Vereinbarung zur Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO

Präambel
Die S&F Software GmbH, nachfolgend „S&F Software“, „Auftragsverarbeiter“ oder „-nehmer“ genannt, stellt Software bereit, die zur Verwaltung und Bearbeitung personenbezogener Daten genutzt wird. Komvor verarbeitet personenbezogene Daten insbesondere dann, wenn die Cloud-Version ihrer Software eingesetzt wird. Ferner kann es bei Fernwartungen, Fehleranalysen oder Datenübernahmen erforderlich sein, dass personenbezogene Daten eingesehen werden. Für diese Fälle wird die folgende Vereinbarung getroffen.

1. Verantwortlicher (Auftraggeber)

Der Kunde gilt als Verantwortlicher und Auftraggeber im Sinne dieser Vereinbarung.

2. Auftragsverarbeiter (Auftragnehmer)

S&F Software GmbH, Reimersstraße 41b, 26789 Leer

3. Gegenstand und Dauer der Vereinbarung

Gegenstand

- Hosting der Daten (bei Nutzung der Cloud-Version)
- Fernwartung
- Fehleranalysen
- Datenübernahmen (nur bei Beauftragung des Auftraggebers)

Die Verarbeitung personenbezogener Daten erfolgt auf Grundlage dieser Vereinbarung und wird ausschließlich in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) durchgeführt. Eine Verlagerung in ein Drittland ist nur mit vorheriger Zustimmung des Verantwortlichen und unter Einhaltung der Vorgaben der Art. 44 ff. DS-GVO zulässig.

Dauer

Diese Vereinbarung wird auf unbestimmte Zeit, entsprechend der Dauer des Hauptvertrages, geschlossen. Der Verantwortliche kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, oder der Auftragsverarbeiter Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

4. Zweck und Art der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Zweck der Verarbeitung

Komvor bietet innovative Softwarelösungen für Aufgaben rund um die Entsorgung an.
Die modular aufgebaute Software ermöglicht eine flexible Anpassung an die spezifischen Anforderungen, daher können die in der Praxis genutzten Zwecke der Verarbeitung je nach Einsatzgebiet kundenspezifisch abweichen.

Der Auftraggeber empfiehlt die Software zu den Zwecken einzusetzen, die in „Anlage 1 – Arten, Kategorien und Zweck der verarbeiteten Daten“ im Absatz „Zweck der zu verarbeitenden Daten“ aufgelistet sind.

Art der Verarbeitung

Um den effektiven Einsatz und größtmöglichen Nutzen der Software sicherzustellen, bietet der Auftragnehmer von einer gründlichen Vorbereitung, der Anpassung des Programmes bis hin zur Schulung der Anwender eine breite Palette von Dienstleitungen an. Dazu gehört auch die Wartung der Software.
Bei diesen Aktivitäten kann es unausweichlich sein, dass auch personenbezogene Daten des Auftraggebers, seiner Kunden und Mitarbeiter für den Auftragnehmer sichtbar werden. Arten der personenbezogenen Daten
Die Arten der personenbezogenen Daten sind in „Anlage 1 – Arten, Kategorien und Zweck der verarbeiteten Daten“ dem Absatz „Arten der personenbezogenen Daten“ zu entnehmen. Kategorien betroffener Personen
Der Kreis von Personen, die von der Datenverarbeitung betroffen sind, ist aus der Anlage „Anlage 1 – Arten, Kategorien und Zweck der verarbeiteten Daten“ dem Absatz „Kategorien betroffener Personen“ zu entnehmen.

5. Rechte und Pflichten des Verantwortlichen

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Verantwortliche verantwortlich. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Verantwortlichen gerichtet sind, unverzüglich an diesen weiterzuleiten.
Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Verantwortlichem und Auftragsverarbeiter abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
Der Verantwortliche erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
Der Verantwortliche ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

6. Rechte und Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).
Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Verantwortlichen nicht erstellt.
Der Auftragsverarbeiter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Verantwortlichen verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
Die Datenträger (falls vorhanden), die vom Verantwortlichen stammen bzw. für den Verantwortlichen genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.
Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine vom Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Verantwortlichen nach Überprüfung bestätigt oder geändert wird.
Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Verantwortliche dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragsverarbeiters dem nicht entgegenstehen. Unabhängig davon hat der Auftragsverarbeiter personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Weisung des Verantwortlichen ein berechtigter Anspruch des Betroffenen aus Art. 16, 17 und 18 DS-GVO zugrunde liegt.
Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Verantwortlichen erteilen.
Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche - grundsätzlich nach Terminvereinbarung und angemessener Aufwandsentschädigung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Verantwortlichen beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).
Der Verantwortliche kann die Einhaltung eines genehmigten Zertifizierungsverfahrens gem. Art. 42 DS-GVO durch den Auftragsverarbeiter als Faktor heranziehen, um die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen zu beurteilen.
Der Auftragsverarbeiter sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.
Der Auftragsverarbeiter bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind.
Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Verantwortlichen die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der Auftragsverarbeiter

überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb. Kontaktinformationen zu dem bestellten Datenschutzbeauftragten befinden sich auf der Homepage des Auftragsverarbeiters.

