VERTRAG ÜBER AUFTRAGSVERARBEITUNG IM SINNE VON ART. 28 ABS. 3 DSGVO

ZWISCHEN

- im Folgenden: Auftraggeber -

UND

AccountOne GmbH
Schiffbrücke 66
24939 Flensburg

- im Folgenden: Auftragnehmer -

1. Allgemeine Bestimmungen und Vertragsgegenstand

1. 1. Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragnehmer (Art. 28 DSGVO). Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist der Auftraggeber. Die Auftragsdetails entnehmen Sie der **Anlage 1**.

1. 2. Die Verarbeitung der vertragsgegenständlichen personenbezogenen Daten außerhalb der Europäischen Union ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

2. Vertragslaufzeit und Kündigung

2. 1. Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

4. Weisungen des Auftraggebers

3. 1. Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragnehmer zu. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragnehmer substantiiert anzweifelt, ist der Auftragnehmer berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert. Besteht die Möglichkeit, dass der Auftragnehmer durch das Befolgen der Weisung einem Haftungsrisiko ausgesetzt wird, kann die Durchführung der Weisung bis zur Klärung der Haftung im Innenverhältnis ausgesetzt werden.

3. 2. Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z. B. per E-Mail) zu erteilen. Mündliche Weisung sind in begründeten Einzelfällen zulässig und werden vom Auftraggeber unverzüglich schriftlich oder in einem elektronischen Format bestätigt. In der Bestätigung ist ausdrücklich zu begründen, warum keine schriftliche Weisung erfolgen konnte. Der Auftragnehmer hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3. 3. Der Auftraggeber benennt auf Verlangen des Auftragnehmers eine oder mehrere weisungsberechtigte Personen. Personelle Änderungen sind dem Auftragnehmer unverzüglich mitzuteilen.

Kontrollbefugnisse des Auftraggebers

4. 1. Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren. Der Auftraggeber hat dafür

zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragnehmers nicht mehr als erforderlich beeinträchtigen.

4. 2. Die Ergebnisse der Kontrollen und Weisungen sind vom Auftraggeber in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragnehmers

5. 1. Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragnehmer erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z. B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragnehmer dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5. 2. Der Auftragnehmer hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

6. Technische und organisatorische Maßnahmen

6. 1. Der Auftragnehmer hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 2 dieses Vertrags dokumentiert. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben von Art. 32 DSGVO ausgewählt. Der Auftragnehmer wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen.

7. Unterstützungspflichten des Auftragnehmers

7. 1. Der Auftragnehmer wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO, unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Der Auftragnehmer wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflichten bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der Informationen, die dem Auftragnehmer zur Verfügung stehen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

8. 1. Der Auftragnehmer ist zum Einsatz von Unterauftragsverarbeitern (Subunternehmern) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden Subunternehmerverhältnisse des Auftragnehmers sind diesem Vertrag abschließend in Anlage 3 beigefügt. Für die in Anlage 3 aufgezählten Subunternehmer gilt die Zustimmung mit Abschluss dieses Vertrags als erteilt.

8. 2. Beabsichtigt der Auftragnehmer den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber rechtzeitig - spätestens jedoch zwei Wochen - vor deren Einsatz in schriftlicher oder elektronischer Form anzeigen. Der Auftraggeber hat nach dieser Mitteilung zwei Wochen Zeit, der Hinzuziehung des / der Subunternehmer zu widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Hinzuziehung des / der Subunternehmer(s) als genehmigt. Im Falle eines Widerspruchs dürfen die betroffenen Subunternehmer nicht eingesetzt werden. Widersprüche sind nur zulässig, wenn der Auftraggeber begründete Anhaltspunkte dafür hat, dass durch den Einsatz des Unterauftragnehmers die Datensicherheit oder der Datenschutz eingeschränkt würde, die Einhaltung gesetzlicher oder vertraglicher Bestimmungen gefährdet wäre und / oder sonstige berechtigte Interessen des Auftraggebers entgegenstehen; die entsprechenden Verdachtsmomente sind dem Widerspruch beizufügen.

8. 3. Subunternehmer werden vom Auftragnehmer unter Beachtung der gesetzlichen und vertraglichen

Vorgaben ausgewählt. Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Nebenleistungen, welche der Auftragnehmer zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse im Sinne des Art. 28 DSGVO dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit und / oder Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragnehmer wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards (insbesondere durch entsprechende Vertraulichkeitsvereinbarungen) sicherstellen.

8. 4. Sämtliche Verträge zwischen dem Auftragnehmer und dem Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen.

8. 5. Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten des Auftragnehmers

9. 1. Verstöße gegen diesen Vertrag, gegen Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragnehmer selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

9. 2. Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragnehmer um Auskunft, Berichtigung, Einschränkung der Verarbeitung oder Löschung, wird der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragnehmer dem Ersuchen des Betroffenen ohne Weisung / Zustimmung des Auftraggebers nachkommen.

9. 3. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragnehmer den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch welche die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

10. 1. Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine rechtliche oder vertragliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z. B. gesetzliche Aufbewahrungsfristen).

11. Datengeheimnis und Vertraulichkeit

11. 1. Der Auftragnehmer ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln. Der Auftragnehmer verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragnehmer aufnehmen.

12. Schlussbestimmungen

12. 1. Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

12. 2. Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

12. 3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

12. 4. Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

12. 5. Sind die Vertragsparteien Kaufleute, juristische Personen des öffentlichen Rechts oder öffentlichrechtliches Sondervermögen, ist der Sitz des Auftragnehmers Gerichtsstand für alle Streitigkeiten aus diesem Vertrag, sofern insoweit hierfür ein ausschließlicher Gerichtsstand nicht begründet wird.

