

# Vertrag über die Verarbeitung der personenbezogenen Daten

<b>Vertrag über die Verarbeitung der personenbezogenen Daten.....</b>	<b>2</b>
<b>Präambel .....</b>	<b>2</b>
1. <b>Begriffsbestimmungen.....</b>	<b>3</b>
2. <b>Datenschutzrollen.....</b>	<b>5</b>
3. <b>Pflichten von Swizzonic.....</b>	<b>5</b>
4. <b>Pflichten des Kunden .....</b>	<b>6</b>
5. <b>Zustimmung zur Verarbeitung der Daten seitens der Unterauftragsverarbeiter .....</b>	<b>6</b>
6. <b>Übermittlung der personenbezogenen Daten .....</b>	<b>7</b>
7. <b>Pflichten in Sachen Zusammenarbeit und Verantwortlichkeit .....</b>	<b>8</b>
8. <b>Rechte der betroffenen Person .....</b>	<b>8</b>
9. <b>Herausgabe der Daten und Löschung.....</b>	<b>8</b>
10. <b>Übermittlung.....</b>	<b>9</b>
11. <b>Verletzung der personenbezogenen Daten .....</b>	<b>9</b>
12. <b>Disaster Recovery und Business Continuity.....</b>	<b>10</b>
13. <b>Auftrag.....</b>	<b>10</b>
<b>ANHANG 1 .....</b>	<b>11</b>
<b>ANHANG 2 .....</b>	<b>13</b>
<b>ANHANG 3 .....</b>	<b>17</b>

# Vertrag über die Verarbeitung der personenbezogenen Daten

## Präambel

### Voraussetzungen:

- A.** Die in Sachen Datenschutz anwendbaren gesetzlichen Bestimmungen erlauben jedem für die Verarbeitung personenbezogener Daten Verantwortlichen, eine natürliche oder juristische Person, eine öffentliche Verwaltung oder sonstige Einrichtung oder Organisation vorzuschlagen, die als Auftragsverarbeiter der personenbezogenen Daten im Auftrag des Verantwortlichen tätig sind. Die Auswahl ist unter Personen/Einrichtungen möglich, die aufgrund ihrer Erfahrung, Fähigkeiten und Verlässlichkeit eine angemessene Garantie für die volle Einhaltung der in Sachen Datenschutz anwendbaren gesetzlichen Bestimmungen einschließlich des Sicherheitsprofils liefern.
- B.** Der ernannte Auftragsverarbeiter muss ausreichende Garantien liefern, dass technische und organisatorische Maßnahmen mit dem Ziel getroffen werden, den Schutz der personenbezogenen Daten und den Schutz der Rechte der betroffenen Person zu gewährleisten.
- C.** Dieser Vertrag über die Verarbeitung der personenbezogenen Daten wird gemeinsam mit den entsprechenden Anhängen (gemeinsam „**Vertrag**“) zwischen dem Kunden (im Folgenden: „**Kunde**“), das heißt der natürlichen oder juristischen Person, die den Dienst (siehe nachstehende Definition) gekauft hat und deren Daten weiter unten angeführt sind, und Swizzonic AG (im Folgenden: „**Swizzonic**“) unterzeichnet; der Kunde und Swizzonic, die gemeinsam als die „**Vertragspartner**“ und einzeln als der „**Vertragspartner**“ bezeichnet werden, schließen diesen Vertrag zum Zweck ab, die zwischen den Vertragspartnern in Bezug auf die Verarbeitung der personenbezogenen Daten des Kunden unter Einhaltung der anwendbaren gesetzlichen Datenschutzbestimmungen getroffenen Vereinbarungen widerzuspiegeln.
- D.** Swizzonic liefert dem Kunden den/die von ihm aktivierten Dienst(e) („**Dienst(e)**“) zu den im Dienstauftrag / in den Dienstaufträgen und in den Allgemeinen Servicebedingungen vorgesehenen Bedingungen, die allgemein über den Link <https://www.swizzonic.ch/company/legal/> („**Master-Vertrag**“) erhältlich sind. Um genannten Dienst nach den Vorgaben dieses Vertrags zu liefern, könnte Swizzonic personenbezogene Daten im Auftrag des Kunden verarbeiten.
- E.** Genauer wird der Zweck / werden die Zwecke der Verarbeitung der personenbezogenen Daten des Kunden in Verbindung mit dem Dienst im Anhang 1 beschrieben.
- F.** Der Kunde ist sich bewusst, dass seine Nutzung des Dienstes den anwendbaren gesetzlichen Datenschutzbestimmungen in Bezug auf Gerichtsbarkeiten, die bestimmte Voraussetzungen für die Verarbeitung aller personenbezogenen Daten auferlegen, unterliegen könnte.
- G.** Die Vertragspartner haben diesen Vertrag zum Zweck abgeschlossen, die Einhaltung der anwendbaren gesetzlichen Datenschutzbestimmungen zu gewährleisten und angemessene Sicherheitsmaßnahmen und Prozeduren festzulegen, um die personenbezogenen Daten rechtmäßig zu verarbeiten. Der Kunde bestätigt, dass die in diesem Vertrag angeführten Vorgaben die Pflichten widerspiegeln, an die sich Swizzonic unter Einhaltung der anwendbaren gesetzlichen Datenschutzbestimmungen halten muss, deren Gegenstand die Verarbeitung der personenbezogenen Daten des Kunden für die Leistung des Dienstes sind. Im Sinne des

vorangehenden Inhalts verpflichtet sich Swizzonic, sich an die in diesem Vertrag enthaltenen Bestimmungen zu halten.

H. Sobald dieses Dokument heruntergeladen, ausgefüllt, unterzeichnet und an [legal@swizzonic.com](mailto:legal@swizzonic.com) gesendet und von Swizzonic gegengezeichnet wird, ersetzt es den „Vertrag über die Verarbeitung der personenbezogenen Daten für Kunden, die Endbenutzer der Dienste von Swizzonic sind“ ebenso wie den „Vertrag für Kunden, die Dienste von Swizzonic im Auftrag Dritter beantragen“, auf die in der Klausel „Verarbeitung der personenbezogenen Daten“ der Allgemeinen Servicebedingungen Bezug genommen wird, zur Gänze, da es darauf abzielt, gewisse Elemente der von Swizzonic als Auftragsverarbeiter durchgeführten Verarbeitung der personenbezogenen Daten seitens des Kunden genauer zu präzisieren.

Die vorangehende Präambel bildet einen ergänzenden Teil des Vertrags.

