Auftragsverarbeitungsvertrag

Vereinbarung über eine Auftragsverarbeitung

zwischen

- nachstehend «**Verantwortlicher**» genannt -

und

Creanet Internet Services AG
Schäracher 9
6232 Geuensee

- nachstehend «**Auftragsverarbeiter**» genannt -

I. Gegenstand und Begriffe

(1) Gegenstand dieser Vereinbarung sind Internetdienstleistungen im Rahmen der vom Auftragnehmer auf seinen Internetseiten angebotenen und in den jeweiligen Leistungsbeschreibungen konkretisierten Produkten. Diese Vereinbarung ist als Ergänzung zu den AGB Dieser Auftragsverarbeitungsvertrag ("AVV") regelt die Verarbeitung der Daten des Kunden durch den Auftragsverarbeiter im Sinne des (neuen) Bundesgesetz über den Datenschutz (Datenschutzgesetz DSG).

(2) Der Auftragsverarbeiter – mit Standort in der Schweiz – bearbeitet Personendaten des Verantwortlichen. Bei dem Vertragsgegenstand handelt es sich deshalb um eine Auftragsverarbeitung.

Die Parteien sind sich darin einig, dass auf diesen Vertrag die Vorschriften des Schweizer Datenschutzgesetzes, insbesondere die Vorschriften über die Datenbearbeitung im Auftrag, anzuwenden sind.

Diese Vorschriften ergeben sich ausfolgenden revidierten Gesetzgebungen, u. z.

- dem (neuen) Bundesgesetz über den Datenschutz, (Datenschutzgesetz, nDSG), vom 25. September 2020 (Stand am 1. September 2023)
- in Verbindung mit der (neuen) Verordnung über den Datenschutz, (Datenschutzverordnung, DSV-neu), vom 31. August 2022, die spätestens mit Inkrafttreten des neuen Schweizer Datenschutzgesetzes (nDSG) ab dem 1. September 2023 zur

Anwendung kommen. Der Auftragsverarbeiter erklärt, dass er in der Lage ist, die aufgetragenen Leistungen nach Massgabe des nDSG sowie der DSV-neu durchzuführen.

Dieser Vertrag regelt die Rechte und Pflichten des Verantwortlichen (als Auftraggeber) sowie des Auftragsverarbeiters (als Auftragnehmer).

(3) Dieser Vertrag ist für alle Tätigkeiten anwendbar, bei denen der Auftragsverarbeiter Personendaten im Auftrag des Verantwortlichen (als Auftraggeber) bearbeitet oder bearbeiten lässt. Dieser Vertrag ist nicht auf Tätigkeiten anwendbar, bei denen der Auftragsverarbeiter allein über Mittel und Zwecke der Bearbeitung von Personendaten entscheidet; wäre das der Fall, läge keine Auftragsverarbeitung vor.

(4) Der Auftragsverarbeiter bearbeitet Personendaten gemäss den Nutzungsbedingungen sowie gemäss sonstigen vertraglichen Vereinbarungen zwischen den Parteien.

II. Art und Zweck der Bearbeitung

(1) Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Eine betroffene Person ist eine Person, über die Personendaten bearbeitet werden.

Die Bearbeitung umfasst jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Archivieren, Aufbewahren, Bekanntgeben, Beschaffen, Umarbeiten, Vernichten und Verwenden von Personendaten.

Die Bearbeitung dient ausschliesslich der Vertragserfüllung zwischen den Parteien.

(2) Die Bearbeitung kann insbesondere folgende Kategorien von Personendaten umfassen: Bankdaten, Kontaktdaten, Kommunikationsdaten, Firmendaten, Protokolldaten, Stammdaten, Vertragsdaten, Vertragssteuerungsdaten, Zahlungsdaten.

(3) Die Bearbeitung kann insbesondere folgende Kategorien von betroffenen Personen umfassen: Webshop-Eigentümer und -Betreiber, Webagenturen, Zahlungsverarbeitungsunternehmen, Ansprechpartnerinnen und Ansprechpartner, Kundinnen und Kunden, Geschäftspartnerinnen und Geschäftspartner, Mitarbeiterinnen und Mitarbeiter.

III. Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter bearbeitet Personendaten ausschliesslich wie vertraglich mit dem Verantwortlichen vereinbart oder vom Auftraggeber angeordnet, es sei denn, der Auftragsverarbeiter ist gesetzlich zu einer bestimmten Bearbeitung verpflichtet.

Der Auftragsverarbeiter verwendet darüber hinaus die zur Bearbeitung überlassenen Personendaten in personenbezogener Form für keine anderen Zwecke, insbesondere nicht für eigene Zwecke.

Der Auftragsverarbeiter bestätigt, dass ihm die anwendbaren datenschutzrechtlichen Vorschriften in der Schweiz bekannt sind. Der Auftragsverarbeiter beachtet insbesondere die allgemeinen datenschutzrechtlichen Grundsätze für die Bearbeitung von Personendaten insbesondere gemäss der Artikel 4, 5 u. 7 DSG bzw. der ab dem 1. September 2023 in diesem Zusammenhang gültigen Artikel 6 und Art. 8 nDSG.

(2) Der Auftragsverarbeiter verpflichtet sich, bei der Bearbeitung die Vertraulichkeit zu wahren. Personen, die Kenntnis von den im Auftrag bearbeiteten Personendaten erhalten können, haben sich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(3) Der Auftragsverarbeiter sichert zu, dass die bei ihm zur Bearbeitung eingesetzten Personen vor Beginn der Bearbeitung mit den anwendbaren datenschutzrechtlichen Vorschriften und mit den massgeblichen Bestimmungen dieses Vertrages bekannt gemacht wurden.

Der Auftragsverarbeiter trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der anwendbaren datenschutzrechtlichen Vorschriften angemessen angeleitet und überwacht werden.

(4) Im Zusammenhang mit der beauftragten Bearbeitung hat der Auftragsverarbeiter den Verantwortlichen bei Erstellung und Fortschreibung eines allenfalls erforderlichen Verzeichnisses der Bearbeitungstätigkeiten sowie bei einer Durchführung einer allenfalls erforderlichen Datenschutz-Folgenabschätzung im erforderlichen Umfang zu unterstützen. Die entsprechenden Kosten des Auftragsverarbeiters für die Unterstützung trägt der Verantwortliche bzw. der Auftraggeber.

(5) Wird der Auftragsverarbeiter oder der Verantwortliche durch Aufsichtsbehörden oder andere zuständige Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber datenschutzrechtlichen Ansprüchen geltend, verpflichtet sich der Auftragsverarbeiter, den Verantwortlichen bzw. den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Auftragsverarbeitung betroffen ist. Die entsprechenden Kosten des Auftragsverarbeiters für die Unterstützung trägt der Verantwortliche bzw. der Auftraggeber.

(6) Auskünfte an Behörden, betroffene Personen oder an Dritte darf der Auftragsverarbeiter nur nach vorheriger Zustimmung durch den Verantwortlichen bzw. den Auftraggeber erteilen. Vorbehalten bleiben Auskünfte, die aufgrund von zwingendem Recht ohne vorherige Zustimmung durch den Verantwortlichen bzw. den Auftraggeber erteilt werden müssen.

Direkt an den Auftragsverarbeiter gerichtete Anfragen, welche die Auftragsverarbeitung betreffen, leitet der Auftragsverarbeiter unverzüglich an den Verantwortlichen bzw. den Auftraggeber weiter.

(7) Sofern und soweit gesetzlich verpflichtet, bestellt der Auftragsverarbeiter eine fachkundige und zuverlässige Person als Datenschutzverantwortlichen bzw. -berater.

Der Auftragsverarbeiter stellt sicher, dass für den Datenschutzverantwortlichen keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftragsverarbeiter oder der Verantwortliche bzw. der Auftraggeber direkt an einen allfälligen Datenschutzverantwortlichen wenden.

