Vereinbarung zur Auftragsverarbeitung personenbezogener Daten

Vereinbarung zur Auftragsverarbeitung personenbezogener Daten

I. PRÄAMBEL

In Anbetracht der Tatsache, dass:

A. Anwendbare Datenschutzgesetze gestatten es jedem für die Verarbeitung personenbezogener Daten verantwortlichen Datenverantwortlichen, eine natürliche oder juristische Person, eine öffentliche Verwaltung oder eine andere Einrichtung oder Vereinigung zu benennen, die als Datenverarbeiter für die Verarbeitung personenbezogener Daten im Namen des Datenverantwortlichen tätig wird, unter der Voraussetzung, dass diese auf Grundlage ihrer Erfahrung, Fähigkeiten und Zuverlässigkeit hinreichend garantieren kann, die anwendbaren Datenschutzgesetze einzuhalten, auch in Bezug auf Sicherheitsaspekte.
B. Der benannte Datenverarbeiter hat ausreichende Garantien zu bieten, um geeignete technische und organisatorische Massnahmen umzusetzen, die auf den Schutz personenbezogener Daten und der Rechte der betroffenen Personen abzielen.
C. Diese Vereinbarung zur Datenverarbeitung, zusammen mit ihren Anhängen (gemeinsam „DPA“ (engl. Data Processing Agreement, deutsch: Auftragsverarbeitungsvertrag), wird zwischen dem Kunden (nachfolgend: „Kunde“), also der natürlichen oder juristischen Person, die den Dienst (wie nachstehend definiert) erworben hat und deren Einzelheiten unten aufgeführt sind, und der Swizzonic AG („Swizzonic“) geschlossen; der Kunde und Swizzonic werden gemeinsam als „Parteien“ und einzeln als „Partei“ bezeichnet und schliessen diese DPA ab, um die Vereinbarung der Parteien hinsichtlich der Verarbeitung personenbezogener Daten des Kunden gemäss den Anforderungen der anwendbaren Datenschutzgesetze zu dokumentieren.
D. Swizzonic stellt dem Kunden die vom Letzteren aktivierten Dienst(e) („Dienst(e)“) gemäss den vertraglichen Bedingungen zur Verfügung, die in der/den Dienstbestellung(en) und in den Allgemeinen Geschäftsbedingungen, gemeinsam abrufbar unter dem Link https://www.swizzonic.ch/company/legal/allgemeine-geschaeftsbedingungen/ („AGB“), festgelegt sind, und kann, um die vorgenannten Dienste im Rahmen dieser DPA bereitzustellen, personenbezogene Daten im Auftrag des Kunden verarbeiten.
E. Genauer gesagt ist/sind der Zweck/die Zwecke der Verarbeitung personenbezogener Daten des Kunden im Zusammenhang mit dem Dienst in Anhang 1 beschrieben.
F. Der Kunde erkennt an, dass seine Nutzung des Dienstes den jeweiligen anwendbaren Datenschutzgesetzen von Rechtsordnungen unterliegen kann, die bestimmte Anforderungen in Bezug auf die Verarbeitung personenbezogener Daten stellen.

G. Die Parteien haben diese DPA abgeschlossen, um sicherzustellen, dass sie die anwendbaren Datenschutzgesetze einhalten und Schutzmassnahmen und Verfahren für die rechtmässige Verarbeitung personenbezogener Daten festlegen. Der Kunde bestätigt, dass die in dieser DPA festgelegten Bestimmungen die Verpflichtungen widerspiegeln, denen Swizzonic gemäss den anwendbaren Datenschutzgesetzen in Bezug auf die Verarbeitung personenbezogener Daten des Kunden zur Bereitstellung des Dienstes nachzukommen hat. Dementsprechend verpflichtet sich Swizzonic, die in dieser DPA enthaltenen Bestimmungen einzuhalten.

Die obige Präambel ist integraler Bestandteil der DPA.

1. BEGRIFFSBESTIMMUNGEN

Sofern in dieser DPA nicht anders definiert, haben alle hierin verwendeten, grossgeschriebenen Begriffe die Bedeutung, die ihnen in den AGB zugewiesen wird. Im Falle eines Widerspruchs oder einer Unstimmigkeit hinsichtlich der Datenschutzbestimmungen zwischen dieser DPA und dem Hauptdienstleistungsvertrag hat diese DPA Vorrang.

„Angemessenheitsbeschluss“ bezeichnet eine rechtsverbindliche Entscheidung der Europäischen Kommission und/oder des Schweizer Bundesrates, die die Übermittlung personenbezogener Daten aus dem Europäischen Wirtschaftsraum und/oder der Schweiz in ein Drittland erlaubt, das hinsichtlich der geltenden Datenschutzbestimmungen als angemessen eingestuft wurde.

„Anwendbare Datenschutzgesetze“ bezeichnet in EU-Mitgliedstaaten die Verordnung sowie ergänzende Datenschutzgesetze in den EU-Mitgliedstaaten, einschliesslich aller Leitlinien und/oder Verhaltensregeln, die von der zuständigen Aufsichtsbehörde innerhalb der EU herausgegeben wurden; und/oder in Nicht-EU-Ländern jedes geltende Datenschutzgesetz, das sich auf den Schutz und die rechtmässige Verarbeitung personenbezogener Daten bezieht.

„Kunde“ bezeichnet die Person, die den Dienst erworben hat.

