AGB Smartbridge AG, Anhang 1

Datenschutzvereinbarung

Inhaltsverzeichnis

1 PRÄAMBEL 2

2 GEGENSTAND, DAUER UND SPEZIFIZIERUNG DER AUFTRAGSBEARBEITUNG 2

3 KATEGORIEN VON BETROFFENEN PERSONEN UND PERSONENDATEN 2

4 ANWENDUNGSBEREICH UND VERANTWORTLICHKEIT 2

5 PFLICHTEN VON SMARTBRIDGE 4

6 PFLICHTEN DES KUNDEN 5

7 ANFRAGEN BETROFFENER PERSONEN 5

8 AUDIT / INSPEKTION 6

9 SUBUNTERNEHMER (WEITERE AUFTRAGSBEARBEITER) 6

10 ORT DER DURCHFÜHRUNG DER DATENBEARBEITUNG 7

11 SCHRIFTFORMKLAUSEL, RECHTSWAHL 7

1 Präambel

(a) Die vorliegende Datenschutzvereinbarung konkretisiert die Pflichten der Parteien in Bezug auf datenschutzrechtliche Aspekte basierend auf den Vorgaben der europäischen Datenschutzgrundverordnung (DSGVO) sowie des Schweizer Datenschutzgesetzes (Stand 2023) und ergänzt die vertraglichen Bestimmungen unter dem zwischen den Parteien abgeschlossenen Hauptvertrag und den zugehörigen Allgemeinen Geschäftsbedingungen von Smartbridge, welche integrierenden Bestandteil des Hauptvertrags bilden. Diese Datenschutzvereinbarung findet Anwendung auf alle Tätigkeiten unter dem Hauptvertrag, bei denen der Kunde und Smartbridge personenbezogene Daten des Kunden bearbeiten.

2 Gegenstand, Dauer und Spezifizierung der Auftragsbearbeitung

(a) Der Kunde ist für die Rechtmässigkeit der Datenbearbeitung an sich, inklusive der Zulässigkeit der Auftragsbearbeitung, verantwortlich. Smartbridge bearbeitet die Daten des Kunden ausschliesslich zu den im Hauptvertrag genannten Zwecken. Vorbehalten bleibt die Erfüllung gesetzlicher, regulatorischer oder behördlicher Verpflichtungen durch Smartbridge.

(b) Die Laufzeit dieser Datenschutzvereinbarung richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieser Datenschutzvereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.

3 Kategorien von betroffenen Personen und Personendaten

(a) Die Kategorien von betroffenen Personen und Personendaten, welche im Rahmen des Hauptauftrags von Smartbridge im Auftrag des Kunden bearbeitet, sind in Annex 1 aufgeführt.

4 Anwendungsbereich und Verantwortlichkeit

(a) Smartbridge bearbeitet personenbezogene Daten im Auftrag des Kunden. Dies umfasst Tätigkeiten, die im Hauptvertrag bzw. den AGB konkretisiert sind. Der Kunde bleibt für die Einhaltung des Datenschutzes verantwortlich und entscheidet allein über Zwecke und Mittel der Bearbeitung der Personendaten, die er an Smartbridge übergibt („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO und Art. 5 lit. j DSG). Der Kunde ist im Rahmen dieser Datenschutzvereinbarung für die Einhaltung der auf ihn vorliegend anwendbaren gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmässigkeit der Datenweitergabe an Smartbridge sowie für die Rechtmässigkeit der Datenbearbeitung allein verantwortlich.

(b) Der Kunde verpflichtet sich und gewährleistet insbesondere, dass

(i) die Datenbearbeitung und die dazugehörigen Aufträge an Smartbridge gesetzeskonform sind;

(ii) er die für eine gesetzeskonforme Bearbeitung der Personendaten durch Smartbridge (einschliesslich Bekanntgabe an Smartbridge) allenfalls erforderlichen Meldungen, Registrierungen, aufsichtsrechtlichen Anerkennungen und Genehmigungen eingeholt hat.