Der Auftragsverarbeiter teilt dem Verantwortlichen bzw. dem Auftraggeber unverzüglich die Kontaktdaten eines allfälligen bestellten Datenschutzverantwortlichen mit. Massgebliche Änderungen in der Person oder den Aufgaben des Datenschutzverantwortlichen teilt der Auftragsverarbeiter dem Verantwortlichen bzw. dem Auftraggeber unverzüglich mit.

(8) Die Auftragsverarbeitung erfolgt ausschliesslich in der Schweiz, oder nach vorheriger Abklärung mit dem Verantwortlichen bzw. Auftraggeber in Mitgliedstaaten des Europäischen Wirtschaftsraumes (EWR) einschliesslich Europäischer Union und Fürstentum Liechtenstein, oder in sonstigen Staaten und Territorien auf der Erde sowie anderswo im Universum, deren Datenschutzrecht nach Einschätzung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) oder des Schweizerischen Bundesrates einen angemessenen Datenschutz gewährleistet, oder wenn im Einzelfall aus anderen Gründen, wie beispielsweise durch eine entsprechende vertragliche Vereinbarung, insbesondere Standardvertragsklauseln, oder eine entsprechende Zertifizierung, ein angemessener Datenschutz gewährleistet ist. Jegliche weitere Verarbeitung darf nur mit Zustimmung des Auftraggebers sowie unter den Bedingungen gemäss Art. 6 DSG bzw. der Artikel 16 und 17 nDSG und unter Einhaltung dieses Vertrages erfolgen.

IV. Technische und organisatorische Massnahmen

(1) Der Auftragsverarbeiter schützt Personendaten durch angemessene technische und organisatorische Massnahmen insbesondere gemäss Art. 7 DSG und Art. 8 ff. VDSG bzw. ab dem 1. September 2023 gemäss Art. 8 nDSG und Art. 3 DSV-neu.

Die Massnahmen müssen fortlaufend der technischen und organisatorischen Weiterentwicklung angepasst werden. Zur Aufrechterhaltung der Datensicherheit erforderliche Massnahmen hat der Auftragsverarbeiter unverzüglich umzusetzen.

(2) Der Auftragsverarbeiter sichert zu, dass die im Auftrag verarbeiteten Personendaten von sonstigen Datenbeständen getrennt werden.

(3) Kopien werden ohne Wissen des Verantwortlichen bzw. des Auftraggebers nicht erstellt. Ausgenommen sind Vervielfältigungen, die technisch, aus gesetzlichen oder regulatorischen Gründen, gemäss diesem Vertrag oder zur Vertragserfüllung zwischen den Parteien notwendig sind, soweit solche Kopien nicht zu einer Beeinträchtigung der Datensicherheit führen.

(4) Der Auftragsverarbeiter führt Nachweis über die Erfüllung ihrer datenschutzrechtlichen Pflichten, insbesondere zum Schutz von Personendaten durch angemessene technische und organisatorische Massnahmen gemäss Art. 7 DSG und Art. 8 ff. VDSG bzw. ab dem 1. September 2023 gemäss Art. 8 nDSG und Art. 3 DSV-neu.

(5) Der Auftragsverarbeiter sichert die Einhaltung der in der Selbstauskunft in Anlage 1 genannten Massnahmen und Regelungen zu. Diese Massnahmen gelten als vereinbart und die Beschreibung der Massnahmen wird Bestandteil dieses Vertrages.

V. Berichtigung, Löschung und Sperrung von Personendaten

(1) Im Rahmen der Auftragsverarbeitung wird der Auftragsverarbeiter Personendaten nur entsprechend den getroffenen vertraglichen Vereinbarungen oder nach Weisungen des Verantwortlichen bzw. des Auftraggebers berichtigen, löschen oder sperren.

(2) Den entsprechenden Weisungen des Verantwortlichen bzw. des Auftraggebers wird der Auftragsverarbeiter jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten. Die entsprechenden Kosten des Auftragsverarbeiters – auch nach Beendigung dieses Vertrages – trägt der Verantwortliche bzw. der Auftraggeber.

