VERTRAG ÜBER AUFTRAGSVERARBEITUNG

IM SINNE VON ART. 28 ABS. 3 DSGVO

ZWISCHEN

dem Unternehmen/
Gewerbetreibenden der das
Social Selling Cockpit nutzt

- im Folgenden: Auftraggeber -

UND

iDot digital UG (haftungsbeschränkt)
Adalbertsteinweg 276
52066 Aachen

- 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. Die Laufzeit des vorliegenden Vertrags richtet sich nach der Laufzeit des Hauptvertrags. Findet nach Beendigung des Hauptvertrags weiterhin eine Auftragsverarbeitung statt, gilt dieser Vertrag für die betreffenden Verarbeitungsvorgänge fort. Eine ordentliche, vom Hauptvertrag unabhängige Kündigung des vorliegenden Vertrags ist unzulässig. Das Recht zur außerordentlichen fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3. 1. Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten, insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit. 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.

4. 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.

Anlage 1 – Auftragsdetails

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

Der Auftrag umfasst die Services, die funktionalität des Produkts Social Selling Cockpits und allen damit verbundenen Funktionen und Datenverarbeitungen, die der Auftragnehmer (und von uns entwickelte Software) durchführt. Dazu zählen die Verarbeitung folgender Daten:
- Einsehbare Daten der vernetzten Kontakte (in LinkedIn)
- Chats (in LinkedIn)
- Notizen zu Kontakten
- Vom Nutzer zugewiesene Kategorien und Tags
- Interaktionen mit den Beiträgen des Nutzers (in LinkedIn)

Neben der Speicherung der Daten verarbeitet das Social Selling Cockpit diese Daten auch, um den Nutzer bei Vertriebstätigkeiten zu unterstützen.

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

2. 1. E-Mail-Adresse (Direkterhebung: öffentliches Profil auf Linkedin)

2. 2. Namen (Direkterhebung: öffentliches Profil auf Linkedin)

2. 3. Kundendaten (Direkterhebung: öffentliches Profil auf Linkedin)

2. 4. Kontaktdaten (Telefon, E-Mail) (Direkterhebung: öffentliches Profil auf Linkedin)

2. 5. Kommunikationsinhalte (ggf. Gesprächsnotizen)

2. 6. Gesprächsnotizen

2. 7. Profilbilder (LinkedIn) (Direkterhebung: öffentliches Profil auf Linkedin)

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

3. 1. LinkedIn Nutzer (vernetzt mit dem Nutzer)

3. 2. LinkedIn Nutzer (potentielle Kunden)

Anlage 2: Technisch organisatorische Maßnahmen

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle:

- Kundendaten werden in Rechenzentren von Hetzner und AWS Frankfurt verarbeitet und gespeichert (Zertifiziert nach DIN ISO/IEC 27001)

Zugangskontrolle:

- Es existieren technische Policies zur Passwortkomplexität
- Bei iDot gilt das Prinzip der Minimalberechtigung. Jeder Benutzer erhält nur die Zugriffsrechte, die erforderlich sind, um seine vertraglichen Tätigkeiten durchzuführen. Benutzerkonten werden immer zunächst mit den wenigsten Zugriffsrechten ausgestattet. Für die Einräumung von Zugriffsrechten über die Minimalberechtigung hinaus, muss eine entsprechende Berechtigung vorliegen.
- Der Zugriff auf iDot Serversysteme erfolgt SSH-Verschlüsselt („Public key“) und nur innerhalb des Firmen-VPN, der den Zugriff auf Netzwerkgeräte und andere Cloud-Komponenten beschränkt
- Personenbezogene Daten werden nur in den entsprechenden Tools oder innerhalb des gesicherten VPN-Netzes gespeichert. Eine Speicherung der Daten auf anderen Geräten wird vermieden und erfolgt ausschließlich temporär.

Zugriffskontrolle:

- Zugriffsberechtigung auf iDot Produktivsysteme ist auf einen kleinen Kreis von Mitarbeitern beschränkt
- Mitarbeitergeräte (z.B. Laptops, Desktop-PCs, Smartphones) die Zugriff auf personenbezogene Daten haben und/oder diese Verarbeiten und/oder temporär Speichern nutzen folgende Einstellungen:
    - Festplattenverschlüsselung: Die Festplatte des Systems wird verschlüsselt.
    - Bildschirmsperre: Der Bildschirm wird nach 1 Minute nicht Benutzung gesperrt und muss per Passwort oder biometrisch entsperrt werden
    - Zugangsbegrenzung: Die Geräte werden ausschließlich mit Personen mit gleichen Zugangsberechtigungen geteilt.

Trennungskontrolle:

- Datensätze verschiedener Kunden werden in separaten Datenbanken gespeichert oder in einer einheitlichen Datenbank speziell markiert und durch serverseitige Mandantenfähigkeit getrennt

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle:

- Soweit Daten zu beauftragten Partnern übertragen werden, sind diese Datenübertragungskanäle immer verschlüsselt
- Wo dies technisch möglich ist, kommen VPN-Verbindungen zum Einsatz

- Für Kommunikation mit externen Nutzern bieten wir Ende-zu-Ende verschlüsselte E-Mails an
- Interne Kommunikation verläuft ausschließlich Ende-zu-Ende verschlüsselt
- E-Mails werden nur mit kryptographischer Signatur versendet

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle:

- Es werden regelmäßig automatische Sicherungskopien und Backups aller Kundendaten erstellt
- Es gibt ein dediziertes Konzept zur Rekonstruktion der Datenbestände und zudem eine regelmäßige Überprüfung, dass die Datensicherungen auch tatsächlich wieder eingespielt werden können (Datenintegrität der Backups)
- Backups und Sicherungskopien sind über mehrere redundante Serversysteme verteilt
- Produktivsysteme sind mehrfach redundant ausgelegt
- Zur Ausstattung der Rechenzentren von Hostserver, AWS Frankfurt und Azure Deutschland vgl. technisch organisatorische Maßnahmen bei Hostserver, AWS Frankfurt, Azure Deutschland in Anlage 3 zu diesem Vertrag

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- Mehrfachredundante Auslegung von Serversystemen und Datenbanken
- Backups werden regelmäßig auf Wiedereinspielbarkeit geprüft

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Wir haben einen Datenschutzbeauftragten bestellt, der die hier beschriebenen Maßnahmen kontrolliert und die Konformität mit anwendbaren Datenschutzgesätzen sicherstellt

Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

Name des Unternehmens	Anschrift (Hauptsitz)	Ort der Leistungs-erbringung	Leistungsbeschreibung
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen, Deutschland	EU/EWR	Hosting: Server & Cloud-Services
Amazon Web Services Inc (“AWS Frankfurt”)	410 Terry Avenue North, Seattle WA 98109, United States	EU/EWR	Hosting: Server & Cloud-Services, E-Mails
1blu AG	Riedemannweg 60 13627 Berlin, Deutschland	EU/EWR	Hosting: Server, MySQL, Webspace
PlanetScale Inc	535 Mission St. San Francisco, CA, 94015, United States	EU/EWR	Hosting von MySQL/Vitess-DB
InfluxData Inc	548 Market St, PMB 77953 San Francisco, California 94104, United States	EU/EWR	Datenbank für Statistik im SSC. (Alle Daten sind pseudonymisiert)
Upstash Inc	San Jose, CA	EU/EWR	Hosting von Redis (Alle Daten sind pseudonymisiert)