(iii) er die gesetzlich notwendigen Einwilligungen der Betroffenen eingeholt hat und seinen diesbezüglichen Informationspflichten vollumfänglich nachgekommen ist, insbesondere indem er die Betroffenen über den Verantwortlichen, den Zweck der Datenerhebung, allfällige Rechtfertigungsgründe für die Datenerhebung, die Kategorie von Datenempfänger, mögliche Transfers der Daten in Drittstaaten, die Dauer der Datenaufbewahrung, die Auskunfts-, Berichtigungs-, und Löschungsrechte, und die Möglichkeit der Beschwerde an die zuständige Datenschutzbehörde informiert hat. Auf Wunsch des Kunden kann die eingeholte Einwilligung in das Applikation von Smartbridge integriert werden, damit der Kunde die Einwilligungen aktenkundig jederzeit zur Verfügung hat.

(c) Der Kunde trifft in seinem Verantwortungsbereich (z.B. auf seinen eigenen Systemen, Gebäuden, Applikationen/Umgebungen in seiner Betriebsverantwortung) selbständig angemessene technische und organisatorische Massnahmen zum Schutz der relevanten Daten. Der Kunde ist primär für die Einhaltung der datenschutzrechtlichen Vorgaben, insbesondere auch für die Einhaltung des Datenschutzes im Arbeitsverhältnis bzw. Beschäftigtendatenschutzes, verantwortlich.

(d) Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Kunden danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die von Smartbridge bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Mündliche Weisungen hat der Kunde unverzüglich schriftlich / in Textform zu bestätigen. Smartbridge informiert den Kunden unverzüglich, wenn Smartbridge der Auffassung ist, dass eine Weisung gegen die DSGVO, das Schweizer DSG oder andere anwendbare Datenschutzgesetze verstösst. Smartbridge darf diesfalls die Umsetzung der Weisung solange aussetzen, bis diese vom Kunden schriftlich bestätigt oder abgeändert wurde. Smartbridge darf bei Weisungen des Kunden im Zusammenhang mit der Vergabe von Zugriffsberechtigungen oder der Herausgabe von relevanten Daten an den Kunden selbst davon ausgehen, dass diese Weisungen gesetzeskonform sind.

(e) Führen solche Weisungen zu Mehrkosten von Smartbridge oder einem geänderten Leistungsumfang, so sind die Parteien verpflichtet, einen entsprechenden Nachtrag zum Hauptvertrag einzugehen.

5 Pflichten von Smartbridge

(a) Datenschutz und Datensicherheit sind für Smartbridge höchste Priorität. Smartbridge hält sich strikt an die geltenden Datenschutzgesetze in der Schweiz. Smartbridge hat wird die innerbetriebliche Organisation so gestaltet, dass diese den Anforderungen des Datenschutzes gerecht wird. Smartbridge hat technische und organisatorische Massnahmen getroffen, welche die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Datenbearbeitung auf Dauer sicherstellen. Diese Massnahmen werden in Annex 2 detailliert beschrieben. Dem Kunden sind diese technischen und organisatorischen Massnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu bearbeitenden Daten ein angemessenes Schutzniveau bieten.

(b) Eine Änderung der getroffenen Sicherheitsmassnahmen bleibt Smartbridge vorbehalten, wobei jedoch sichergestellt wird, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen, von denen Smartbridge annimmt, dass sie für den Kunden von Interesse sein könnten, weil sie bspw. Auswirkungen auf die Nutzung durch den Kunden haben oder solche, die darin resultieren, dass der Kunden Anpassungen vornehmen muss, teilt Smartbridge dem Kunden mit.

(c) Smartbridge unterstützt soweit vereinbart den Kunden im Rahmen ihrer Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche von betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Artt. 33 bis 36 DSGVO genannten Pflichten bzw. den entsprechenden Bestimmungen des DSG. Solche Zusatzaufwände stellt Smartbridge dem Kunden separat in Rechnung.