VI. Unterauftragsverarbeiter

(1) Der Verantwortliche bzw. der Auftraggeber stimmt allgemein zu, dass der Auftragsverarbeiter Unterauftragsverarbeiter hinzuziehen darf. Der Auftragsverarbeiter wählt Unterauftragsverarbeiter unter Berücksichtigung der Eignung der von dem Unterauftragsverarbeiter getroffenen technischen und organisatorischen Massnahmen sorgfältig aus.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen bzw. den Auftraggeber vorgängig über die geplante Hinzuziehung oder geplante Ersetzung von Unterauftragsbearbeiten.

Der Verantwortliche bzw. der Auftraggeber kann der geplanten Hinzuziehung oder geplanten Ersetzung – innerhalb einer angemessenen, allenfalls vom Auftragsverarbeiter gesetzten Frist – aus wichtigem Grund widersprechen.

Erfolgt kein Widerspruch innerhalb einer solchen Frist, gilt die Zustimmung zur geplanten Hinzuziehung oder geplanten Ersetzung als gegeben. Liegt ein wichtiger

datenschutzrechtlicher Grund vor und ist keine einvernehmliche Klärung zwischen den Parteien möglich, wird dem Verantwortlichen bzw. dem Auftraggeber das Recht eingeräumt, die Auftragsverarbeitung durch den Auftragsverarbeiter ebenfalls per sofort zu kündigen.

(3) Sofern und soweit der Auftragsverarbeiter Unterauftragsverarbeiter hinzuzieht, obliegt es dem Auftragsverarbeiter, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Unterauftragsverarbeiter aufzuerlegen.

(4) Der Verantwortliche bzw. der Auftraggeber stimmt zu, dass der Auftragsverarbeiter Unterauftragsverarbeiter hinzuziehen darf und verzichtet auf einen Widerspruch, da der Auftragsverarbeiter ohne diese Unterauftragsverarbeiter die Nutzung seiner Dienstleistungen nicht ermöglichen kann.

Folgende Unterauftragsverarbeiter werden von uns eingesetzt:

Clever Elements GmbH (Clever Elements Newsletter)
Lohmühlenstr. 65, D-12435 Berlin, Deutschland
https://www.cleverelements.com

VII. Mitteilungspflichten

(1) Der Auftragsverarbeiter teilt dem Verantwortlichen bzw. dem Auftraggeber Verletzungen des Schutzes von Personendaten unverzüglich nach Kenntnisnahme mit. Auch begründete Verdachtsfälle sind mitzuteilen. Die Mitteilung muss alle erforderlichen Angaben enthalten.

(2) Der Auftragsverarbeiter informiert – sofern und soweit zulässig – den Verantwortlichen bzw. den Auftraggeber unverzüglich über Kontrollen oder sonstige Massnahmen von Aufsichtsbehörden oder Dritten, soweit diese einen Bezug zur Auftragsverarbeitung aufweisen.

(3) Der Auftragsverarbeiter informiert – sofern zulässig – den Verantwortlichen bzw. den Auftraggeber unverzüglich über Anfragen von Behörden, die eine Herausgabe oder Übermittlung von Personendaten beinhalten, soweit diese einen Bezug zur Auftragsverarbeitung ausweisen.

Sofern eine solche Information aufgrund von zwingendem Recht nicht oder vorläufig nicht zulässig ist, trifft der Auftragsverarbeiter angemessene Schutzmassnahmen im Interesse des Verantwortlichen bzw. des Auftraggebers sowie im Rahmen dieses Vertrages.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen bzw. den Auftraggeber unverzüglich über erhebliche Störungen bei der Auftragsverarbeitung sowie über Verstösse des Auftragsverarbeiters oder der bei ihr beschäftigten Personen gegen datenschutzrechtliche Vorschriften oder gegen diesen Vertrag.

(5) Der Auftragsverarbeiter teilt dem Verantwortlichen bzw. dem Auftraggeber mit, wenn er der Auffassung ist, dass eine Weisung gegen das anwendbare Datenschutzrecht verstösst.

