Vereinbarung zur Auftragsdatenverarbeitung gemäß Artikel 28 DSGVO

https://dsgvo-gesetz.de/art-28-dsgvo/

VERS Versicherungsberater-Gesellschaft mbH
GGF: Hans-Hermann Lüschen
Versnavi Software
Alexanderstr. 226
26127 Oldenburg

- nachstehend VERS GmbH genannt

1. Gegenstand / Leistungsumfang

Der Kunde wünscht die Lizenzverwaltung der Versnavi Software der VERS GmbH. Zu deren Umsetzung, insbesondere der Vertragsverwaltung, soll die VERS GmbH alle in Betracht kommenden Daten des Kunden verarbeiten, erhalten, verwenden, speichern, übermitteln und weitergeben dürfen.

Support

Bei Supportanfragen an die VERS GmbH aufgrund einer Frage zu einem konkreten Vorgang (z.B. Störungen bei der Schnittstellennutzung) werden ggf. personenbezogene Daten verarbeitet.

2. Dauer

Diese Vereinbarung zur Auftragsdatenverarbeitung gilt seit dem 16.05.2018 und kann von beiden Parteien mit einer Frist von 3 Monaten gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt. Alle anderen ggf. bestehenden Vereinbarungen werden hierdurch ersetzt.

3. Kategorien betroffener Personen

- Interessenten / Testkunden
- Kunden / Mitarbeiter der Kunden
- Kontoinhaber
- weitere Geschäftspartner

4. Art der Daten

- Kundendaten (Name, Vorname, Geburtsdatum, Geschlecht, Anschrift)
- Kommunikationsdaten
- Zahlungsdaten
- Benutzerkennungen, Lizenzdaten
- Internetnutzungs- und Kommunikationsdaten
- Pflichtauskunftsangaben von Dritten (z.B. Bonität)

5. Zweck der Verarbeitung

- E-Mail Kommunikation
- Support
- Erstellung von Statistiken
- Webauftritt / Betrieb einer Internetseite
- Verarbeiten und Speichern von Dokumenten (z.B. Rechnungen)

6. Örtlichkeit

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in Deutschland statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers.

7. Auskunft, Berichtigung, Einschränkung und Löschung von Daten

Die VERS GmbH darf Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Kunden oder einer betroffenen Person berichtigen, löschen oder deren Verarbeitung einschränken. Soweit vom Leistungsumfang umfasst, ist Löschkonzept, Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft unmittelbar durch die VERS GmbH sicher zu stellen.

8. Qualitätssicherung und sonstige Pflichten der VERS GmbH

Die VERS GmbH hat zusätzlich zur Einhaltung der Regelungen dieses Auftrages gesetzlichen Pflichten gemäß Art. 28-33 DSGVO zu wahren. Insofern gewährleistet sie insbesondere die Einhaltung folgender Vorgaben:
a) Die VERS GmbH setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf Vertraulichkeit verpflichtet und zuvor mit allen für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.
b) Die VERS GmbH gewährleistet die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artikel 28 Abs. 3.
c) Der Kunde und die VERS GmbH arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
d) Die VERS GmbH informiert den Kunden unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.
e) Die VERS GmbH unterstützt den Kunden nach besten Kräften, wenn dieser Kontrollen, Haftungsansprüchen oder einem anderen Anspruch im Zusammenhang mit dieser Vereinbarung ausgesetzt ist.
Der Kunde ist zur Übernahme der daraus entstehenden Mehrkosten verpflichtet.
f) Die VERS GmbH kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen.
g) Sollten Daten bei der VERS GmbH durch Pfändung, Beschlagnahme, Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat die VERS GmbH den Kunden unverzüglich zu informieren.
Die VERS GmbH ist außerdem verpflichtet alle Verantwortlichen darüber zu informieren, dass Eigentum und Hoheit an den Daten ausschließlich beim Kunden als Verantwortlichen im Sinne der DSGVO liegen.

9. Pflichten des Kunden

Der Kunde ist Verantwortlicher im Sinne der DSGVO und insoweit zur Umsetzung der gesetzlichen Vorschriften verpflichtet:
a) Der Kunde ist alleine für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Der Kunde trägt Sorge, dass die gesetzlich notwendigen Voraussetzungen geschaffen werden, damit die VERS GmbH die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.
b) Der Kunde ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen der VERS GmbH vertraulich zu behandeln.