(d) Smartbridge gewährleistet, dass es den mit der Bearbeitung der Daten des Kunden befassten Mitarbeitern und anderen für Smartbridge tätigen Personen untersagt ist, die Daten ausserhalb der Weisungen des Kunden zu bearbeiten. Ferner gewährleistet Smartbridge, dass sich die zur Bearbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Geheimhaltungspflicht unterliegen. Die Vertraulichkeits-/ Geheimhaltungspflicht besteht auch nach Beendigung des Auftrages fort.

(e) Smartbridge unterrichtet den Kunden unverzüglich, wenn ihr Verletzungen des Schutzes personenbezogener Daten des Kunden bei Smartbridge oder einem Subunternehmer bekannt werden. Smartbridge informiert den Kunden in angemessener

Weise über Art und Ausmass der Verletzung sowie mögliche Abhilfemassnahmen um den Kunden in die Lage zu versetzen, seinen Pflichten im Zusammenhang mit Datensicherheitsverletzungen, insbesondere Meldepflichten, nachkommen zu können. Die Parteien treffen in so einem Fall die erforderlichen Massnahmen zur Sicherstellung des Schutzes der relevanten Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

(f) Smartbridge nennt dem Kunden den Ansprechpartner für im Rahmen des Hauptvertrages anfallende Datenschutzfragen.

(g) Smartbridge gewährleistet, ein Verfahren zur regelmässigen Überprüfung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Bearbeitung einzusetzen.

(h) Smartbridge berichtigt oder löscht die relevanten Daten, wenn der Kunde dies anweist und dies vom Weisungsrahmen umfasst ist. Zusatzaufwände stellt Smartbridge dem Kunden gemäss den geltenden Ansätzen in Rechnung.

(i) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen und Kosten des Kunden entweder herauszugeben oder zu löschen. Smartbridge setzt dabei branchenübliche Verfahren ein.

(j) Im Falle einer Inanspruchnahme des Kunden durch eine betroffene Person hinsichtlich Ansprüche nach Art. 82 DSGVO oder Art. 28 ZGB, verpflichtet sich Smartbridge, den Kunden auf dessen Kosten bei der Abwehr des Anspruches im Rahmen ihrer Möglichkeiten zu unterstützen.

6 Pflichten des Kunden

(a) Der Kunde hat Smartbridge unverzüglich und vollständig zu informieren, wenn er bei der Erbringung der vertraglichen Leistungen gemäss Hauptvertrag Fehler oder Unregelmässigkeiten betreffend datenschutzrechtlicher Bestimmungen feststellt.

(b) Der Kunde nennt Smartbridge den Ansprechpartner für im Rahmen des Hauptvertrages anfallende Datenschutzfragen (vgl. AGB Ziffer „Mitteilungen“).

7 Anfragen betroffener Personen

(a) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an Smartbridge, wird Smartbridge die betroffene Person an den Kunden verweisen, sofern eine Zuordnung an den Kunden nach Angaben der betroffenen Person möglich ist. Smartbridge leitet den Antrag der betroffenen Person

unverzüglich an den Kunden weiter. Smartbridge unterstützt den Kunden im Rahmen ihrer Möglichkeiten. Smartbridge haftet nicht, wenn das Ersuchen der betroffenen Person vom Kunden nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

8 Audit / Inspektion

(a) Smartbridge weist dem Kunden auf Wunsch die Einhaltung der in dieser Datenschutzvereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach.