Der Auftragsverarbeiter ist berechtigt, die Ausführung einer solchen Weisung auszusetzen, bis sie durch den Verantwortlichen bzw. den Auftraggeber ausdrücklich bestätigt oder geändert wird.

(6) Der Auftragsverarbeiter sichert zu, den Verantwortlichen bzw. den Auftraggeber bei dessen datenschutzrechtlichen Meldepflichten im erforderlichen Umfang zu unterstützen. Die entsprechenden Kosten des Auftragsverarbeiters für eine solche Unterstützung trägt der Verantwortliche bzw. der Auftraggeber.

VIII. Rechte und Pflichten des Verantwortlichen bzw. des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Auftragsverarbeitung sowie für die Wahrung der Rechte von betroffenen Personen ist allein der Verantwortliche bzw. der Auftraggeber verantwortlich.

(2) Der Verantwortliche bzw. der Auftraggeber behält sich hinsichtlich der Auftragsverarbeitung ein umfassendes Weisungsrecht vor.

Der Verantwortliche bzw. der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in dokumentierter Form, die einen Nachweis durch Text erlaubt. In Einzelfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Verantwortliche bzw. der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der Verantwortliche bzw. der Auftraggeber informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmässigkeiten bei der Auftragsverarbeitung feststellt.

(4) Der Verantwortliche bzw. der Auftraggeber ist berechtigt, die Einhaltung von Vorschriften über den Datenschutz und dieses Vertrages beim Auftragsverarbeiter in angemessenem Umfang selbst oder durch Dritte, insbesondere durch das Einholen von Auskünften und die Einsichtnahme in die gespeicherten Personendaten und die Bearbeitungsprogramme sowie durch sonstige Kontrollen vor Ort, zu kontrollieren.

Kontrollen sind vom Verantwortlichen bzw. vom Auftraggeber rechtzeitig anzumelden. Den mit der Kontrolle betrauten Personen ist durch den Auftragsverarbeiter – sofern und soweit erforderlich – Einblick und Zutritt zu ermöglichen.

Der Auftragsverarbeiter ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Die Kosten des Auftragsverarbeiters für solche Kontrollen trägt der Verantwortliche bzw. der Auftraggeber.

IX. Rechte der Betroffenen

(1) Für die Wahrung der Rechte der Betroffenen ist allein der Verantwortliche bzw. der Auftraggeber verantwortlich und zuständig. Der Auftragsverarbeiter darf Rechte der Betroffenen nur nach Weisung des Verantwortlichen bzw. des Auftraggebers umsetzen. Der Auftragsverarbeiter unterstützt jedoch den Verantwortlichen bzw. den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen.

(2) Anfragen von Betroffenen zu ihren Rechten oder von einem Betroffenen verlangte Auskünfte, Berichtigungen, Löschungen von Daten werden vom Auftragsverarbeiter unverzüglich an den Verantwortlichen bzw. den Auftraggeber zur Erledigung weitergeleitet. Auskünfte an Dritte dürfen nur nach Weisung des Verantwortlichen bzw. des Auftraggebers erteilt werden oder sind an ihn zur Erledigung weiterzuleiten. Ebenso dürfen Auskünfte an Beschäftigte des Verantwortlichen bzw. des Auftraggebers nicht unmittelbar an diese, sondern nur über die vereinbarten Kontaktpersonen erteilt werden.

X. Haftung und Schadenersatz

(1) Für den Ersatz von Schaden, den eine betroffene Person wegen einer datenschutzrechtlich pflichtwidrigen oder nicht weisungsgemässen Bearbeitung durch den Auftragsverarbeiter im Rahmen der Auftragsverarbeitung erleidet, haftet der

Auftragsverarbeiter gegenüber einer betroffenen Person gemeinsam mit dem Verantwortlichen bzw. dem Auftraggeber für den gesamten Schaden.

