Vertrag zur Auftragsverarbeitung
gemäß Art. 28 DS-GVO

Zwischen dem

.....
- Kunden der Plattform SCRT, siehe hinterlegte Rechnungsadresse in Stripe -
- nachstehend Auftraggeber genannt -

und

SCRT – Niklas Henneberger, Brüder-Becker-Straße 49, 97437 Haßfurt, Deutschland
- nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Vertrags

(1) Gegenstand

Der Gegenstand des Vertrags ergibt sich aus der Leistungsvereinbarung/ dem SLA/dem Auftrag Allgemeine Geschäftsbedingungen von SCRT (AGB) in der bei Vertragsschluss gültigen Fassung, auf die/den/das hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Dauer

Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

(3) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

(4) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

2. Konkretisierung des Vertragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Vertragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Bereitstellung und Betrieb der cloudbasierten SaaS-Plattform SCRT zur datenbasierten Prozess- und Workspace-Verwaltung für gewerbliche Kunden, einschließlich der Gewährleistung von Systemstabilität, technischem Support und Datensicherheit.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Planungs- und Steuerungsdaten
- **Jede weitere Datenkategorie**, welche der Auftraggeber eigenverantwortlich im Rahmen des Vertragsverhältnisses in den Workspaces der Plattform ablegt.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Beschäftigte
- Ansprechpartner

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorischen Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung [Anlage 1]. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.

(2) Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzen.

4. Rechte von betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die berechtigterweise Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

c) Die unverzügliche Informationspflicht des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

e) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.

g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.

i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Die Auslagerung auf Unterauftragnehmer oder der Wechsel der gemäß Anlage 2 bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

Der Auftraggeber stimmt der Beauftragung der in Anlage 2 bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2–4 DS-GVO zu. Die vertragliche Vereinbarung wird dem Auftraggeber auf Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug ausgenommen sind.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform).
Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Internationale Datentransfers

(1) Die primäre Speicherung und Verarbeitung mandantenbezogener Plattformdaten erfolgt in der EU (Rechenzentrum Frankfurt, AWS eu-central-1, über Supabase).

(2) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland an die in Anlage 2 genannten Empfänger. In der Anlage werden die vom Auftraggeber genehmigten Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DS-GVO im Rahmen der Unterbeauftragung spezifiziert.

(3) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Unternehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb während der üblichen Geschäftszeiten zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch:

- die Vorlage und Aktualisierung der in Anlage 1 dokumentierten technisch-organisatorischen Maßnahmen
- aktuelle interne Compliance- und Sicherheitsdokumentation des Auftragnehmers
- auf Anfrage bereitgestellte Auskünfte zu Unterauftragsverhältnissen gemäß Anlage 2 einschließlich abgeschlossener Auftragsverarbeitungsverträge mit Unterauftragnehmern (soweit ohne geschäftliche Geheimhaltung möglich)

9. Weisungsbefugnis des Auftraggebers

(1) Weisungen erteilt der Auftraggeber in Textform an datenschutz@scrt.de.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Vor Löschung kann der Auftraggeber einen Datenexport im JSON-Format über die Plattform anfordern. Operative Löschung nach Vertragsende erfolgt nach den technischen Prozessen des Auftragnehmers (insbesondere 30 Kalendertage nach Workspace-Soft-Delete), soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen (insbesondere Abrechnungsunterlagen bis zu 10 Jahren gemäß § 147 AO). Der reguläre Export ist ohne Zusatzvergütung; außergewöhnliche Sonderformate können nach vorheriger Ankündigung berechnet werden.

(2) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(3) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Anlage 1 - Technisch-organisatorische Maßnahmen

Pseudonymisierung und Verschlüsselung personenbezogener Daten
Transportverschlüsselung: Sämtliche Kommunikation zwischen Browser/Client und Backend über HTTPS/TLS (mindestens TLS 1.2).
Speicherung: Verschlüsselung im Ruhezustand durch den Cloud-Anbieter (Supabase/AWS).
Passwörter: Speicherung nur als Hash über Supabase Auth; keine Klartextpasswörter.
IP-Adressen: Wo verarbeitet (z. B. AGB-/Consent-Nachweise), nur gehasht oder gekürzt, keine vollständigen IPs in operativen Logs.

Kontinuierliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
Mandantentrennung: Row Level Security (RLS) auf allen mandantenfähigen Tabellen; Zugriff nur für authentifizierte Nutzer im jeweiligen Workspace.
Kein öffentlicher DB-Zugriff; API-Zugriff über authentifizierte Tokens (JWT) bzw. Service Role nur in Edge Functions/Cron-Jobs.
Webhook-Sicherheit: Signaturprüfung bei externen Webhooks (z. B. Stripe).
Rate Limiting auf sensiblen Edge Functions.
Verfügbarkeit: Bereitstellung unter dem Vorbehalt der Verfügbarkeit (vgl. AGB); angestrebte hohe Verfügbarkeit, keine 100%-Garantie.
Backups: Automatisierte Backups durch Supabase (täglich, Retention gemäß Anbieter-Paket).

Verfügbarkeit und rascher Zugang bei Zwischenfällen
Wiederherstellung aus Backup-Infrastruktur des Hosting-Anbieters.
Dokumentierte Lösch- und Purge-Prozesse (Account- und Workspace-Löschung mit Fristen und Registries).
Monitoring/Cron für abgelaufene Daten und DSGVO-SLA-Überwachung.