(b) Sollten im Einzelfall Audits bei Smartbridge durch den Kunden oder einen von diesem beauftragten unabhängigen externen Prüfer erforderlich sein, werden diese nach Voranmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit zu den üblichen Geschäftszeiten von Smartbridge ohne Störung ihres Betriebsablaufs durchgeführt. Smartbridge darf diese von der Voranmeldung mit angemessener Vorlaufzeit sowie von der Unterzeichnung einer Geheimhaltungserklärung abhängig machen. Sollte der durch den Kunden beauftragte Prüfer in einem Wettbewerbsverhältnis zu Smartbridge stehen, hat Smartbridge ein Einspruchsrecht.

(c) Der Kunde stellt Smartbridge eine Kopie des Auditberichts des beauftragten Prüfers zur Verfügung.

(d) Der Aufwand eines Audits ist für Smartbridge grundsätzlich auf einen Tag pro Kalenderjahr begrenzt. Für die Unterstützung bei der Durchführung des Audits stellt Smartbridge eine Vergütung in Rechnung.

(e) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Kunden eine Inspektion vornehmen, gilt grundsätzlich Ziffer 8(b) entsprechend. Eine Unterzeichnung einer Geheimhaltungserklärung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Geheimhaltung unterliegt, bei der ein Verstoss strafbewehrt ist.

9 Subunternehmer (weitere Auftragsbearbeiter)

(a) Die vertraglich vereinbarten Leistungen werden unter Beizug der in Annex 3 aufgeführten Subunternehmer durchgeführt.

(b) Smartbridge informiert den Kunden über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern via E-Mail. Hierfür muss sich der Kunde im Informationssystem von Smartbridge registrieren. Dieses wird ihm während des Onboardings gezeigt. Der Kunde kann gegen derartige Änderungen innert 30 Tagen ab Mitteilung Einspruch erheben. In diesem Fall gilt der Hauptvertrag

und diese Datenschutzvereinbarung per Datum des Beizugs des neuen Subunternehmens ausserordentlich gekündigt.

(c) Smartbridge hat Subunternehmer vertraglich zu verpflichten, die nach dieser Datenschutzvereinbarung dem Kunden gegenüber bestehenden Pflichten ihrerseits zu erfüllen. Smartbridge wird insbesondere hinreichende Garantien dafür vorsehen, dass die geeigneten technischen und organisatorischen Massnahmen so durchgeführt werden, dass die Bearbeitung entsprechend den einschlägigen Datenschutzbestimmungen und des Hauptvertrages erfolgt.

10 Ort der Durchführung der Datenbearbeitung

(a) Die Datenbearbeitungstätigkeiten haben grundsätzlich in der Schweiz und/oder im Europäischen Wirtschaftsraum (EWR) zu erfolgen. Datenbearbeitungstätigkeiten ausserhalb dieses Gebiets sind nur zulässig, wenn die Vorgaben dieses Vertrages eingehalten und vorgängig geeignete Massnahmen zur Wahrung der gesetzlichen Vorgaben getroffen wurden. Konkret muss ein Angemessenheitsbeschluss der zuständigen Behörde vorliegen. Fehlt ein solcher, hat die Übermittlung von Personendaten auf Grundlage geeigneter Garantien (insbesondere von der Europäischen Kommission und dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten [EDÖB] genehmigten Standardvertragsklauseln) zu erfolgen oder es bestehen Ausnahmeregelungen für bestimmte Situationen (Vertragsabwicklung, Rechtsdurchsetzung im Ausland etc.).

11 Schriftformklausel, Rechtswahl

(a) Änderungen und Ergänzungen dieser Datenschutzvereinbarung bedürfen einer schriftlichen Vereinbarung (die auch in einem elektronischen Format (Textform) erfolgen kann) und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(b) Bei etwaigen Widersprüchen gehen Regelungen dieser Datenschutzvereinbarung den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Datenschutzvereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Datenschutzvereinbarung im Übrigen nicht.

(c) Es gilt Schweizer Recht.