Der Auftragsverarbeiter stimmt eine allfällige Erfüllung von Haftungs- und Schadenersatzansprüchen mit dem Verantwortlichen bzw. dem Auftraggeber ab. Die Haftung des Auftragsverarbeiters entfällt, wenn er nachweisen kann, dass er in keinerlei Hinsicht für den Umstand, durch den ein solcher Schadeneingetreten ist, verantwortlich ist.

(2) Im Übrigen gelten allfällige Vereinbarungen zu Haftung und Schadenersatz im Hauptvertrag sowie sonstigen vertraglichen Vereinbarungen zwischen den Parteien auch für die Auftragsverarbeitung.

XI. Beendigung

(1) Dieser Vertrag wird auf unbestimmte Zeit geschlossen.

Die Parteien sind berechtigt, diesen Vertrag per sofort zu kündigen, wenn ein wichtiger Grund wie insbesondere ein schwerwiegender Verstoss gegen das Datenschutzrecht oder gegen diesen Vertrag vorliegt.

(2) Bei Beendigung dieses Vertrages oder des Hauptvertrages sowie jederzeit auf Verlangen des Verantwortlichen bzw. des Auftraggebers hat der Auftragsverarbeiter die im Auftrag bearbeiteten Personendaten einschliesslich Kopien nach Wahl des Verantwortlichen bzw. des Auftraggebers entweder zu vernichten oder an den Verantwortlichen bzw. den Auftraggeber zu übergeben, es sei denn, der Auftragsverarbeiter ist gesetzlich oder regulatorisch zur Aufbewahrung verpflichtet.

(3) Der Auftragsverarbeiter ist verpflichtet, bei Beendigung dieses Vertrages unverzüglich die Löschung oder Rückgabe von Personendaten auch bei Unterauftragnehmern herbeizuführen, es sei denn, diese sind gesetzlich oder regulatorisch zur Aufbewahrung verpflichtet.

(4) Die Dokumentation, die dem Nachweis der ordnungsgemässen Bearbeitung dient, ist durch den Auftragsverarbeiter den jeweiligen Aufbewahrungsfristen entsprechend auch über die Beendigung dieses Vertrages hinaus aufzubewahren. Der Auftragsverarbeiter kann sie zu seiner Entlastung dem Verantwortlichen bzw. dem Auftraggeber bei Beendigung dieses Vertrages übergeben.

XII. Verfahren nach Beendigung des Auftrags

(1) Nach Abschluss der Bearbeitung, spätestens nach Beendigung dieses Vertrages, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen und erstellten Bearbeitungs- oder Nutzungsergebnisse oder zur Leistungserfüllung hergestellten oder kopierten Personendaten oder sonstige vertrauliche Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen bzw. dem Auftraggeber auszuhändigen oder in Abstimmung mit ihm datenschutzgerecht zu vernichten oder sicher zu löschen.

Test- und Ausschussmaterial ist unverzüglich datenschutzgerecht zu vernichten oder dem Verantwortlichen bzw. dem Auftraggeber auszuhändigen. Diese Verpflichtung gilt in gleichem Masse auch für eventuell beauftragte Unterauftragsverarbeiter.

Unberührt bleiben Daten, deren Löschung aus technischen Gründen nicht möglich ist oder einen unverhältnismässig hohen Aufwand verursachen würde, sowie Kopien, die zum

Nachweis der Ordnungsmässigkeit der Datenbearbeitung oder zur Erfüllung von Haftungs- und Gewährleistungsansprüchen erforderlich sind.

(2) Der Auftragsverarbeiter hat dem Verantwortlichen bzw. dem Auftraggeber nach Beendigung dieses Vertrages die sichere Löschung bzw. die sichere Vernichtung aller in seinem Besitz befindlichen Unterlagen schriftlich zu bestätigen.

XIII. Sonstige Bestimmungen

(1) Die Parteien können diesen Vertrag mit Anhängen ergänzen, beispielsweise in Bezug auf die Kategorien von bearbeiteten Personendaten und betroffenen Personen, die angemessenen technischen und organisatorischen Massnahmen sowie die hinzugezogenen Unterauftragsverarbeiter.