## 1. BEGRIFFSBESTIMMUNGEN

Sofern in diesem Vertrag nichts anderes festgelegt wird, haben alle in diesem Vertrag verwendeten Begriffe die Bedeutung, die ihnen im Master-Vertrag zugewiesen wurde. Im Fall eines Konflikts oder von Widersprüchen bezüglich des Datenschutzes zwischen diesem Vertrag und dem Master-Vertrag haben die in diesem Vertrag festgelegten Bestimmungen Vorrang.

„**Aufsichtsbehörde**“ steht für jede Behörde, die dafür zuständig ist, die Anwendung der einschlägigen gesetzlichen Bestimmungen in Sachen Schutz der personenbezogenen Daten in Bezug auf die anhand des Dienstes erfolgte Verarbeitung der personenbezogenen Daten des Kunden zu beaufsichtigen und gewährleisten.

„**Besondere Kategorien von personenbezogenen Daten**“ steht für personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, sowie die Verarbeitung von genetischen Daten, um eine natürliche Person eindeutig zu identifizieren, Gesundheitsdaten oder das Sexualleben der Person betreffende Daten oder die entsprechenden Sicherheitsmaßnahmen, Verwaltungsverfahren, Strafen und Maßnahmen zur sozialen Sicherheit.

„**Standardvertragsklauseln**“ steht für die von der Europäischen Kommission im Durchführungsbeschluss (EU) 2021/914 der Kommission angewendeten und vom EDÖB übernommenen Standardvertragsklauseln.

„**Kunde**“ steht für die Person/Organisation, die den Dienst aktiviert hat;

„**Master-Vertrag**“ steht für die zwischen den Vertragspartnern vereinbarten, im Serviceauftrag / in den Serviceaufträgen und in den Allgemeinen Servicebedingungen vorgesehenen Vertragsbedingungen zur Regelung der Lieferung des Dienstes, die gemeinsam unter dem Link <https://www.swizzonic.ch/company/legal/> verfügbar sind.

„**Vertrag**“ steht für diesen Vertrag über die Verarbeitung der personenbezogenen Daten und die Anhänge 1, 2 und 3.

„**Personenbezogene Daten des Kunden**“ steht für die personenbezogenen Daten in Bezug auf die Betroffenen, die in Verbindung mit dem von Swizzonic an den Kunden gelieferten Dienst verarbeitet werden. In Schweiz sind auch die Daten in Bezug auf juristische Personen gemeint.

„**Personenbezogene Daten**“ steht für alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche oder juristische Person beziehen; als identifizierbar wird eine natürliche oder juristische Person erachtet, die direkt oder indirekt insbesondere mittels Zuordnung zu einer Kennung wie

einem Namen, einer Kennnummer, zu Standortdaten, zu 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, identifiziert werden kann; um Widersprüche bezüglich der Interpretation zu vermeiden, hat „personenbezogene Daten“ die in der Verordnung und den anwendbaren gesetzlichen Datenschutzbestimmungen vorgesehene Bedeutung.

„**Angemessenheitsbeschluss**“ bezieht sich auf einen verbindlichen von der Europäischen Kommission erlassenen Beschluss und/oder von der Schweizer Datenschutzbehörde, dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten („EDÖB“) gelieferte Anweisungen, die die Übermittlung der personenbezogenen Daten aus dem Europäischen Wirtschaftsraum und/oder der Schweiz in ein Drittland, deren interne Rechtsordnung ein angemessenes Schutzniveau der personenbezogenen Daten bietet, zulässt.

„**Rechte der betroffenen Person**“ sind die Rechte, die der betroffenen Person durch die anwendbaren gesetzlichen Datenschutzbestimmungen eingeräumt werden. „Rechte der betroffenen Person“ bedeutet zum Beispiel das Recht, vom Verantwortlichen die Auskunft, Berichtigung oder Löschung der personenbezogenen Daten zu verlangen, das Recht auf die Einschränkung der Verarbeitung der Daten der betroffenen Person oder das Recht auf Widerspruch gegen die Verarbeitung sowie das Recht auf die Übertragbarkeit der Daten.

„**Anwendbare gesetzliche Datenschutzbestimmungen**“ bedeutet in den Mitgliedstaaten der Europäischen Union die Verordnung und die ergänzenden einzelstaatlichen Rechtsvorschriften in Sachen Schutz der personenbezogenen Daten einschließlich aller Leitlinien und/oder aller von der zuständigen Aufsichtsbehörde in der Europäischen Union erlassenen *Codes of practice*; und/oder, in Nicht-EU-Ländern, jede einschlägigen Datenschutzgesetzgebung bezüglich des Schutzes und der rechtmäßigen Verarbeitung von personenbezogenen Daten.

„**Verzeichnis der Unterauftragsverarbeiter**“ steht für das Verzeichnis, das auf schriftliche Anfrage an [legal@swizzonic.com](mailto:legal@swizzonic.com) zur Verfügung gestellt wird.

„**Datenexporteur(e)**“ hat die in den Standardvertragsklauseln vorgesehene Bedeutung.

„**Datenimporteur(e)**“ hat die in den Standardvertragsklauseln vorgesehene Bedeutung.

„**Betroffene Person(en)**“ hat die in den anwendbaren gesetzlichen Datenschutzbestimmungen vorgesehene Bedeutung.

„**Verordnung**“ steht für 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.

„**Auftragsverarbeiter**“ steht allgemein für eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

„**EWR**“ steht für den Europäischen Wirtschaftsraum.

„**Dienst(e)**“ steht für den Dienst, der Gegenstand des Master-Vertrags ist.

„**Dienste, an denen ein Unterauftragsverarbeiter aus Nicht-EWR-Ländern beteiligt ist**“ bedeutet den Dienst „Micro Site, Simply Site und Simply Shop“, für die der Serviceauftrag unter folgendem Link verfügbar ist: <https://www.swizzonic.ch/company/legal/website-wprodukte/>

„**Unterauftragsverarbeiter**“ steht für eine von Swizzonic ermittelte Einrichtung, um das Unternehmen bei der Verarbeitung der personenbezogenen Daten des Kunden unter Einhaltung der von Swizzonic

vorgesehenen und in diesem Vertrag beschriebenen Pflichten zu unterstützen (oder sie direkt zu erledigen), die im Verzeichnis der Unterauftragsverarbeiter zu finden ist, das vom Kunden im Sinne des Art. 5 dieses Vertrags genehmigt wurde.

