
Auftrag gemäß § 11 BDSG

Vereinbarung

zwischen der

- nachstehend Auftraggeber genannt -

und

der

voba solutions GmbH, Frankfurter Strasse 1, 64720 Michelstadt

- nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

- Supportleistungen, sofern vom Auftraggeber nicht selbst durchführbar
- Präsentationen
- Installation und Administration von vertraglich vereinbarten Anwendungen
- Überprüfung von System-Einstellungen und -parametern
- Zugriff auf Operativsystem zur Analyse evtl. vorhandener Abweichungen
- Austausch von Informationen (z.B. über Log-Dateien)

Die Dauer des Auftrags (Laufzeit) entspricht der Laufzeit des Vertrages zur Nutzung der jeweiligen Anwendung.

2. Konkretisierung des Auftragsinhalts

Der Auftragnehmer übernimmt den Support für vertraglich vereinbarte Anwendungen; aus diesem Grund kann es notwendig sein, mittels Fernwartung Zugriff auf die DV-Systeme des Auftraggebers zu nehmen. System- und Softwareparameter, sowie Datenversorgungen werden überprüft und ggf. angepasst. Ein Informationsaustausch in Form von z.B. Log-Dateien kann stattfinden.

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.

Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien:

- Personenstammdaten
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten

Kreis der Betroffenen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst die Kunden des Auftraggebers.

3. Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat technische und organisatorische Maßnahmen zum Datenschutz (gemäß Anlage zu § 9 BDSG) ergriffen, über die sich der Auftraggeber in Kenntnis setzen kann. Der Auftragnehmer sichert zu, dass diese Maßnahmen insgesamt mindestens ausreichend sind, um die vom Auftraggeber überlassenen Daten gegen Gefährdungen abzusichern. Soweit erforderlich können Ergänzungen der Sicherheitsmaßnahmen zwischen Auftraggeber und Auftragnehmer vereinbart werden. Der Auftragnehmer hat auf Anforderung die Angaben nach §4g Abs. 2 Satz 1 BDSG (Verfahrensverzeichnis) dem Auftraggeber zur Verfügung zu stellen.

4. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren.

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach §11 Abs. 4 BDSG folgende Pflichten:

- Ein Datenschutzbeauftragter ist schriftlich bestellt.
- Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, sind zur Wahrung des Datengeheimnisses entsprechend §5 BDSG verpflichtet.
- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und Anlage.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach §38 BDSG. Dies gilt auch, soweit eine zuständige Behörde nach §§43, 44 BDSG beim Auftragnehmer ermittelt.

6. Unterauftragsverhältnisse

Unterauftragnehmer werden zur Durchführung der beauftragten Tätigkeiten nicht eingesetzt. Ansonsten ist eine Einschaltung von Unterauftragnehmern nur mit schriftlicher Zustimmung des Auftraggebers gestattet.

7. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht sich über die Einhaltung der Datensicherheitsmaßnahmen und die Durchführung des Auftrags auch in den Räumen des Auftragnehmers in Kenntnis zu setzen und Auskünfte vom Auftragnehmer zu erhalten. Kontrollen sind rechtzeitig anzumelden.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind. Der Auftragnehmer hat bei Sicherheitsvorfällen im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach §42a BDSG treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

9. Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. §11 Abs. 3 Satz 1 BDSG).

10. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte 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.

Auftraggeber

voba solutions GmbH

Ort, Datum	Ort, Datum
Unterschrift	Unterschrift

Anlage 1 zur Datenschutzvereinbarung nach §11

Allgemeine technische und organisatorische Maßnahmen nach §9 BDSG und Anlage

In Verbindung mit Nr. 3 der Rahmenvereinbarung Datenschutz verpflichten sich die Vertragspartner in ihrem jeweiligen Verfügungsbereich und bezogen auf den Vertragsgegenstand, die technischen und organisatorischen Maßnahmen gemäß §9 BDSG und Anlage zu §9 BDSG im erforderlichen sowie angemessenen Umfang und nach dem allgemein anerkannten Stand der Technik umzusetzen.

Die von der voba solutions GmbH definierten und umgesetzten Maßnahmen sind im wesentlichen wie folgt:

1. Zutrittskontrolle

Der unbefugte Zutritt zu Gebäuden, Räumen und Einrichtungen, in denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ist zu verhindern.

