsetzung des Auftrags so lange aussetzen, bis er vom Auftraggeber bestätigt oder abgeändert wurde, so dass diese rechtmässig ist.

Bei Aufträgen des Auftraggebers im Zusammenhang mit der Vergabe von Zugriffsberechtigungen oder der Herausgabe von personenbezogenen Daten an den Auftraggeber selbst gilt das Vorstehende nicht. Der Service-Anbieter darf jederzeit davon ausgehen, dass diese Aufträge gesetzeskonform sind. Er ist jedoch berechtigt, vom Auftraggeber entsprechende schriftliche Bestätigungen zu verlangen.

4 Art der verarbeiteten Daten

4.1 Allgemeines

Der Auftraggeber überlässt dem Service-Anbieter im Zusammenhang mit dem Hauptvertrag und seinem Auftrag personenbezogene Daten zur Verarbeitung. Dabei werden zwischen den Daten für administrative und kommerzielle Zusammenarbeit und Daten für die Erfüllung der vereinbarten Leistung unterschieden.

Der Service-Anbieter klassifiziert Systeme und Daten (personenbezogene und nicht personenbezogene Daten) für die Leistungserbringung, um sicherzustellen, dass die Informationen ein angemessenes Schutzniveau erhalten. Es wird in drei Kategorien der Informationsklassifizierung unterschieden:

- Vertraulich: Daten, die sich auf Personen beziehen und deren Privatsphäre betreffen (personenbezogene und besonders schützenswerte personenbezogene Daten) sowie explizit als vertraulich bezeichnete Daten.
- Intern: Daten, die keine personenbezogenen Daten betreffen, aber für die Auftragserfüllung relevant sind.
- Öffentlich: Informationen, die für alle zugänglich sind.

Personenbezogene Daten sind als vertrauliche Daten klassifiziert und geniessen damit den höchsten Schutz.

4.2 Betroffene Personen

Die Verarbeitung der personenbezogenen Daten durch den Service-Anbieter im Rahmen des Hauptvertrags betreffen die folgenden betroffenen Personen:

- Potenzielle Kunden, Kunden, Geschäftspartner, Lieferanten und Dienstleister.
- Mitarbeitende oder andere Hilfspersonen von potenziellen Kunden, Kunden, Geschäftspartnern, Lieferanten und Dienstleistern.
- Mitarbeitende oder andere Hilfspersonen des Kunden, welche durch den Kunden berechtigt wurden die Services zu nutzen.

4.3 Art von personenbezogenen Daten

Es kann sich bei der Verarbeitung von personenbezogenen Daten im Rahmen des Hauptvertrags insbesondere um folgende Arten von personenbezogenen Daten handeln:

- Kontaktdaten wie E-Mail-Adresse, Telefonnummer oder Adresse.
- Weitere Daten wie Vertrags-, Abrechnungs- oder Zahlungsdaten.
- Persönliche Informationen wie Vorname, Nachname, Geburtsdatum, Geschlecht oder Nationalität.
- Informationen über das Berufsleben wie Stellenbezeichnung oder Funktion.
- Benutzerinformationen wie Login Daten, Kundennummer, Personennummer oder Personalnummer.
- Technische Informationen wie IP-Adresse oder Geräteinformationen.
- Weitere personenbezogene Daten, die der Auftraggeber im Rahmen der Leistungserbringung zur Verfügung stellt.

4.4 Ausnahmen

Wurden die Daten durch den Auftraggeber verschlüsselt und sind sie für den Service-Anbieter daher nicht einsehbar, handelt es sich nicht um eine Auftragsdatenverarbeitung durch den Service-Anbieter. Ferner handelt es sich nicht um eine Auftragsdatenverarbeitung, wenn die personenbezogenen Daten durch den Auftraggeber direkt an einen Unterauftragsverarbeiter übergeben wurden und diese für den Service-Anbieter nicht zugänglich sind. In diesen Fällen ist die vorliegende AVV nicht anwendbar.