„**Unterauftragsverarbeiter aus Nicht-EWR-Ländern / der Schweiz**“ steht für jede Einrichtung, die als Auftragsverarbeiter (oder als Unterauftragsverarbeiter) tätig ist und personenbezogene Daten des Kunden für die Leistung des Dienstes in einem Nicht-EWR-Land, das nicht die Schweiz ist, verarbeitet.

„**Verantwortlicher**“ oder „**Verantwortlicher für die Verarbeitung**“ steht allgemein für die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

„**Verantwortlicher aus Nicht-EWR-Ländern / der Schweiz**“ steht für jede Stelle, die als Verantwortlicher tätig ist und der Swizzonic die Dienste leistet, die keinen Sitz im EWR und der Schweiz hat.

„**Verarbeiten**“ oder „**Verarbeitung**“ steht für 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.

„**EU**“ steht für die Europäische Union.

„**Verletzung des Schutzes personenbezogener Daten**“ steht für eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

## 2. DATENSCHUTZROLLEN

2.1. Die Vertragspartner vereinbaren Folgendes:

- a) Der Kunde ist der Verantwortliche der personenbezogenen Daten des Kunden mit Ausnahme der Fälle, in denen der Kunde als Auftragsverarbeiter der personenbezogenen Daten des Kunden im Auftrag eines Dritten, der selbst als Verantwortlicher oder als Auftragsverarbeiter tätig ist, agiert. Der Kunde oder der entsprechende Verantwortliche bestimmt die Zwecke der Erfassung und der Verarbeitung der personenbezogenen Daten des Kunden;
- b) Swizzonic agiert in jedem Fall als Auftragsverarbeiter der personenbezogenen Daten des Kunde bei der Leistung des Dienstes; und
- c) dieser Vertrag regelt das Verhältnis zwischen den Vertragspartnern in Bezug auf die jeweiligen Aufgaben und Pflichten in Bezug auf die Verarbeitung der personenbezogenen Daten des Kunden, die von Swizzonic als Auftragsverarbeiter bei der Leistung des Dienstes erfolgt.

## 3. PFLICHTEN VON SWIZZONIC

3.1. Der Kunde oder der entsprechende Verantwortliche bestimmt die Zwecke der Verarbeitung der personenbezogenen Daten des Kunden bei der Leistung des Dienstes.

3.2. In Bezug auf die Leistung des Dienstes verpflichtet sich Swizzonic, folgende Pflichten einschließlich der in den Anhängen 1 und 2, die als ergänzender Teil dieses Vertrags erachtet werden, festgelegten einzuhalten:

- a) Swizzonic verarbeitet die personenbezogenen Daten des Kunden nur soweit dies unbedingt für die Leistung des Dienstes erforderlich ist unter Einhaltung der schriftlich vom Kunden mit diesem Vertrag erteilten Anweisungen;
- b) Swizzonic verständigt den Kunden, sollte er der Meinung sein, dass die schriftlich erteilten Anweisungen die anwendbaren gesetzlichen Datenschutzbestimmungen verletzen. In keinem Fall ist Swizzonic von der Pflicht befreit, die schriftlich vom Kunden erteilten Anweisungen einer ausführlichen rechtlichen Prüfung zu unterziehen;
- c) Swizzonic verständigt in seiner Rolle als Auftragsverarbeiter den Kunden unverzüglich von jeder Kontaktaufnahme oder Mitteilung seitens einer Aufsichtsbehörde in Bezug auf die Verarbeitung der personenbezogenen Daten des Kunden. Diesbezüglich stimmen die Vertragspartner zu und vereinbaren, dass ausschließlich der Kunde und nicht der Auftragsverarbeiter für die Beantwortung dieser Anfragen verantwortlich ist.
- d) Swizzonic hat operative, technische und organisatorische Maßnahmen einschließlich der im Anhang 2 an diesen Vertrag beschriebenen getroffen, um die personenbezogenen Daten des Kunden zu schützen. Die Vertragspartner sind sich bewusst und vereinbaren, dass Swizzonic ausdrücklich befugt ist, alternative Maßnahmen zu treffen oder alternative Aufbewahrungsorte der Daten festzulegen, sofern das Sicherheitsniveau der gewählten Maßnahmen oder der gewählten Orte im Vergleich zu den erklärten Maßnahmen beibehalten oder verbessert wird.
- e) Im Fall, dass Swizzonic die personenbezogenen Daten des Kunden dem eigenen Personal mitteilt, das direkt und ausschließlich mit der Lieferung des Dienstes beauftragt ist, gewährleistet Swizzonic, dass genanntes Personal: 1) sich verpflichtet hat, die Vertraulichkeit zu wahren, oder einer gesetzlichen Vertraulichkeitspflicht unterliegt und; 2) die personenbezogenen Daten des Kunden entsprechend den Anweisungen des Auftragsverarbeiters unter Einhaltung der in diesem Vertrag enthaltenen Pflichten verarbeitet.

#### 4. PFLICHTEN DES KUNDEN

4.1. Der Kunde ist sich bewusst und stimmt zu, dass er dem Auftragsverarbeiter personenbezogene Daten des Kunden liefert, um die Leistung des Dienstes seitens des Auftragsverarbeiters zu ermöglichen. Der Kunde verpflichtet sich, zu überprüfen, dass die im Anhang 2 dieses Vertrags angeführten Sicherheitsmaßnahmen mit den Arten von personenbezogenen Daten vereinbar sind, die der Kunde dem Auftragsverarbeiter anzuvertrauen beabsichtigt, und dem Auftragsverarbeiter eventuelle kritische Aspekte mitzuteilen, um gemeinsam mit Swizzonic über eventuelle auszuführende Eingriffe sowie die Vereinbarkeit des Dienstes mit den personenbezogenen Daten des Kunden zu entscheiden.

4.2. Der Kunde gewährleistet und garantiert, dass:

- a) eine geeignete rechtliche Grundlage (z. B. Zustimmung der betroffenen Person, berechtigtes Interesse, Genehmigung der zuständigen Aufsichtsbehörde usw.) besteht, um mit der Verarbeitung und Übermittlung der personenbezogenen Daten des Kunden an den Auftragsverarbeiter als Teil der Lieferung des Dienstes fortzufahren; und
- b) die in diesem Vertrag angeführten Vorgaben die Pflichten widerspiegeln, an die sich Swizzonic unter Einhaltung der anwendbaren gesetzlichen Datenschutzbestimmungen halten muss, deren Gegenstand die Verarbeitung der personenbezogenen Daten des Kunden für die Leistung des Dienstes sind.

