Allgemeine Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

Der **Verantwortliche** ist der jeweilige Lizenznehmer der Software der recordIT GmbH, im Folgenden Auftraggeber genannt.

Der **Auftragsverarbeiter** ist die recordIT GmbH, Griesgasse 1, 8020 Graz, im Folgenden Auftragnehmer genannt.

1. GEGENSTAND DER VEREINBARUNG

(1) Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben:
   a. Bereitstellung der vereinbarten Funktionalität der Software,
   b. gegebenenfalls auch die Bereitstellung des Hostings der Software, sofern vertraglich vereinbart.

   Diese Vereinbarung ist als Ergänzung zur Lizenzvereinbarung, den allgemeinen Geschäftsbedingungen und des abgeschlossenen Werkvertrages in der jeweilig geltenden Version zu verstehen.

(2) Folgende Datenkategorien werden möglicherweise verarbeitet: Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bestelldaten, alle der Software zur Verfügung gestellten Daten (Bilder, Kommentare, Text- und Zahlenwerte, Bewertungen und weitere), also sämtliche Daten, die vom Auftraggeber in die Software eingegeben werden.

(3) **Der Auftraggeber verpflichtet sich ausdrücklich, weder sensible Daten gemäß Art 9 Abs 1 DSGVO, noch strafrechtlich relevante Daten gemäß Art 10 DSGVO in die Software der recordIT GmbH einzugeben und/oder der Verarbeitung zu übergeben.** Eine Verarbeitung sensibler Daten benötigt weitergehender Schutzmaßnahmen und muss daher gesondert schriftlich vereinbart werden.

(4) Folgende Kategorien betroffener Personen unterliegen möglicherweise der Verarbeitung: Die übergebenen Daten aller Personen, die die Software benutzen, Kunden und Lieferanten des Auftraggebers und deren Kontaktpersonen, sowie Dritte (z.B. Gesprächspartner, Beteiligte, anwesende Personen, während der Dokumentations-vorhaben), deren Daten durch den Auftraggeber in die Software eingegeben werden.

(5) Welche Kategorie und Art an Daten in die Software eingegeben wird, kann durch den Auftragnehmer nicht beeinflusst werden, daher sind die Auflistungen in (2) und (4), sowie andere Listen in diesem Dokument nicht abschließend.

2. DAUER DER VEREINBARUNG

Die Vereinbarung wird auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit durch die Beendigung des Lizenzabkommens jederzeit gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Die Vereinbarung wird automatisch gelöst, falls keine Lizenz zur Benutzung der Software mehr vorhanden ist.

3. PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er – sofern gesetzlich zulässig – den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung von persönlichen Daten, die zur Verarbeitung übergeben wurden, für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage 1 zu entnehmen).

(4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Personen nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenverarbeitung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

(6) Der Auftraggeber wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat. Aufgrund der Vielfältigkeit und Konfigurierbarkeit der Nutzung der recordIT-Software kann das Verarbeitungsverzeichnis nicht durch den Auftragnehmer erstellt werden.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch von ihm beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind. Dieser Nachweis kann insbesondere durch die Vorlage aktueller Testate, Berichte oder Zertifikate von unabhängigen Instanzen oder durch einen geeigneten Nachweis eines externen Datenschutzbeauftragten erbracht werden. Eine Inspektion vor Ort durch den Auftraggeber ist nach rechtzeitiger Ankündigung (in der Regel mindestens vier Wochen im Voraus) während der üblichen Geschäftszeiten und auf Kosten des Verantwortlichen möglich, wobei sichergestellt wird, dass der Betriebsablauf des Auftragverarbeiters nicht unangemessen gestört wird und die Sicherheit der Daten anderer Kunden gewahrt bleibt.

(8) Nach Beendigung dieser Vereinbarung stellt der Auftragnehmer die Daten des Auftraggebers für einen Zeitraum von 30 Tagen zum Export über die in der Software vorgesehenen Funktionen zur Verfügung. Nach Ablauf dieser Frist ist der Auftragnehmer verpflichtet, alle personenbezogenen Daten, die sich auf seinen Systemen befinden und die im Auftrag des Auftraggebers verarbeitet wurden, sicher und unwiderruflich zu löschen, sofern keine gesetzlichen Aufbewahrungspflichten (z.B. aus dem Handels- oder Steuerrecht) oder sonstige rechtliche Grundlagen einer Löschung entgegenstehen.

(9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

5. SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer ist befugt folgende Unternehmen als Sub-Auftragsverarbeiter hinzuziehen:

- Midlight GmbH, Griesgasse 1, 8020 Graz
- Sub-Net e.U., Obertiefenbach 6, 8224 Hartl
- Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen (DE)

Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

ANLAGE 1 – TECHNISCH-ORGANISATORISCHE MASSNAHMEN

A. VERTRAULICHKEIT

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:

- Videoanlage
- Elektrische Türöffner
- Schlüssel
- Einbruchshemmende Fenster und/oder Sicherheitstüren
- Begleitung von Besuchern im Unternehmensgebäude

Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch:

- Kennwörter (einschließlich entsprechender Policy)
- Automatische Sperrmechanismen
- Zwei-Faktor-Authentifizierung
- Verschlüsselung von Datenträgern
- Least-Privilege-System, Zugriff aufs Live-System auf Datenbankebene nur für einzelne Benutzer

Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

- Standard-Berechtigungsprofile auf „need to know-Basis“
- Periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten
- Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger
- Sichere Aufbewahrung von Speichermedien
- Datenschutzgerechte Wiederverwendung von Datenträgern
- Clear-Desk/Clear-Screen Policy

B. DATENINTEGRITÄT[1]

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

- Verschlüsselung von Datenträgern, u.a. Zwang für Verschlüsselung auf für die Systemplatten
- Verschlüsselung von Dateien
- Verschlüsselung der Kommunikation, auch im Produkt (Frontend-Backend-Verbindung)
- Virtual Private Networks (VPN), unternehmensinterne Zugänge nur über VPN möglich
- Elektronische Signatur
- Two-Factor-Authentifikation für Zugänge inkl. Datenspeicherung und Kommunikationskanäle

Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:

- Protokollierung
- Dokumentenmanagement

[1] Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.

C. VERFÜGBARKEIT UND BELASTBARKEIT

Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

- Backup-Strategie (online/offline; on-site/off-site)
- Unterbrechungsfreie Stromversorgung (USV)
- Virenschutz
- Firewall
- Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum
- Security Checks auf Infrastruktur- und Applikationsebene
- Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
- Rasche Wiederherstellbarkeit der Daten

D. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen
- Datenschutzfreundliche Voreinstellungen

Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers durch eindeutige Vertragsgestaltung und Verpflichtung der Subunternehmer zu ebendiesen Pflichten.