Der Service-Anbieter darf die personenbezogenen Daten des Auftraggebers (nachstehend auch «**Auftraggeber-Daten**») zu eigenen Zwecken anonymisieren, z.B. durch eine Aggregation der Daten, so dass die Identifizierung einzelner betroffener Personen nicht mehr möglich ist. Die Parteien stimmen darin überein, dass anonymisierte Auftraggeber-Daten nicht mehr dieser AVV unterstehen.

Sofern es sich um Daten handelt, die für die Leistungserbringung (z.B. Testdaten) durch den Kunden zur Verfügung gestellt werden oder die Mitarbeitenden des Service-Anbieters Zugang zu diesen Daten auf der Infrastruktur des Auftraggebers erhalten, so ist der Umgang mit diesen Daten im Hauptvertrag geregelt. Sollte dies nicht der Fall sein, gilt diese AVV subsidiär.

5 Sicherheitsmassnahmen des Service-Anbieters

5.1 Einhaltung der gesetzlichen Bestimmungen

Der Service-Anbieter verpflichtet sich, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die Auftraggeber-Daten nicht an Dritte weiterzugeben.

5.2 Technische und organisatorische Massnahmen (TOMs)

Der Service-Anbieter unterhält angemessene technische und organisatorische Massnahmen («**TOM**») und ein Qualitätsmanagement System. Das Information Security Management System («**ISMS**») ist integraler Bestandteil es Qualitätsmanagementsystems, das gemäss den ISO 9001 und ISO 13485 Standards zertifiziert ist. Das ISMS definiert die TOMs. Das Zertifikat ist auf der Webseite vom Service-Anbieter öffentlich abrufbar. bbv entwickelt ihr Informationssicherheitsmanagementsystem kontinuierlich weiter und richtet dieses an anerkannten Standards aus.

Die in **Anhang 1** beschriebenen Massnahmen sind generisch zu verstehen und gelten für die Fälle, in welchen der Service-Anbieter selbst personenbezogenen Daten verarbeitet. Sie kommen jeweils dann zur Anwendung, wenn im Hauptvertrag nichts Abweichendes definiert wird. Eine Änderung der getroffenen Sicherheitsmassnahmen bleibt bbv vorbehalten, wobei sichergestellt wird, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. bbv wird alle Personen, die Auftraggeber-Daten verarbeiten, zur Vertraulichkeit verpflichten.

Findet die Datenverarbeitung durch vom Service-Anbieter beauftragte Dritte statt, sorgt der Service-Anbieter mittels geeigneter vertraglicher Vereinbarungen dafür, dass die Dritten vergleichbare Massnahmen wie in dieser AVV einhalten.

Der Auftraggeber prüft, ob die beschriebenen technischen und organisatorischen Massnahmen seinen gesetzlichen und vertraglichen Anforderungen entsprechen.

6 Pflichten des Service-Anbieters

6.1 Datenverarbeitung

Der Service-Anbieter bearbeitet die relevanten Daten ausschliesslich gemäss den Bestimmungen aus dem Hauptvertrag und dieser AVV. Vorbehalten bleibt die Erfüllung gesetzlicher, regulatorischer oder behördlicher Verpflichtungen durch den Service-Anbieter.

6.2 Überprüfung der technischen und organisatorischen Massnahmen

Der Service-Anbieter überprüft periodisch die vereinbarten technischen und organisatorischen Massnahmen hinsichtlich dem aktuellen Stand der Technik und passt diese bei Bedarf an, um das in dieser AVV definierte Sicherheitsniveau nicht zu unterschreiten.

6.3 Verzeichnis von Verarbeitungstätigkeiten

Der Service-Anbieter verpflichtet sich, in Bezug auf die personenbezogenen Daten ein Verzeichnis der Verarbeitungstätigkeiten im Einklang mit Art. 12 Abs. 1 DSG bzw. Art. 30 Abs. 2 EU-DSGVO zu führen. Der Service-Anbieter gewährt dem Auftraggeber jederzeit auf Anfrage Einblick in die Teile dieses Verzeichnisses, die ihn betreffen.