#### 5. ZUSTIMMUNG ZUR VERARBEITUNG DER DATEN SEITENS DER UNTERAUFTRAGSVERARBEITER

5.1. Der Kunde erkennt an, akzeptiert und stimmt zu, dass die personenbezogenen Daten des Kunden ausschließlich zum Zweck der Lieferung des Dienstes und unter Einhaltung der Bestimmungen in diesem

Vertrag vom Auftragsverarbeiter oder seinen Unterauftragsverarbeitern entsprechend den Angaben im Verzeichnis der Unterauftragsverarbeiter verarbeitet werden könnten.

5.2. Gemäß Art. 5.1 ist Swizzonic berechtigt, unter folgenden Bedingungen auf Unterauftragsverarbeiter zurückzugreifen:

- a) dass der Kunde im Vorhinein von der Identität der Unterauftragsverarbeiter entsprechend den Angaben im Verzeichnis der Unterauftragsverarbeiter verständigt wird und dem Kunden jede Aktualisierung des genannten Verzeichnisses mitgeteilt wird, damit der Kunde die Möglichkeit hat, sich dem Einsatz genannter Unterauftragsverarbeiter zu widersetzen;
- b) dass Vereinbarungen mit dem Unterauftragsverarbeiter abgeschlossen werden, die die gleichen in diesem Vertrag vorgesehenen Pflichten bezüglich der Verarbeitung der personenbezogenen Daten des Kunden enthalten;
- c) dass angemessene Kontrollen bei der Auswahl der Unterauftragsverarbeiter durchgeführt werden und Swizzonic weiterhin für die Erfüllung der in diesem Vertrag enthaltenen Pflichten seitens der beteiligten Unterauftragsverarbeiter verantwortlich bleibt;
- d) dass Swizzonic dem Kunden auf dessen Anfrage angemessene Informationen bezüglich der Handlungen und Maßnahmen liefert, die Swizzonic und seine Unterauftragsverarbeiter getroffen haben, um die Einhaltung der Bestimmungen dieses Vertrags zu gewährleisten.

## 6. ÜBERMITTLUNG DER PERSONENBEZOGENEN DATEN

6.1. Sollte der Kunde einen oder mehrere Dienste kaufen, an denen Unterauftragsverarbeiter aus Nicht-EWR-Ländern / der Schweiz beteiligt sind, kann Swizzonic gemäß den vorangehenden Art. 5.1 und 5.2 die personenbezogenen Daten des Kunden an einen oder mehrere weitere Unterauftragsverarbeiter übermitteln, die Unterauftragsverarbeiter aus Nicht-EWR-Ländern / der Schweiz sind und zu den Zwecken der Standardvertragsklauseln als Datenimporteure erachtet werden. In diesem Fall erklärt Swizzonic im Fall, dass es keine an den Unterauftragsverarbeiter aus Nicht-EWR-Ländern / der Schweiz anwendbaren Angemessenheitsbeschlüsse gibt, dass die Standardvertragsklauseln mit dem Unterauftragsverarbeiter aus Nicht-EWR-Ländern / der Schweiz unterzeichnet wurden, und erkennt an, dass nur die im MODUL DREI genannten Klauseln der Standardvertragsklauseln angewendet werden: Übermittlung von Auftragsverarbeiter an Auftragsverarbeiter (mit Ausnahme der anderen MODULE). Falls dies von den anwendbaren gesetzlichen Datenschutzbestimmungen vorgeschrieben wird, verpflichtet sich Swizzonic auch, diese Standardvertragsklauseln für Übermittlungen personenbezogener Daten des Kunden aus der Schweiz an einen oder mehrere Unterauftragsverarbeiter mit Sitz im EWR abzuschließen.

6.2. Kein Teil dieses Vertrags ist gegenüber den Klauseln der Standardvertragsklauseln vorrangig.

6.3. Auf Anfrage kann der Kunde die Standardvertragsklauseln überarbeiten. Es gilt als vereinbart, dass Swizzonic im zum Schutz von Betriebsgeheimnissen oder sonstigen vertraulichen Informationen einschließlich von personenbezogenen Daten erforderlichen Ausmaß einen Teil des Textes der Standardvertragsklauseln schwärzen kann, bevor eine Kopie geteilt wird.

6.4. Der Kunde ist einverstanden, dass er dafür verantwortlich ist, alle eventuellen Aufgaben und zusätzlichen anwendbaren Pflichten zu beachten, um die Rechtmäßigkeit der Übermittlung der personenbezogenen Daten an die Auftragsverarbeiter und die Unterauftragsverarbeiter gemäß den anwendbaren gesetzlichen Datenschutzbestimmungen zu ermöglichen.

6.5. Sollte der Kunde ein Verantwortlicher aus Nicht-EWR-Ländern / der Schweiz sein, vereinbaren Swizzonic und der Verantwortliche aus Nicht-EWR-Ländern / der Schweiz, dass die Standardvertragsklauseln hiermit als in diese Datenschutzvereinbarung zur Bezugnahme integriert angenommen werden, was jede Übermittlung personenbezogener Daten des Kunden vom Verantwortlichen aus Nicht-EWR-Ländern / der Schweiz an Swizzonic im Rahmen der Lieferung der Dienste betrifft. In diesem Fall gelten für die Standardvertragsklauseln folgende Spezifikationen:

- (i) Die Klausel 7 der Standardvertragsklauseln kommt zur Anwendung.
- (ii) Nur die im MODUL VIER genannten Klauseln der Standardvertragsklauseln kommen zur Anwendung: Übermittlung von Auftragsverarbeitern an Verantwortliche (mit Ausnahme der anderen MODULE).
- (iii) Die Klauseln 14 und 15 kommen nicht zur Anwendung, da die Dienste keine Kombination der vom Verantwortlichen aus Nicht-EWR-Ländern / der Schweiz erhaltenen personenbezogenen Daten des Kunden mit von Swizzonic in der EU und in der Schweiz erfassten anderen personenbezogenen Daten bedingt.
- (iv) Gemäß Klausel 17 der Standardvertragsklauseln kommt die Option 2 zur Anwendung. Das italienische Gesetz wird angewendet.
- (v) Gemäß Klausel 18 der Standardvertragsklauseln geben die Vertragspartner die Gerichte von Florenz (Italien) an.
- (vi) Nur Anhang 1 dieser DPA kommt zur Anwendung und wird als Anhang I der Standardvertragsklauseln erachtet.