Den gesicherten Zutritt zu den Betriebsräumen der voba solutions GmbH, sowie die Legitimation der Berechtigten gewährleistet die voba solutions GmbH durch

- persönliche Überwachung
- Der Eingangsbereich am Standort Michelstadt ist verschlossen
- Sicherheitsschlösser

2. Zugangskontrolle

Das Eindringen Unbefugter in Systeme und Anwendungen, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden, ist zu verhindern.

Um Zugang zu den technischen Systemen und Anwendungen der voba solutions GmbH zu erhalten, muss ein Kennwort geschützter Benutzerstammsatz, das persönliche Benutzerkonto, technisch eingerichtet werden. Mit diesem authentifiziert sich der Nutzer gegenüber dem System oder der Anwendung. Das Benutzerkonto muss zunächst beantragt und vom jeweiligen Vorgesetzten genehmigt werden. Die Ausgestaltung, die Nutzung und den persönlichen Umgang mit dem Kennwort hat die voba solutions GmbH in einer Passwortrichtlinie organisatorisch geregelt, deren Einhaltung technisch unterstützt wird.

3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen und mit DV-Anwendungen, die zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten dienen, sind zu verhindern.

Zugriffsberechtigungen werden in der voba solutions GmbH nach den Prinzipien „need-to-know“ und „need-to-do“ erteilt. Daher liegen den Zugriffsberechtigungen bedarfsorientierte Berechtigungskonzepte, Benutzerprofile und Funktionsrollen zugrunde. Eine Zugriffsberechtigung wird auf Basis des Rollenkonzepts beantragt und vom Vorgesetzten genehmigt. In den Genehmigungsprozess sind weitere Kontrollinstanzen integriert. Zur technischen Zugriffssicherung verwendet die voba solutions GmbH anerkannte Sicherheitssysteme. Zugriffe werden technisch überwacht. Die Ausführung administrativer Zugriffe wird protokolliert und kontrolliert. Auf die Anwendung bezogene Zugriffe werden mit den Mitteln und Möglichkeiten der Anwendung protokolliert und überwacht.

4. Weitergabekontrolle

Aspekte im Zusammenhang mit der Weitergabe personenbezogener Daten innerhalb und außerhalb der DV-Systeme und DV-Anwendungen sind zu regeln.

Firewallsysteme und ständig aktualisierte Virensoftware sichern neben einer Secure Socket Layer (SSL) Verschlüsselung und dem Einsatz von VPN Technologie die Kommunikation im Internet. Ansonsten werden möglichst sogenannte „geschlossene“ Datennetze verwendet.

5. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverarbeitung sind zu gewährleisten.

Die zur Zweckerfüllung eingesetzten Mitarbeiter sind ausschließlich in der voba solutions GmbH tätig. Alle Mitarbeiter der voba solutions GmbH wurden in ihren Arbeitsverträgen zur Einhaltung des Bundesdatenschutzgesetzes verpflichtet.

Die beauftragte Verarbeitung bzw. Abwicklung über die voba solutions GmbH sieht grundsätzlich keine Eingabe oder Veränderung von Daten im Operativsystem über die Mitarbeiter der voba solutions GmbH vor. Eine Eingabe oder Änderung kann nur mit Zustimmung und unter Beobachtung eines Mitarbeiters des Auftraggebers durchgeführt werden.

Entsprechende Vorgehensweisen werden über Aufzeichnungen und Protokolle dokumentiert und werden durch die voba solutions GmbH archiviert.

6. Auftragskontrolle

Es ist eine auftrags- und weisungsgemäße Auftragsdatenverarbeitung zu gewährleisten.

Die voba solutions GmbH bearbeitet die ihr überlassenen Daten nur aufgrund und anhand von vertraglich vereinbarten Weisungen des Auftraggebers. Kompetenzen und Kontrollmaßnahmen werden in Abstimmung mit dem Auftraggeber definiert und technisch oder organisatorisch in die Betriebsabläufe eingebunden.

7. Verfügbarkeitskontrolle

Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Die Systeme sind gegen Angriffe von außen geschützt. Eine Vorhaltung von personenbezogenen Daten findet in der voba solutions GmbH nur in Ausnahmefällen und nur temporär statt. Eine redundante Datenvorhaltung ist nicht notwendig, da Originaldaten beim Auftraggeber vorhanden sind.

8. Zwecktrennungsgebot

Daten verschiedener Auftraggeber sind zumindest sachlogisch getrennt zu verarbeiten. Systeme und Anwendungen sind speziell auf eine zweckgebundene und mandantengetrennte Verarbeitung ausgerichtet. Test- und Produktionssysteme sind getrennt.