(2) Die Parteien sind verpflichtet, alle im Rahmen dieses Vertrages erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmassnahmen der jeweils anderen Partei auch über die Beendigung dieses Vertrages hinaus vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur ausdrücklichen Freigabe durch die jeweils andere Partei als vertraulich zu behandeln.

XIV. Wirksamkeit der Vereinbarung

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

XV. Anwendbares Recht und Gerichtsstand

Es gilt das Recht der Schweiz.

Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung und datenschutzrelevante Streitigkeiten ist am Sitz des Auftragnehmers.

Gesetzliche Regelungen über ausschliessliche Zuständigkeiten bleiben unberührt.

XVI. Anlage 1 Beschreibung der vereinbarten technischen und organisatorischen Massnahmen beim Auftragsverarbeiter

TOM - Technisch organisatorische Maßnahmen

Hinweis: Art. 32 DS-GVO / Art. 7 und Art. 8 revDSG: Sicherheit der Verarbeitung (1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Massnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Massnahmen schliessen gegebenenfalls unter anderem Folgendes ein: a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten; b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; d) ein Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung. (2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmässig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugtem Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden. (3) Die Einhaltung genehmigter Verhaltensregeln gemäss Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäss Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen. (4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

* 1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Massnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Massnahmen schliessen gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

1.1 TOM - Zutrittskontrolle - Technische Massnahmen

Hinweis: Technische Massnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu versperren.

- Alarmanlage
- Chipkarten / Transpondersysteme
- Manuelles Schliesssystem
- Sicherheitsschlösser
- Türen mit Absicherung Aussenseite
- Videoüberwachung
- Zaun um das Gelände des Unternehmens
- Chipkarten / Transpondersysteme

1.2 TOM - Zutrittskontrolle - Organisatorische Massnahmen

Hinweis: Organisatorische Massnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu versperren.

- Ansprache unbekannter Personen
- Besucher sind immer in Begleitung von Mitarbeitern
- Schlüsselregelung / Liste

2.1 TOM - Zugangskontrolle - Technische Massnahmen

Hinweis: Technische Massnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten verwendet werden können.

- Anti-Virus-Software für Clients und Server
- Anti-Virus-Software mobile Geräte
- Automatische Sperre des Systems
- Einsatz von VPN-Technologien
- Einsatz von Firewall Systemen
- Gehäuseverriegelung
- Intrusion Detection Systeme
- Verschlüsselung von Datenträgern
- Verschlüsselung von Notebooks
- Verschlüsselung Smartphones / Tablets
- Login mit Benutzername + Passwort
- Login mit biometrischen Daten

2.2 TOM - Zugangskontrolle - Organisatorische Massnahmen

Hinweis: Organisatorische Massnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten verwendet werden können.

- Erstellen von Benutzerprofilen
- Richtlinie „Sicheres Passwort“
- Richtlinie Clean-Desk
- Richtlinie IT-Sicherheit und Datenschutz
- Verwalten von Benutzerberechtigungen
- Zentrale Passwortvergabe

3.1 TOM - Zugriffskontrolle - Technische Massnahmen

Hinweis: Technische Massnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und die personenbezogenen Daten bei der Verarbeitung nicht unbefugt verwendet werden können.

- Akten Schredder (cross cut)
- Physische Löschung von Datenträgern
- Protokollierung von Zugriffen auf Anwendungen
- Verschlüsselung von Datenträgern

3.2 TOM - Zugriffskontrolle - Organisatorische Massnahmen

Hinweis: Organisatorische Massnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und die personenbezogenen Daten bei der Verarbeitung nicht unbefugt verwendet werden können.