Annex 1: Kategorien von betroffenen Personen und Personendaten

Im Rahmen der Auftragsbearbeitung gemäss Hauptvertrag sind folgende Personenkategorien betroffen:

(d) Personal, welches über eine Applikation von Smartbridge vermittelt oder dessen Einsatz geplant werden soll;

(e) Sonstige für den Kunden tätige Personen;

(f) Kunden und Interessenten des Kunden.

Im Rahmen der Auftragsbearbeitung werden im Wesentlichen folgende Kategorien von Personendaten bearbeitet:

(a) Stammdaten, Namen, Adressdaten, E-Mail-Adressen, Telefonnummern;

(b) Fotos, Arbeitsverträge und dazugehörige Dokumente wie Lebensläufe, Arbeitszeugnisse und Ausbildungszertifikate, Bewertungen;

(c) Lohnrelevante Daten, Bankverbindungen und sonstige Lohn- und Finanzdaten.

Annex 2: Technische und organisatorische Massnahmen des Datenschutzes (TOM)

Smartbridge verpflichtet sich, bei der Bearbeitung von Personendaten die nachfolgenden technischen und organisatorischen Massnahmen umzusetzen und dem aktuellen Stand der Technik jeweils anzupassen.

1 Zugangskontrollen

Mit folgenden Massnahmen wird sichergestellt, dass unberechtigte Personen keinen Zugang erhalten zu den Einrichtungen, in denen Personendaten bearbeitet werden:

(a) Der Zutritt zu den Räumlichkeiten von Smartbridge ist nur mit einer berührungslosen und personalisierten Chipkarte möglich. Zwei Sicherheitstüren (Haupteingang und Büroeingang) können nur mit Chipkarte geöffnet werden.

(b) Zugangskontrollen bei den Data Centers erfolgt gemäss den Bestimmungen der beigezogenen Subunternehmer, siehe Ziffer 9 der Datenschutzvereinbarung.

2 Physische Verfügbarkeitssicherung

(a) Verfügbarkeitssicherstellung erfolgt gemäss den Bestimmungen der beigezogenen Subunternehmer, siehe Ziffer 9 der Datenschutzvereinbarung.

(b) Smartbridge verfügt über keinen root Zugriff auf die Infrastruktur von AWS, sondern erfolgt nach dem Prinzip der geringsten Privilegien (PoLP) und ist beschränkt auf die Privilegien, die das Entwicklungsteam braucht, um ihre Arbeit durchzuführen.

3 Berechtigungen

(a) Mittels folgender technischer Massnahmen wird sichergestellt, dass unbefugtes Bearbeiten verhindert wird:

3.1 Authentifizierung

(a) Zugang zur Infrastruktur auf Staffcloud wird von Skaylink gemäss ihren AGB (siehe Ziffer 9 der Datenschutzvereinbarung) kontrolliert. Entwickler und Mitarbeiter von Smartbridge haben nur die nötigsten Privilegien, um ihre Arbeit zu erledigen (PoLP):

(i) Auf allen Rechnern und Servern wird Benutzerkennung mit Passwort verlangt;

(ii) Zugang auf Server sind zudem nur per persönlichem Zertifikat und von einem definierten Jumphost möglich. Auf die Jumphosts haben nur Personen mit freigeschaltetem Account (Username/Passwort) Zugriff, welche sich zusätzlich durch ein Zertifikat oder OneTimeToken ausweisen können;

(iii) Servermanagement über SSH.

(b) Zudem wird auch in den Räumlichkeiten von Smartbridge für den Zugang zu Rechnern und Servern immer Benutzerkennung mit Passwort verlangt. Das Netzwerk in den Räumlichkeiten von Smartbridge ist ferner mit einer Firewall geschützt.

(c) Kunden-Authentifizierung beim Staffcloud-Login: 2-Factor-Authentifizierung wird unterstützt.

(d) Staffcloud ist keine öffentliche Plattform. Alle Bereiche (Kunden- oder Mitarbeiterbereich) sind nur über eine Authentifizierung zugänglich.