„Personenbezogene Daten des Kunden“ bezeichnet personenbezogene Daten, die sich auf betroffene Personen beziehen und im Zusammenhang mit dem von Swizzonic für den Kunden erbrachten Dienst verarbeitet werden.

„Datenverantwortlicher“ bezeichnet im Allgemeinen die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

„Datenexporteur“ hat die in den Standardvertragsklauseln festgelegte Bedeutung.

„Datenimporteur“ hat die in den Standardvertragsklauseln festgelegte Bedeutung.

„Datenverarbeiter“ bezeichnet im Allgemeinen eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

„Betroffene Person“ hat die Bedeutung, die in den anwendbaren Datenschutzgesetzen festgelegt ist.

„Rechte der betroffenen Person“ bezeichnet die der betroffenen Person gemäss den anwendbaren Datenschutzgesetzen zustehenden Rechte. „Rechte der betroffenen Person“ umfassen z. B. das Recht, vom Verantwortlichen Auskunft über die betreffenden personenbezogenen Daten sowie deren Berichtigung oder Löschung oder die Einschränkung der Verarbeitung zu verlangen oder der Verarbeitung zu widersprechen sowie das Recht auf Datenübertragbarkeit.

„DPA“ bezeichnet diese globale Vereinbarung zur Datenverarbeitung zusammen mit ihren Anhängen 1, 2 und 3.

„EWR“ bezeichnet den Europäischen Wirtschaftsraum.

„EU“ bezeichnet die Europäische Union.

„Liste der Unterauftragsverarbeiter“ bezeichnet die Liste, die auf schriftliche Anfrage an legal@swizzonic.com erhältlich ist.

„AGB“ bezeichnet die in der/den Dienstbestellung(en) und in den Allgemeinen Geschäftsbedingungen zum Dienst enthaltenen Vertragsbedingungen, die zwischen den Parteien vereinbart wurden und unter folgendem Link verfügbar sind: https://www.swizzonic.ch/company/legal/allgemeine-geschaeftsbedingungen/.

„Nicht-EWR-/Schweizer-Unterauftragsverarbeiter“ bezeichnet jede Stelle, die als Datenverarbeiter (oder Unterauftragsverarbeiter) handelt und personenbezogene Daten des Kunden zur Bereitstellung des Dienstes in einem Land ausserhalb des EWR und der Schweiz verarbeitet.

„Nicht-EWR-/Schweizer-Verantwortlicher“ bezeichnet jede Stelle, die als Datenverantwortlicher handelt, an die Swizzonic die Dienste erbringt und die in einem Land ausserhalb des EWR und der Schweiz niedergelassen ist.

„Personenbezogene Daten“ bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten, einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Zur Vermeidung von Zweifeln hat „personenbezogene Daten“ die Bedeutung gemäss der Verordnung und den anwendbaren Datenschutzgesetzen.

„Verarbeiten“ oder „Verarbeitung“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

„Verordnung“ bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

„Verletzung des Schutzes personenbezogener Daten“ bezeichnet eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmässigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zum unbefugten Zugang zu übermittelten, gespeicherten oder auf andere Weise verarbeiteten personenbezogenen Daten führt.

„Dienst(e)“ hat die in Buchstabe D. der Präambel festgelegte Bedeutung.

„Dienste unter Einbeziehung von Nicht-EWR-/Schweizer-Unterauftragsverarbeitern“ bezeichnet die Dienste „Micro Site, Simply Site und Simply Shop“, deren Dienstbestellung unter folgendem Link abrufbar ist: https://www.swizzonic.ch/company/legal/website-produkte/.

„Besondere Kategorien personenbezogener Daten“ bezeichnet personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen

oder Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung genetischer Daten, biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten zur Gesundheit oder zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person, einschliesslich Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherheitsmassnahmen, Verwaltungsverfahren und Sanktionen sowie Massnahmen der sozialen Sicherheit.

„Standardvertragsklauseln“ bezeichnet die Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer gemäss der Verordnung, wie von der Europäischen Kommission im Durchführungsbeschluss (EU) 2021/914 genehmigt und vom EDÖB anerkannt, vorbehaltlich etwaiger vom EDÖB geforderter Ergänzungen.

„Unterauftragsverarbeiter“ bezeichnet eine von Swizzonic beauftragte Stelle, die Swizzonic bei der Verarbeitung der personenbezogenen Daten des Kunden zur Erfüllung der Verpflichtungen gemäss dieser DPA unterstützt (oder selbst eine Verarbeitung durchführt), wie in der vom Kunden gemäss Art. 5 dieser DPA genehmigten Liste der Unterauftragsverarbeiter aufgeführt.

„Aufsichtsbehörde“ bezeichnet jede Behörde, die befugt ist, die Anwendung der anwendbaren Datenschutzgesetze im Hinblick auf die Verarbeitung personenbezogener Daten des Kunden im Rahmen der Erbringung des Dienstes zu überwachen und durchzusetzen.

