ESHO
IT BERATUNG & SOFTWAREENTWICKLUNG

ANLAGE ZUM RIFA ODER HOSTING HAUPTVERTRAG

Auftragsverarbeitung

Fassung für RIFA (SaaS) sowie Webspace, E-Mail und DNS · gilt für Verträge ab 17. Oktober 2026

Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO.

Anbieter: Stefan Drews / ESHO An der Küchenbreite 18, 06311 Helbra Stand: 18. Oktober 2026

Vertragsparteien

Verantwortlicher	Auftragsverarbeiter
[Firmenname] [vertreten durch] [Straße und Hausnummer] [PLZ und Ort] *– im Folgenden „Verantwortlicher“ –*	Stefan Drews handelnd unter ESHO An der Küchenbreite 18 06311 Helbra *– im Folgenden „ESHO“ –*

Diese Vereinbarung ist Anlage zum Vertrag über RIFA und/oder Webspace, E-Mail und DNS zwischen den Parteien („Hauptvertrag“) und gilt für alle Tätigkeiten, bei denen ESHO personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. „ESHO“ entspricht „eSho.de“ im Sinne der AGB.

§ 1 Gegenstand, Dauer und Rangfolge

(1) ESHO verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen nach Art. 28 DSGVO. Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1.

(2) Die Vereinbarung gilt für die Laufzeit des Hauptvertrags; ihre Pflichten bestehen bis zur vollständigen Rückgabe und Löschung der Daten fort. Für den Datenschutz geht sie dem Hauptvertrag vor.

(3) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung und die Wahrung der Betroffenenrechte verantwortlich.

§ 2 Weisungen

(1) ESHO verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, auch hinsichtlich Übermittlungen in Drittländer, und nicht zu eigenen Zwecken, es sei denn, ESHO ist

nach Unionsrecht oder dem Recht eines Mitgliedstaats dazu verpflichtet; in diesem Fall informiert ESHO den Verantwortlichen vorab, soweit dies rechtlich zulässig ist. Die Standardweisungen ergeben sich aus dem Hauptvertrag und Anlage 1.

(2) Weisungen erfolgen in Textform. Hält ESHO eine Weisung für datenschutzwidrig, informiert ESHO den Verantwortlichen unverzüglich und darf die Ausführung bis zur Klärung aussetzen.

(3) Weisungsberechtigt beim Verantwortlichen: [vom Verantwortlichen auszufüllen: Name, Funktion, E-Mail]. Weisungsempfänger bei ESHO: Stefan Drews, datenschutz@esho.de.

§ 3 Vertraulichkeit

ESHO setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen; die Verpflichtung gilt über das Ende der Tätigkeit hinaus.

§ 4 Technische und organisatorische Maßnahmen

ESHO trifft die nach Art. 32 DSGVO erforderlichen Maßnahmen gemäß Anlage 2 und überprüft sie regelmäßig. ESHO darf sie durch gleichwertige oder bessere Maßnahmen ersetzen, sofern das Schutzniveau nicht unterschritten wird; wesentliche Änderungen werden dokumentiert.

§ 5 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt die allgemeine Genehmigung, weitere Auftragsverarbeiter hinzuzuziehen. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anlage 3 genehmigt.

(2) ESHO informiert den Verantwortlichen mindestens 14 Kalendertage vor jeder beabsichtigten Hinzuziehung oder Ersetzung in Textform. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen; findet sich keine zumutbare Lösung, kann jede Partei den betroffenen Leistungsteil mit einer Frist von einem Monat kündigen.

(3) ESHO verpflichtet jeden Unterauftragsverarbeiter vertraglich auf die Datenschutzpflichten dieser Vereinbarung und bleibt nach Art. 28 Abs. 4 DSGVO für dessen Pflichterfüllung verantwortlich.

§ 6 Unterstützung des Verantwortlichen

(1) ESHO unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen (Art. 12 bis 23 DSGVO) und leitet an ESHO gerichtete Anfragen unverzüglich weiter.

(2) ESHO unterstützt den Verantwortlichen unter Berücksichtigung der verfügbaren Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO.