3.2 Berechtigungskonzepte

(a) Registrierung, Rechtezuteilung und Rechtevergabe für Administratoren sind auf Prozessebene getrennt.

(b) Zugriff auf Kundendaten ist nur möglich unter Verwendung besonderer Support-Zugänge, bei welchen alle Bearbeitungsvorgänge protokolliert werden.

4 Weitergabekontrolle und Verschlüsselung

(a) Alle Daten inklusive Personendaten werden im Ruhezustand und bei der Übertragung nach dem Stand der Technik verschlüsselt.

5 Trennungskontrolle

(a) Die Datenbanken verschiedener Kunden sind getrennt.

6 Nachvollziehbarkeit

(a) Logdaten erlauben die nachträgliche Kontrolle aller Zugriffe auf und Übermittlungen von Personendaten von Kunden und deren Zuordnung zum entsprechenden Mitarbeitenden.

(b) Die Logdaten werden 90 Tage gespeichert.

(c) Die Protokolldateien werden mit einem Zeitstempel versehen und sind nur über SSH mit einem autorisierten SSL-Schlüssel zugänglich.

(d) Die Anwendung wird auf Linux-Maschinen gehostet, so dass verschiedene Aktionen wie Authentifizierungsversuche, Sudo-Zugriff und SSH-Anmeldungen protokolliert werden.

(e) Basierend auf dem Prinzip der geringsten Rechte haben die Benutzer keine Rechte, um Systemressourcen zu ändern oder zu löschen, einschliesslich der Protokolldateien.

(f) Auf der Grundlage von Protokollen und anderen Ressourcen gibt es Überwachungssysteme, um mögliche verdächtige Aktivitäten zu erkennen und diese zu melden und zu verhindern.

7 Vertragliche Verpflichtungen von Mitarbeitenden

(a) Der Zugriff der berechtigten Personen wird auf diejenigen Personendaten beschränkt, die sie für die Erfüllung ihrer Aufgabe benötigen. Dies wird unter anderem (zusätzlich zu den Massnahmen unter Ziffer 3 oben) mit folgenden Massnahmen sichergestellt:

(i) Schriftliche Verpflichtung der Mitarbeitenden zur Einhaltung des Datenschutzes, bzw. des Datengeheimnisses gemäss Ziffer 3 oben; Smartbridge hat eine Richtlinie zur Informationssicherheit und eine Richtlinie zur akzeptablen Nutzung erstellt und dokumentiert, die beide von der Geschäftsleitung genehmigt und gemäss ISO 27002 A.5.1.1 an alle Mitarbeiter weitergegeben werden.

(ii) Zugang zu Personendaten für Mitarbeitende nur auf einer "need-to-know"-Basis.

(iii) Wir haben einen eigenen Sicherheitskoordinator, die für die Koordinierung von Reaktionen auf Vorfälle und Datenschutzanfragen zuständig sind, in Übereinstimmung mit ISO 27002 6.1.1.

(iv) Es gibt ein Datenschutzinformationssystem (Privacy Information Management System, PIMS), das die Einhaltung der anwendbaren Datenschutzgesetze, die Identifizierung und Kontrolle von personenbezogenen Daten, die Zugriffsverwaltung, Datenschutzrichtlinien, einen Notfallplan und einen benannten Datenschutzbeauftragten gemäss ISO 27701 6.4.2.2 umfasst und für die Mitarbeiter einsehbar ist.

8 Weitere Schutzmassnahmen

(a) Ferner bilden folgende Massnahmen Teil der umfassenden Datensicherheitsmassnahmen von Smartbridge:

(i) Regelmässige Sicherheitsaudits.

(ii) Die Mitarbeiter werden regelmässig über potenzielle Risiken, Schwachstellen und Handhabungsverfahren informiert, was den Schulungsaspekt von ISO 27002 7.2.2 widerspiegelt.

(iii) Dokumentierte Geschäftskontinuitäts- und IT-Notfallpläne sind in Kraft.