- Einsatz Berechtigungskonzepte
- Minimale Anzahl an Administratoren
- Protokollierung der Vernichtung von Datenträgern
- Rechteverwaltung durch einen Systemadministrator

4.1 TOM - Weitergabekontrolle - Technische Massnahmen

Hinweis: Technische Massnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Bereitstellung von Diensten über verschlüsselte Verbindungen wie SFTP, HTTPS, etc.
- Einsatz von VPN
- Protokollierung der Zugriffe und Abrufe

4.2 TOM - Weitergabekontrolle - Organisatorische Massnahmen

Hinweis: Organisatorische Massnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Sorgfältige Auswahl von Personal und Transportfahrzeugen

5.1 TOM - Eingabekontrolle - Technische Massnahmen

Hinweis: Technische Massnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Manuelle oder automatisierte Kontrolle der Protokolle
- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten

5.2 TOM - Eingabekontrolle - Organisatorische Massnahmen

Hinweis: Organisatorische Massnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können

6.1 TOM - Auftragskontrolle - Technische Massnahmen

Hinweis: Technische Massnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Datenaustausch mit Auftragnehmer verschlüsselt

6.2 TOM - Auftragskontrolle - Organisatorische Massnahmen

Hinweis: Technische Massnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (Datenschutz und Datensicherheit)
- Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
- Regelung zum Einsatz weiterer Subunternehmer
- Schriftliche Weisungen an den Auftragnehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer, wenn Bestellpflicht vorliegt

7.1 TOM - Verfügbarkeitskontrolle - Technische Massnahmen

Hinweis: Technische Massnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Feuer- und Rauchmeldeanlagen
- Feuerlöscher Serverraum
- RAID- System/ Festplattenspiegelung
- Schutzsteckdosenleisten Serverraum
- Serverraum klimatisiert
- Serverraumüberwachung Temperatur und Feuchtigkeit
- USV - Unterbrechungsfreie Stromversorgung
- Videoüberwachung Serverraum

7.2 TOM - Verfügbarkeitskontrolle - Organisatorische Massnahmen

Hinweis: Organisatorische Massnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Aufbewahrung der Sicherungsmedien an einem sicheren Ort ausserhalb des Serverraums
- Backup & Recovery-Konzept (in schriftlicher Form vorhanden)
- Existenz eines Notfallplans
- Getrennte Partitionen für Betriebssysteme und Daten
- Kontrolle des Sicherungsvorgangs
- Regelmässige Tests zur Datenwiederherstellung und Protokollierung

8.1 TOM - Trennungsgebot - Technische Massnahmen

Hinweis: Technische Massnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Logische Mandantentrennung (softwareseitig)
- Physikalische Trennung (Systeme/Datenbanken/Datenträger)

8.2 TOM - Trennungsgebot - Organisatorische Massnahmen

Hinweis: Organisatorische Massnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Festlegung von Datenbankrechten
- Steuerung über Berechtigungskonzept

9.1 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung - Datenschutz-Management

Hinweis: Datenschutz-Management (Massnahmen, die gewährleisten, dass die innerbetriebliche Organisation so gestaltet wird, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird).

- Schriftliche Bestellung eines Datenschutzbeauftragten
- Regelmäßige Schulung der Mitarbeiter zum Datenschutz
- Ein Verzeichnis der Verarbeitungstätigkeiten ist vorhanden, vollständig und aktuell
- Datenschutz-Folgenabschätzungen (sofern erforderlich) werden durchgeführt und protokolliert
- Es bestehen Standards für die IT-Sicherheit
- Die Aufbewahrung der elektronischen Protokolle ist geregelt
- Nachweise über die Verpflichtung auf das Datengeheimnis sind vorhanden
- Ein Datenschutzkonzept ist vorhanden
- Datenschutz- und Datensicherungs-Maßnahmen werden gelegentlich kontrolliert

9.2 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung - Incident-Response-Management

Hinweis: Datenschutz-Management (Massnahmen, die gewährleisten, dass die innerbetriebliche Organisation so gestaltet wird, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird).

- Schulung der Mitarbeiter bzgl. Erkennen einer Datenpanne
- Es existiert ein internes Incident-Response-Management-Konzept
- Es gibt ein Konzept zur Meldung von Datenpannen an den Auftraggeber

Creanet Internet Service AG

Ersteller: Yvan Jeanmonod
Version: v2024.04