2. DATENSCHUTZROLLEN

2.1. Die Parteien vereinbaren, dass:

a) Der Kunde der Datenverantwortliche für die personenbezogenen Daten des Kunden ist, ausser wenn und soweit der Kunde als Datenverarbeiter der personenbezogenen Daten des Kunden im Auftrag eines Dritten handelt, der selbst als Datenverantwortlicher oder Datenverarbeiter agiert. Der Kunde oder der entsprechende Datenverantwortliche bestimmt die Zwecke der Erhebung und Verarbeitung der personenbezogenen Daten des Kunden;

b) Swizzonic in jedem Fall als Datenverarbeiter der personenbezogenen Daten des Kunden für die Erbringung des Dienstes fungiert; und

c) diese DPA die Beziehung zwischen den Parteien hinsichtlich der jeweiligen Pflichten und Verpflichtungen im Zusammenhang mit der Verarbeitung der personenbezogenen Daten des Kunden durch Swizzonic als Datenverarbeiter bei der Erbringung des Dienstes regelt.

3. VERPFLICHTUNGEN VON SWIZZONIC

3.1. Der Kunde oder der jeweilige Datenverantwortliche bestimmt die Zwecke der Verarbeitung personenbezogener Daten des Kunden im Rahmen der Erbringung des Dienstes.

3.2. Im Zusammenhang mit der Erbringung des Dienstes verpflichtet sich Swizzonic, die folgenden Verpflichtungen einzuhalten, einschliesslich jener, die in den Anhängen 1 und 2 dieser DPA definiert sind:

a) Swizzonic verarbeitet die personenbezogenen Daten des Kunden nur, soweit dies zur Erbringung des Dienstes erforderlich ist, und ausschliesslich gemäss den schriftlichen Anweisungen des Kunden in dieser DPA;

b) Swizzonic benachrichtigt den Kunden, falls es der Auffassung ist, dass eine schriftliche Anweisung des Kunden gegen anwendbare Datenschutzgesetze verstösst. Swizzonic ist jedoch in keinem Fall verpflichtet, eine umfassende rechtliche Prüfung in Bezug auf eine schriftliche Anweisung des Kunden durchzuführen;

c) Swizzonic als Datenverarbeiter informiert den Kunden unverzüglich über jegliche Kontakte oder Mitteilungen, die es von einer Aufsichtsbehörde im Zusammenhang mit der Verarbeitung personenbezogener Daten des Kunden erhält. Die Parteien erkennen in diesem Zusammenhang an und vereinbaren, dass die Verantwortung für die Beantwortung solcher Anfragen beim Kunden liegt und nicht bei Swizzonic;
d) Swizzonic hat betriebliche, technische und organisatorische Massnahmen implementiert – einschliesslich jener, die in Anhang 2 dieser DPA beschrieben sind – mit dem Ziel, die personenbezogenen Daten des Kunden zu schützen. Die Parteien erkennen an und vereinbaren, dass Swizzonic ausdrücklich berechtigt ist, angemessene alternative Massnahmen umzusetzen oder alternative Standorte zu nutzen, sofern das Sicherheitsniveau der Massnahmen oder der Standorte im Vergleich zu den angegebenen Massnahmen beibehalten oder erhöht wird;
e) Falls Swizzonic personenbezogene Daten des Kunden gegenüber eigenem Personal offenlegt, das unmittelbar und ausschliesslich mit der Erbringung des Dienstes betraut ist, stellt Swizzonic sicher, dass dieses Personal: i) zur Vertraulichkeit verpflichtet ist oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegt und; ii) die personenbezogenen Daten des Kunden gemäss den Anweisungen von Swizzonic und in Übereinstimmung mit den Verpflichtungen aus dieser DPA verarbeitet.

4. Verpflichtungen des Kunden

4.1. Der Kunde erkennt an und stimmt zu, dass zur Erbringung des Dienstes durch Swizzonic die Übermittlung personenbezogener Daten des Kunden an Swizzonic erforderlich ist. Der Kunde verpflichtet sich, zu prüfen, ob die in Anhang 2 dieses Vertrags aufgeführten Sicherheitsmassnahmen mit den Arten personenbezogener Daten, die der Kunde Swizzonic anvertrauen möchte, kompatibel sind.

4.2. Der Kunde sichert zu und gewährleistet, dass:

a) er über eine geeignete Rechtsgrundlage verfügt (z. B. Einwilligung der betroffenen Person, berechtigtes Interesse, Genehmigung der zuständigen Aufsichtsbehörde usw.), um die personenbezogenen Daten des Kunden im Rahmen der Erbringung des Dienstes zu verarbeiten und an Swizzonic weiterzugeben; und
b) die in dieser DPA festgelegten Bestimmungen die Verpflichtungen widerspiegeln, die die anwendbaren Gesetze Swizzonic im Hinblick auf die Verarbeitung personenbezogener Daten des Kunden im Rahmen der Dienstleistung auferlegen.

5. Zustimmung zu Unterauftragsverarbeitung

5.1. Der Kunde erkennt an, stimmt zu und willigt ein, dass zum alleinigen Zweck der Erbringung des Dienstes und unter Einhaltung der Bestimmungen dieser DPA personenbezogene Daten des Kunden von Swizzonic oder dessen Unterauftragsverarbeitern verarbeitet werden dürfen, wie in der Liste der Unterauftragsverarbeiter beschrieben.

