Captns ● Konzept und Gestaltung
Bernstrasse 4, CH–3122 Kehrsatz +41 (0)31 331 76 36
www.captns.ch contact@captns.ch

Diese Vereinbarung basiert auf den von den Verbänden Swico und swissICT erstellten Branchenstandards.

AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV)

«Auftraggeber» oder «Verantwortlicher»:

_____
Vollständiger Name des Unternehmens

_____
Adresse (gemäss Handelsregistereintrag)

_____
Postleitzahl & Ort

«Auftragnehmer» oder «Auftragsverarbeiter»:
Captns & Partner GmbH,
Bernstrasse 4,
3122 Kehrsatz

(je einzeln eine «Partei», gemeinsam die «Parteien» genannt).

Captns ● Konzept und Gestaltung
Bernstrasse 4, CH–3122 Kehrsatz +41 (0)31 331 76 36
www.captns.ch contact@captns.ch

1. PRÄAMBEL UND GELTUNGSBEREICH

Die Parteien haben Vereinbarungen in Leistungen im Bereich Kommunikationsdesign und IT-Dienstleistungen geschlossen, in denen der Auftragnehmer als Leistungserbringer gegenüber dem Auftraggeber oder dessen Kunden auftritt.

Die Erbringung der Dienstleistungen gemäss Vertrag durch den Auftragnehmer kann als Verarbeitung von personenbezogenen Daten im Sinne des anwendbaren Datenschutzrechts qualifiziert werden. Soweit der Auftragnehmer im Rahmen der Zusammenarbeit als Auftragsverarbeiter oder Unterauftragsverarbeiter personenbezogene Daten des Auftraggebers oder dessen Kunden (Personendaten) verarbeitet (jeder Umgang mit Personendaten), ergänzt die vorliegende Auftragsverarbeitungsvereinbarung («AVV» oder «Vereinbarung») den Vertrag und konkretisiert die Verpflichtungen der Parteien zum Datenschutz. Als anwendbares Datenschutzrecht gilt das Schweizer Datenschutzgesetz sowie die europäische Datenschutzgrundverordnung (DSGVO), sofern und soweit diese anwendbar ist («anwendbares Datenschutzrecht»).

2. GEGENSTAND, DAUER, ART UND ZWECK DER VEREINBARUNG

Der Gegenstand des Auftrages sowie Art und Zweck der Verarbeitung ergeben sich durch die Vereinbarung der Leistungen und deren Bestätigung durch die Erteilung eines Auftrages in schriftlicher oder mündlicher Form oder mit der Akzeptanz unserer Auftragsbestätigung. Die vorliegende Vereinbarung tritt mit gegenseitiger Unterzeichnung in Kraft. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Vertrages (bzw. bei mehreren Verträgen des letzten aktiven Vertrages) zwischen dem Auftraggeber und dem Auftragnehmer, unter welchen der Auftragnehmer für den Auftraggeber Personendaten verarbeitet, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben. Zudem endet die AVV automatisch, sobald der Auftragnehmer keine Personendaten mehr für den Auftraggeber gemäss dem Vertrag besitzt und verarbeitet oder mit Beendigung des (letzten aktiven) Vertrages.

Die Möglichkeit zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Als wichtiger Grund gelten insbesondere ein wiederholter oder schwerwiegender Verstoss einer Partei gegen die Regelungen des Vertrages, dieser AVV oder gegen anwendbares Datenschutzrecht. Auch das Sonderkündigungsrecht gemäss Ziffer 10 berechtigt zur fristlosen Kündigung. Eine fristlose Kündigung dieser Vereinbarung berechtigt auch zur fristlosen Kündigung des Vertrages.

Soweit sich die Art der verarbeiteten Personendaten, die Art und der Zweck der Datenverarbeitung sowie die Kategorien der durch die Verarbeitung betroffenen Personen nicht bereits aus dem jeweiligen Vertrag ergeben, werden sie in einem oder mehreren Anhängen zu dieser Vereinbarung aufgeführt.

3. ANWENDUNGSBEREICH UND WEISUNGSRECHT

Der Auftragnehmer verarbeitet Personendaten ausschliesslich zweckgebunden gemäss dem jeweiligen Vertrag, dieser AVV oder den dokumentierten Weisungen des Auftraggebers.

Weisungen sind in der Regel in Textform (d.h. schriftlich, per E-Mail oder in einem dokumentierten elektronischen Format) zu erteilen. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Der Auftraggeber ist für den Nachweis der vollständigen Dokumentation zuständig.