(3) Für Unterstützungsleistungen, die über die gesetzlich geschuldete Mitwirkung hinausgehen und nicht durch eine Pflichtverletzung von ESHO veranlasst sind, kann ESHO nach vorheriger Information eine angemessene Vergütung nach Aufwand verlangen.

§ 7 Verletzungen des Schutzes personenbezogener Daten

(1) ESHO meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens 48 Stunden nach Kenntniserlangung, an die nach § 2 Abs. 3 benannte Stelle. Die Meldung enthält die verfügbaren Angaben nach Art. 33 Abs. 3 DSGVO und wird ohne unangemessene Verzögerung ergänzt.

(2) ESHO ergreift unverzüglich Maßnahmen zur Eindämmung und Schadensminderung. Meldungen an die Aufsichtsbehörde und Benachrichtigungen betroffener Personen obliegen dem Verantwortlichen.

§ 8 Nachweise und Kontrollen

(1) ESHO stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung von Art. 28 DSGVO zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten, zur Vertraulichkeit verpflichteten Prüfer.

(2) Vorrangig werden Unterlagen und Fernprüfungen genutzt. Vor-Ort-Kontrollen werden mindestens 14 Kalendertage vorher angekündigt und finden ohne besonderen Anlass höchstens einmal im Kalenderjahr statt; Daten anderer Kunden und der Betrieb sind zu schützen. Für zusätzlichen Aufwand, der nicht durch eine Pflichtverletzung von ESHO veranlasst ist, kann ESHO eine angemessene Vergütung verlangen.

§ 9 Rückgabe und Löschung

(1) Nach Ende der Leistungen gibt ESHO nach Wahl des Verantwortlichen die Daten zurück oder löscht sie einschließlich Kopien, soweit keine gesetzliche Speicherpflicht besteht. Ohne abweichende Weisung steht der Export 30 Kalendertage zum Download in RIFA bereit (§ 11 AGB); danach werden die Daten gelöscht.

(2) Sicherungskopien werden in der regulären Rotation gelöscht, spätestens nach zwölf Monaten; zeitlich begrenzte Objektsperren können die physische Löschung verzögern, die Daten bleiben bis dahin gesperrt und geschützt. Daten im Belegarchiv werden nur aufbewahrt, soweit dies gesetzlich erforderlich oder vereinbart ist. Für Webspace, E-Mail und DNS gilt Abs. 1 entsprechend.

(3) ESHO bestätigt die Löschung auf Anfrage in Textform. Löschnachweise ohne Inhaltsdaten verarbeitet ESHO als eigener Verantwortlicher bis zum Ablauf der regelmäßigen Verjährungsfrist.

§ 10 Haftung

Gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Verhältnis der Parteien gelten die Haftungsregelungen der AGB von eSho.de (§ 9), soweit zwingendes Datenschutzrecht nicht entgegensteht.

§ 11 Schlussbestimmungen

(1) Diese Vereinbarung wird wirksam, wenn der Verantwortliche ihr vor Beginn der Verarbeitung schriftlich oder in einem elektronischen Format zugestimmt hat, insbesondere durch protokollierte Bestätigung im Bestell- oder Freischaltprozess (Art. 28 Abs. 9 DSGVO). Änderungen bedürfen derselben Form.

(2) Es gilt deutsches Recht. Die Anlagen 1 bis 3 sind Bestandteil dieser Vereinbarung.

