AGB Smartbridge AG, Anhang 1

Datenschutzvereinbarung

Inhaltsverzeichnis

1 Präambel

(a) Der vorliegende Anhang konkretisiert die Pflichten der Parteien in Bezug auf datenschutzrechtliche Aspekte basierend auf den Vorgaben der europäischen Datenschutzgrundverordnung (DSGVO) sowie des Schweizer Datenschutzgesetzes (Stand 2018) 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. Dieser Anhang findet Anwendung auf alle Tätigkeiten unter dem Hauptvertrag, bei denen der Kunde und Smartbridge personenbezogene Daten des Kunden verarbeiten.

(b) Smartbridge anerkennt, dass der Kunde unter folgenden Voraussetzungen verpflichtet ist, Smartbridge bestimmte Pflichten aus der DSGVO zu überbinden, auch wenn die DSGVO nicht direkt auf Smartbridge anwendbar ist:

(i) Der Kunde entweder Verantwortlicher oder Auftragsverarbeiter im Anwendungsbereich der EU-DSGVO ist; und

(ii) Der Kunde Smartbridge im Rahmen des Hauptvertrages als Auftragsverarbeiter oder Subunternehmer für die Verarbeitung von personenbezogenen Daten beizieht, welche vom Anwendungsbereich der EU-DSGVO erfasst sind.

2 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(a) Der Kunde ist für die Rechtmässigkeit der Datenverarbeitung an sich, inklusive der Zulässigkeit der Auftragsverarbeitung, verantwortlich. Smartbridge verarbeitet 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 dieses Anhangs richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieses Anhangs nicht darüber hinausgehende Verpflichtungen ergeben.

3 Personendaten und betroffene Personenkategorien

(a) Im Rahmen der Auftragsverarbeitung werden im Wesentlichen folgende Personendaten bearbeitet:

(i) Namen, Adressdaten, E-Mail-Adressen, Telefonnummern;

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

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

(b) Im Rahmen der Auftragsverarbeitung sind folgende Personenkategorien betroffen:

(i) Mitarbeitende des Kunden;

(ii) Sonstige für den Kunden tätige Personen;

(iii) Kunden und Interessenten des Kunden.

4 Anwendungsbereich und Verantwortlichkeit

(a) Smartbridge verarbeitet 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. Der Kunde ist im Rahmen dieses Anhangs für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmässigkeit der Datenweitergabe an Smartbridge sowie für die Rechtmässigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

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

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

(ii) er die für eine gesetzeskonforme Verarbeitung 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 Datenverarbeiter, 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.

(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 Datenschutzgesetz 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 Verarbeitung auf Dauer sicherstellen. Dem Kunden sind diese technischen und organisatorischen Massnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden 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.

(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. Solche Zusatzaufwände stellt Smartbridge dem Kunden separat in Rechnung.

(d) Smartbridge gewährleistet, dass es den mit der Verarbeitung der Daten des Kunden befassten Mitarbeitern und anderen für Smartbridge tätigen Personen untersagt ist, die Daten ausserhalb der Weisung zu verarbeiten. Ferner gewährleistet Smartbridge, dass sich die zur Verarbeitung 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. 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 Verarbeitung 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, 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.

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 die Einhaltung der in diesem Anhang 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 dessen Betriebsablaufs durchgeführt. Smartbridge darf diese von der Voranmeldung mit angemessener Vorlaufzeit sowie von der Unterzeichnung einer Geheimhaltungserklärung betreffend der Daten anderer Kunden von Smartbridge und der eingerichteten technischen und organisatorischen Massnahmen 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 zur Verfügung.

(d) Der Aufwand eines Audits ist für Smartbridge grundsätzlich auf einen Tag pro Kalenderjahr begrenzt. Für die Unterstützung bei der Durchführung einer Inspektion darf Smartbridge eine Vergütung verlangen.

(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 Auftragsverarbeiter)

(a) Die vertraglich vereinbarten Leistungen werden unter Beizug folgender Subunternehmer durchgeführt:

(i) 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);

(ii) Das von Amazon Web Services genutzte Datencenter hat seinen Standort in Frankfurt.

(iii) root360 GmbH, Beethovenstraße 35, 04107 Leipzig, als implementiert und betreibt skalierbare Cloud-Hosting-Lösungen auf Basis von Amazon Web Services (AWS) als Amazon Web Partner.

10 Schriftformklausel, Rechtswahl

(a) Änderungen und Ergänzungen dieses Anhangs 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 dieses Anhangs den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieses Anhangs unwirksam sein, so berührt dies die Wirksamkeit des Anhangs im Übrigen nicht.

(c) Es gilt Schweizer Recht.

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) Sicherung des Datencenters:

- (i) Umzäunung des gesamten Areals;
- (ii) Gesicherte Zufahrt mit Sicherheitstor und Barriere;
- (iii) Zufahrt durch Schrankenanlage mit Sicherheitstoren;
- (iv) 24h-Überwachung des Areals und Gebäudes durch Sicherheits- und Betriebsleitwarte;
- (v) Zugangskontrollen per berührungsloser Chipkarte sowie biometrischem Fingerabdruck-Scanner;
- (vi) Zutritt nur nach erfolgter Freigabe mit Voranmeldung und Ausweiskontrolle;
- (vii) Videoüberwachung auf dem ganzen Areal und im Gebäude;
- (viii) Diverse Sensoren innerhalb und ausserhalb der Gebäude zur Intrusionserfassung;
- (ix) Schutz vor Diebstahl über Perimeterschutz Datacenter.