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstosse gegen anwendbares Datenschutzrecht. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisungen so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.
Meldungen an die Behörden oder an betroffene Personen bezügliche Datenschutzverletzungen und -verstösse, darf der Auftragnehmer nur nach vorheriger Weisung des Auftraggebers selbst durchführen. Vorbehalten bleiben abweichende Pflichten des anwendbaren Rechts (z.B. verbindliche Anordnungen zuständiger Behörden), worüber der Auftraggeber zeitnah zu informieren ist, soweit dies rechtlich zulässig ist.

4. DATENSICHERHEIT

Der Auftragnehmer ergreift geeignete technische und organisatorische Massnahmen (TOM) gemäss Anhang 2, um in seinem Verantwortungsbereich die innerbetriebliche Organisation zu gestalten, zu überprüfen und laufend anzupassen, damit er stets ein angemessenes Datenschutzniveau gemäss anwendbaren Datenschutzrecht, einschliesslich - falls anwendbar - Art. 32 DSGVO, gewährleisten kann, um die Personendaten vor unbeabsichtigter oder unrechtmässigen Zerstörung, Verlust, Veränderung, Weitergabe etc. zu schützen. Der Auftragnehmer berücksichtigt dabei den Stand der Technik, die Implementierungskosten sowie die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und die Schwere des Risikos für die Rechte und Freiheiten von betroffenen Personen.
Die Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es können alternative oder zusätzliche Massnahmen umgesetzt werden, wenn das Schutzniveau der festgelegten Massnahmen nicht unterschritten wird.

5. VERTRAULICHKEIT

Der Auftragnehmer verpflichtet sich, unter dem Vertrag oder dieser AVV erhaltene Personendaten vertraulich zu behandeln und nur Personen zugänglich zu machen, die für die Erfüllung ihrer Pflichten gegenüber dem Auftragnehmer auf Zugang zu den Personendaten angewiesen sind. Der Auftragnehmer stellt sicher, dass sich die zur Verarbeitung der Personendaten befugten Personen zur Vertraulichkeit/Geheimhaltung verpflichtet haben, soweit sie nicht einer gesetzlichen Verschwiegenheitspflicht unterliegen. Den mit der Verarbeitung der relevanten Personendaten befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen ist es untersagt, die relevanten Personendaten ausserhalb des Vertrags und dieser AVV zu verarbeiten. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung dieser AVV für eine Dauer von fünf Jahren fort.

6. ANSPRECHPARTNER

Die Parteien geben in Anhang 1 (– Subunternehmerliste) je einen Ansprechpartner für alle Datenschutz-

belange im Rahmen der Zusammenarbeit bekannt sowie in den Fällen in denen dies vorgeschrieben ist, auch den Datenschutzbeauftragten.

7. RECHTE VON BETROFFENEN PERSONEN

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung, Auskunft oder anderen Ansprüchen zu personenbezogenen Personendaten direkt an den Auftragnehmer, wird der Auftragnehmer die betroffene Person ohne Verzug an den Auftraggeber verweisen, sofern eine Zuordnung zum Auftraggeber nach Angaben der betroffenen Person möglich ist.
Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung mit geeigneten technischen und organisatorischen Massnahmen dabei, seiner Pflicht nachzukommen, Anträge von betroffenen Personen auf zustehende Rechte gemäss anwendbarem Datenschutzrecht zu beantworten.
Die Unterstützungspflichten des Auftragnehmers gegenüber dem Auftraggeber gemäss dieser Ziffer 7 erfolgen kostenlos. Über weitergehende Unterstützungsleistungen können die Parteien eine Vergütungsregelung treffen.