6.4 Verschwiegenheitspflicht

Der Service-Anbieter stellt sicher, dass es den mit der Verarbeitung der personenbezogenen Daten des Auftraggebers befassten Mitarbeitenden und anderen Hilfspersonen vom Service-Anbieter untersagt ist, die personenbezogenen Daten zu anderen als den im Hauptvertrag genannten Zwecken und abweichend von dieser AVV zu verarbeiten.

Ferner stellt der Service-Anbieter sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben. Die Verschwiegenheitspflicht besteht auch nach Beendigung des Hauptvertrages fort.

6.5 Informationspflicht

Der Service-Anbieter unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der personenbezogenen Daten oder andere Unregelmässigkeiten bei der Verarbeitung der Auftraggeber-Daten durch bbv oder einem seiner Unterauftragsverarbeiter bekannt werden.

Der Service-Anbieter informiert den Auftraggeber schriftlich (E-Mail ausreichend) in angemessener Weise über Art und Ausmass der Verletzung sowie mögliche Abhilfemassnahmen. Die Parteien treffen in so einem Fall die erforderlichen Massnahmen zur Sicherstellung des Schutzes der personenbezogenen Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen sowie die Parteien und sprechen sich hierzu unverzüglich ab.

6.6 Ansprechpartner

Für Fragen in Zusammenhang mit dieser AVV kann sich der Auftraggeber an datenschutz@bbv.ch wenden, sofern der Hauptvertrag keinen abweichenden Kontakt definiert hat.

6.7 Datenlöschung

Relevante personenbezogene Daten sind nach Ende des Hauptvertrages gemäss den Bestimmungen im Hauptvertrag herauszugeben oder zu löschen, es sei denn, das anwendbare Recht schreibt die Aufbewahrung der personenbezogenen Daten für eine längere Zeitdauer vor. Der Service-Anbieter setzt für die Löschung von personenbezogenen Daten in der IT-Branche etablierte Verfahren ein.

7 Informationspflicht des Auftraggebers

Der Auftraggeber hat den Service-Anbieter unverzüglich zu informieren, wenn er in der Leistungserbringung vom Service-Anbieter Verletzungen datenschutzrechtlicher Bestimmungen feststellt.

Der Auftraggeber nennt dem Service-Anbieter den Ansprechpartner für im Rahmen des Hauptvertrages anfallende Datenschutzfragen sowie in den Fällen, in denen dies gemäss Art. 37 EU-DSGVO vorgeschrieben ist, den Datenschutzbeauftragten.

8 Anfragen von Drittpersonen

Wendet sich eine Drittperson mit Forderungen zur Berichtigung, Löschung, Auskunft oder anderen Ansprüchen zu personenbezogenen Daten direkt an den Service-Anbieter, wird der Service-Anbieter die Drittperson an den Auftraggeber verweisen, sofern eine Zuordnung zum Auftraggeber möglich ist.

9 Nachweismöglichkeiten, Berichte und Audits

Grundsätzlich erfolgt der Nachweis von angemessenen technischen und organisatorischen Massnahmen durch die Zertifizierung ISO/IEC 9001:2015 des Service-Anbieters. Im Hauptvertrag definierte Audit-Rechte sowie gesetzlich zwingend vorgeschriebene Prüfrechte des Auftraggebers oder seiner Aufsichtsbehörden bleiben vorbehalten. Im Rahmen solcher Audits sind ausdrücklich der Grundsatz der Verhältnismässigkeit einzuhalten sowie die schutzwürdigen Interessen vom Service-Anbieter (z.B. Verschwiegenheitspflicht) angemessen zu berücksichtigen. Der Auftraggeber trägt sämtliche Kosten solcher Audits (einschliesslich nachgewiesene interne Kosten vom Service-Anbieter zu seinen üblichen Stundensätzen, die bei der Mitwirkung am Audit entstehen).

Werden nach Vorlage von Nachweisen oder Berichten oder im Rahmen eines Audits Verletzungen dieser AVV oder Mängel bei der Umsetzung der Pflichten des Service-Anbieters festgestellt, so implementiert der Service-Anbieter geeignete Korrekturmassnahmen.