10. Mitarbeiter

Der Kunde erklärt seine Einwilligung, dass alle Mitarbeiter der VERS GmbH seine personenbezogenen und betrieblichen Daten, speichern, einsehen und für die Beratung gegenüber dem Kunden und der VERS GmbH verwenden dürfen. Zu den Mitarbeitern der VERS GmbH zählen alle Arbeitnehmer und sonstige Erfüllungsgehilfen, die mit der VERS GmbH eine vertragliche Regelung unterhalten und die Bestimmungen des Bundesdatenschutzgesetzes beachten. Der Kunde ist damit einverstanden, dass seine personenbezogenen und betrieblichen Daten an diese und künftige Mitarbeiter der VERS GmbH zum Zwecke der Lizenzbetreuung weitergegeben werden und ihre Mitarbeiter berechtigt sind, die Kundendaten/ Firmendaten im Rahmen des Vertragszweckes einzusehen und verarbeiten und verwenden zu dürfen.

11. Rechtsnachfolger

Der Kunde willigt ein, dass die von der o.g. Firma aufgrund der vorliegenden Datenschutzerklärung erhobenen, verarbeiteten und gespeicherten Informationen und Daten an einen etwaigen Rechtsnachfolger der o.g. Firma weitergegeben werden, damit auch dieser seine vertraglichen und gesetzlichen Verpflichtungen Als Rechtsnachfolger der o.g. Firma erfüllen kann.

Die zur Bewertung der o.g. Firma erforderlichen Kundendaten können auch an einen potenziellen Erwerber der o.g. Firma weitergeleitet werden. Besondere personenbezogene Daten, insbesondere Bankdaten zählen nicht zu den erforderlichen Kundendaten. Diese dürfen daher nicht an einen potenziellen Erwerber übermittelt werden. Eine Überlassung dieser Daten erfolgt erst nach der tatsächlichen Veräußerung oder Rechtsnachfolge.

12. Unterauftragsverhältnisse

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 z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Dokumenten und Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.
Die VERS GmbH ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Kunden auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
a) Die VERS GmbH darf Unterauftragnehmer (weitere Auftragsverarbeiter) beauftragen.
Der Kunde stimmt der Beauftragung von Unterauftragnehmern zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zwischen der VERS GmbH und dem Unterauftragnehmer.
b) Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.
c) Eine Liste der Unterauftragnehmer mit der Verarbeitung von personenbezogenen Daten und deren Umfang wird auf Wunsch zur Verfügung gestellt.

13. Kontrollrechte des Kunden

Die VERS GmbH gestattet dem Auftraggeber oder einem Bevollmächtigten, sich nach Anmeldung zu Prüfzwecken in den Betriebsräumen zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufes von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze zu überzeugen.
Der Kunde hat die VERS GmbH unverzüglich zu informieren, wenn er z.B. bei der Prüfung von Ergebnissen Fehler oder Unregelmäßigkeiten feststellt. Für die Ermöglichung von Kontrollen durch den Kunden kann die VERS GmbH einen Vergütungsanspruch geltend machen.

14. Mitteilung bei Verstößen

Die VERS GmbH unterstützt den Kunden bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Hierzu gehören u.a.:
a) Sicherstellung eines angemessenen Schutzniveaus, das Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigt und eine Feststellung von relevanten Verletzungsereignissen ermöglicht.
b) Die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Kunden zu melden.
c) Den Kunden im Rahmen seiner Informationspflicht gegenüber Betroffenen zu unterstützen.
d) Den Kunden für dessen Folgeabschätzung zu unterstützen.
e) Die Unterstützung des Kunden im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

15. Weisungsbefugnis des Kunden

Mündliche Weisungen bestätigt der Kunde unverzüglich, mindestens in Textform.
Die VERS GmbH hat den Kunden unverzüglich zu informieren, wenn er der Meinung ist, dass eine Weisung gegen geltendes Recht verstößt. Die VERS GmbH ist zur Aussetzung der Weisung berechtigt, bis sie geändert oder bestätigt wird.

16. Löschung und Rückgabe von personenbezogenen Daten

Kopien oder Duplikate der Daten werden ohne Wissen des Kunden nicht erstellt. Ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung notwendig sind sowie Daten,
die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
Nach Beendigung der Auftragsdatenverarbeitung hat die VERS GmbH sämtliche in seinem Besitz befindliche Unterlagen, Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände datenschutzgerecht zu vernichten,
soweit dem keine gesetzlichen Pflichten entgegenstehen. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

17. Schlussbestimmungen / salvatorische Klausel

a) Die VERS GmbH ist verpflichtet, auch über das Ende des Vertragsverhältnisses hinaus, Stillschweigen über alle in diesem
Zusammenhang mit dem Auftrag bekannt gewordenen Daten zu wahren.
b) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen
oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen
Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.
c) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten,
die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.
d) Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen
und im Falle des Bedachtwerdens vereinbart worden wären.
e) Existieren mehrere wirksame und durchführbare Bestimmungen, so muss die Bestimmung gewählt werden,
welche den Schutz der personenbezogenen Daten im Sinne dieses Vertrages am besten gewährleistet.

18. Rechtswahl, Gerichtsstand

Für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag gilt das deutsche Recht. Gerichtsstand ist der Sitz der VERS GmbH.