5.2. Gemäss Art. 5.1. verfügt Swizzonic über eine generelle Genehmigung zur Beauftragung von Unterauftragsverarbeitern, vorausgesetzt, dass Swizzonic:

a) dem Kunden vorab Informationen über die Identität der Unterauftragsverarbeiter gemäss der Liste der Unterauftragsverarbeiter bereitstellt und den Kunden über Änderungen informiert, damit dieser der Beauftragung widersprechen kann;
b) mit den Unterauftragsverarbeitern Vereinbarungen abschliesst, die dieselben Verpflichtungen zur Verarbeitung der personenbezogenen Daten des Kunden enthalten wie in dieser DPA festgelegt;
c) eine angemessene Sorgfalt bei der Auswahl der Unterauftragsverarbeiter walten lässt und weiterhin für deren Einhaltung der in dieser DPA festgelegten Pflichten verantwortlich bleibt;
d) dem Kunden auf dessen Anfrage hin angemessene Informationen über Massnahmen und Vorkehrungen bereitstellt, die Swizzonic und seine Unterauftragsverarbeiter zur praktischen Einhaltung dieser DPA getroffen haben.

6. ÜBERMITTLUNG PERSONENBEZOGENER DATEN

6.1. Sofern der Kunde einen oder mehrere Dienste erwirbt, die den Einsatz von Nicht-EWR-/Schweizer-Unterauftragsverarbeitern beinhalten, darf Swizzonic gemäss Art. 5.1 und 5.2 personenbezogene Daten des Kunden an einen oder mehrere dieser Unterauftragsverarbeiter übermitteln. Diese gelten im Sinne der Standardvertragsklauseln als Datenimporteure. Falls für den betreffenden Nicht-EWR-/Schweizer-Unterauftragsverarbeiter kein Angemessenheitsbeschluss vorliegt, sichert Swizzonic zu, dass Standardvertragsklauseln mit dem betreffenden Unterauftragsverarbeiter abgeschlossen wurden und ausschliesslich die Bestimmungen der **MODULE THREE: Transfer processor to processor** gelten (unter Ausschluss der übrigen Module). Sofern nach anwendbarem Datenschutzrecht erforderlich, verpflichtet sich Swizzonic zudem, Standardvertragsklauseln auch für die Übermittlung personenbezogener Daten des Kunden von der Schweiz an Unterauftragsverarbeiter im EWR abzuschliessen.

6.2. Keine Bestimmung dieser DPA ist so auszulegen, dass sie Vorrang vor einer widersprüchlichen Klausel der Standardvertragsklauseln hat.

6.3. Auf Anfrage erhält der Kunde Einsicht in die Standardvertragsklauseln. Soweit dies zum Schutz von Geschäftsgeheimnissen oder anderer vertraulicher Informationen, einschliesslich personenbezogener Daten, erforderlich ist, ist Swizzonic berechtigt, bestimmte Teile der Standardvertragsklauseln vor Weitergabe zu schwärzen.

6.4. Der Kunde erkennt an, dass es in seiner Verantwortung liegt, alle weiteren anwendbaren rechtlichen Anforderungen zu erfüllen, damit die Übermittlung personenbezogener Daten an Swizzonic und an Nicht-EWR-/Schweizer-Unterauftragsverarbeiter im Einklang mit dem geltenden Datenschutzrecht rechtmässig erfolgt.

6.5. Soweit der Kunde ein Nicht-EWR-/Schweizer-Verantwortlicher ist, vereinbaren Swizzonic und der Kunde, dass die Standardvertragsklauseln durch Verweis Bestandteil dieser DPA sind – im Hinblick auf jede Übermittlung personenbezogener Daten vom Nicht-EWR-/Schweizer-Verantwortlichen an Swizzonic im Rahmen der Dienstleistungserbringung. In diesem Fall gelten für die Standardvertragsklauseln folgende Bestimmungen:

(i) Klausel 7 der Standardvertragsklauseln findet Anwendung;
(ii) Es gelten ausschliesslich die Klauseln unter **MODULE FOUR: Transfer processor to controller** (unter Ausschluss aller anderen Module);
(iii) Klauseln 14 und 15 finden keine Anwendung, da die Dienste keine Kombination der vom Nicht-EWR-/Schweizer-Verantwortlichen erhaltenen personenbezogenen Daten mit anderen von Swizzonic in der EU oder der Schweiz erhobenen Daten beinhalten;
(iv) Gemäss Klausel 17 der Standardvertragsklauseln gilt italienisches Recht;
(v) Gemäss Klausel 18 der Standardvertragsklauseln sind die Gerichte in Florenz (Italien) zuständig;
(vi) Es gilt ausschliesslich Anhang 1 dieser DPA, der zugleich als Anhang I der Standardvertragsklauseln angesehen wird.

7. KOOPERATION UND RECHENSCHAFTSPFLICHT

7.1. Die Parteien arbeiten in gutem Glauben zusammen, um die Einhaltung der Bestimmungen dieser DPA sicherzustellen, einschliesslich, aber nicht beschränkt auf die ordnungsgemässe und rechtzeitige Ausübung der Rechte der betroffenen Personen sowie das Management von Vorfällen bei Sicherheits- oder Datenschutzverletzungen, um mögliche negative Auswirkungen zu minimieren.

7.2. Die Parteien arbeiten in gutem Glauben zusammen, um einander und den Aufsichtsbehörden die notwendigen Informationen zur Verfügung zu stellen, die zur Nachweisführung der Einhaltung der anwendbaren Datenschutzgesetze erforderlich sind.

8. Rechte der betroffenen Personen

8.1. Unter Berücksichtigung der Art der Verarbeitung unterstützt Swizzonic den Kunden durch geeignete technische und organisatorische Massnahmen bei der Erfüllung seiner Verpflichtung, Anfragen zur Ausübung der Rechte betroffener Personen zu beantworten.

