

ADV-Vertrag gemäß DSGVO Verordnung

Dieser Vertrag gilt als geschlossen, sobald der Auftraggeber die AGBs der ting Beratungs-gmbH anerkannt wird.

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in einen Drittstaat bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu 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.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogene Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrischen Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde

(1) Zuständige Aufsichtsbehörde für den Auftragnehmer ist **Unabhängiges Datenschutzzentrum Saarland (UDZ), Fritz-Dobisch-Str. 12, 66111 Saarbrücken.**

(2) Zuständige Aufsichtsbehörde für den Auftraggeber ist _____

(4) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 Vertragsgegenstand und Laufzeit

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich **Beratung, Weiterentwicklung, Unterstützung und Ausführung von Social Media-Aktivitäten** auf Grundlage des Vertrags mit dem Auftragnehmer („Leistungsvertrag“). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung). Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Leistungsvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Leistungsvertrages und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittstaat oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit

zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus **Anlage 1**. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Art und Umfang der verarbeiteten Daten, Kreis der Betroffenen

(1) Art und Umfang der vom Auftragsverarbeiter zu erbringenden Leistungen

Beratung, Weiterentwicklung, Unterstützung und Ausführung von Social Media-Aktivitäten.

(2) Die Erhebung, Verarbeitung und Nutzung der Daten erfolgt für folgende Zwecke:

Kundendialog, Betreuung von Onlinepräsenzen in Social Media, Gewinnspiele

(3) Art der Daten

Personenbezogenen Adressdaten, z.B. Namen, Anschrift, Telefonnummern, E-Mail-Adressen, anonymisierte Umfrageergebnisse zu Produkten oder Dienstleistungen.

(4) Betroffene Personengruppen

Endverbraucher, Kunden, Lieferanten etc. im Bereich B2B und B2C

(5) Staaten und Orte der Verarbeitung

Bundesrepublik Deutschland, Frankreich, Luxemburg, Irland

§ 6 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in **Anlage 2** aufgeführten Maßnahmen der Zutrittskontrolle, Zugangskontrolle,

Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungskontrolle. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter/als Ansprechpartner für den Datenschutz (sofern ein Datenschutzbeauftragter nach Art. 37 Abs. 1 DS-GVO nicht bestellt werden muss) bestellt: **netvocat GmbH, (Ansprechpartner: Eric Wagner) Großherzog-Friedrich-Straße 40, 66111 Saarbrücken**. Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegen.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

(7) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

§ 9 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 3** genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des

Subunternehmers vorab schriftlich zugestimmt hat. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. Der Vertrag mit dem Subunternehmer hat schriftlich zu erfolgen, was auch in einem elektronischen Format erfolgen kann. Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Sofern eine Einbeziehung von Subunternehmern in einem Drittstaat erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist. Der Auftragnehmer wird dem Verantwortlichen auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 10 Anfragen und Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 - 36 DS-GVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

(3) Soweit der Auftragnehmer aufgrund gesetzlicher Bestimmungen Dritten Auskunft über Daten des Auftraggebers erteilen muss, ist der Auftragnehmer verpflichtet, den Auftraggeber rechtzeitig vor Auskunftserteilung über Empfänger, Zeitpunkt und Inhalt der zu erteilenden Auskunft und deren Rechtsgrundlage schriftlich zu informieren.

§ 11 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 12 Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

§ 13 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen bzw. Datenträger sind nach den entsprechenden DIN-Normen datenschutzkonform zu vernichten.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 14 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer im Sinne des § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Saarbrücken.

Anlagen

Anlage 1 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 2 – Genehmigte Subunternehmer

Auftragnehmer:

Thorsten Bost (Geschäftsführender Gesellschafter)

ting Beratungs-GmbH, Uhlandstraße 5, 66121 Saarbrücken

Tel. (06 81) 91 00 56 10

t.bost@ting.info

Anlage 1: Datensicherungsmaßnahmen

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- | | |
|--|--|
| <input type="checkbox"/> Alarmanlage | <input type="checkbox"/> Absicherung von Gebäudeschächten |
| x Automatisches Zugangskontrollsystem | <input type="checkbox"/> Chipkarten-/Transponder-Schließsystem |
| x Schließsystem mit Codesperre | <input type="checkbox"/> Manuelles Schließsystem |
| <input type="checkbox"/> Biometrische Zugangssperren | <input type="checkbox"/> Videoüberwachung der Zugänge |
| <input type="checkbox"/> Lichtschranken / Bewegungsmelder | x Sicherheitsschlösser |
| <input type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> Personenkontrolle beim Pfortner / Empfang |
| <input type="checkbox"/> Protokollierung der Besucher | x Sorgfältige Auswahl von Reinigungspersonal |
| x Sorgfältige Auswahl von Wachpersonal | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen |

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- | | |
|--|--|
| x Zuordnung von Benutzerrechten | <input type="checkbox"/> Erstellen von Benutzerprofilen |
| <input type="checkbox"/> Passwortvergabe | <input type="checkbox"/> Authentifikation mit biometrischen Verfahren |
| x Authentifikation mit Benutzername / Passwort | <input type="checkbox"/> Zuordnung von Benutzerprofilen zu IT-Systemen |
| x Gehäuseverriegelungen | x Einsatz von VPN-Technologie |