(iv) Die IT-Infrastruktur wird von einem nach ISO 27001, 9001, 20000-1 und 22301 zertifizierten spezialisierten Partner und Amazon Web Services verwaltet, der die Einhaltung von ISO 27002 17.1.1 und 17.1.2 nachweist.

(v) Die Informationssicherheit ist integraler Bestandteil unseres Entwicklungszyklus, wobei wir bewährte Sicherheitspraktiken, Code-Reviews, automatisierte Schwachstellentests und ein Authentifizierungs- und Autorisierungssystem im Einklang mit den ISO 27002-Klauseln 14.2.1, 14.2.5 und 14.2.6 einsetzen.

9 Vorkehrungen bei technischen Vorfällen

Für technische Vorfälle gibt es einen dokumentierten Prozess, der eine effiziente und ordnungsgemässe Verwaltung von Sicherheitsvorfällen gewährleistet und ein wesentlicher Bestandteil unserer Sicherheitsstrategie ist.

Annex 3: Subunternehmer

Smartbridge zieht für die Erbringung der Leistungen gemäss Hauptvertrag die folgenden Subunternehmer bei:

Vertragspartner	**Rolle und betroffene Leistungen**	**Art und Kategorie der betroffenen Personendaten**	**Ort der Datenbearbeitung**
Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109, United States. Amazon Web Services, Inc. ist eine nach dem Recht des Staates Delaware gegründete und registrierte Gesellschaft (Registernummer: 4152954, Secretary of State, State of Delaware)	Datacenter Services	Alle Daten gemäss Annex 1 der Smartbridge Datenschutzvereinbarung	Frankfurt, Deutschland (s.u.)
Skaylink GmbH Zielstattstr. 42 81379 München	Implementiert und betreibt skalierbare Cloud-Hosting-Lösungen auf Basis von Amazon Web Services (AWS) als Amazon Web Partner. Die Dienstleistungen beinhalten insbesondere: Core Compliance Core Security Standart Logging Standard DDoS-Protection	Alle Daten gemäss Annex 1 der Smartbridge Datenschutzvereinbarung	Frankfurt, Deutschland https://www.skaylink.com/de/datenschutzhinweise/
ActiveCampaign, 1 North Dearborn Street, 5th floor, Chicago, IL 60602 privacy@activecampaign.com	ActiveCampaign betreibt den E-Maildienst Postmark	E-Mail Versand aus Staffcloud	Chicago, USA DPA und SCC gemäss: https://postmarkapp.com/eu-privacy https://postmarkapp.com/dpa https://postmarkapp.com/support/article/1218-gdpr-faq

			Aufbewahrungsdauer: 45 Tage Speicherung E-Mails bei Postmark, 45 Tage +1Löschung aller E-Mail + Log. https://post-markapp.com/terms-of-service
Hubspot GmbH, Am Postbahnhof 17, 10243 Berlin	Hubspot ist ein CRM, um Kundendaten zu verwalten. Smartbridge verwendet es für die Zusammenarbeit mit dem Kunden.	Vor- und Nachname, E-Mailadresse und Telefonnummer, Firmenname des Kunden.	Auf AWS-Servern in der EU Hubspot Regional Data Policy https://knowledge.hubspot.com/account-security/hubspot-cloud-infrastructure-and-data-hosting-frequently-asked-questions
Syncfunction Inc. 2501 Aerial Center Parkway Suite 111 Morrisville, North Carolina 27560, USA	Bolddesk ist ein Support System. Smartbridge nutzt das System um die Support-Anfragen der Kunden zu beantworten. Es werden dabei nur Personendaten der Ansprechpersonen beim Kunden (Personal) bearbeitet. https://www.bold-desk.com/legal/privacy-policy	E-Mailadresse des Kunden	EEA DPA und SCC gemäss https://www.bold-desk.com/legal/privacy-policy
JoinCube, Inc. 3500 S Dupont Hwy Dover, DE, 19901-6041 United States	JoinCube betreibt den Informationsdienst Get Beamer. Dies ist das Informationssystem von Smartbridge für ihre Kunden.	E-Mailadresse des Kunden	DPA und SCC gemäss https://www.getbeamer.com/privacy-policy