## **7. PFLICHTEN IN SACHEN ZUSAMMENARBEIT UND VERANTWORTLICHKEIT**

7.1. Die Vertragspartner verpflichten sich, nach bestem Wissen und Gewissen zusammenzuarbeiten, um die Einhaltung der Bestimmungen in diesem Vertrag zu gewährleisten. Darunter fällt unter anderem die Pflicht, die korrekte und zeitgerechte Ausübung der Rechte der betroffenen Person zu gewährleisten und Sicherheitsvorfälle/Verletzungen der personenbezogenen Daten zu managen, um die möglichen unerwünschten Auswirkungen, die sich daraus ergeben, zu mindern.

7.2 Die Vertragspartner arbeiten nach bestem Wissen und Gewissen zusammen, um einander gegenseitig und der Aufsichtsbehörde die Informationen zur Verfügung zu stellen, die notwendig sind, um die Einhaltung der anwendbaren gesetzlichen Datenschutzbestimmungen zu beweisen.

## **8. RECHTE DER BETROFFENEN PERSON**

8.1. In Erachtung der Natur der Verarbeitung unterstützt Swizzonic den Kunden mit technischen und organisatorischen Maßnahmen, die geeignet sind, um die Erfüllung der Pflichten des Kunden zur Beantwortung der Anfragen um die Ausübung der Rechte der betroffenen Person zu gewährleisten.

8.2. Swizzonic liefert dem Kunden eine angemessene Zusammenarbeit und Unterstützung und liefert alle vernünftigerweise zum Zweck, der betroffenen Person zu antworten oder dem Kunden zu ermöglichen, die Einhaltung seiner Pflichten bezüglich der Rechte der betroffenen Person gemäß den anwendbaren gesetzlichen Datenschutzbestimmungen zu beweisen, verlangten Informationen. Der Kunde erkennt an und akzeptiert, dass im Fall, dass diese Zusammenarbeit und Unterstützung einen beachtlichen Einsatz von Ressourcen seitens des Auftragsverarbeiters erfordern, diese Bemühungen dem Kunden nach Vorankündigung und Einvernehmen in Rechnung gestellt werden können.

## **9. HERAUSGABE DER DATEN UND LÖSCHUNG**

9.1. Nach dem Ablaufdatum oder der vorgezogenen Auflösung dieses Vertrags und/oder auf Anfrage des Kunden gibt Swizzonic die personenbezogenen Daten des Kunden heraus oder vernichtet sie unter der Bedingung, dass angemessen im Voraus eine schriftliche Anfrage gestellt wird, sofern keine spezifischen gesetzlich vorgesehenen Aufbewahrungspflichten bestehen (einschließlich zum Beispiel, aber nicht beschränkt auf in den anwendbaren gesetzlichen Datenschutzbestimmungen vorgesehene Pflichten oder Anfragen seitens der Justizbehörde), darunter unter anderem die von der Aufsichtsbehörde stammenden, die den Auftragsverarbeiter an der Erfüllung hindern.

9.2. Um die spezifische Anfrage des Kunden mit dem Ziel der Herausgabe der personenbezogenen Daten des Kunden zu erfüllen, wird diese Anfrage im Rahmen des Möglichen vorbehaltlich der wirtschaftlich vertretbaren technischen und organisatorischen Einschränkungen im Verhältnis zum Volumen, der Einstufung und der Menge an personenbezogenen Daten, die Gegenstand der Verarbeitung sind, erfüllt.

9.3. Die personenbezogenen Daten des Kunden, die von der Herausgabe betroffen sind, müssen nach der internen Standardprozedur von Swizzonic ohne Kosten für den Kunden herausgegeben werden oder alternativ dazu zu vernünftigen Kosten für den Kunden zurückgegeben werden.

9.4. Im Fall, dass der Kunde sich für die Löschung der personenbezogenen Daten des Kunden entscheidet, liefert Swizzonic unbeschadet der Vorgaben im folgenden Art. 9.5 eine Bescheinigung zur Gewährleistung dieser Löschung.

9.5. Swizzonic kann die personenbezogenen Daten des Kunden beibehalten, die mit regelmäßigen Backup-Vorgängen unter Einhaltung der *Disaster Recovery*- und *Business Continuity*-Protokolle des Auftragsverarbeiters gespeichert wurden (siehe Art. 12), sofern Swizzonic jene personenbezogenen Daten des Kunden nicht aktiv oder absichtlich zu anderen Zwecken als der Lieferung des Dienstes verarbeitet oder seine Unterauftragsbearbeitern hierzu befugt.

## 10. ÜBERMITTLUNG

10.1. Die vom Auftragsverarbeiter in Bezug auf den Dienst über Internet übermittelten personenbezogenen Daten müssen angemessen verschlüsselt werden. Die Vertragspartner sind sich außerdem bewusst, dass die Sicherheit der Übermittlungen im Internet nicht vollkommen garantiert werden kann. Swizzonic haftet nicht für den Zugang des Kunden ins Internet, für ein eventuelles Abfangen oder Unterbrechungen jeder Kommunikation über Internet oder Änderungen oder Verluste von personenbezogenen Daten über Internet.

10.2. Im Fall, dass der Verdacht auf eine Verletzung der personenbezogenen Daten besteht, kann Swizzonic in Erwartung der Suche nach den Ursachen die Nutzung des Dienstes über Internet seitens des Kunden unverzüglich aussetzen, unter der Bedingung, dass Swizzonic diese Aussetzung meldet, sobald dies vernünftigerweise möglich ist, sowie alle angemessenen Maßnahmen trifft, um den Dienst über Internet schnell wieder herzustellen, und mit dem Kunden zusammenarbeitet, um die Leistung des Dienstes über andere verfügbare Kommunikationskanäle fortzusetzen.

10.3. Der Kunde wird alle angemessenen und notwendigen Maßnahmen treffen, um die Vertraulichkeit der Namen und der Passwörter der Kunden für die Leistung des Dienstes zu wahren. Der Kunde haftet für die Folgen jeder unangemessenen Nutzung des Dienstes seitens der Arbeitnehmer des Kunden.

## 11. VERLETZUNG DER PERSONENBEZOGENEN DATEN

11.1 Der Kunde ist sich bewusst und stimmt zu, dass Swizzonic im Fall der Verletzung der personenbezogenen Daten, die nicht der Nachlässigkeit von Swizzonic zuzuschreiben sind, nicht zur Verantwortung gezogen wird.