- | | | | |
|---|---|--|---|
| <input type="checkbox"/> Sperren von externen Schnittstellen (USB etc.) | x | Sicherheitsschlösser | |
| <input type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> | Personenkontrolle beim Pförtner / Empfang | |
| <input type="checkbox"/> Protokollierung der Besucher | x | Sorgfältige Auswahl von Reinigungspersonal | |
| x | Sorgfältige Auswahl von Wachpersonal | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen | |
| <input type="checkbox"/> Einsatz von Intrusion-Detection-Systemen | <input type="checkbox"/> | Verschlüsselung von mobilen Datenträgern | |
| x | Verschlüsselung von Smartphone-Inhalten | <input type="checkbox"/> Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten) | |
| x | Einsatz von Anti-Viren-Software | x | Verschlüsselung von Datenträgern in Laptops / Notebooks |
| x | Einsatz einer Hardware-Firewall | <input type="checkbox"/> | Einsatz einer Software-Firewall |

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- | | | | |
|---|--|--------------------------|---|
| x | Erstellen eines Berechtigungskonzepts | x | Verwaltung der Rechte durch Systemadministrator |
| x | Anzahl der Administratoren auf das „Notwendigste“ reduziert | <input type="checkbox"/> | Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel |
| x | Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten | x | Sichere Aufbewahrung von Datenträgern |

- | | | | |
|---|--|---|---|
| x | physische Löschung von Datenträgern vor Wiederverwendung | x | ordnungsgemäße Vernichtung von Datenträgern |
| x | Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) | x | Protokollierung der Vernichtung |
| x | Verschlüsselung von Datenträgern | | |

4. Weitergabekontrolle

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.

- | | | | |
|--------------------------|--|--------------------------|--|
| x | Einrichtungen von Standleitungen bzw. VPN-Tunneln | <input type="checkbox"/> | Weitergabe von Daten in anonymisierter oder pseudonymisierter Form |
| x | E-Mail-Verschlüsselung | x | Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen |
| x | Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen | x | Beim physischen Transport: sichere Transportbehälter/-verpackungen |
| <input type="checkbox"/> | Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen | | |

5. Eingabekontrolle

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

- | | |
|---|---|
| <ul style="list-style-type: none"> x Protokollierung der Eingabe, Änderung und Löschung von Daten | <ul style="list-style-type: none"> x Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. |
| <ul style="list-style-type: none"> x Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) | <ul style="list-style-type: none"> <input type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind |
| <ul style="list-style-type: none"> x Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts | |

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.

- | | |
|---|--|
| <ul style="list-style-type: none"> x Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) | <ul style="list-style-type: none"> x vorherige Prüfung und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen |
| <ul style="list-style-type: none"> x schriftliche Weisungen an den Auftragsverarbeiter (z. B. durch Auftragsverarbeitungsvereinbarung) | <ul style="list-style-type: none"> x Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis bzw. Vertraulichkeit |
| <ul style="list-style-type: none"> x Auftragsverarbeiter hat Datenschutzbeauftragten bestellt | <ul style="list-style-type: none"> x Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags |
| <ul style="list-style-type: none"> x Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart | <ul style="list-style-type: none"> x laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten |
| <ul style="list-style-type: none"> <input type="checkbox"/> Vertragsstrafen bei Verstößen | |

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- | | |
|--|---|
| <input checked="" type="checkbox"/> Unterbrechungsfreie Stromversorgung (USV) | <input type="checkbox"/> Klimaanlage in Serverräumen |
| <input type="checkbox"/> Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | <input checked="" type="checkbox"/> Schutzsteckdosenleisten in Serverräumen |
| <input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen | <input type="checkbox"/> Feuerlöschgeräte in Serverräumen |
| <input type="checkbox"/> Alarmmeldung bei unberechtigten Zutritten zu Serverräumen | <input checked="" type="checkbox"/> Erstellen eines Backup- & Recovery-konzepts |
| <input checked="" type="checkbox"/> Testen von Datenwiederherstellung | <input checked="" type="checkbox"/> Erstellen eines Notfallplans |
| <input checked="" type="checkbox"/> Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort | <input checked="" type="checkbox"/> Serverräume nicht unter sanitären Anlagen |
| <input checked="" type="checkbox"/> In Hochwassergebieten: Serverräume über der Wassergrenze | |

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- | | |
|---|--|
| <input checked="" type="checkbox"/> physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern | <input checked="" type="checkbox"/> Logische Mandantentrennung (softwareseitig) |
| <input checked="" type="checkbox"/> Erstellung eines Berechtigungskonzepts | <input checked="" type="checkbox"/> Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden |

x Versehen der Datensätze mit
Zweckattributen/Datenfeldern

Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

x Festlegung von Datenbankrechten

Trennung von Produktiv- und Testsystem

Anlage 2: **Genehmigte Subunternehmer**

	Unternehmen, Sitz	Auftragsleistungen
	hmstr GmbH, 66121 Saarbrücken	Monitoring-, Analyse-, Webseite-, dienstleistungen
	Die Socialisten (Social Software Development GmbH), A-1070 Wien	Ticketingsystem Social Media
	whami UG, 66123 Saarbrücken	Webhosting
	one4vision GmbH, 66119 Saarbrücken	Webhosting
	Talkwalker Sàrl, L-2163 Luxembourg	Monitoring
	Uphill GmbH, 10999 Berlin	Analyse von Social Media Kanälen