10 Unterauftragsverhältnisse

Soweit der Hauptvertrag keine einschränkenden Bestimmungen zum Beizug Dritter enthält, ist der Service-Anbieter zum Beizug von Unterauftragsverarbeitern berechtigt. Der Service-Anbieter stellt sicher, dass der Unterauftragsverarbeiter, soweit möglich, denselben Pflichten untersteht, wie sie bbv kraft dieser AVVs obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein dieser AVV entsprechendes Schutzniveau aufweist.

Die eingesetzten Unterauftragsverarbeiter sind nach Leistungsart kategorisiert und in **Anhang 2** aufgeführt. Die dort aufgeführten Unterauftragsverarbeiter gelten zum Zeitpunkt des Abschlusses des Hauptvertrags.

Der Service-Anbieter informiert den Auftraggeber über wesentliche Änderungen in Bezug auf die Hinzuziehung weiterer oder die Ersetzung vonService-Anbietern , die die Verarbeitung personenbezogener Daten betreffen.

11 Haftung

Der Auftraggeber und der Auftragsverarbeiter haften gegenüber betroffenen Personen entsprechend der im anwendbaren Datenschutzgesetz getroffenen Regelung. Der Auftragsverarbeiter stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.

Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist.

Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

12 Schlussbestimmungen

Sollten einzelne Bestimmungen dieser AVV unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des anwendbaren Datenschutzrechts am besten gerecht wird.

Änderungen zu dieser AVV vorbehältlich der in dieser AVV explizit ausgenommenen Ausnahmen bedürfen zur Gültigkeit der Schriftform.

Das anwendbare Recht und der Gerichtsstand richten sich nach dem Hauptvertrag, sofern in diesem Vertrag keine abweichenden Regelungen getroffen wurden.

Anhang 1 – Technische und organisatorische Massnahmen (TOM)

Der Service-Anbieter implementiert angemessene technische und organisatorische Massnahmen zum Schutz personenbezogener Daten gemäss den anwendbaren Datenschutzgesetzen sowie dem Stand der Technik.

Diese Massnahmen sind Bestandteil des Informationssicherheitsmanagementsystems (ISMS) des Service-Anbieters und unterliegen einer kontinuierlichen Überprüfung und Weiterentwicklung.

1. Vertraulichkeit

Die nachfolgend aufgeführten Massnahmen beschreiben die im Unternehmen umgesetzten Verfahren zur Sicherstellung der Vertraulichkeit von Personendaten. Sie dienen dazu, den Zugang zu Systemen sowie den Zugriff auf Personendaten auf berechtigte Personen zu beschränken und eine ausschliesslich autorisierte Nutzung der Daten sicherzustellen.

ID	Bestehend	Massnahme
1.1	☒	Zugriffsrechte werden nach dem Principle of Least Privilege (POLP) erstellt.
1.2	☒	Der Zugriff auf die Systeme des Service-Anbieters erfolgt ausschliesslich über eine dedizierte Infrastruktur mit starker Authentisierung. Es gilt die Zweifaktor-Authentifzierung.
1.3	☒	Der Zugriff über das Internet auf relevante Daten erfolgt in der Regel über eine verschlüsselte Verbindung. Dabei verwendet der Service-Anbieter aktuelle Protokolle und Schutzmechanismen.
1.4	☒	Bei der Übermittlung von Zugangsdaten werden getrennte Kommunikationskanäle eingesetzt.
1.5	☒	Es werden keine Wechseldatenträger zur Speicherung sensibler Informationen verwendet.
1.6	☒	Der Service-Anbieter stellt sicher, dass personenbezogene Daten von Auftraggebern nicht gegenseitig einsehbar sind. Mithilfe aktueller Sicherheitsverfahren wird auf logischer Ebene die Trennung von Kundendaten gewährleistet.
1.7	☒	Beim Austritt von Mitarbeitenden werden Zugriffsberechtigungen entzogen und betriebliche Arbeitsmittel zurückgegeben oder deaktiviert.

