Vertrag zur Auftragsverarbeitung

nach Art. 28 Datenschutz-Grundverordnung (DSGVO)

Auftraggeber	**Auftragnehmer**
Name / Firma: _____ Anschrift: _____	Denis Reuck (re-guard) Rübenhäulestraße 44, 72461 Albstadt info@re-guard.de

Dieser Vertrag regelt den Datenschutz bei der Zusammenarbeit zwischen dem Auftraggeber (dem Kunden von re-guard) und dem Auftragnehmer (Denis Reuck, re-guard). Er ergänzt den Vertrag über das Hosting-Paket und die gebuchten Module (der „Hauptvertrag“ mit den AGB) und gilt für alle Tätigkeiten, bei denen der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet.

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer betreibt das Hosting-Paket des Auftraggebers und die gebuchten Module (re-guard Büro, re-guard Bau) und gegebenenfalls Websites des Auftraggebers auf seinen Servern, hält sie technisch aktuell (Updates), sichert sie, überwacht sie, leistet Support und führt vereinbarte Arbeiten aus. Beim Support greift er auf Daten nur zu, soweit es zur Behebung einer Störung oder zur Beantwortung einer Anfrage nötig ist. Auf Wunsch des Auftraggebers registriert er eine Domain bei einer Registrierungsstelle. Dabei verarbeitet er personenbezogene Daten im Auftrag des Auftraggebers.

(2) Der Vertrag gilt für die Laufzeit des Hauptvertrags und endet mit ihm. Die Pflichten zu Löschung und Rückgabe (§ 9) bleiben danach bestehen, bis sie erfüllt sind.

§ 2 Art und Zweck der Verarbeitung, Daten und Betroffene

(1) Art und Zweck: Speichern, Bereitstellen, Sichern, Wiederherstellen, Aktualisieren, Überwachen, Übertragen und Löschen der Daten, die auf den Systemen des Auftragnehmers für die Programme und Websites des Auftraggebers liegen, damit sie erreichbar und sicher betrieben werden, sowie Unterstützung im Support.

(2) Arten von Daten: Inhalte der Website; Angaben, die Besucher über Formulare, Kommentare oder Shop-Funktionen der Website eingeben (zum Beispiel Name, E-Mail-Adresse, Nachricht); Daten, die der Auftraggeber in den Modulen erfasst (zum Beispiel Kundendaten, Anschriften, Kontaktdaten, Angebote, Aufträge, Lieferscheine, Rechnungen, Rapporte, Arbeitszeiten, Baustellen- und Bautagebuch-Angaben, Fotos, Unterschriften); Benutzerkonten (zum Beispiel Name, E-Mail-Adresse, Rolle und ein nicht umkehrbarer Prüfwert des Passworts); Support-Tickets und Wünsche; Zugriffsprotokolle (gekürzte IP-Adresse, Zeitpunkt, aufgerufene Adresse, Browserkennung).

(3) Betroffene: Besucherinnen und Besucher und Nutzerinnen und Nutzer der Website, Beschäftigte, Kundschaft, Ansprechpersonen und Subunternehmer des Auftraggebers, soweit ihre Daten in den Programmen oder auf der Website verarbeitet werden.

(4) Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) verarbeitet der Auftragnehmer nur, wenn der Auftraggeber sie in seinen Programmen oder auf seiner Website verarbeitet und dies dem Auftragnehmer vorher in Textform mitgeteilt hat.

§ 3 Weisungen

(1) Der Auftragnehmer verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, ein Gesetz verpflichtet ihn zu einer anderen Verarbeitung. In diesem Fall teilt er dies dem Auftraggeber vorher mit, soweit das Gesetz es nicht verbietet.

(2) Die Weisungen ergeben sich aus dem Hauptvertrag und diesem Vertrag. Weitere Weisungen erteilt der Auftraggeber in Textform (E-Mail oder Ticket im Kundenbereich). Mündliche Weisungen bestätigt er

unverzüglich in Textform.

(3) Hält der Auftragnehmer eine Weisung für rechtswidrig, weist er den Auftraggeber darauf hin. Er darf die Ausführung aussetzen, bis die Weisung bestätigt oder geändert ist.

