Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Art. 28 DSGVO stellt spezifische Anforderungen an eine Auftragsverarbeitung. Zur Wahrung dieser speziellen Anforderungen schließen die Vertragsparteien zusätzlich diesen Vertrag zur Auftragsverarbeitung. Er findet Anwendung auf alle Tätigkeiten, die mit dem abgeschlossenen Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers, oder durch den Auftragnehmer Beauftragte personenbezogene Daten (nachstehend „Daten") des Auftraggebers verarbeiten. Es gelten die Begriffsbestimmungen der DSGVO.

Dieser Vertrag zur Auftragsverarbeitung bildet zusammen mit unserem Angebot sowie unseren AGB eine verbindliche Vereinbarung (die "Vereinbarung") zwischen dem Auftraggeber und dem Auftragnehmer.

1. Vertragsgegenstand und Weisungsrecht des Auftraggebers

(1) Gegenstand dieses Vertrages sind Leistungen des Auftragnehmers für den Auftraggeber im Bereich Erstellen einer Website und, soweit vom Auftrag erfasst, Warten der Website. Darüber hinaus wird auf die **Anlage 1** dieses Vertrages verwiesen. Bei Änderungen der beauftragten Leistung ist dieser Vertrag zur Auftragsverarbeitung in der Anlage 1 entsprechend anzupassen und zu ergänzen.

(2) Dem Auftraggeber als verantwortliche Stelle obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung nach der DSGVO.

(3) Bei der Erbringung der Leistung erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers, sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist.

(4) Die Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt und können vom Auftraggeber in zumindest dokumentiert elektronischem Format durch Einzelweisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). 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. (Art. 28 Abs. 3 lit. a) DSGVO).

(5) 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, ohne dass ihm hierdurch negative Konsequenzen entstehen. Der Auftraggeber ist für die Erteilung rechtsgültiger Weisungen verantwortlich. (Art. 28 Abs. 3 Satz 3 DSGVO).

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

2. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer beachtet die gesetzlichen Bestimmungen über den Datenschutz. Eine Weitergabe oder Offenlegung von Informationen des Auftraggebers an Dritte erfolgt ohne eine ausdrückliche Weisung des Auftraggebers nicht. Unterlagen und Daten werden

gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik gesichert.

(2) Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO getroffen hat. Hierzu wird auf **Anlage 2** verwiesen.

(3) Der Auftraggeber überprüft vor der Aufnahme der Datenverarbeitung und sodann regelmäßig die technischen und organisatorischen Maßnahmen des Auftragnehmers. Änderungen an den vereinbarten Sicherheitsmaßnahmen können vorgenommen werden, soweit diese das vertraglich vereinbarte Schutzniveau nicht unterschreiten.

3. Vertraulichkeit

Dem Auftragnehmer und dessen Beschäftigten ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Der Auftragnehmer verpflichtet alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden zur Vertraulichkeit. Die Vertraulichkeits-Verpflichtungen gelten auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und dem Auftragnehmer.

4. 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 dokumentiertem elektronischen Format informieren, soweit sie sich auf diesen Vertrag beziehen. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen.

(2) Die Meldung über eine Verletzung des Schutzes personenbezogener Daten an den Auftraggeber enthält, soweit möglich, folgende Informationen:

a) 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;

b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und

c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

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

(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 DSGVO liegt.

(5) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 (Art. 28 Abs. 3 lit. e) DSGVO) sowie Art. 32 bis 36 DS-GVO (Art. 28 Abs. 3 lit. f) DSGVO).

5. Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche, schriftliche oder elektronische 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.

(2) Inspektionen durch den Auftraggeber bzw. dessen beauftragen Prüfern, die in keinem Wettbewerbsverhältnis zum Auftragnehmer stehen dürfen, können zu den üblichen Geschäftszeiten und mit einer Vorlaufzeit der Ankündigung von 14 Tagen durchgeführt. Der Auftraggeber führt Kontrollen nur im erforderlichen Umfang durch und stört Betriebsabläufe des Auftragnehmers dabei nur in verhältnismäßiger Weise. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Die Vergütung wird einzelvertraglich vereinbart.

6. Einsatz von Subauftragnehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Hinzuziehung der in **Anlage 3** genannten Subauftragnehmer (Subdienstleister) durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Subunternehmers vorab zumindest in einem dokumentiert elektronischen Format 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) wahrnehmen kann. (Art. 28 Abs. 4 DSGVO)

(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.

7. Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

8. 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 eine gesetzliche 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.

(2) 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.

9. Schlussbestimmungen

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

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines dokumentierten elektronischen Formats.

(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 und es gelten die gesetzlichen Regelungen des Art. 28 DSGVO.