8. DATENSCHUTZVERLETZUNG

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn:
(i) vom Auftragnehmer oder einem Unterauftragsverarbeiter eine Datenschutzverletzung festgestellt oder vermutet wird. Dabei sind diejenigen Informationen gemäss anwendbarem Datenschutzrecht (u.a. Art, Umfang, Ausmass der Verletzung) zu liefern, damit der Auftraggeber einer eventuellen Meldepflicht an die zuständige Datenschutzbehörde und/oder die betroffenen Personen gemäss anwendbarem Datenschutzrecht nachkommen kann;
(ii) die Personendaten an eine zuständige Behörde weitergegeben werden sollen;
(iii) eine Anfrage, Vorladung oder Antrag auf Einsichtnahme oder Prüfung der Verarbeitung durch eine zuständige Behörde eingeht, ausser die Mitteilung an den Auftraggeber ist gesetzlich untersagt.
Im Falle einer Datenschutzverletzung beim Auftragnehmer oder einem Unterauftragsverarbeiter, trifft der Auftragnehmer auf eigene Kosten die vernünftigerweise zumutbaren Massnahmen, um die Ursache der Datenschutzverletzung zu ermitteln sowie zur Sicherung des Schutzes der Personendaten und zur Minderung möglicher nachteiligen Folgen für die betroffenen Personen.
Die Unterstützungspflichten des Auftragnehmers gegenüber dem Auftraggeber gemäss dieser Ziffer 8 erfolgen kostenlos. Über weitergehende Unterstützungsleistungen können die Parteien eine Vergütungsregelung treffen.

9. HERAUSGABE UND LÖSCHUNG VON PERSONENDATEN

Der Auftragnehmer gibt alle Daten, Datenträger sowie sonstige Materialien auf erste Instruktion des Auftraggebers hin unverzüglich an den Auftraggeber zurück. Der Auftragnehmer darf Daten nicht länger aufbewahren, als dies für die Erfüllung seiner Verpflichtungen gemäss dem Vertrag erforderlich ist, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht.
Bei Beendigung des Vertrages sind die unter dem Vertrag oder dieser AVV erhaltenen Personendaten gemäss

den vertraglichen Bestimmungen entweder dem Auftraggeber herauszugeben oder zu löschen, falls eine solche Bestimmung fehlt, sind nach Wahl des Auftraggebers die Personendaten entweder dem Auftraggeber herauszugeben und bestehende Kopien zu löschen oder sie sind zu löschen, sofern nicht von Gesetzes wegen einer Verpflichtung des Auftragnehmers besteht, die Personendaten aufzubewahren oder zu speichern. Bis zur Löschung oder Herausgabe stellt der Auftragnehmer weiterhin die Einhaltung dieser AVV sicher.

10. BEIZUG VON UNTERAUFTRAGSVERARBEITERN

Der Auftragnehmer erhält hiermit eine vorherige allgemeine schriftliche Genehmigung, für die Verarbeitung von Personendaten Unterauftragsverarbeiter beizuziehen. Soweit sich die zulässigen Unterauftragsverarbeiter nicht bereits aus dem Vertrag ergeben, sind sie in Anhang 1 (– Subunternehmerliste) aufzuführen. Die Liste der Unterauftragsverarbeiter ist laufend auf dem aktuellen Stand zu halten.
Ein Hinzufügen sowie der Austausch von Unterauftragsverarbeitern durch den Auftragnehmer erfolgen nach dem Ermessen des Auftragnehmers. Der Auftragnehmer ist verpflichtet, die erforderlichen Vereinbarungen mit dem Unterauftragsverarbeiter abzuschliessen, um sicherzustellen, dass der Unterauftragsverarbeiter denselben Verpflichtungen unterliegt, wie sie dem Auftragnehmer auf Grund vorliegender AVV und des jeweiligen Vertrages obliegen. Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf seine Anforderung hin Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen durch den Unterauftragsverarbeiter zu erteilen.
Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für etwaige Verstösse durch den Unterauftragsverarbeiter gemäss den Bestimmungen dieser AVV.

11. DOKUMENTATION, VERARBEITUNGSVERZEICHNIS

Jede Partei ist für die Einhaltung ihrer Dokumentationspflichten verantwortlich, insbesondere für die Führung von Verarbeitungsverzeichnissen, soweit dies nach dem anwendbaren Datenschutzrecht erforderlich ist. Jede Partei unterstützt die andere Partei in angemessener Weise bei der Erfüllung von deren Dokumentationspflichten, einschliesslich der Bereitstellung der Informationen, die die andere Partei von ihr benötigt, in einer von der anderen Partei in angemessener Weise angeforderten Form (z.B. durch die Verwendung eines elektronischen Systems), damit die andere Partei den Verpflichtungen im Zusammenhang mit der Führung von Verarbeitungsverzeichnissen nachkommen kann.

12. DATENSCHUTZ-FOLGENABSCHÄTZUNG

Wenn der Auftraggeber gemäss anwendbarem Datenschutzrecht verpflichtet ist, eine Datenschutz-Folgenabschätzung oder eine vorherige Konsultation mit einer Aufsichtsbehörde durchzuführen, stellt der Auftragnehmer auf Wunsch des Auftraggebers diejenigen Dokumente kostenlos zur Verfügung, die für die Dienstleistungen des jeweiligen Vertrages allgemein verfügbar sind (z.B. diese AVV, der Vertrag, Auditberichte oder Zertifizierungen). Jede zusätzliche Unterstützung wird zwischen den Parteien einvernehmlich vereinbart.