(4) Weisungsberechtigte Personen und Ansprechpartner stehen in Anlage 3.

§ 4 Pflichten des Auftragnehmers

(1) Vertraulichkeit: Der Auftragnehmer verpflichtet alle Personen, die an der Verarbeitung beteiligt sind, zur Vertraulichkeit, soweit sie nicht bereits einer gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Sicherheit der Verarbeitung: Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind. Er entwickelt sie nach dem Stand der Technik weiter und unterschreitet das dort beschriebene Schutzniveau nicht.

(3) Betroffenenrechte: Wendet sich eine betroffene Person wegen ihrer Daten an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Auftraggeber weiter und antwortet nicht selbst. Er unterstützt den Auftraggeber im Rahmen des Möglichen bei Auskunft, Berichtigung, Löschung, Einschränkung, Übertragbarkeit und Widerspruch.

(4) Unterstützung: Der Auftragnehmer unterstützt den Auftraggeber angemessen bei der Einhaltung der Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, Konsultation der Aufsichtsbehörde), soweit diese Pflichten mit der Verarbeitung im Auftrag zusammenhängen.

(5) Verletzung des Schutzes personenbezogener Daten: Der Auftragnehmer meldet dem Auftraggeber eine Verletzung unverzüglich, spätestens innerhalb von 48 Stunden nach Bekanntwerden, mit den ihm vorliegenden Angaben (Art, betroffene Daten, mögliche Folgen, ergriffene Maßnahmen) und ergänzt sie, sobald er mehr weiß.

(6) Verzeichnis: Der Auftragnehmer führt das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

(7) Datenschutzbeauftragter: Der Auftragnehmer hat keinen Datenschutzbeauftragten benannt, weil er dazu nicht verpflichtet ist. Ansprechpartner in Datenschutzfragen ist er selbst (Anlage 3).

§ 5 Unterauftragsverarbeiter

(1) Der Auftraggeber genehmigt den Einsatz der in Anlage 2 genannten Unterauftragsverarbeiter.

(2) Will der Auftragnehmer einen weiteren Unterauftragsverarbeiter einsetzen oder einen bestehenden ersetzen, kündigt er das mindestens 14 Tage vorher in Textform an. Der Auftraggeber kann aus einem wichtigen datenschutzrechtlichen Grund widersprechen. Einigen sich die Parteien nicht, kann der Auftraggeber den Hauptvertrag außerordentlich zum Zeitpunkt des Wechsels kündigen.

(3) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf ein gleichwertiges Datenschutzniveau und bleibt dem Auftraggeber gegenüber für dessen Handeln verantwortlich.

§ 6 Verarbeitung außerhalb der EU und des EWR

(1) Die Daten werden auf Servern in Deutschland gespeichert. Vorgeschaltete Dienste, insbesondere Cloudflare (Anlage 2), die die Auslieferung und die Namensauflösung übernehmen, können dabei Daten auch in Ländern außerhalb der EU und des EWR verarbeiten. Grundlage ist nach Angabe des Auftragnehmers der Angemessenheitsbeschluss der EU-Kommission zum EU-US Data Privacy Framework (Art. 45 DSGVO) und der Vertrag zur Auftragsverarbeitung mit Standardvertragsklauseln (Art. 46 DSGVO).

(2) Eine darüber hinausgehende Übermittlung in ein Land außerhalb der EU oder des EWR findet nur mit vorheriger Zustimmung des Auftraggebers in Textform und nur statt, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 7 Nachweise und Kontrollen

(1) Der Auftragnehmer weist dem Auftraggeber auf Anfrage nach, dass er die Pflichten aus diesem Vertrag einhält. Als Nachweis dienen insbesondere die Beschreibung der Maßnahmen in Anlage 1, die Protokolle der regelmäßigen Wiederherstellungstests und die Berichte und Prüfprotokolle im Kundenbereich.