Anlagen:

Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3 – Subunternehmer

Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien

Gegenstand der Verarbeitung Art **und** Zweck der Verarbeitung	Die konkrete Leistung ergibt sich aus dem Vertrag sowie dem Angebot. Zur Erbringung der Leistungen kann der Auftragnehmer Zugriff auf Softwareanwendungen wie Newslettertools, CRM, Buchungstools sowie Social Media Accounts des Auftraggebers nehmen. Je nach Organisationsform kann auch Zugriff genommen werden auf Mitglieder oder Funktionärsdaten. Art der Verarbeitung, soweit vom Angebot umfasst:

	• Erfassung: Sammlung von Daten zur Integration in die Website. • Verwendung: Nutzung der Daten zur Optimierung, Personalisierung und Anpassung der Website an die Bedürfnisse der Endbenutzer. • Löschung: Entfernung von Daten aus Systemen, wenn diese nicht mehr benötigt werden oder auf Wunsch des Betroffenen. • Wartung • Zugriff auf Newsletter-Abonnenten Zweck der Verarbeitung: • Gestaltung einer benutzerfreundlichen, responsiven und funktionsfähigen Website. • Sicherstellung der technischen Funktionsfähigkeit und Sicherheit der Website im Rahmen der Wartung. • Analyse und Optimierung der Websiteperformance sowie Content Marketing Maßnahmen
Art der personenbezogenen Daten	Grundlegende Identifikationsdaten: Name, Adresse, Kommunikationsdaten: Telefonnummer, E-Mail-Adresse, Newsletter- Abonnenten. Technische Daten: IP-Adresse, Browser-Typ, Betriebssystem, Gerätetyp, Zugriffszeiten. Nutzungsdaten: Besuchte Seiten, Verweildauer, Klickverhalten. Andere spezifische Datenkategorien, die im Rahmen des Projekts erforderlich sein könnten (z. B. Zahlungs- oder Buchungsdaten, wenn ein Webshop integriert ist). Werden besondere Kategorien personenbezogener Daten verarbeitet? ☐Ja ☒Nein
Kategorien betroffener Personen	• Interessenten • Webseitenbesucher • Kunden des Auftraggebers

	• Newsletter-Abonnenten

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Informationen zu den getroffenen technisch-organisatorischen Maßnahmen	
Version	1.0
Datum	20.03.2025

Nachfolgende Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung wurden implementiert.

1. Vertraulichkeit

Vertraulichkeit = personenbezogene Daten dürfen unberechtigten Personen oder Organisationen nicht verfügbar gemacht oder offengelegt werden

a. Zutrittskontrolle zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden

= Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verhindern

Keine externen Termine vor Ort; Arbeit ausschließlich digital oder beim Kunden vor Ort

b. Zugangskontrolle zu Datenverarbeitungssystemen

= Maßnahmen, dass Datenverarbeitungssysteme nicht von Unbefugten genutzt werden können

Anmeldung mittels Benutzername und Passwort; Passwortregelungen: mindestens 8 Zeichen, Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen; Verwendung eines Passwort-Safes; Automatisches Sperren des Bildschirms & Passworteingabe zum erneuten Zugang; Multi-Faktor-Authentifizierung, soweit möglich; Einsatz von Anti-Viren-Software; aktive Firewall; Verschlüsselung von Smartphones/Laptops/Tablets; Sorgfältige Auswahl von Dienstleistern; Clean-Desk-Policy

c. Trennungskontrolle

=Daten verschiedener Auftraggeber werden getrennt aufbewahrt

logische Trennung (Ordnerstruktur, strukturierte Dateiablage)

2. Integrität

Wahrung der Richtigkeit, Unveränderheit und Vollständigkeit von personenbezogenen Daten

a. Weitergabekontrolle

= Kein unbefugtes Lesen, Kopieren oder Verändern von Daten bei elektronischen Übertragungen (z. B. E-Mails) oder Transport

Weitergabe ausschließlich nach dem Need-To-Know-Prinzip und nach Zustimmung der Kunden; Weitergabe von Papierdokumenten in verschlossenen, undurchsichtigen Umschlägen; https-Verschlüsselung auf der Website;

3. Auftragskontrolle

Es ist ein auftrags- und weisungsgemäße Auftragsdatenverarbeitung zu gewährleisten. Daten des Auftraggebers werden ausschließlich nach dessen Weisungen verarbeitet. Hierzu wurde ein Vertrag zur Auftragsverarbeitung abgeschlossen. Unterauftragnehmer werden vom Auftraggeber nur nach den Vorgaben der vertraglichen Regelung eingeschaltet.

4. Verfügbarkeit & Belastbarkeit

Schutz gegen Zerstörung und Verlust sowie Gewährleistung der Nutzung von Daten

Backupkonzept umgesetzt

5. Regelmäßige Überprüfung, Bewertung & Evaluierung der getroffenen technisch-organisatorischen Maßnahmen

kontinuierliche Überprüfung der TOMs; dokumentierte Prozesse zur Einhaltung der DSGVO etabliert (Auskunftsersuchen fristgerecht beantworten, Verletzung an die Aufsichtsbehörde melden); sorgfältige Auswahl von Dienstleistern; Umsetzung des Zweckbindungsgrundsatzes;

Anlage 3 – Genehmigte Subauftragnehmer

Genehmigte Subauftragnehmer nach § 6 dieses Vertrages:

Beauftragtes Unternehmen	**Verarbeitungstätigkeit**	**Verarbeitungsort**
Adobe Systems Software Ireland Limited mit Sitz in 4-6 Riverwalk, City West Business Campus, Saggart D24, Dublin, Irland	Verwendung der Adobe-Anwendungen zur Erstellung von Grafiken und Entwürfen; Verwendung von Adobe Sign zur Einholung digitaler Unterschriften	Irland sowie Amerika Zum Data Processing Agreement Die Zertifizierung nach dem Data Privacy Framework können Sie hier einsehen.