8.2. Swizzonic gewährt dem Kunden eine angemessene Zusammenarbeit und Unterstützung und stellt die Informationen zur Verfügung, die in zumutbarem Rahmen erforderlich sind, um auf Anfragen betroffener Personen zu reagieren oder dem Kunden die Einhaltung seiner Pflichten gemäss den anwendbaren Datenschutzgesetzen im Zusammenhang mit den Rechten betroffener Personen zu ermöglichen. Der Kunde erkennt an und stimmt zu, dass im Falle eines erheblichen Ressourcenaufwands seitens Swizzonic für diese Unterstützung ein Entgelt erhoben werden kann – vorbehaltlich vorheriger Mitteilung und Zustimmung durch den Kunden.

9. Rückgabe und Löschung von Daten

9.1. Swizzonic wird auf Wunsch des Kunden sowie bei Ablauf oder vorzeitiger Beendigung dieser DPA die personenbezogenen Daten des Kunden unentgeltlich zurückgeben oder löschen, vorbehaltlich eines schriftlichen Antrags des Kunden mit angemessener Vorankündigung, es sei denn, zwingende anwendbare Gesetze (einschliesslich, aber nicht beschränkt auf Datenschutzgesetze oder Anordnungen von Strafverfolgungs- oder Aufsichtsbehörden) verbieten Swizzonic dies.

9.2. Spezifische Anfragen des Kunden zur Rückgabe der personenbezogenen Daten werden im Rahmen des technisch und organisatorisch Zumutbaren erfüllt, unter Berücksichtigung des Umfangs, der Kategorisierung und der Menge der verarbeiteten personenbezogenen Daten.

9.3. Personenbezogene Daten des Kunden, die gemäss den internen Standardverfahren von Swizzonic zurückgegeben werden, erfolgen für den Kunden kostenfrei. In allen anderen Fällen kann die Rückgabe zu angemessenen Kosten für den Kunden erfolgen.

9.4. Entscheidet sich der Kunde für die Löschung der personenbezogenen Daten des Kunden – vorbehaltlich Art. 9.5 – stellt Swizzonic eine Bestätigung über die erfolgte Löschung aus.

9.5. Swizzonic darf personenbezogene Daten des Kunden, die im Rahmen regulärer Datensicherungen gespeichert wurden, im Einklang mit den internen Notfallwiederherstellungs- und Geschäftskontinuitätsprotokollen (siehe Art. 12), aufbewahren – vorausgesetzt, dass Swizzonic (und deren Unterauftragsverarbeiter) diese Daten nicht aktiv oder absichtlich für andere Zwecke als die Erbringung der Dienstleistung verarbeitet.

10. Übermittlungen

10.1. Personenbezogene Daten, die von Swizzonic im Zusammenhang mit dem Dienst über das Internet übermittelt werden, werden angemessen verschlüsselt. Die Parteien erkennen jedoch an, dass die Sicherheit von Übertragungen über das Internet nicht garantiert werden kann. Swizzonic ist nicht verantwortlich für den Internetzugang des Kunden, für Abfangen oder Unterbrechungen von Internetkommunikation oder für Veränderungen oder Verluste personenbezogener Daten über das Internet.

10.2. Bei Verdacht auf eine Datenschutzverletzung kann Swizzonic die Nutzung des Dienstes über das Internet durch den Kunden unverzüglich aussetzen, bis eine Untersuchung erfolgt ist, vorausgesetzt, Swizzonic informiert den Kunden über eine solche Aussetzung so bald wie zumutbar möglich und ergreift alle vertretbaren Massnahmen, um die Nutzung des Dienstes über das Internet schnellstmöglich wiederherzustellen und mit dem Kunden zusammenzuarbeiten, um die Dienstleistung über alternative Kommunikationskanäle fortzusetzen.

10.3. Der Kunde hat alle angemessenen Massnahmen zu ergreifen, um die Vertraulichkeit der Namen und Passwörter seiner Mitarbeiter für die Nutzung der Dienste zu wahren. Der Kunde ist für die Folgen jeder missbräuchlichen Nutzung des Dienstes durch einen seiner Mitarbeiter verantwortlich.

11. DATENSCHUTZVERLETZUNG

11.1 Der Kunde erkennt an und stimmt zu, dass Swizzonic nicht für Datenschutzverletzungen verantwortlich ist, die nicht auf Fahrlässigkeit von Swizzonic zurückzuführen sind.

11.2 Wird Swizzonic eine Datenschutzverletzung bekannt, wird Swizzonic:

a) geeignete Massnahmen zur Eindämmung und Minderung ergreifen und den Kunden unverzüglich benachrichtigen, damit dieser seine Reaktionsmassnahmen einleiten kann. Swizzonic behält sich das Recht vor, eigenständig Massnahmen zur Einhaltung der Datenschutzgesetze oder zum Schutz eigener Interessen zu bestimmen;
b) mit dem Kunden zur Untersuchung des Vorfalls zusammenarbeiten – insbesondere in Bezug auf Art, Umfang, betroffene Datenkategorien und mögliche Folgen;
c) falls gesetzlich erforderlich, den Anweisungen des Kunden folgen, wenn dieser zur Benachrichtigung von Aufsichtsbehörden oder betroffenen Personen verpflichtet ist. Der Kunde entscheidet allein über:
    i. ob und an wen Meldungen erfolgen (z. B. Behörden, betroffene Personen);
    ii. den Inhalt der Meldung sowie etwaige angebotene Abhilfemassnahmen.