13. NACHWEISPFLICHTEN UND AUDITRECHT

Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser AVV festgehaltenen Pflichten mit geeigneten Mitteln (z.B. Zertifikate) nach.

Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen oder vertraglichen Pflichten in Bezug auf die Verarbeitung von Personendaten selbst oder durch von ihm beauftragten Prüfer, welche zum Schutz des Auftragnehmers unter strikter Vertraulichkeit und nicht in unmittelbaren Wettbewerbsverhältnis mit dem Auftragnehmer stehen, mittels Inspektionen oder Audits zu prüfen, wenn

(i) der Auftragnehmer keinen ausreichenden Nachweis (u.a. Zertifikat, Auditbericht) über die Einhaltung der technischen und organisatorischen Massnahmen über den Schutz der eingesetzten Systeme und Verarbeitungsprozesse erbringt;
(ii) eine Verletzung des Schutzes von Personendaten vorliegt;
(iii) eine Prüfung offiziell durch eine Aufsichtsbehörde des Auftraggebers verlangt wird; oder
(iv) der Auftraggeber gemäss zwingendem, anwendbarem Datenschutzrecht über ein direktes Auditrecht verfügt.

Der Auftragnehmer ist verpflichtet, bei einem Audit angemessen mitzuwirken. Die Parteien einigen sich im Vorfeld über Zeitpunkt, Dauer und Gegenstand der Prüfungen und über anwendbare Sicherheits- und Vertraulichkeitsbestimmungen, sofern nicht eine Prüfung ohne vorherige Anmeldung erforderlich erscheint, weil andernfalls der Prüfzweck gefährdet wäre. Das Audit ist so durchzuführen, dass keine Betriebsabläufe des Auftragnehmers übermässig gestört werden. Audits und Inspektionen des Auftraggebers sind grundsätzlich auf maximal drei Werktage pro Jahr beschränkt.

Jede Partei trägt die bei ihr anfallenden Kosten und Ausgaben im Zusammenhang mit dem Audit oder der Inspektion selber. Bei einem über drei Werktage hinausgehenden Aufwand kann der Auftragnehmer für die Unterstützung bei der Durchführung einer vom Auftraggeber veranlassten Inspektion bzw. Audit vom Auftraggeber eine Vergütung verlangen.

Werden nach Vorlage von Nachweisen oder Berichten oder im Rahmen eines Audits wesentliche Verletzungen dieser AVV oder Mängel bei der Umsetzung der Pflichten des Auftragnehmers festgestellt, so hat der Auftragnehmer umgehend und kostenlos geeignete Korrekturmassnahmen zu implementieren.

14. DATENVERARBEITUNG IN DRITTSTAATEN

Die Verarbeitung der Daten findet ausschliesslich in der Schweiz, in einem Mitgliedsstaat der Europäischen Union (EU), in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) oder in einem Land, welches gemäss Angemessenheitsbeschluss der Europäischen Kommission oder des Eidgenössischen Datenschutzbeauftragten über einen angemessenen Schutzniveau verfügt, statt. Die Verarbeitung von Daten ausserhalb dieses Gebietes ist nur nach schriftlicher Information an den Auftraggeber und in Übereinstimmung mit den anwendbaren gesetzlichen Bestimmungen zulässig. Der Auftragnehmer verpflichtet sich für den Fall einer Datenbekanntgabe in einen Staat ohne angemessenes Datenschutzniveau insbesondere, mit den Datenempfängern einen Zusatzvertrag auf der Basis der aktuellen EU-Standardvertragsklauseln (wo notwendig angepasst auf die Schweiz) abzu-

schliessen sowie zusätzlich angemessene rechtliche, technische oder organisatorische Massnahmen zu treffen.

15. HAFTUNG

Der Auftragnehmer haftet gegenüber dem Auftraggeber für schuldhafte Verletzungen dieser AVV. Der Auftragnehmer haftet für ein Verschulden seiner Unterauftragsverarbeiter wie für eigene Handlungen. Der Umfang der Haftung der Parteien unter diesem AVV richtet sich nach den Haftungsbestimmungen und -beschränkungen unter dem Vertrag bzw. bei mehreren Verträgen unter dem betroffenen Vertrag. Weitergehende gesetzliche Haftungsansprüche bleiben vorbehalten.