2. Verfügbarkeit

Die nachfolgend aufgeführten Massnahmen beschreiben die im Unternehmen umgesetzten Verfahren zur Sicherstellung der Verfügbarkeit und Belastbarkeit der Personendaten sowie der eingesetzten Systeme. Sie dienen dem Schutz von Datenträgern und gespeicherten Daten, der sicheren Übermittlung von Personendaten, der Wiederherstellung der Verfügbarkeit nach Störungen oder Ausfällen sowie der laufenden Aktualisierung und Absicherung der eingesetzten Systeme.

ID	Bestehend	Massnahme
2.1	☒	Der Service-Anbieter speichert Daten in Rechenzentren mit dem notwendigen Schutzniveau.
2.2	☒	Um die Verfügbarkeit der Daten zu gewährleisten, werden die Speichersysteme des Service-Anbieters so konfiguriert, dass eine oder mehrere Komponenten ausfallen können und die Daten trotzdem noch verfügbar sind.
2.3	☒	Der Service-Anbieter sichert die Daten gemäss der Servicebeschreibung. Dabei erfolgt die Sicherung immer auf separierten Speichersystemen in einem weiteren Rechenzentrum mit einer genügenden geografischen Distanz zwischen den beiden Standorten.
2.4	☒	Der Service-Anbieter hat die nötigen Prozesse implementiert, um Meldungen über Softwareschwachstellen und Patches zu identifizieren, zu bewerten und daraus notwendigen weiteren Schritte abzuleiten. Der Standard Patch-Management Prozess stellt sicher, dass Ankündigungen von Patches zu Systemen bewertet und nach einer Prüfung auf den relevanten Systemen installiert werden. Die Installation von Patches benötigt unter Umständen die Zusammenarbeit und Freigabe des Auftraggebers. Dies ist in den standardisierten Prozessen vom Service-Anbieter berücksichtigt. Falls ein Patch dringend installiert werden muss, gibt es je nach Service einen sogenannten Emergency Patch Prozess.

3. Integrität

Die nachfolgend aufgeführten Massnahmen dokumentieren die im Unternehmen umgesetzten Verfahren zur Sicherstellung der Integrität von Personendaten. Sie dienen dem Schutz von Personendaten bei der Übermittlung und Speicherung sowie der Nachvollziehbarkeit von Eingaben, Änderungen und Löschungen.

ID	Bestehend	Massnahme
3.1	☒	Die permanenten Speicher in den Rechenzentren werden mit physischen Schutzmassnahmen gegen Verlust geschützt.
3.2	☒	Datenträger werden bei Defekt vom Service-Anbieter physisch unbrauchbar gemacht, um einen möglichen Zugriff vollständig auszuschliessen.
3.3	☒	Funktionierende Datenträger werden mit branchenüblichen Löschverfahren so gelöscht, dass eine Rekonstruktion der beinhalteten Daten beinahe unmöglich ist. Ist ein solches Verfahren nicht möglich, werden die Datenträger physisch unbrauchbar gemacht, respektive zerstört.
3.4	☒	Der Service-Anbieter stellt für den Fall, in der Service-Anbieter für die Eingabe und Verarbeitung von personenbezogenen Daten zuständig ist, mit den notwendigen technischen und organisatorischen Massnahmen sicher, dass diese Daten korrekt erfasst und verarbeitet werden.
3.5	☒	Der Service-Anbieter erfasst für die Service-Erbringung weitere personenbezogene Daten des Auftraggebers. Diese Daten dienen zum Beispiel zur Erfassung von Störungsmeldungen, Änderungswünschen oder zur Rechnungsstellung. Der Service-Anbieter stellt durch geeignete Qualitätsmassnahmen sicher, dass diese Daten ebenfalls korrekt erfasst und verarbeitet werden.

4. Nachvollziehbarkeit

Die nachfolgend aufgeführten Massnahmen beschreiben die im Unternehmen umgesetzten Verfahren zur Überprüfung, Bewertung, Evaluierung und kontinuierlichen Verbesserung des Datenschutzes und der Informationssicherheit. Sie dienen der Sicherstellung und kontinuierlichen Verbesserung der technischen und organisatorischen Massnahmen.