12. WIEDERHERSTELLUNG IM NOTFALL UND SICHERUNG DER GESCHÄFTSABWICKLUNG

12.1 Swizzonic unterhält angemessene Notfallwiederherstellungs- und Geschäftskontinuitätsprotokolle, die je nach Dienstleistung variieren. Eine Zusammenfassung kann der Kunde auf Anfrage einsehen. Swizzonic kann diese Pläne jederzeit ändern, darf dabei jedoch die Wiederherstellungsfähigkeit nicht unter das zum Zeitpunkt des Vertragsbeginns geltende Niveau reduzieren.

13. AUFTRÄGE

13.1 Mit der Unterzeichnung dieser DPA, einschliesslich der Anhänge 1, 2 und 3, bevollmächtigt der Kunde Swizzonic ausdrücklich, die in Art. 5 genannten Tätigkeiten im Auftrag des Kunden durchzuführen.

13.2 Mit der Unterzeichnung dieser DPA nimmt Swizzonic das Mandat an, das unentgeltlich im Zusammenhang mit der Dienstleistung ausgeführt wird, und bestätigt rechtlich, dass Swizzonic die übertragenen Anweisungen gelesen und verstanden hat.

ANHANG 1

1. BETROFFENE PERSONENATA SUBJECTS

Die verarbeiteten personenbezogenen Daten können sich, je nach aktiviertem Dienst, auf folgende Kategorien von betroffenen Personen beziehen, die im Voraus nicht bestimmbar sind:

- Kunde und/oder Mitarbeiter und Mitarbeiterinnen des Kunden;
- Anbieter des Kunden;
- Nutzer des Kunden;
- Kunden des Kunden;
- betroffene Personen, deren personenbezogene Daten vom Kunden unter Nutzung der von Swizzonic bereitgestellten Dienste verarbeitet werden:

2. KATEGORIEN VON PERSONENBEZOGENEN DATEN, DIE FÜR JEDE DIENSTLEISTUNG VERARBEITET WERDEN

Die für jede Dienstleistung verarbeiteten personenbezogenen Daten, die dem Kunden bereitgestellt werden können und nicht im Voraus bestimmbar sind, beziehen sich ausschliesslich auf personenbezogene Daten im Sinne der geltenden Datenschutzgesetze, **mit ausdrücklichem Ausschluss von personenbezogenen Daten, die sich auf strafrechtliche Verurteilungen und Straftaten sowie andere besondere Kategorien personenbezogener Daten beziehen.**

Insbesondere werden folgende Kategorien personenbezogener Daten übermittelt/verarbeitet:

- Daten zur Kontaktaufnahme (Name und Nachname, E-Mail-Adresse, Postanschrift, Telefonnummer);
- Geburtsdatum;
- Alter;
- Geschlecht;
- Weitere Kategorien personenbezogener Daten, die vom Kunden unter Nutzung der von Swizzonic bereitgestellten Dienste verarbeitet werden.

3. BESONDERE KATEGORIEN VON DATEN

Die verarbeiteten personenbezogenen Daten **betreffen keine personenbezogenen Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten sowie keine besonderen Kategorien personenbezogener Daten.**

4. ZWECKE DER VERARBEITUNG

Personenbezogene Daten dürfen nur für die Erbringung der im GTC beschriebenen Dienstleistung verarbeitet werden.

5. ART DER VERARBEITUNG

Die Art der Verarbeitungsvorgänge variiert je nach dem spezifisch über die AGB aktivierten Service.

6. HÄUFIGKEIT DER VERARBEITUNG

Die Häufigkeit der Verarbeitungsvorgänge variiert je nach dem über die AGB aktivierten spezifischen Dienst.

7. DAUER DER VERARBEITUNG

Die personenbezogenen Daten des Kunden werden so lange gespeichert, wie der Service aktiv ist.

ANHANG 2

Beschreibung der technischen und organisatorischen Sicherheitsmassnahmen

Swizzonic und die Sub-Prozessoren verpflichten sich, mindestens die unten beschriebenen technischen und organisatorischen Massnahmen einzuhalten.

Informationen zu den Sicherheitsmassnahmen

Informationssicherheitsverfahren
Interne Organisation
Es wurden getrennte Rollen und Verantwortlichkeiten für die Informationssicherheit definiert und den für die Verarbeitungstätigkeiten zuständigen Personen des Unternehmens (nachfolgend auch *"Benutzer"*) zugewiesen, um Interessenkonflikte zu vermeiden und unangemessene Tätigkeiten zu verhindern.

Sicherheit im Personalwesen
Mobile Geräte und Telearbeit
Es gibt eine Sicherheitsrichtlinie für die Nutzung aller Unternehmensgeräte, insbesondere mobiler Geräte, und angemessene Kontrollen sind implementiert.
Beendigung oder Änderung des Beschäftigungsverhältnisses
Nach Beendigung des Arbeitsverhältnisses eines Benutzers oder bei wesentlicher Änderung der übernommenen Rolle werden Zugriffsrechte umgehend aktualisiert, während Geschäftswerkzeuge physisch und systemseitig zurückgegeben und zurückgesetzt werden.