(2) Kontrollen durch den Auftraggeber oder eine von ihm beauftragte, zur Verschwiegenheit verpflichtete Person sind nach Anmeldung mit mindestens 14 Tagen Vorlauf während der üblichen Geschäftszeiten möglich, ohne den Betrieb unverhältnismäßig zu stören. Der Aufwand des Auftragnehmers wird nach dem im Hauptvertrag vereinbarten Stundensatz vergütet.

(3) Die Sicherheit der Rechenzentren der Unterauftragsverarbeiter weist der Auftragnehmer durch deren Zertifikate und Nachweise nach; Vor-Ort-Kontrollen dort sind ausgeschlossen.

§ 8 Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung in seinen Programmen und auf seiner Website verantwortlich. Dazu gehören insbesondere die Rechtsgrundlage, die Datenschutzerklärung und Informationspflichten gegenüber Besuchern, Einwilligungen (zum Beispiel für Cookies) und der Umgang mit Anfragen betroffener Personen.

(2) Der Auftraggeber erteilt Weisungen in Textform und informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

(3) Der Auftraggeber geht mit seinen Zugangsdaten sorgfältig um, wählt sichere Passwörter und sendet Passwörter nicht per E-Mail oder über ein Formular.

§ 9 Löschung und Rückgabe

(1) Vor dem Ende des Hauptvertrags kann der Auftraggeber seine Daten in den Programmen exportieren (zum Beispiel als CSV-Datei und PDF) und seine Website (Dateien und Datenbank) im Kundenbereich unter „Meine Daten“ als Archiv herunterladen. Nach dem Ende des Hauptvertrags bleibt der Zugang 30 Tage lang nur lesend.

(2) Danach deaktiviert der Auftragnehmer den Zugang und die Programme und löscht die Daten auf den Produktivsystemen frühestens 90 Tage nach Vertragsende. Ein beim Entfernen einer Website erzeugtes Abschiedsarchiv löscht er nach 90 Tagen. Zugriffsprotokolle werden nach acht Wochen gelöscht.

(3) Daten in Sicherungskopien werden nicht gesondert gelöscht, sondern laufen bei der turnusmäßigen Rotation der Sicherungen innerhalb von bis zu zwölf Monaten aus. Sie werden bis dahin nicht wiederverwendet.

(4) Gesetzliche Aufbewahrungspflichten des Auftragnehmers bleiben unberührt. Sie betreffen nur die Abrechnungsdaten des Auftraggebers als Kunde, nicht die Daten in seinen Programmen und auf seiner Website.

§ 10 Haftung

Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Verhältnis der Parteien zueinander gelten die Haftungsregeln des Hauptvertrags (AGB).

§ 11 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Eine neue Fassung dieses Vertrags legt der Auftragnehmer dem Auftraggeber im Kundenbereich zur Bestätigung vor; bis dahin gilt die zuletzt bestätigte Fassung.

(2) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen in Fragen des Datenschutzes die Regelungen dieses Vertrags vor.

(3) Es gilt deutsches Recht. Sind einzelne Bestimmungen unwirksam, bleibt der übrige Vertrag wirksam.

(4) Der Vertrag kommt zustande, indem der Auftraggeber im Kundenbereich seine Angaben macht und den Abschluss bestätigt. Zeitpunkt, Fassung und Angaben werden gespeichert und genügen der Textform.

Anlage 1: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Zutrittskontrolle: Die Server stehen in den Rechenzentren der Unterauftragsverarbeiter (Anlage 2). Zutritt dort regeln deren Sicherheitskonzepte. Der Auftragnehmer selbst betreibt keine Server in eigenen Räumen.

Zugangskontrolle: Zugriff auf die Server nur mit Schlüssel (keine Passwort-Anmeldung per SSH), Firewall am Server, automatische Sperre von Adressen nach Fehlversuchen (fail2ban), Verwaltungsbereich mit Passwort und Zwei-Faktor-Anmeldung, Kundenbereich mit Passwort und optionalem zweiten Faktor, Begrenzung der Anmeldeversuche.