Anlage 1: Beschreibung der Verarbeitung

MERKMAL	BESCHREIBUNG
Gegenstand	RIFA: Bereitstellung und Betrieb der ERP-Cloud-Lösung mit den gebuchten Modulen einschließlich Archiv, Anhängen, Export, Administration und Datensicherung. Hosting: Betrieb von Webspace, E-Mail-Postfächern und, soweit beauftragt, DNS einschließlich Datensicherung, Wartung und Störungsbeseitigung.
Dauer	Laufzeit des Hauptvertrags einschließlich Abrufphase, gegebenenfalls vereinbarter Archivhaltung und der Löschfristen nach § 9.
Art der Verarbeitung	Speichern, Strukturieren, Übermitteln, Abrufen, Sichern, Wiederherstellen und Löschen sowie technische Protokollierung. Inhalte werden nur eingesehen, soweit dies für Administration, Fehler- und Sicherheitsbearbeitung oder auf Weisung erforderlich ist.
Zweck	Durchführung der vom Verantwortlichen veranlassten ERP-Prozesse beziehungsweise Bereitstellung der Hosting-, E-Mail- und DNS-Dienste einschließlich Betrieb, Sicherung, Rückgabe und Löschung (zugleich Standardweisungen).
Arten personenbezogener Daten	RIFA: Stamm- und Kontaktdaten von Kunden, Lieferanten, Beschäftigten und Benutzern; Auftrags-, Rechnungs-, Zahlungs-, Bank-, Buchungs-, Service- und Vertragsdaten; bei gebuchtem Personalmodul Lohn- und Zeitdaten; Beleg-, Anhang-, Archiv- und Protokolldaten. Hosting: Bestands-, Kontakt- und Zugangsdaten; E-Mail-Inhalte und -Metadaten; Webspace-Inhalte; Verbindungs- und Protokolldaten (insbesondere IP-Adressen); DNS- und Domaindaten.
Besondere Datenkategorien	Nur soweit der Verantwortliche sie zulässigerweise verarbeitet, insbesondere beim Personalmodul (z. B. Kirchensteuermerkmal, Arbeitsunfähigkeitszeiten); vor Freischaltung prüfen die Parteien die Angemessenheit der Maßnahmen nach Anlage 2.
Kategorien betroffener Personen	Kunden, Interessenten, Lieferanten, Geschäftspartner und deren Ansprechpartner; Beschäftigte, Bewerber und Benutzer des Verantwortlichen; Kommunikationspartner; Besucher der Webseiten des Verantwortlichen; sonstige in Belegen und Dateien erfasste Personen.

Primäre Verarbeitungsorte	RIFA: Contabo GmbH, Rechenzentren in Deutschland und Frankreich; Dateiablage bei der IONOS Cloud GmbH in Berlin; Belegarchiv in Objektspeichern der IONOS Cloud GmbH in Berlin und Frankfurt am Main; Datensicherungen in Frankfurt am Main. Webspace und E-Mail: Contabo GmbH, Frankreich. DNS: Schlund Technologies GmbH. Fernwartung über AnyDesk: grundsätzlich EU/EWR, siehe Anlage 3.
Domainregistrierung	Registrare, Registries und Vergabestellen handeln, soweit sie Zwecke und Mittel selbst bestimmen, als eigene Verantwortliche und sind nicht Gegenstand dieser Vereinbarung. Drittlandübermittlungen erfolgen nur nach Art. 44 ff. DSGVO.

Anlage 2: Technische und organisatorische Maßnahmen

Stand bei Vertragsschluss. Physische Maßnahmen der Rechenzentren erbringen die Unterauftragsverarbeiter nach Anlage 3.