16. SCHLUSSBESTIMMUNGEN

16.1. Vereinbarungsinhalt

Diese AVV und deren Anhänge regeln die Beziehungen zwischen den Parteien in Bezug auf die Verarbeitung von Personendaten abschliessend und ersetzen die vor Vertragsschluss geführten Verhandlungen und Korrespondenzen.
Im Falle von Widersprüchen zwischen dem Vertrag und dieser AVV, geht die AVV den Bestimmungen des Vertrages vor, wenn und soweit die Verarbeitung von Personendaten durch den Auftragnehmer im Rahmen des betreffenden Vertrages betroffen ist.
Im Falle von Widersprüchen geht ein Anhang dieser Vereinbarung vor; im Falle von mehreren Anhängen gehen die jeweils letzten gültig zustande gekommenen Bestimmungen der Anhänge den widersprüchlichen Bedingungen in einem älteren Anhang vor.

16.2. Änderungen

Sollte eine der Parteien zum Schluss kommen, dass diese AVV den Anforderungen des Datenschutzrechts nicht mehr genügt, werden sie diesen AVV in guten Treuen einvernehmlich anpassen.

16.3. Schriftform

Diese Vereinbarung, deren Änderungen und Ergänzungen sowie alle vertragsrelevanten Willenserklärungen und Erklärungen zur Ausübung von Gestaltungsrechten, insbesondere Kündigungen, Mahnungen oder Fristsetzungen bedürfen der Schriftform. Der Schriftform gleichgestellt sind Unterschriften in elektronischer Form (z.B. Skribble, DocuSign oder AdobeSign oder mit einem elektronischen Scan der Unterschrift), welche per Post, Kurier oder E-Mail zugestellt werden. Der so unterschriebene und zugestellte Vertragsteil gilt als ordnungsgemäss ausgefertigt und gültig zugestellt und ist für alle Zwecke gültig und wirksam.

16.4. Mitteilungen

Sofern nicht explizit abweichend geregelt, sind zur Ausübung von Rechten und Pflichten aus dieser Vereinbarung bestimmte Mitteilungen in schriftlicher Form, per Brief oder mit E-Mail an die auf der Titelseite der Vereinbarung oder im Anhang angegebenen Adressen der Parteien zu richten.

16.5. Teilnichtigkeit
Sollten sich einzelne Bestimmungen oder Teile dieser Vereinbarung bzw. eines Anhanges als nichtig oder unwirksam erweisen, so wird dadurch die Gültigkeit der Vereinbarung im Übrigen nicht berührt. Die Parteien werden in einem solchen Fall die Vereinbarung so anpassen, dass der mit dem nichtigen oder unwirksam gewordenen Teil angestrebte Zweck so weit wie möglich erreicht wird.

16.6. Abtretung und Übertragung
Diese Vereinbarung darf nur nach vorgängiger schriftlicher Zustimmung der anderen Partei an Dritte abgetreten oder auf sie übertragen werden, wobei die Zustimmung nur aus wichtigem Grund verweigert werden darf.

16.7. Vertragsexemplare
Diese Vereinbarung und alle Anhänge werden in 2 Exemplaren ausgefertigt, von denen jede Partei ein Exemplar erhält.

16.8. Streiterledigung
Beide Parteien verpflichten sich, im Falle von Meinungsverschiedenheiten im Zusammenhang mit dieser Vereinbarung in guten Treuen eine einvernehmliche Regelung anzustreben.

16.9. Anwendbares Recht und Gerichtsstand
Wenn trotz der Bemühungen der Parteien auf gütlichem Wege keine Einigung zustande kommt, wird eine rechtliche Auseinandersetzung gemäss den Bestimmungen im jeweiligen Vertrag (anwendbares Recht und Gerichtsstand) geführt.