7. Unterauftragsverhältnisse

Subunternehmer werden nur nach vorheriger Genehmigung des Verantwortlichen eingesetzt. Aktuell beauftragter Subunternehmer (nur im Falle der Nutzung der Cloudlösung):
1&1 IONOS Cloud GmbH, Greifswalder Str. 207, 10405 Berlin (Cloud-Lösung)

8. Technische und organisatorische Maßnahmen

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Niveau der Sicherheit der Verarbeitung gewährleistet. Dazu werden einerseits mindestens die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Verfügbarkeit und Integrität der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird (Art. 28 Abs. 3 lit. c).
Die Formulierung in Art. 32 Abs. 1 DS-GVO „diese Maßnahmen schließen unter anderem Folgendes ein“ verdeutlicht andererseits, dass die dort vorgenommene Aufzählung nicht abschließend ist. Für die Auftragsverarbeitung sind auch technische und organisatorische Maßnahmen umzusetzen, die in Kapitel III der DS-GVO genannten Rechte der betroffenen Personen wahren (Art. 28 Abs. 3 lit. e).

Beispiele für typische, bewährte technische und organisatorische Maßnahmen in den einzelnen Bereichen können den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO“ (Abschnitte 6.7 bis 6.9) entnommen werden. Die Auflistung dort ist nicht vollständig oder abschließend. In Abhängigkeit von den konkreten Verarbeitungstätigkeiten können weitere oder andere Maßnahmen geeignet und angemessen sein.

Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen.

Die Datensicherheitsmaßnahmen beim Auftragsverarbeiter können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Sicherheitsstandards nicht unterschreiten.
Wesentliche Änderungen sind vom Auftragsverarbeiter mit dem Verantwortlichen in dokumentierter Form (schriftlich, elektronisch) abzustimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

Die technischen und Organisatorischen Maßnahmen des Auftragnehmers werden in der Anlage „Technische und organisatorische Maßnahmen“ im einzelnen aufgelistet.

9. Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Für die Rückgabe kann von dem Auftragsverarbeiter eine angemessene Aufwandsentschädigung verlangt werden. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben hierbei grundsätzlich unberührt.

Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Zum Schutz anderer Kunden kann die Einsichtsname durch den Auftraggeber nach Bedarf eingeschränkt werden. Eine Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

10. Haftung

Es gelten die Haftungsregelungen nach Art. 82 DS-GVO.

11. Weisungsberechtigte des Verantwortlichen, Weisungsempfänger des Auftragsverarbeiters Weisungsberechtigte Personen oder Gruppen des Verantwortlichen:

Die Weisungsberechtigten Personen oder Gruppen des Verantwortlichen werden von dem Verantwortlichen umgehend nach Akzeptieren dieses Vertrages durch einen Geschäftsführer oder einer vergleichbaren Position beim Verantwortlichen mitgeteilt. Solange diese Mitteilung nicht erfolgt ist, sieht der Auftragnehmer die Geschäftsführer oder vergleichbare Positionen beim Auftraggeber als weisungsberechtigt an.

Weisungsempfänger beim Auftragsverarbeiter:
Der Abteilungsleiter Customer Support, oder nach Absprache definierte Personen oder Personenkreise.

Für Weisungen zu nutzende Kommunikationskanäle:
Serviceportal unter https://service.synqony.com, Telefon, E-Mail

12. Sonstiges

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein, bleibt die Gültigkeit der übrigen Regelungen unberührt.

Dokumentenversion: 18.12.2024

Anlagen:
Arten, Kategorien und Zwecke der Datenverarbeitung
Technische und organisatorische Maßnahmen

Anlage 1 – Arten, Kategorien und Zweck der verarbeiteten Daten

Hinweis: Die Arten, Kategorien und Zwecke der Verarbeitung stehen immer in Abhängigkeit der Module und individuellen Anpassungen, die der Auftragnehmer tatsächlich nutzt.