- Zutritt: Rechenzentren der Unterauftragsverarbeiter mit auf autorisiertes Personal beschränktem Zutritt.
- Zugang: personalisierte Administratorkonten, Mehr-Faktor-Authentifizierung für alle administrativen Zugänge, SSH mit Schlüsselpaaren. RIFA: Zwei-Faktor-Authentifizierung für Konten mit administrativen oder zahlungsrelevanten Rechten standardmäßig verpflichtend (auf Wunsch des Verantwortlichen für seinen Mandanten abschaltbar), für alle weiteren Benutzer aktivierbar; Sperre nach fünf Fehlversuchen für 15 Minuten; Abmeldung nach 60 Minuten Inaktivität; maximale Sitzungsdauer 12 Stunden.
- Zugriff und Trennung: rollenbasierte Berechtigungen nach dem Erforderlichkeitsprinzip, regelmäßige Überprüfung; Mandantentrennung durch eine eigene Datenbank je Mandant; Protokollierung administrativer Zugriffe und Änderungen.
- Weitergabe: Transportverschlüsselung (HTTPS/TLS, IMAPS, SMTPS, SFTP); Sicherungskopien vor dem Upload clientseitig mit AES-256 verschlüsselt; E-Mail-Versand aus RIFA über den SMTP-Server des Kunden; Fernwartung nur nach Freigabe je Sitzung, vom Kunden jederzeit beendbar.
- Datensicherung: RIFA: Datenbank und Dateien einmal täglich, zusätzlich fortlaufende Archivierung der Datenbank-Transaktionsprotokolle; Sicherungen werden verschlüsselt und getrennt vom Produktivsystem in Frankfurt am Main gespeichert; Löschung in Rotation, spätestens nach zwölf Monaten. Das Belegarchiv wird in Objektspeichern der IONOS Cloud GmbH in Berlin und Frankfurt am Main abgelegt, für die eine Objektsperre aktiviert ist. Zeitlich begrenzte Objektsperren können die physische Löschung verzögern. Webspace und E-Mail: Webspace- und E-Mail-Daten werden regelmäßig verschlüsselt gesichert; Einzelheiten zu Häufigkeit und Aufbewahrungsdauer teilt der Auftragsverarbeiter dem Verantwortlichen auf Anfrage mit.
- Wiederherstellung: dokumentiertes Verfahren mit regelmäßigen Tests; bereits umgesetzte Löschungen werden nach einer Wiederherstellung erneut angewendet.
- Betriebssicherheit: Firewall, Spam- und Malwarefilter, zeitnahe Sicherheitsupdates, Monitoring. Ticket-, E-Mail- und Push-Systeme von ESHO auf eigenen Servern in Deutschland beziehungsweise der EU.
- Organisation: Verfahren zur Erkennung, Bewertung und Meldung von Sicherheitsvorfällen; regelmäßige Überprüfung der Maßnahmen und Berechtigungen; AVV mit allen

Unterauftragsverarbeitern; dokumentiertes Lösch- und Rückgabeverfahren einschließlich physischer Bereinigung der Sicherungen.

Anlage 3: Genehmigte Unterauftragsverarbeiter

UNTERNEHMEN / ANSCHRIFT	LEISTUNG UND ROLLE	VERARBEITUNGSORT / HINWEIS
Contabo GmbH Welfenstraße 22 81541 München Deutschland	Server für RIFA (Anwendung und Datenbank) sowie für Webspace und E-Mail; die Rechenzentren in Deutschland und Frankreich betreibt die Contabo GmbH selbst.	Deutschland und Frankreich (EU)
Schlund Technologies GmbH Johanna-Dachs-Str. 55 93055 Regensburg Deutschland	DNS-/Nameserverleistungen, soweit personenbezogene Daten im Auftrag verarbeitet werden.	Deutschland / EU-EWR
IONOS Cloud GmbH Elgendorfer Straße 57 56410 Montabaur Deutschland	Objektspeicher für Dateiablage (Berlin), Belegarchiv (Berlin und Frankfurt am Main) und Datensicherungen (Frankfurt am Main). AVV abgeschlossen.	Deutschland
AnyDesk Software GmbH Türlenstraße 2 70191 Stuttgart Deutschland	Fernwartung; Auftragsverarbeitungsvertrag abgeschlossen (AnyDesk-AVV, Stand 10. Oktober 2025, Bestandteil der AnyDesk-Lizenzbedingungen)	Grundsätzlich EU/EWR (AnyDesk-AVV Ziff. 2.9); etwaige Drittübermittlungen nur unter den Voraussetzungen der Art. 44 ff. DSGVO, insbesondere auf Grundlage von Standardvertragsklauseln. Aktuelle Unterauftragsverarbeiter: https://trust.anydesk.com/subprocessors

Weitere Unterauftragsverarbeiter setzt ESHO derzeit nicht ein; Änderungen erfolgen nach § 5. Aktiviert der Verantwortliche in RIFA Anbindungen an Dienste Dritter, wird der jeweilige Anbieter aufgrund eines eigenen Vertrags mit dem Verantwortlichen tätig und ist kein Unterauftragsverarbeiter von ESHO.