Unterschriften auf nächster Seite

Captns ● Konzept und Gestaltung
Bernstrasse 4, CH–3122 Kehrsatz
www.captns.ch
+41 (0)31 331 76 36
contact@captns.ch

Unterschriften

Ort, Datum

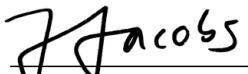
«Auftraggeber» oder «Verantwortlicher»:

Unterschrift Auftraggeber

Vor- und Nachname der unterzeichnenden Person

Funktion oder Titel der unterzeichnenden Person

«Auftragnehmer» oder «Auftragsverarbeiter»:
Captns&Partner GmbH,
Bernstrasse 4,
3122 Kehrsatz



Unterschrift Auftragnehmer

J. Jacobs

Vor- und Nachname der unterzeichnenden Person

IT-Dienstleistung / Datenschutzbeauftragte

Funktion oder Titel der unterzeichnenden Person

Captns ● Konzept und Gestaltung
Bernstrasse 4, CH–3122 Kehrsatz +41 (0)31 331 76 36
www.captns.ch contact@captns.ch

ANHANG 1 – SUBUNTERNEHMERLISTE
Zur Auftragsverarbeitungsvereinbarung

vom 14.8.2023

1. VERTRAGLICHE GRUNDLAGE DER AUFTRAGSVERARBEITUNG («AVV»)

Gemäss Ziffer 1 AVV haben die Parteien, durch die Erteilung eines Auftrages in schriftlicher oder mündlicher Form oder mit der Akzeptanz unserer Auftragsbestätigung, eine Vereinbarungen geschlossen, in denen der Auftragnehmer als Leistungserbringer gegenüber dem Auftraggeber oder dessen Kunden auftritt.

2. UMFANG DER VERARBEITUNG GEMÄSS ZIFFER 2 AVV

2.1. Gegenstand, Art und Zweck der Verarbeitung:

Gegenstand, Art und Zweck der Datenverarbeitung ergeben sich aus dem in Ziffer 1 aufgeführten Vertrag.

2.2. Datenkategorien

Die betroffenen Datenkategorien umfassen:
Persönliche Identifikationsdaten (Name, Anschrift, Firmenzugehörigkeit, Kalender), Elektronische Identifikationsdaten (IP-Adresse, Verbindungs-/Protokolldaten, Cookies), Zeiterfassungsdaten (Arbeitszeit), Auftragsdaten, Kommunikationsdaten, Vertragsbeziehung, Vertragsabrechnungs- und Zahlungsdaten, Kundenstammdaten und Kundenhistorie, Bilder

2.3. Personenkategorien

Die Kategorien betroffener Personen umfassen:
Klienten, Arbeitnehmer, Abonnenten, Dienstleiter

3. KONTAKTPERSON GEMÄSS ZIFFER 6 AVV

3.1. Ansprechpartner beim Auftraggeber

Name und Vorname: Jasmin Jacobs, Captns Partner GmbH
Funktion: IT-Dienstleistung
Adresse: Adresse (Handelsregister), 3000 Bern
Telefon: 031 331 76 36
Email: jasmin.jacobs@captns.ch

3.2. Meldung datenschutzrelevanter Vorfälle

Datenschutzrelevante Vorfälle sind unmittelbar nach ihrer Feststellung und ohne schuldhafte Verzögerung vom Auftragnehmer an den Auftraggeber zu melden.
Hierfür sind auf Seiten des Auftraggebers die folgende(n) Person(en) innerhalb der üblichen Geschäfts-

zeiten zu informieren:
Jasmin Jacobs, IT-Dienstleistung; Tobias Steiner, IT-Dienstleistung; 031 331 76 36

3.3. Ansprechpartner beim Auftragnehmer
Name und Vorname: Jasmin Jacobs
Funktion: IT-Dienstleitung
Adresse: Bernstrasse 4, 3122 Kehrsatz
Telefon: 031 331 76 36
Email: jasmin.jacobs@captns.ch

4. AUFSTELLUNG DER UNTERAUFTRAGSVERARBEITER GEMÄSS ZIFFER 10 AVV
Der Auftraggeber stimmt dem Beizug nachstehender Unternehmen als Unterauftragsverarbeiter zu:

Bexio	Administrations-Software bexio AG, Alte Jonastrasse 24, 8640 Rapperswil	Schweiz
Metanet	Webhosting Metanet AG, Josefstrasse 218, 8005 Zürich	Schweiz
Kreativmedia	Webhosting Kreativ Media GmbH, Höschgasse 45, 8008 Zürich	Schweiz
iWay	Telekommunikation iWay AG, Badenerstrasse 569, 8048 Zürich	Schweiz
Dropbox Business	Cloud-Service Dropbox International Unlimited Company One Park Place, Floor 5, Upper Hatch Street, Dublin 2	Ireland
DigitalOcean, LLC	Cloud-Service 101 Avenue of the Americas, New York, NY 10013	USA
MailerLite	Newsletter 71 Lower Baggot Street, Dublin 2, D02 P593	Ireland