Zugriffskontrolle: Jede Website und jede Installation der Programme läuft unter einem eigenen Systembenutzer mit eigenem PHP-Prozess und eigener Datenbank; die Daten verschiedener Kunden sind voneinander getrennt. In den Programmen sieht jede Benutzerin und jeder Benutzer nur, was die zugewiesene Rolle erlaubt. Der Kundenbereich zeigt jedem Kunden nur seine eigenen Daten. Passwörter werden nur als nicht umkehrbare Prüfwerte gespeichert; hinterlegte Zugangsdaten sind mit einem öffentlichen Schlüssel verschlüsselt, jeder Abruf wird protokolliert.

Weitergabekontrolle: Alle Verbindungen zu den Websites und zum Kundenbereich sind per HTTPS verschlüsselt. Sicherungskopien werden verschlüsselt auf einen externen Speicher übertragen; der Schlüssel liegt getrennt davon.

Eingabe- und Protokollkontrolle: Zugriffsprotokolle der Websites mit gekürzten IP-Adressen und einer Aufbewahrung von acht Wochen. Änderungen am Server laufen über dokumentierte Werkzeuge; Abrufe hinterlegter Zugangsdaten werden mit Zeitpunkt festgehalten.

Verfügbarkeitskontrolle: Sicherung zweimal täglich, verschlüsselte externe Kopie, wöchentliche Wiederherstellungsprüfung mit Protokoll, stündliche Überwachung der Erreichbarkeit, automatische Sicherheitsupdates des Systems, WordPress-Updates mit vorheriger Sicherung und automatischem Zurücksetzen bei Fehlern, nächtliche Prüfung auf Schadsoftware und auffällige Dateien.

Trennungskontrolle: Daten verschiedener Auftraggeber werden getrennt verarbeitet (eigene Verzeichnisse, Benutzer, Datenbanken und Sicherungsstände je Website und je Installation).

Überprüfung: Die Maßnahmen werden regelmäßig geprüft (Überwachung, Testläufe, Berichte und Prüfprotokolle) und bei Bedarf angepasst.

Anlage 2: Unterauftragsverarbeiter

Unternehmen	Sitz	Leistung
myLoc managed IT AG	Düsseldorf, Deutschland	Betrieb der Server (Rechenzentrum, Hardware), auf denen die Websites und ihre lokalen Sicherungen liegen
Hetzner Online GmbH	Gunzenhausen, Deutschland	Verschlüsselte externe Sicherungskopien (Storage Box); auf Wunsch des Auftraggebers Registrierung einer Domain (Registrar)
Cloudflare, Inc. (in der EU: Cloudflare Germany GmbH)	San Francisco, USA (EU: München)	Auslieferung und Schutz vorgeschalteter Angebote (zum Beispiel Kundenbereich), Namensauflösung; Verarbeitung auch außerhalb der EU möglich (§ 6)
Discord Netherlands B.V. / Discord Inc.	Niederlande / USA	Nicht öffentlicher interner Kanal zur Bearbeitung von Support-Tickets; Verarbeitung auch außerhalb der EU möglich (§ 6)

Webspace und E-Mail-Postfächer bucht der Auftraggeber bei Bedarf selbst bei seinem Anbieter. Das ist keine Unterauftragsverarbeitung durch den Auftragnehmer. Bei einer Domain-Registrierung über den Auftragnehmer gibt dieser die erforderlichen Angaben an die Registrierungsstelle (für .de die DENIC eG) weiter, die die Daten nach ihren eigenen Bedingungen verarbeitet.

Anlage 3: Ansprechpartner und Weisungsberechtigte

Auftragnehmer: Denis Reuck, Rübenhäulestraße 44, 72461 Albstadt, E-Mail info@re-guard.de.

Auftraggeber: die Person, die das Konto des Auftraggebers im Kundenbereich führt, sowie weitere Personen, die der Auftraggeber dem Auftragnehmer in Textform nennt.

Abschluss: Im Kundenbereich von re-guard bestätigt der Auftraggeber diesen Vertrag mit seinen Angaben; Zeitpunkt und Fassung werden gespeichert. Alternativ kann dieses Muster ausgefüllt und unterschrieben werden.

_____ _____

Ort, Datum, Auftraggeber Ort, Datum, Auftragnehmer