Verwaltung von Unternehmensressourcen
Verantwortlichkeit für Ressourcen und Unternehmenswerte
Alle Unternehmenswerkzeuge und -werte sind sorgfältig inventarisiert und deren Zuweisung an die jeweiligen Benutzer, die für deren Sicherheit verantwortlich sind, wird überwacht. Zudem wurde eine Richtlinie für deren ordnungsgemässe Nutzung definiert.
Klassifikation von Informationen
Alle Informationen werden von den jeweiligen Benutzern gemäss den Sicherheitsanforderungen klassifiziert und katalogisiert sowie entsprechend verarbeitet.
Medienverwaltung
Die auf den Speichermedien abgelegten Informationen werden so verwaltet, kontrolliert, verändert und genutzt, dass deren Inhalt nicht kompromittiert wird, und werden angemessen gelöscht.

Zugangskontrolle
Organisatorische Anforderungen an die Zugangskontrolle
Die organisatorischen Anforderungen des Unternehmens zur Überwachung des Zugriffs auf Informationsressourcen sind in einer Richtlinie dokumentiert und werden praktisch durch ein Zugangskontrollverfahren umgesetzt; dies bedeutet, dass der Zugang zum Netzwerk und zu Verbindungen beschränkt ist.
Benutzerzugangsverwaltung
Die Zuweisung von Benutzerzugangsrechten wird vom erstmaligen Registrieren des Benutzers bis zur Aufhebung der Zugangsrechte kontrolliert, wenn diese nicht mehr benötigt werden, einschliesslich spezieller Beschränkungen für privilegierte Zugriffsrechte und Verwaltung von *"geheimen Authentifizierungsinformationen"*. Dies unterliegt regelmässigen Überprüfungen und Kontrollen, einschliesslich Aktualisierungen der Zugangsrechte bei Bedarf. Im Zugangsmanagement wird das Prinzip der Minimalrechte angewendet, wobei Benutzer nur Zugriff auf die Daten erhalten, die für ihre Arbeitsfunktion und Geschäftstätigkeit notwendig sind. Zusätzliche Zugriffsrechte bedürfen einer speziellen Autorisierung.
Verantwortung des Benutzers
Benutzer sind sich ihrer Verantwortung auch durch die Aufrechterhaltung einer wirksamen Zugangskontrolle bewusst, z. B. durch Wahl eines komplexen Passworts, dessen Komplexität vom System geprüft wird, und durch die Geheimhaltung dieses Passworts.
Systeme und Anwendungen zur Zugangskontrolle
Der Zugang zu Informationen unterliegt Einschränkungen in Übereinstimmung mit der

Zugangskontrollrichtlinie, durch ein System für sicheren Zugang, Passwortverwaltung sowie Kontrolle privilegierter Werkzeuge und eingeschränktem Zugang zu allen Quellcodes.

Verschlüsselung

Kryptographische Kontrolle

Es besteht eine Richtlinie zur Verwendung von Medienverschlüsselung und Nutzerdaten. Authentifizierungen sind verschlüsselt.

Physische und umgebungsbezogene Sicherheit

Physische und umgebungsbezogene Sicherheitsmassnahmen sind implementiert, um unbefugten oder versehentlichen Zugriff, Verlust oder Verbreitung von Daten zu verhindern.

Sichere Bereiche: Rechenzentrum

Die Dienstleistungen des Unternehmens werden in mehreren Rechenzentren weltweit bereitgestellt und gehostet, wobei dasjenige, das die personenbezogenen Daten der Kunden speichert, eines der wenigen zertifizierten Tier-IV-Rechenzentren in Italien ist, was die maximale Garantie bietet, die ein Rechenzentrum bieten kann. Alle Rechenzentren in der Lieferkette bieten vollständige Redundanz aller elektrischen, Kühl- und Netzwerkkreise. Alle Rechenzentren verfügen über Perimeterbeleuchtung sowie ein Präsenzdetektionssystem mit CCTV-Kameras; die Notausgänge sind mit Alarmen ausgestattet. Alle Alarme werden in Kontrollräumen gebündelt.
Der physische Zugang wird durch Autorisierungs-, Erkennungs- und Registrierungsvorgänge geregelt und kontrolliert und ist dank des Zugangskontrollsystems auf die Bereiche beschränkt, für die eine Berechtigung vorliegt.

Ausrüstung

Es besteht eine Richtlinie für die Entsorgung ausgemusterter Ausrüstung, um alle darin enthaltenen Informationen sicher zu vernichten.

Sicherheit der Abläufe

Verfahren und operative Verantwortlichkeiten

Operative Verantwortlichkeiten in der IT sind dokumentiert und Änderungen an IT-Einrichtungen und Systemen werden kontrolliert. Entwicklungs-, Verifizierungs- und Betriebssysteme sind getrennt. Es gibt Benutzer, die für das ordnungsgemässe Funktionieren der Verfahren verantwortlich sind. Andererseits liegt die Verwaltung der logischen Sicherheit der Betriebssysteme und der vom Kunden installierten Anwendungen in der Verantwortung des Kunden der vom Unternehmen erbrachten einzelnen Dienste (nachfolgend auch *"Kunde"*).