Captns ● Konzept und Gestaltung
Bernstrasse 4, CH–3122 Kehrsatz +41 (0)31 331 76 36
www.captns.ch contact@captns.ch

ANHANG 2 – TOM
Zur Auftragsverarbeitungsvereinbarung

Beschreibung der technischen und organisatorischen Massnahmen (TOM) gemäss Ziffer 4 AVV vom 14.8.2023

Im Folgenden werden die technischen und organisatorischen Massnahmen beschrieben, die der Auftragnehmer im Zusammenhang mit der Verarbeitung von Personendaten und der Erfüllung seiner Verpflichtungen im Rahmen des bestehenden Vertrages, Art. 7 DSG (Art. 8 revDSG i.V.m. Art. 2 ff. DSV) und, soweit anwendbar, Art. 32 DSGVO trifft :

1. VERTRAULICHKEIT
Massnahmen zur Umsetzung des Gebots der Vertraulichkeit sind unter anderem solche, welche die Zutritts-, Zugriffs-, oder Benutzerkontrolle festlegen.

1.2. Zugangskontrolle (physische Zutrittskontrolle)
Kein unbefugter Zugang zu den Räumlichkeiten und Anlagen in denen Personendaten verarbeitet werden. Es existieren folgende Massnahmen zur Zugangskontrolle:
Begleitung von Besuchern und Fremdpersonal, Schlüssel, Schlüsselregelung (Schlüsselausgabe etc.), «Jeder kennt jeden im Unternehmen»

1.3. Benutzerkontrolle (digitale Zutritts- bzw. Zugangskontrolle)
Keine unautorisierte Nutzung von IT-Systemen, mit denen Personendaten verarbeitet werden. Es existieren folgende Massnahmen zur Benutzerkontrolle:
Zugangsschutz (Authentisierung mit sicheren Passwörtern und Benutzername; persönliche Benutzerkonten), Passwortregeln inkl. Vorgaben für die Komplexität des Passwortes, Zwei-Faktor-Authentifizierung, Regelmässige Schulung der Mitarbeitenden (insb. Sensibilisierung für Phishing-Methoden)

1.4. Zugriffskontrolle
Nur berechtigte Personen haben Zugriff auf diejenigen Daten, die sie zur Erfüllung ihrer Aufgaben benötigen. Es existieren folgende Massnahmen zur Zugriffskontrolle:
Passwortregeln inkl. Vorgaben für die Komplexität des Passwortes, Identifizierungs- und Authentifizierungssystem, Zugriffsbeschränkungen, Verwaltung der Rechte durch Systemadministrator, Reduktion der Anzahl Administratoren, mit vollen Zugriffsberechtigungen

1.5. Trennungskontrolle
Gewährleistung der getrennten Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden. Es existieren folgende Massnahmen zur Trennungskontrolle: Mandantentrennung

1.5. Pseudonymisierung
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehen zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Massnahmen unterliegen. Es existieren folgende Massnahmen zur Pseudonymisierung:
automatische Verschlüsselung von Datensätzen inkl. Ablage des Schlüssels zur Entschlüsselung mit Zugriffsberechtigung, interne Anweisung, Personendaten sind im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren

2. VERFÜGBARKEIT UND INTEGRITÄT
Massnahmen zur Verfügbarkeit sind solche, welche gewährleisten, dass Personendaten und IT-Systeme zur Verfügung stehen und von autorisierten Personen genutzt werden können. Eine unbefugte Unterbrechung z.B. durch Serverausfall oder Ausfall von Kommunikationsmitteln stellt einen Angriff auf die Verfügbarkeit dar.
Massnahmen zur Umsetzung des Gebots der Integrität sind beispielsweise solche, die zum Schutz vor unbefugter oder unrechtmässiger Verarbeitung, Zerstörung oder unbeabsichtigter Schädigung beitragen. In diesem Zusammenhang sollen die folgenden technischen und organisatorischen Massnahmen des Auftragnehmers die Integrität von personenbezogenen Personendaten gewährleisten.