ID	Bestehend	Massnahme
4.1	☒	Die Informationssicherheitsrichtlinie ist dokumentiert (ISMS).
4.2	☒	Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit sind schriftlich definiert und dokumentiert. Mitarbeiter sind darüber informiert, wo sie Sicherheitsvorfälle melden können.
4.3	☒	Es besteht ein dokumentierter Prozess für die Behandlung von Informationssicherheitsvorfällen. Sicherheitsvorfälle werden nach einem definierten Verfahren bearbeitet und dokumentiert.

5. Überprüfung, Bewertung, Evaluierung und Schulung

Die nachfolgend aufgeführten Massnahmen dokumentieren die im Unternehmen implementierten Verfahren zur Überprüfung, Bewertung, Evaluierung und Schulung im Bereich Datenschutz und Informationssicherheit.

ID	Bestehend	Massnahme
5.1	☒	Der Service-Anbieter kontrolliert periodisch die internen Prozesse sowie die technischen und organisatorischen Massnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.
5.2	☒	Basierend auf einer Risiko-Analyse werden neue Leistungen und Dienste einer technischen Prüfung unterzogen. Festgestellte Mängel werden von den verantwortlichen Stellen beim Service-Anbieter behoben. Je nach Schwere der Mängel wird eine ergänzende Prüfung durchgeführt, um die Wirksamkeit der Behebung nachzuweisen.
5.3	☒	Der Service-Anbieter führt periodisch interne und externe Audits zur Überprüfung und Optimierung der Informationssicherheit. Die festgestellten Mängel werden innerhalb des definierten Zeitrahmens behoben und je nach Schwere nochmals von der internen Auditstelle geprüft.

ID	Bestehend	Massnahme
5.4	☒	Der Service-Anbieter führt periodisch eine Risikobewertung durch. Ziel der Risikobewertung ist es, die potenziellen Informationssicherheitsrisiken und deren Auswirkungen und Eintrittswahrscheinlichkeit zu identifizieren. In einem periodisch wiederkehrenden Risikobewertungsbericht werden die Massnahmen beschrieben, die vom Service-Anbieter ergriffen werden, um das Risikopotenzial und deren Auswirkungen zu verringern.
5.5	☒	Neue Mitarbeitende vom Service-Anbieter werden vor Beginn ihrer Anstellung einer Prüfung unterzogen. Eine Geheimhaltungsklausel und die Datenschutzrichtlinien werden unterschrieben.
5.6	☒	Neue Mitarbeitende werden bei ihrem Arbeitsbeginn mit den relevanten Regeln zur eigenen Sicherheit und zur Datensicherheit vertraut gemacht.
5.7	☒	Bestehende Mitarbeitende vom Service-Anbieter erhalten periodisch ein Awareness Training.

Anhang 2 – Unterauftragsverarbeiter des Service-Anbieter im Rahmen der Leistungserbringung

Leistung in Bezug zum bbv AI Hub

Die nachfolgend aufgeführten Unterauftragsverarbeiter werden von der bbv eingesetzt, sofern die Leistungen durch im Rahmen des AI Hub Angebots erbracht werden. Die bbv ist darüber hinaus berechtigt, für andere Leistungen oder Angebote weitere Unterauftragsverarbeiter beizuziehen bzw. einzusetzen. In diesen Fällen findet ein anderer Auftragsdatenverarbeitungsvertrag für diese Leistungserbringung Anwendung.

Name des Unterauftragsverarbeiters	Adresse	Funktion	Massnahmen zur Sicherstellung eines geeigneten Datenschutzes
stepping stone AG	Wasserwerkgasse 7, CH-3011 Bern, Schweiz	Cloud Infrastructure as a Service, GPU-/Server-Infrastruktur für LLM-Dienste, LLM as a Service	Auftragsverarbeitungsvereinbarung (AVV), ISO/IEC 27001-zertifiziert, technische und organisatorische Massnahmen (TOM), Datenverarbeitung in Schweizer Rechenzentren
Phoenix Technologies AG	Churerstrasse 54 8808 Pfäffikon SZ, Schweiz	LLM as a Service	Auftragsverarbeitungsvereinbarung (AVV), ISO/IEC 27001 (sofern anwendbar), TOM nach Art. 32 DSGVO/DSG, Confidential Computing, Datenhaltung in Schweizer Sovereign Cloud
Infomaniak Network SA	Rue Eugène-Marziano 25, 1227 Les Acacias (Genf), Schweiz	LLM as a Service	Auftragsverarbeitungsvereinbarung (AVV), ISO/IEC 27001, technische und organisatorische Massnahmen (TOM), Datenverarbeitung in der Schweiz
OVHcloud SAS	2 Rue Kellermann, 59100 Roubaix, Frankreich	LLM as a Service	AVV (OVHcloud Data Processing Agreement), ISO/IEC 27001, ISO/IEC 27701 (für ausgewählte Dienste), ISO/IEC 27017, ISO/IEC 27018, technische und organisatorische Massnahmen (TOM), Standardvertragsklauseln (SCC)