Auftragnehmer Auftraggeber

Gordian-Philipp Brockstedt

28.11.2022, AccountOne GmbH
Datum, Unterschrift

Datum, Unterschrift

Anlage 1 – Auftragsdetails

1. Der vorliegende Vertrag umfasst (ggf. im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:

Den Abruf von Bestelldaten aus verschiedenen Verkaufskanälen des Auftraggebers, sowie die Annahme von Dateien die ebensolche Verkaufsdaten enthalten. Darüber hinaus die umsatzsteuerliche Würdigung und Bewertung jedes einzelnen Umsatzes und die Umformatierung in kompatible Datensätze für die Buchhaltung. Sofern beauftragt, werden aus den empfangenen Daten Rechnungen erstellt und den betroffenen Endkunden des Auftraggebers per Emails zugesendet.

2. Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

2. 1. Anschrift

2. 2. Demographische Daten

2. 3. E-Mail-Adresse

2. 4. Kontaktdaten (Telefon, E-Mail)

2. 5. Kundendaten

2. 6. Namen

2. 7. Rechnungsdaten

2. 8. Standort

2. **9.** Zahlungseingänge und Zahlungsausgänge

3. **Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:**

1. Kunden des Auftraggebers

Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Der Auftragnehmer setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

Folgende Maßnahmen werden gewährleistet:

1. Datenschutz-Management (organisatorisch)

1. 1. Datenschutzbeauftragter - externer Datenschutzbeauftragter Name /Prive

2. Datenschutz-Management (technisch)

2. 1. Dokumentiertes Sicherheitskonzept - Anderweitiges dokumentiertes Sicherheitskonzept

2. 2. Datenschutz-Management-Tools - Software-Lösungen für Datenschutz , Management im Einsatz

3. Incident-Response-Management (technisch)

3. 1. Spamfilter - Einsatz von Spamfilter und regelmäßige Aktualisierung

3. 2. Virenscanner - Einsatz von Virenscanner und regelmäßige Aktualisierung

4. Transport- und Weitergabekontrolle (technisch)

4. 1. Email-Verschlüsselung - Nutzung von Verschlüsselungstechnologie für Emailverkehr

4. 2. Protokollierung der Zugriffe und Abrufe - Protokollierung der Zugriffe und Abrufe

4. 3. Webseitenverschlüsselung - Nutzung von Verschlüsselungstechnologie für die Website

4. 4. Verschlüsselte Verbindungen - Bereitstellung über verschlüsselte Verbindungen wie sftp, https

5. Trennungskontrolle (organisatorisch)

5. 1. Zweckattribute - Datensätze sind mit Zweckattributen versehen

6. Trennungskontrolle (technisch)

6. 1. Berechtigungskonzept - Steuerung über Berechtigungskonzept

6. 2. Gesonderte Aufbewahrung - Physische und elektronisch Daten aus dieser Verarbeitungstätigkeit werden von anderen Datensätzen getrennt aufbewahrt

7. Verfügbarkeitskontrolle (organisatorisch)

7. 1. Backupkonzept - Backup & Recovery-Konzept (ausformuliert)

7. 2. Backupprotokollierung - Kontrolle des Sicherungsvorgangs

7. 3. Dezentrale Aufbewahrung - Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums

8. Verfügbarkeitskontrolle (technisch)

8. 1. Festplattenspiegelung - RAID System / Festplattenspiegelung

8. 2. Videoüberwachung Serverraum - Videoüberwachung im Serverraum

8. 3. Zutrittsmeldeanlage im Serverraum - Alarmmeldung bei unberechtigtem Zutritt zu Serverraum

9. Zugangskontrolle (organisatorisch)

9. 1. Passwort-Richtlinien - regelmäßige Änderung, Mindestlänge, Komplexität etc.

Telefonate - Telefonate werden grundsätzlich hinter verschlossener Tür geführt

9. 2.

9. 3. Verschlossene Postfächer - Verschlossene Postfächer

9. 4. Videokonferenzen - Videokonferenzen werden grundsätzlich hinter verschlossener Tür mit Sichtschutz geführt

10. Zugangskontrolle (technisch)

10. 1. Anti-Viren-Software Clients - Anti-Viren-Software Clients

10. 2. Anti-Viren-Software Server - Anti-Viren-Software Server

10. 3. Benutzerprofil Login - Login mit Benutzername + Passwort

10. 4. Datenträgerverschlüsselung - Verschlüsselung von Datenträgern in Laptops / Notebooks

10. 5. Mobile Device Management - Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)

10. 6. Firewall - Einsatz einer Firewall

10. 7. Passwortschutz - Zugang ist mittels eines Passworts geschützt

10. 8. Smartphone Verschlüsselung - Smartphone Verschlüsselung

11. Zugriffskontrolle/Pseudonymisierung (organisatorisch)

11. 1. Autorisierter Zugriff - Zugriff nur für dafür autorisiertes Personal

12. Zutrittskontrolle (organisatorisch)

12. 1. Besucherbegleitung - Besucher in Begleitung durch Mitarbeiter

12. 2. Schlüsselregelung - Schlüsselregelung (Schlüsselausgabe etc.)

13. Zutrittskontrolle (technisch)

13. 1. Mechanisches Schließsystem - Manuelles Schließsystem

13. 2. Sicherheitsschlösser - Verwendung von Sicherheitsschlössern in Türen

Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

(Keine Subunternehmer vorhanden)