(c) Sicherung der Räume:

- (i) Zugangskontrollen per berührungsloser Chipkarte; Lückenlose Videoüberwachung von Türen und Zugängen mit automatischem Intrusionsalarm;
- (ii) Diverse Sensoren innerhalb und ausserhalb der Gebäude zur Intrusionserfassung.

2 Physische Verfügbarkeitssicherung

(a) Im Datencenter werden folgende Massnahmen zum physischen Schutz der Daten vor Zerstörung und Verlust umgesetzt:

(i) Brandfrühesterkennungssysteme (Rauchansaugsystem RAS);

(ii) Getrennte, redundante Stromeinspeisungen zu je 30 MVA aus zwei separaten Unterwerken;

(iii) Netzanbindung mit dedizierten Kabeln auf der 16-kV-Ebene, an denen keine anderen Fremdnutzer angeschlossen sind;

(iv) Zwei unabhängige Einspeisungen auf der Mittelspannungsebene 16 kV;

(v) Zwei separate USV-Systeme (A- und B-Versorgung); Redundant ausgelegte Netzersatzanlage mit Dieselgeneratoren;

(vi) Temperatur- und Feuchtigkeitsregulierung nach dem neusten technischen Stand:

(1) Nutzungsadaptive Kaltwassersätze mit übergeordneter Steuerung als Kältemanager;

(2) Innovative Kaltwasserverteiler und Transportsysteme wie Schichtspeicher und hydraulische Spezialweichen, Pumpenmanagementsysteme und automatischer hydraulischer Abgleich;

(3) Neue Freikühlsysteme mit integrierter EC-Ventilatortechnik und eigenprogrammierte, witterungsabhängige Energiemanagementsysteme;

(4) Dezentrale Be- und Entlüftungssysteme mit energetisch optimierten Betriebspunkten (Drehzahlregelung, feuchteabhängige Steuerung usw.); Dezentrale Be- und Entfeuchtungssysteme zur Regelung der Feuchtigkeit der IT-Flächen;

(5) Adiabatische Unterstützung der Kälteerzeugung und Klimatisierung (Befeuchtung und Kondensationskälte);

(vii) Sicherstellung von Redundanz durch RAID (redundant array of independent discs), Levels 1 und 6 (bei zwei, resp. mehreren Platten);

(viii) Tägliche Erstellung und georedundante Speicherung von Backups.

3 Berechtigungen

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

3.2 Authentisierung

(a) Zugang zu Rechnern/Systemen im Datencenter (Authentisierung):

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

(ii) Zugang auf Kundenserver sind zudem als root nur per persönlichem Zertifikat und von 3 definierten Jumphosts möglich. Auf die Jumphosts haben nur Personen mit freigeschaltetem Account (Username/Passwort)

Zugriff, welche sich zusätzlich durch ein Zertifikat oder OneTimeToken ausweisen können;

(iii) Auf allen Serven ist eine lokale Firewall mit iptables aktiv. Auf die Kundenserver ist ein Login als root nur von den definierten Jumphosts möglich.

(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.

3.3 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.

3.4 Gesicherte Schnittstellen (USB, Firewire, Netzwerk, etc.)

(a) Im Netzwerk wird zwischen Rootservern und managed Servern segmentiert und der Netzwerkverkehr getrennt behandelt.

4 Weitergabekontrolle

(a) Es wird verhindert, dass Personendaten, insbesondere beim Transport, unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

(b) Sicherung bei der elektronischen Übertragung:

(i) Verschlüsselung per TLS (Transport Layer Security, 128bit PKCS 1 SHA-1 RSA SSL-Verschlüsselung);

(ii) Servermanagement über SSH;

(iii) Einrichtung von VPN auf Kundenwunsch und Site-to-Site;

(c) Firewall:

(i) Auf allen Servern läuft eine Firewall mit iptables lokal. Ausser SSH sind sämtliche Ports gesperrt und werden nur mit den entsprechend gebuchten Services freigeschaltet.

(d) Transportsicherung:

(i) Entfernen von Datenträgern aus dem Datencenter nur dann, wenn sie nicht mehr betriebsfähig sind;

(ii) Ansonsten werden Datenträger für den Transport immer auf der Person getragen und unverzüglich entmagnetisiert und entsorgt.

5 Trennungskontrolle

(a) Mit folgenden Massnahmen wird sichergestellt, dass Datenstämme verschiedener Kunden getrennt bleiben:

(i) Eigene Datenbank und eigener Dateisystemspeicher für jede Instanz der durch den Kunden lizenzierten Software;

6 Nachvollziehbarkeit

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

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;

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

8 Weitere Schutzmassnahmen

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

(i) Verschlüsselte Ablage der Kundendaten auf Datenbanken mittels AES/Rijndael 256bit-Verschlüsselung;

(ii) Kurze Session-Time-Outs für Dateneingabe durch den Kunden, um sogenanntes Session-Highjacking zu verhindern;

(iii) ISO 27001-Zertifizierung des Datencenters sowie Bestehen eines umfassenden Virenschutzkonzepts;

(iv) Regelmässige Penetration Tests und Sicherheitsaudits.