11.2 Sollte Swizzonic in Kenntnis einer Verletzung der personenbezogenen Daten gelangen, muss Swizzonic:

- angemessene Maßnahmen treffen, um die Auswirkungen dieser Verletzung der personenbezogenen Daten abzuwachen, einschließlich der unverzüglichen Benachrichtigung des Kunden, um ihm zu ermöglichen, schnell die notwendigen Gegenmaßnahmen zu treffen. Unbeschadet des oben gesagten behält sich Swizzonic das Recht vor, die Maßnahmen festzulegen, die getroffen werden müssen, um sich an die anwendbaren gesetzlichen Datenschutzbestimmungen anzupassen oder Ihre Rechte und Interessen zu schützen;
- mit dem Kunden zusammenarbeiten, um folgendes herauszufinden: die Natur, die Kategorien und die ungefähre Anzahl an betroffenen Personen und die Kategorien und die ungefähre Anzahl an betroffenen

personenbezogenen Daten und die wahrscheinlichen Folgen dieser Verletzung mit Modalitäten, die der Ernsthaftigkeit der Verletzung und ihren Gesamtauswirkungen auf den Kunden und auf die Leistung des in diesem Vertrag vorgesehenen Dienst angemessen sind;

c) falls die anwendbaren gesetzlichen Datenschutzbestimmungen die Verständigung der zuständigen Aufsichtsbehörden und der von der Verletzung der personenbezogenen Daten betroffenen Personen erfordern und falls diese sich auf personenbezogenen Daten des Kunden bezieht, muss Swizzonic den Kunden befragen und Anweisungen bei ihm einholen, wobei der Kunde als einziger das Recht hat, die Maßnahmen festzulegen, die getroffen werden müssen, um die anwendbaren gesetzlichen Datenschutzbestimmungen zu erfüllen oder jedes Risiko abzuwenden, darunter unter anderem:

- i. festlegen, ob ein Individuum, eine Regulierungsbehörde, Justizbehörde, Konsumentenschutzeinrichtung oder sonstige entsprechend den Vorgaben nach den anwendbaren gesetzlichen Datenschutzbestimmungen oder im Ermessen des Kunden liegende Einrichtung benachrichtigt werden muss; und
- ii. den Inhalt dieser Benachrichtigung festlegen, festlegen, ob es möglich ist, der von der Verletzung betroffenen Person Abhilfemaßnahmen anzubieten sowie die Natur und das Ausmaß dieser Mittel festlegen.

## 12. DISASTER RECOVERY UND BUSINESS CONTINUITY

12.1 Swizzonic wendet nach den Kriterien der beruflichen Sorgfalt Disaster Recovery- und Business Continuity-Protokolle an, die je nach Dienst unterschiedlich sind und die dem Kunden auf Anfrage in zusammengefasster Version zur Verfügung gestellt werden, und aktualisiert diese. Swizzonic kann dieses Programm jederzeit ändern, sofern seine Fähigkeit, eine Disaster Recovery zu bewältigen, nicht auf ein niedrigeres Niveau als das im genannten Programm bei der Unterzeichnung dieses Vertrags vorgesehene sinkt.

## 13. AUFTRAG

13.1 Durch die Unterzeichnung dieses Vertrags einschließlich der Anhänge 1, 2 und 3 gibt der Kunde dem Auftragsverarbeiter ausdrücklich den Auftrag, im Namen des Kunden die in den vorangehenden Klauseln 5 und 6 beschriebenen Tätigkeiten auszuführen.

13.2 Durch die Unterzeichnung dieses Vertrags akzeptiert Swizzonic den Auftrag, der ohne finanzielle Entlohnung ausgeführt wird, da er mit der Lieferung des Dienstes verbunden ist, und bestätigt, die erteilten Anweisungen gelesen und verstanden zu haben.

Der Kunde

Swizzonic A.G.

Vor- und Nachname / Firmenbezeichnung

St.-Nr. / USt-IdNr. \_\_\_\_\_

St.-Nr. / USt-IdNr. \_\_\_\_\_

Datum und Ort \_\_\_\_\_

Datum und Ort, \_\_\_\_\_

(Unterschrift) \_\_\_\_\_

(Unterschrift) \_\_\_\_\_

# ANHANG 1

## 1. BETROFFENE PERSONEN

Die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, betreffen folgende Kategorien von betroffenen Personen (mit einem X ankreuzen):

- Kunden und/oder potentielle Kunden
  - Lieferanten
  - Arbeitnehmer und/oder potentielle Arbeitnehmer
  - Berater und/oder Fachleute
  - sonstiges (bitte angeben):
- 

## 2. KATEGORIEN DER FÜR JEDEN DIENST VERARBEITETEN PERSONENBEZOGENEN DATEN

Die von der Verarbeitung betroffenen personenbezogenen Daten beziehen sich auf folgende Datenkategorien von personenbezogenen Daten (mit einem X ankreuzen):

- Kontaktdaten (Vor- und Nachname, E-Mail-Adresse, Postanschrift, Telefonnummer)
  - Geburtsdatum
  - Alter
  - Geschlecht
  - sonstiges (bitte angeben):
- 

## 3. BESONDERE KATEGORIEN VON PERSONENBEZOGENEN DATEN

Die von der Übermittlung/Verarbeitung betroffenen personenbezogenen Daten beziehen sich auf folgende besondere Kategorien von personenbezogenen Daten (mit einem X ankreuzen):

- Behinderungen und/oder Unfälle
  - politische Meinung
  - ethische oder religiöse Überzeugungen
  - sexuelle Orientierung, in der die eheliche Beziehung oder der Familienstand impliziert ist
  - Gewerkschaftszugehörigkeit
  - Gesundheitszustand und/oder Krankheiten
  - strafrechtliche Verurteilungen und Verhaftungen
  - sonstiges (bitte angeben):
- 

## 4. VERARBEITUNGSVORGÄNGE

Die personenbezogenen Daten können nur in Verbindung mit der Lieferung des Dienstes entsprechend der Beschreibung im Master-Vertrag übermittelt/verarbeitet werden.

## 5. NATUR DER VERARBEITUNG

Die Natur der Verarbeitungsvorgänge ist je nach dem spezifischen anhand des Master-Vertrags aktivierten Dienst unterschiedlich.

## 6. HÄUFIGKEIT DER VERARBEITUNG

Die Häufigkeit der Verarbeitungsvorgänge ist je nach dem spezifischen anhand des Master-Vertrags aktivierten Dienst unterschiedlich.

## **7. DAUER DER VERARBEITUNG**

Die personenbezogenen Daten des Kunden werden so lange aufbewahrt, wie der Dienst aktiv bleibt.

## ANHANG 2

### **Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen**

Swizzonic und die Unterauftragsverarbeiter verpflichten sich, ein Sicherheitsniveau zu garantieren, das nicht unter dem in den nachfolgend beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen vorgesehenen liegt.