Zu den von AWS erbrachten Data Center Services stellt AWS die folgenden Informationen zur Verfügung:

(a) Standardvertragsklauseln (SCCs): AWS integriert SCCs in ihr Datenverarbeitungsaddendum (DPA), um legale Datentransfers aus der EU in Länder ausserhalb des EWR zu ermöglichen (Amazon Web Services) https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/aws-data-processing-addendum-dpa.html

(b) Ergänzende Massnahmen: AWS hat technische und organisatorische Massnahmen zum Schutz von Daten implementiert. Dazu gehören starke Verschlüsselung sowohl

während der Übertragung als auch im Ruhezustand, robuste Zugangskontrollen und die Kontrolle der Kunden über die Speicherung und den Zugriff auf ihre Daten (Amazon Web Services): https://aws.amazon.com/de/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/

(c) Anfragen von Strafverfolgungsbehörden: AWS verpflichtet sich, überzogene oder unrechtmässige Anfragen von Regierungsbehörden nach Daten anzufechten. Sie geben nur die minimal notwendigen Daten weiter, wenn sie gesetzlich dazu gezwungen werden, und informieren die Kunden über solche Anfragen, sofern dies gesetzlich zulässig ist (Amazon Web Services): https://aws.amazon.com/de/blogs/security/how-aws-is-helping-eu-customers-navigate-the-new-normal-for-data-protection/

(d) Datenübertragungswerkzeuge: AWS bietet Ressourcen, um Kunden bei der Bewertung von Datentransfers zu unterstützen und die Auswirkungen der Nutzung von AWS-Diensten unter der DSGVO zu verstehen. Dazu gehören detaillierte Dokumentationen zu den Verarbeitungstätigkeiten und den Standorten der Datenverarbeiter (Amazon AWS Docs): https://aws.amazon.com/de/blogs/security/how-aws-is-helping-eu-customers-navigate-the-new-normal-for-data-protection/

(e) Regionale Datenspeicherung: AWS ermöglicht es Kunden, die AWS-Region auszuwählen, in der ihre Daten gespeichert werden, und stellt sicher, dass Daten nicht ohne Zustimmung des Kunden ausserhalb der gewählten Region übertragen werden (Amazon Web Services): https://aws.amazon.com/de/compliance/gdpr-center/

(f) Weitere Informationen sind auf der AWS Compliance Seite zu finden: https://aws.amazon.com/de/compliance/eu-data-protection/

(g) Die Compliance Programme von AWS sind unter https://aws.amazon.com/de/compliance/programs/ gelistet. Speziell die ISO27001 ist unter https://aws.amazon.com/de/compliance/iso-27001-faqs/ beschreiben und einsehbar.

(h) Für ein "Data Transfer Impact Assessment" trifft AWS neben den oben genannten Massnahmen folgende Aussage: "AWS stellt klar, dass der CLOUD Act keine unbegrenzten oder unkontrollierten Zugriffsrechte gewährt und dass sie das Recht haben, Anfragen anzufechten, die im Widerspruch zu den Gesetzen anderer Länder oder nationalen Interessen stehen. AWS hat eine Historie darin, Anfragen von Regierungsbehörden anzufechten, die sie als zu weitreichend oder unangemessen ansehen. Dies gilt für Anfragen aus jedem Land, einschliesslich der USA. AWS prüft sorgfältig jede Anfrage, um sicherzustellen, dass sie den geltenden Gesetzen entspricht, und informiert die Kunden, sofern dies nicht gesetzlich verboten ist. https://aws.amazon.com/de/compliance/cloud-act/