Schutz vor Malware

Virenschutz und Malwarekontrolle sind auf Unternehmensgeräten aktiv, und es besteht ein entsprechendes Bewusstsein bei den Benutzern.
Bezüglich der Dienste Virtual Server oder Dedicated Server ist der Kunde verantwortlich für die Installation von Anti-Virus- und Anti-Malware-Software und – falls der entsprechende Dienst nicht erworben wurde – einer Firewall. Für den Hosting-Dienst besteht ein Echtzeitschutz auf den Front-End-Geräten.
Für den E-Mail-Dienst wird der Mailverkehr in Echtzeit sowohl eingehend als auch ausgehend analysiert, um Viren, Malware zu erkennen sowie Spam zu identifizieren und zu filtern. Die Analyse erfolgt automatisiert und basiert auf dem Inhalt, der Abfrage internationaler Datenbanken und der Reputation, die durch eine Reihe von Parametern erworben wurde.

Backup

Periodische Backups werden durchgeführt, mit Ausnahme der Dienste, für die der Kunde für die Sicherung und Verwaltung der Backups verantwortlich ist (Dedicated Servers und Virtual Servers). Für Hosting- und Post-Dienste werden periodische Backups durchgeführt, auf die der Kunde im Falle von Hosting-Diensten ebenfalls zugreifen kann. Zusätzliche Backups, die für Kunden nicht zugänglich sind, werden ausschliesslich für Zwecke der Disaster Recovery erstellt.

Authentifizierung und Überwachung

Authentifizierung und Synchronisation

Jede Aktivität und jedes Ereignis im Zusammenhang mit der Informationssicherheit durch Systembenutzer und Administratoren/Operatoren erfolgt nach Eingabe der Authentifizierungsdaten oder Identitätszertifikate. Die Uhren aller Geräte sind synchronisiert.

Kontrolle von Betriebssystemsoftware

Die Installation von Software auf Betriebssystemen wird kontrolliert und überwacht.
Bezüglich Virtual Servers und Dedicated Servers werden Betriebssysteme mit aktualisierten Installationsabbildern bereitgestellt, auch während der Installation durch den Kunden. Ebenso obliegt es dem Kunden, Firmware und Anwendungen bzw. Software, die vom Kunden installiert wurden, zu aktualisieren.

Management technischer Schwachstellen
Patch-Management
Jede technische Schwachstelle wird mit geeigneten Patches behoben, und es bestehen Verfahren für alle Testphasen sowie für die anschliessende Installation der Software und Updates, die nur erfolgen, wenn alle Tests positiv verlaufen sind.
Überlegungen zur Prüfung von Informationssystemen
Es werden regelmässige Kontrollen durchgeführt, um sicherzustellen, dass negative Auswirkungen auf Produktionssysteme minimiert werden und kein unbefugter Zugriff auf Daten erfolgt.

Sicherheit der Kommunikation
Netzwerksicherheitsmanagement
Netzwerke und Online-Dienste sind auch durch Trennung und Segmentierung gesichert.
Informationsübertragung
Vereinbarungen über die Übertragung von Informationen zu und von Dritten sind in Kraft.

Sicherheit in Entwicklungs- und Supportprozessen
Die Regeln, die die Sicherheit von Software- und Systementwicklungen regeln, sind in einer Richtlinie definiert. Änderungen am System (sowohl für Anwendungen als auch Betriebssysteme) werden kontrolliert. Die Systemsicherheit wird getestet und Zulassungskriterien, die Sicherheitsaspekte einschliessen, werden definiert.

Beziehung zu Lieferanten
Informationssicherheit in der Beziehung zu Lieferanten
Es bestehen Verträge oder Vereinbarungen, die den Schutz und die Regulierung der Verarbeitung von Informationen der Organisation und der Kunden regeln, die für Dritte im IT-Bereich und andere Drittanbieter in der gesamten Lieferkette zugänglich sind.
Management der vom Lieferanten erbrachten Dienstleistungen
Die Erbringung der vom Lieferanten erbrachten Dienstleistungen wird in Bezug auf den Vertrag oder die Vereinbarung überwacht und überprüft. Jede Änderung des Dienstes wird kontrolliert.

Management von Sicherheitsvorfällen
Management von Informationssicherheitsvorfällen und Verbesserungen
Es gibt spezifische Verantwortlichkeiten und Verfahren zur kohärenten und effektiven Handhabung aller Ereignisse und Vorfälle im Zusammenhang mit der Informationssicherheit (z. B. das sogenannte *Data Breach*-Verfahren).

Informationssicherheitsaspekte im Zusammenhang mit der Geschäftskontinuität
Redundanzen
Alle wichtigen IT-Einrichtungen sind redundant ausgelegt, um Verfügbarkeitsanforderungen zu erfüllen. Wo diese Redundanz nicht vorhanden ist, sind geeignete Massnahmen implementiert, um die Kontinuität des Dienstes oder die Minimierung von Datenverlust sicherzustellen.

Compliance
Einhaltung gesetzlicher und vertraglicher Anforderungen
Das Unternehmen identifiziert und dokumentiert seine Verpflichtungen gegenüber externen Behörden und anderen Dritten in Bezug auf Informationssicherheit, einschliesslich geistigem Eigentum, Buchhaltungsunterlagen und Datenschutzinformationen.
Überprüfung der Informationssicherheit
Die Projekte der Organisation im Bereich Informationssicherheit und Sicherheitsrichtlinien werden überprüft, und bei Bedarf werden Korrekturmassnahmen ergriffen.

ANHANG 3

Annex 3 (Liste der Unterauftragsverarbeiter) ist per E-Mail anzufordern an: legal@swizzonic.com.