#### **Informationen zu den Sicherheitsmaßnahmen**

##### **Prozeduren zur Sicherheit der Informationen**

###### ***Interne Organisation***

Es wurden separate Rollen und Verantwortungen für die Sicherheit der Informationen festgelegt und den zur Verarbeitung der personenbezogenen Daten der Gesellschaft berechtigten Personen (im Folgenden auch „Nutzer“) zugewiesen, um Interessenkonflikte zu vermeiden und unangemessenen Tätigkeiten vorzubeugen.

###### **Sicherheit der Humanressourcen**

###### ***Mobilgeräte und Telearbeit***

Für die Verwendung aller Firmengeräte, insbesondere der Mobilgeräte, ist eine Sicherheitsrichtlinie vorgesehen und angemessene Kontrollen werden durchgeführt.

###### ***Beendigung oder Änderungen des Arbeitsverhältnisses***

Im Moment des Ausscheidens eines Nutzers aus der Organisation oder im Fall einer nennenswerten Änderung der von ihm ausgeübten Rolle werden die Zugangsrechte sofort aktualisiert, die Instrumente des Betriebs zurückgegeben und sowohl physisch als auch logisch rückgesetzt.

###### **Verwaltung der Ressourcen des Firmenvermögens**

###### ***Verantwortung für die Ressourcen des Firmenvermögens***

Alle Ressourcen des Firmenvermögens werden sorgfältig erfasst und ihre Zuweisung zu den verschiedenen Nutzern, die für ihre Sicherheit verantwortlich sind, wird überwacht. Eine Richtlinie für ihre korrekte Verwendung wurde festgelegt.

###### ***Einstufung der Informationen***

Die Informationen werden von den jeweiligen Nutzern im Einklang mit den Vorgaben der Sicherheitsanforderungen eingestuft und katalogisiert sowie angemessen verarbeitet.

###### ***Verwaltung der Medien***

Die auf Medien aufbewahrten Informationen werden so verwaltet, kontrolliert, verändert und verwendet, dass ihr Inhalt nicht beeinträchtigt wird, und angemessen gelöscht.

###### **Zugriffskontrolle**

###### ***Betriebsanforderungen für die Zugriffskontrolle***

Die organisatorischen Betriebsanforderungen für die Zugriffskontrolle zu den Informationsressourcen sind in einer Richtlinie und einer Zugriffskontrollprozedur dokumentiert; der Zugang zum Netz und die Verbindungen ist beschränkt.

###### ***Verwaltung der Zugriffe der Nutzer***

Die Zuweisung der Zugriffsrechte zu den Nutzer wird durch die anfängliche Registrierung des Nutzers bis zum Entzug der Zugriffsrechte, wenn sie nicht mehr notwendig sind, kontrolliert, einschließlich der besonderen Einschränkungen für die Rechte auf privilegierten Zugriff und die Verwaltung der „geheimen Authentifizierungsinformationen“, und unterliegt periodischen Prüfungen und Kontrollen, wozu auch die Aktualisierung der Zugriffsrechte zählt. Bei der Verwaltung der Zugriffe wird das Kriterium der Minimierung der Zugriffsrechte angewendet, die verliehen werden, um dem Nutzer nur den Zugriff auf die Daten zu ermöglichen, die für seine Tätigkeit notwendig sind. Für weitere Zugriffsrechte ist eine spezifische Genehmigung erforderlich.

###### ***Haftung der Benutzer***

Die Nutzer sind sich ihrer Verantwortungen auch anhand der Aufrechterhaltung einer effizienten Zugriffskontrolle bewusst, indem sie zum Beispiel ein komplexes Passwort wählen, wobei diese Komplexität in jedem Fall vom System überprüft wird, und es geheim zu halten.

#### ***Systeme und Anwendungen für die Zugriffskontrolle***

Der Zugriff auf die Informationen unterliegt Einschränkungen entsprechend der Richtlinie über die Zugriffskontrolle anhand eines Systems von sicheren Zugriffen und der Verwaltung der Passwörter für den Zugriff. Hierzu kommt die Kontrolle bezüglich privilegierter Nutzer und der beschränkte Zugriff auf alle Quellcodes.

#### **Verschlüsselung**

##### ***Kryptografische Prüfung***

Eine Richtlinie bezüglich der Verwendung der Verschlüsselung der Datenträger und der Daten der Nutzer gilt. Die Authentifizierungen sind verschlüsselt.

#### **Physische Sicherheit und Sicherheit der Umgebung**

Es werden Maßnahmen zur physischen Sicherheit und Sicherheit der Umgebung angewendet, die darauf abzielen, den Zugriff, Verlust oder die unrechtmäßige oder unabsichtliche Verbreitung der in den verschiedenen Strukturen vorhandenen Daten zu vermeiden.

##### ***Sichere Bereiche: Rechenzentren***

Die Dienste der Gesellschaft werden in mehreren Rechenzentren (Data Center) in der ganzen Welt geleistet und beherbergt. Eines der wichtigsten für die Aufbewahrung der personenbezogenen Daten der Kunden verwendeten zählt zu den wenigen Rechenzentren mit Tier IV-Zertifizierung, das heißt mit der höchsten Garantie, die ein Rechenzentrum bieten kann. Alle Rechenzentren innerhalb der Lieferkette bieten die komplette Redundanz aller Strom- und Kühlkreise und Netzwerke. Alle Rechenzentren verfügen über eine Außenbeleuchtung sowie ein Präsenzmeldersystem mit Videoüberwachung; die Notausgänge sind mit Alarm ausgestattet. Alle Alarme sind im Control Room konzentriert.

Der tatsächliche Zugang wird durch Bewilligungs-, Erkennungs- und Registrierprozeduren geregelt und kontrolliert und dank des Zutrittskontrollsystems auf die Bereiche beschränkt, für die man eine Bewilligung hat.

#### ***Geräte***

Eine Richtlinie für die Entsorgung der ausrangierten Geräte gilt, um die enthaltenen Informationen auf sichere Weise zu vernichten.

#### **Sicherheit der Vorgänge**

##### ***Prozeduren und operative Verantwortungen***

Die operativen Verantwortungen im IT-Bereich sind dokumentiert und die Änderungen an den Strukturen und IT-Systemen sind kontrolliert. Die Entwicklungssysteme, Prüfsysteme und Betriebssysteme sind getrennt. Es wurden Nutzer festgelegt, die dafür verantwortlich sind, dass die Prozeduren korrekt funktionieren. Für die Verwaltung der logischen Sicherheit der vom Kunden installierten Betriebssysteme und Anwendungen ist hingegen der Kunde der einzelnen Dienste der Gesellschaft (im Folgenden auch der „Kunde“) zuständig.