Leistung in Bezug zum Swiss LCDM Hub

Die nachfolgend aufgeführten Unterauftragsverarbeiter werden von der bbv eingesetzt, sofern die Leistungen durch im Rahmen des Swiss LCDM Hub Angebots erbracht werden. Die bbv ist darüber hinaus berechtigt, für andere Leistungen oder Angebote weitere Unterauftragsverarbeiter beizuziehen bzw. einzusetzen. In diesen Fällen findet ein anderer Auftragsdatenverarbeitungsvertrag für diese Leistungserbringung Anwendung.

Name des Unterauftragsverarbeiters	Adresse	Funktion	Massnahmen zur Sicherstellung eines geeigneten Datenschutzes
Microsoft Schweiz GmbH	Microsoft Schweiz GmbH, The Circle, Postfach, 8058 Zürich-Flughafen, Schweiz	Cloud Services (z. B. Microsoft Azure, Microsoft 365)	AVV (Microsoft DPA), ISO/IEC 27001, ISO/IEC 27701, SOC 1/2, technische und organisatorische Massnahmen (TOM)

Leistung in Bezug zur Dienstleistungserbringung

Name des Unterauftragsverarbeiters	Adresse	Funktion	Massnahmen zur Sicherstellung eines geeigneten Datenschutzes
Microsoft Schweiz GmbH	Microsoft Schweiz GmbH, The Circle, Postfach, 8058 Zürich-Flughafen, Schweiz	Cloud Services (z. B. Microsoft Azure, Microsoft 365)	AVV (Microsoft DPA), ISO/IEC 27001, ISO/IEC 27701, SOC 1/2, technische und organisatorische Massnahmen (TOM)
Kudelski Security SA	Route de Genève 22–24, 1033 Cheseaux-sur-Lausanne, Schweiz	Security Monitoring (SOC), Managed Detection & Response (MDR), Security Operations	AVV, ISO/IEC 27001, technische und organisatorische Massnahmen (TOM), Vertraulichkeitsverpflichtungen
Open Systems AG	Räffelstrasse 29, 8045 Zürich, Schweiz	Managed Security Services, IT Monitoring, Firewalls, Secure Access Service Edge (SASE)	AVV, ISO/IEC 27001, technische und organisatorische Massnahmen (TOM), Datenverarbeitung gemäss vertraglichen Weisungen
Slack Technologies Limited (Salesforce-Gruppe)	Salesforce Tower, 60 R801, North Dock, Dublin 1, D01 W028, Irland	Kollaborations- und Kommunikationsplattform (Team-Chat, Datei- und Dokumentenaustausch, Audio-/Videokonferenzen)	AVV (Slack Data Processing Addendum), EU Standardvertragsklauseln (SCC), technische und organisatorische Massnahmen (TOM), ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2 Type II
Net Solutions AG	Früebergstrasse 47, 6340 Baar, Schweiz	Managed IT Services, Systembetrieb, Support	AVV, technische und organisatorische Massnahmen (TOM), Vertraulichkeitsverpflichtungen

Acronis International GmbH	Rheinweg 9, 8200 Schaffhausen, Schweiz	Backup	AVV (Acronis Data Processing Addendum), ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2 Type II, technische und organisatorische Massnahmen (TOM), Verschlüsselung der Daten bei Übertragung und Speicherung