Regelmäßige Überprüfung, Bewertung und Evaluierung der Maßnahmen
Regelmäßige interne Prüfung (release- und quartalsbezogen) der Compliance-Dokumentation.
Technische Kontrollen in CI (z. B. Deletion-Registry-Checks).
Nutzung von Supabase Security Advisors / Hardening-Migrationen.
Anpassung der Maßnahmen bei wesentlichen Änderungen mit Information des Auftraggebers (§ 3 Abs. 3).

Identifizierung und Authentifizierung von Nutzern
Endnutzer: Login per E-Mail/Passwort (Supabase Auth); rollenbasierte Rechte im Workspace (owner/admin/member).
2FA/MFA für Endnutzer: Derzeit nicht im Produkt-UI verfügbar; Einführung ist geplant.
Administrative Systemzugänge (Supabase, Stripe, Resend, GitHub, Hosting): Zugriff nur für berechtigte Personen; Zwei-Faktor-Authentifizierung (2FA) ist auf Provider-Ebene einzurichten bzw. beizubehalten, soweit vom Anbieter angeboten.

Schutz bei Übertragung
Ausschließlich verschlüsselte Verbindungen (HTTPS/TLS).
CORS-Beschränkung auf konfigurierte Frontend-Origins (Produktion: https://scrt.de).

Schutz bei Speicherung
RLS, minimal notwendige Datenbank-Berechtigungen (Least Privilege).
Keine Speicherung unnötiger PII in Anwendungs- und Function-Logs.
Soft-Delete und Retention Policies vor physischem Löschen (fail-closed).
GoBD-/revisionssichere Daten: kein physisches Löschen innerhalb gesetzlicher Fristen; ggf. Redaktion/Anonymisierung.

Physische Sicherheit

Physische Sicherheit der Rechenzentren durch Supabase/AWS (EU-Region Frankfurt).
Lokale Verarbeitung beim Auftragnehmer (Geschäftssitz Deutschland): Zugangskontrolle zu Endgeräten, aktuelle Systemupdates, Verschlüsselung mobiler Geräte wo möglich.

Heim- und Telearbeit
Verarbeitung kann am Geschäftssitz/Heimarbeitsplatz des Auftragnehmers in Deutschland erfolgen.
Verpflichtung zur Vertraulichkeit, keine Weitergabe von Zugangsdaten, gesicherte Netzwerke, Bildschirmsperre.

Ereignisprotokollierung
Audit- und Protokolltabellen (u. a. dsgvo_audit_log, tenant_audit_logs, billing_audit_log, Löschlauf-Protokolle).
Protokollierung sicherheits- und datenschutzrelevanter Aktionen ohne unnötige PII in Logs.
Keine vollständigen personenbezogenen Daten in technischen Debug-Logs.

Unterstützungspflichten (Betroffenenrechte)
Self-Service im Nutzerkonto: Datenexport (JSON), Löschung, Verarbeitungseinschränkung (Art. 18).
Weisungen und Anfragen: datenschutz@scrt.de (Textform).
Weiterleitung direkter Anfragen betroffener Personen an den Auftraggeber.
Technische Unterstützung über Edge Functions und dokumentierte DSGVO-Prozesse.

Anlage 2 - Genehmigte Unterauftragsverhältnisse

Firma Unterauftragnehmer	Anschrift/Land	Leistung	Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland
Sliplane GmbH	Deutschland	Hosting der Web-App (React/Vite SPA, statische Assets)	Nicht erforderlich (Sitz und Datenhaltung in Deutschland)
Hetzner Online GmbH	Deutschland	Domain, DNS, Firmen-E-Mail (MX-Postfächer)	Nicht erforderlich (Sitz und Datenhaltung in Deutschland)
Supabase, Inc.	USA	Bereitstellung und Verwaltung der Datenbank, Authentifizierung, Edge Functions	EU-Infrastruktur (AWS Region Frankfurt, eu-central-1) / Angemessenheitsbeschluss (EU-US Data Privacy Framework)
Stripe Payments Europe Ltd.	Irland	Abwicklung von Kundenzahlungen und Verwaltung von Rechnungsdaten	Verarbeitung in der EU / Ergänzend Standardvertragsklauseln für US-Metadaten
Resend, Inc.	USA	Versand von transaktionalen E-Mails und Benachrichtigungen	Angemessenheitsbeschluss (EU-US Data Privacy Framework) bzw. Standardvertragsklauseln

Schlusserklärung zur Rechtsgültigkeit ohne Unterschrift

(1) Diese Vereinbarung zur Auftragsverarbeitung (AVV) stellt eine rechtsgültige Vereinbarung zwischen den Parteien dar. Sie wird als integraler Bestandteil der Allgemeinen Geschäftsbedingungen (AGB) von SCRT einbezogen.

(2) Der Vertragsschluss erfolgt digital und vollautomatisch: Durch das Setzen des entsprechenden Hakens und den erfolgreichen Abschluss des Registrierungsprozesses auf der Plattform scrt.de erklärt der Auftraggeber seine rechtsverbindliche Zustimmung zu dieser Vereinbarung.

(3) Ein beidseitiger Verzicht auf die Schriftform wird hiermit vereinbart. Diese Vereinbarung ist gemäß Art. 28 Abs. 9 DS-GVO in einem elektronischen Format (Textform) abgefasst und auch ohne handschriftliche Unterschriften vollumfänglich rechtswirksam.

Datum des Vertragsschlusses: *Es gilt der Zeitstempel der erfolgreichen Registrierung des Kundenkontos auf der Plattform.*