##### ***Schutz vor Malware***

Auf den Geräten des Betriebs ist eine Viren- und Malware-Kontrolle aktiv und seitens der Nutzer gibt es ein angemessenes Bewusstsein diesbezüglich.

Bezüglich der Dienste des Virtuellen Servers oder Dedizierten Servers ist der Kunde für die Installation von Antivirus und Anti-Malware und - falls nicht der entsprechende Dienst gekauft wurde - Firewall zuständig. Bezüglich des Hosting-Dienstes hingegen ist ein Echtzeit-Schutz an den Front-End-Maschinen aktiv.

Bezüglich des E-Mail-Dienstes wird sowohl der ein- als auch ausgehende E-Mail-Verkehr in Echtzeit analysiert, um Viren und Malware zu entdecken und Spam zu erkennen und herauszufiltern. Die Analyse erfolgt automatisch und beruht sowohl auf der Natur des Inhalts als auch auf der Befragung internationaler Datenbanken als auch dem dank einer Reihe von Parametern erworbenen Ruf.

##### ***Backup***

Mit Ausnahme der Dienste, für die der Kunde für die Durchführung und Verwaltung der Backups verantwortlich ist (Dedizierte Server und Virtuelle Server), werden periodisch Backups erstellt. Für die

Hosting- und E-Mail-Dienste werden periodisch Backups erstellt, auf die bei den Hosting-Diensten auch der Kunde zugreifen kann. Weitere nicht für die Kunden zugängliche Backups werden nur zum Zweck der Disaster Recovery erstellt.

### **Authentifizierung und Überwachung**

#### ***Authentifizierung und Synchronisierung***

Jede Tätigkeit und jedes Ereignis in Bezug auf die Sicherheit der Informationen seitens der Nutzer des Systems und der Administratoren/Bediener erfolgt nach Eingabe der Authentifizierungsdaten oder Identitätszertifikate. Die Uhren aller Geräte sind synchronisiert.

#### ***Kontrolle der operativen Softwares***

Die Installation von Software auf den Betriebssystemen wird kontrolliert und überwacht.

Bezüglich der Virtuellen Server und der Dedizierten Server werden die dem Kunden überlassenen Betriebssysteme mit Installationsabbildern zur Verfügung gestellt, die auch in der Installationsphase vom Kunden zu aktualisieren sind. Der Kunde ist außerdem für die eventuelle Aktualisierung der Firmware und auch der vom Kunden installierten Anwendungen oder Softwares zuständig.

### **Schwachstellenmanagement**

#### ***Patch Management***

Jede technische Schwachstelle wird mit geeigneten Patches korrigiert und es sind Prozeduren für alle Testphasen und danach für die Installation der Software und der Aktualisierungen vorgesehen, die erst erfolgt, wenn alle Tests positiv ausfallen.

#### ***Überlegungen zur Prüfung für die Systeminformationen***

Periodisch werden Prüfung durchgeführt, um zu kontrollieren, dass eventuelle negative Auswirkungen auf die Produktionssysteme auf ein Mindestmaß reduziert werden und es keine missbräuchlichen Zugriffe auf die Daten gibt.

### **Sicherheit der Mitteilungen**

#### ***Verwaltung der Netzsicherheit***

Die Sicherheit der Netzwerke und die Dienste im Netzwerk wird auch durch ihre Trennung und Abgrenzung erzielt.

#### ***Übermittlung der Informationen***

Es bestehen Abkommen bezüglich der Übermittlung der Informationen von Dritten und an Dritte.

### **Beschaffung, Entwicklung und Wartung des Systems**

#### ***Sicherheit bei der Entwicklung und Unterstützungsverfahren***

Die Regeln für die Sicherheit der Entwicklung der Software und der Systeme werden in einer Richtlinie festgelegt. Änderungen am System (sowohl bezüglich der Anwendungen als auch der Betriebssysteme) sind kontrolliert. Die Sicherheit des Systems wurde getestet und es wurden Zulässigkeitskriterien festgelegt, zu denen auch die Sicherheitsaspekte zählen.

### **Beziehungen zu den Lieferanten**

#### ***Sicherheit der Informationen in den Beziehungen zu den Lieferanten***

Es sind Verträge und Abkommen vorgesehen, um die Verarbeitung der Informationen der Organisation und der Kunden, die im IT-Bereich tätigen Dritten und anderen Drittanbietern innerhalb der Lieferkette zugänglich sind, zu schützen und zu regeln.

#### ***Verwaltung der vom Anbieter gelieferten Dienste***

Die Leistung der von den Anbietern gelieferten Dienste wird in Bezug auf den Vertrag oder die Vereinbarung überwacht und überprüft. Jede Änderung am Dienst wird kontrolliert.

### **Management von Sicherheitsvorfällen in Bezug auf Informationen**

#### ***Management von Sicherheitsvorfällen in Bezug auf Informationen und Verbesserungen***

Es sind Verantwortungen und spezielle Prozeduren vorgesehen, um Ereignisse und eventuelle Vorfälle in Bezug auf die Sicherheit der Informationen konsequent und wirksam zu managen (z. B. sogenannte Data-Breach-Prozedur).

## **Aspekte der Sicherheit der Informationen in Bezug auf die Geschäftskontinuität**

### **Redundanzen**

Alle wichtigen IT-Strukturen sind redundant, um die Verfügbarkeitsanforderungen zu erfüllen. Wo keine solche Redundanz besteht, werden angemessene Maßnahmen getroffen, um die Kontinuität des Dienstes oder die Reduzierung des Datenverlustes auf ein Minimum zu garantieren.

### **Konformität**

#### ***Erfüllung der rechtlichen und vertraglichen Anforderungen***

Die Firma identifiziert und dokumentiert ihre Pflichten gegenüber externen Behörden und anderen Dritten in Bezug auf die Sicherheit der Informationen einschließlich des geistigen Eigentums, der Buchführungsunterlagen und der Informationen in Bezug auf den Datenschutz.

#### ***Prüfung der Sicherheit der Informationen***

Die Pläne der Organisation bezüglich der Sicherheit der Informationen und die Sicherheitsrichtlinien werden geprüft und bei Bedarf werden Korrekturmaßnahmen getroffen.

## ANHANG 3

Der Anhang 3 (Verzeichnis der Unterauftragsverarbeiter) ist schriftlich bei [legal@swizzonic.com](mailto:legal@swizzonic.com) zu beantragen.