2.1. Datenträger- und Speicherkontrolle
Kein unbefugtes Speichern, Lesen, Kopieren, Verändern, Verschieben, Löschen oder Vernichten von Daten. Es existieren folgende Massnahmen zur Datenträger- und Speicherkontrolle:
Passwortregeln inkl. Vorgaben für die Komplexität des Passwortes, Zugriffsbeschränkungen, Verwaltung und Dokumentation von personengebunden Zugriffsberechtigungen, Verwaltung der Rechte durch Systemadministrator, Reduktion der Anzahl Administratoren mit vollen Zugriffsberechtigungen

2.2. Transportkontrolle (Weitergabekontrolle)
Kein unbefugtes Lesen, Kopieren, Verändern, Löschen oder Vernichten von Daten bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern. Es existieren folgende Massnahmen zur Transportkontrolle: sichere Datenübertragung zwischen Server und Client

2.3. Wiederherstellung
Rasche Wiederherstellung der Verfügbarkeit der Daten und dem Zugang zu ihnen nach einem physischen oder technischen Zwischenfall. Es existieren folgende Massnahmen zur Kontrolle der Wiederherstellbarkeit: Aufbewahrung von Backups an einem sicheren, ausgelagerten Ort durch Subunternehmer.

2.4. Verfügbarkeitskontrolle
Personendaten werden von Captns mittels externe Dienstleister verarbeitet (Bexio / Metanet). Es gelten die dort aufgeführten Massnahmen zur Verfügbarkeitskontrolle.

2.5. Systemsicherheit
Aktualisierung der Sicherheit der Betriebssysteme und Anwendungssoftware und Schliessung bekannter kritischer Lücken. Die Arbeitscomputer werden nach bestem Wissen und Gewissen von den Mitarbeitenden aktualisiert. Die Webserver werden von Metanet auf dem aktuellen Stand gehalten. Existiert ein Vertrag zur Wartung der Software zwischen Endkunden und Captns, sind die darin formulierten Bestimmungen und Verpflichtungen gültig (WpManage oder spezifischer Vertrag zur Wartung von Webanwendungen). Die Testserver auf Digital Ocean werden automatisch gepatched.

3. NACHVOLLZIEHBARKEIT
Massnahmen, welche gewährleisten, dass Personendaten nachvollziehbar verarbeitet werden und unbefugte Zugriffe und Missbräuche identifizierbar sind.

3.1. Eingabekontrolle
Es gibt keine zusätzlichen Massnahmen zur Eingabekontrollen, als jene der Drittanbieter.

3.2. Bekanntgabekontrolle
Persönliche Daten werden nicht mit Vorsatz an Dritte bekanntgegeben. Entsprechend besteht kein spezifisches System zur Überwachung.

3.3. Erkennung und Beseitigung von Verletzungen der Datensicherheit
Massnahmen zur raschen Erkennung von Verletzungen der Datensicherheit und zur Minderung oder Beseitigung der Folgen. Es existieren folgende Massnahmen zur Erkennung und Beseitigung von Verletzungen der Datensicherheit: Implementierung reaktiver Massnahmen und Prozesse inkl. Dokumentation zur Erkennung und Meldung von Sicherheitsvorfällen und Datenpannen, Notfall-Konzept (insb. Vorgehensweise zum Umgang mit Sicherheitsvorfällen)

4. VERFAHREN ZUR REGELMÄSSIGEN ÜERPRÜFUNG, BEWERTUNG UND EVALUIERUNG
4.1. Datenschutz-Massnahmen
Es existieren folgende Datenschutz-Massnahmen: regelmässige Schulung der Mitarbeitenden auf Datenschutz inkl. regelmässige Sensibilisierung

4.1. Incident-Response-Management
Captns verfügt über kein Protokoll für das Incidence-Response Management. Fälle werden individuell geprüft und nach bestem technischen Wissen bearbeitet. Die Kund:in wird informiert und über in den Prozess der Aufarbeitung einbezogen.

4.2. Datenschutzfreundliche Voreinstellung (Privacy by design/Privacy by default)
Es existieren folgende Massnahmen zur Sicherstellung der datenschutzfreundlichen Voreinstellung:
Es sollen grundsätzlich nur Daten erhoben und verarbeitet werden, die für die Geschäftstätigkeiten

zweckmässig und erforderlich sind. Verfahren der automatisierten Datenerfassung und -verarbeitung sind so zu gestalten, dass nur die erforderlichen Daten erhoben werden.

4.3. Auftragskontrolle (Outsourcing an Dritte)
Es existieren folgende Massnahmen zur Auftragskontrolle:
strenge Auswahl des Dienstleisters

5. ANPASSUNGEN UND ÄNDERUNGEN
Eine Änderung der getroffenen Sicherheitsmassnahmen bleibt dem Auftragnehmer vorbehalten, wobei sichergestellt werden muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

Diese Vereinbarung basiert auf den von den Verbänden Swico und swissICT erstellten Branchenstandards.