Arten der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Daten von Einwohner, Mitarbeitern, Auftragnehmer, Lieferanten, Kunden, Subunternehmen, Speditionen des Auftraggebers
- Adressdaten
- Telefonnummern
- E-Mailadressen
- Umsatzdaten
- Kontodaten, Zahlungsdaten, Bankdaten
- Geburtsdaten
- Amtliche Identifizierungsnummern
- Steuernummern

Kategorien betroffener Personen

Kreis der von der Datenverarbeitung betroffenen Personen:

- Einwohner
- Mitarbeiter
- Auftragnehmer
- Lieferanten
- Kunden
- Subunternehmen
- Speditionen

Zweck der zu verarbeitenden Daten

Folgende Verarbeitungszwecke sind regelmäßig Gegenstand der Verarbeitung:
Hinweis: Die Zwecke der Verarbeitung stehen immer in Abhängigkeit der Module, individuellen Anpassung und Workflows, die der Auftragnehmer tatsächlich nutzt.

- Support des Auftraggebers und seiner Mitarbeiter
- Schulung des Auftraggebers und seiner Mitarbeiter
- Datenbankreparatur
- Datenübernahme
- Problemanalyse

Anlage 2 – Technische und organisatorische Maßnahmen

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, sichergestellt durch:

- Alarmanlage
- Videoüberwachung der Zufahrt
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe an Empfänger dokumentiert, mehrere Schließkreise)
- Personenkontrolle beim Empfang und ständige Aufsicht der Besucher während des Aufenthalts
- Protokollierung der Besucher (Zeitraum des Aufenthalts)
- Sorgfältige Auswahl von Reinigungspersonal
- Tragepflicht von Berechtigungsausweisen (Besucher)

Zugangskontrolle

Keine **unbefugte** Systembenutzung, sichergestellt durch:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Sichere Kennwortrichtlinie
- Regelmäßiger Kennwortwechsel
- Authentifikation mit Benutzername & Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Reinigungspersonal
- Tragepflicht von Berechtigungsausweisen (Besucher)
- Verschlüsselung von mobilen Datenträgern
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall bei allen Arbeitsplätzen

Zugriffskontrolle

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

- Nutzung eines Berechtigungskonzepts
- Verwaltung der Rechte durch die Systemadministratoren auf Weisung der Geschäftsführung
- Anzahl der Benutzer mit Administratorberechtigungen auf das notwendigste reduziert
- Passwortrichtlinie inkl. Passwortlänge (mindestens acht Zeichen, alphanumerisch plus mindestens ein Sonderzeichen, alle sechs Monate, vorherige fünf Kennwörter können nicht verwendet werden), Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Bei Datenübernahmen keine inhaltliche Änderung der Daten (strukturelle Änderungen möglich)
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Einsatz von Aktenvernichtern
- Einsatz von Dienstleistern zur Aktenvernichtung mit Vernichtungsnachweis
- Verschlüsselung von Datenträgern

Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, sichergestellt durch:

- Getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Erstellung eines Berechtigungskonzepts
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

Weitergabekontrolle

Gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports, oder ihre Speicherung auf Datenträgern nicht unbefugt gelesen, geändert und kopiert oder entfernt werden können durch:

- Verschlüsselte Datenübertragen SFTP und FTPS mit Protokollierung
- Verschlüsselte Datenträger werden ausschließlich angenommen
- Dokumentation von
- Empfängern der Daten
- Zeitspannen der tatsächlichen Speicherung
- Spanne der geplanten Überlassung
- Übertragungsmedium
- Dokumentation des Löschvorgangs
- Automatisierte Warnung bei fehlerhafter Dokumentation
- Zusätzliche manuelle Kontrolle der Dokumentation
- Fernwartungen
- Verschlüsselte Fernwartungs-Verbindung
- Durch Fernwartungs-Software generierte sichere Kennwörter
- Protokollierung aller Fernwartungsverbindungen (Benutzer, Zeitraum, Zweck, Verbindungsziel)

Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Vararbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können durch:

- Übertragung an Drittländer findet nicht statt
- Führung eines Verfahrensverzeichnisses
- Dokumentation der eingesetzten IT-Systeme und Systemkonfiguration
- Mitarbeiter sind über Datensicherheit und –schutz geschult
- Mitarbeiter sind per schriftlicher Erklärung dem Datenschutz verpflichtet
- Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen
- Ein Datensicherheitskonzept/Informationssicherheitsmanagement ist vorhanden
- Eine Datenschutzrichtlinie ist vorhanden