Technische und organisatorische Maßnahmen (TOM)

VERS GmbH, Versnavi / VersnaviAGRAR Software, Alexanderstr. 226, 26127 Oldenburg

Maßnahmen zur Vertraulichkeit

Alle Daten werden von der Hetzner Online GmbH nach ISO 27001 in Deutschland verarbeitet.

Beschreibung der Zutrittskontrolle:

Bewegungsmelder
Einsatz einer Schließanlage
Videoüberwachung der Zugänge

Beschreibung der Zugangskontrolle:

Authentifikation mit Benutzer + Passwort + Keyfile
Einsatz von Firewalls zum Schutz des Netzwerkes
Sorgfältige Auswahl von Reinigungspersonal und Sicherheitspersonal
Benutzerberechtigungen verwalten (z.B. bei Eintritt, Änderung, Austritt)

Beschreibung der Zugriffskontrolle:

Erstellen und Einsatz eines Berechtigungskonzepts
Sichere Löschung von Datenträgern vor deren Wiederverwendung

Beschreibung der Weitergabekontrolle:

Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet
Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen

Beschreibung des Trennungsgebots:

Logische Mandantentrennung (softwareseitig)
Trennung von Produktiv- und Testsystem
Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

Beschreibung der Pseudonymisierung:

Trennung von Kontaktdaten und anderen Daten
Trennung von Kundenstammdaten und Auftragsdaten
Weitere Pseudonymisierung findet nicht statt

Beschreibung der Verschlüsselung:

Verschlüsselte Datenübertragung (VPN, verschlüsselte Internetverbindungen mittels SSL/SFTP)

Maßnahmen zur Integrität

Beschreibung der Eingabekontrolle:

Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
Protokollierung der Eingabe, Änderung und Löschung von Daten
Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.

Maßnahmen zur Verfügbarkeit und Belastbarkeit

Beschreibung der Verfügbarkeitskontrolle:

Einsatz von Antivirensoftware
Aufbewahrung von Datensicherung
Erstellen eines Backup- & Recoverykonzepts
Feuer- und Rauchmeldeanlagen
Erstellung und Anwendung von IT-Notfallplänen
Redundante Datenhaltung (RAID System, zusätzlich Backup an einen anderen Ort und nochmaliges Backup auf einen verschlüsselten Server im Rechenzentrum)
Schutzsteckdosenleisten in Serverräumen
Unterbrechungsfreie Stromversorgung (USV)

Beschreibung der raschen Wiederherstellbarkeit:
Regelmäßige und dokumentierte Datenwiederherstellungen
IT-Notfallpläne und Wiederanlaufpläne

Weitere Maßnahmen zum Datenschutz

Beschreibung der Auftragskontrolle:
Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO
Verpflichtung auf die Vertraulichkeit gem. Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO

Technische und organisatorische Maßnahmen (TOM)

1.Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)
Es findet eine Zutrittskontrolle (kein unbefugter Zutritt zu Datenverarbeitungsanlagen) statt. Dies umfasst die folgenden Maßnahmen:
- Schlüssel / Schlüsselvergabe
- Gebäudesicherung (Zäune, Pforten)

Es findet eine Zugangskontrolle (keine unbefugte Systembenutzung) statt. Dies umfasst die folgenden Maßnahmen:
- Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Automatische Sperrung (z.B. Pausenschaltung)
- Einrichtung eines Benutzerstammsatzes pro User
- Verschlüsselung von Datenträgern und Datensätzen

Es findet eine Trennungskontrolle / Verwendungszweckkontrolle (getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden) statt. Dies umfasst die folgenden Maßnahmen:
- "Interne Mandantenfähigkeit" ist hergestellt
- Kontrolle der Zweckbindung
- Separierung von Datenbanken

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)
Es findet eine Weitergabekontrolle (kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport) statt. Dies umfasst die folgenden Maßnahmen:
- Verschlüsselung / Tunnelverbindung
- Prüfung der Rechtmäßigkeit der Weitergabe von Daten

Es findet eine Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind) statt. Dies umfasst die folgenden Maßnahmen:
- Dokumentenmanagement, Dokumentenlenkung

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)
Es findet eine Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust) statt. Dies umfasst die folgenden Maßnahmen:
- Backup-Strategie (online, z.B. Cloud)
- Virenschutz / Firewall

Es ist eine rasche Wiederherstellbarkeit gegeben. Dies wird durch folgenden Maßnahmen gewährleistet:
- Testen der Wiederherstellungssysteme

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sind im Einsatz.
Dies wird durch folgende Maßnahmen unterstützt:
- Auftragskontrolle für Auftagsdatenverarbeiter (ADV)
- Nachkontrollen

Es liegen folgende Anweisungen, Regeln oder Analysen schriftlich vor:
- Interne Verhaltensregeln