Vertrag zur Auftragsverarbeitung - gemäß Art. 28 DSGVO

Vereinbarung

zwischen dem

- Verantwortlichen - nachstehend Auftraggeber genannt -

……..

……..

……..

Vertreten durch: (Vor- und Nachname, Position)

……

und dem

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

iOSXpert Business auf Mac & iPhone GmbH
Brauereistrasse 2-20
56170 Bendorf

Vertreten durch den Geschäftsführer: Alf Ruppert

HRB 26409, Registergericht Koblenz
Ust.-ID: DE320428593
Webseite: www.iosxpert.biz
E-Mail: hallo@iosxpert.biz
Tel.: +49 (0) 2622 978 0000

1. Gegenstand und Dauer der Vereinbarung

1.1 Gegenstand des Auftrags

Der Gegenstand des Vertrags ergibt sich aus dem bestätigten Auftrag mit der Auftragsnummer …… des Auftraggeber an den Auftragnehmer.

1.2 Dauer des Auftrags

Die Dauer des Auftrags (Laufzeit) entspricht den Angaben des genannten Auftrags mit der Auftragsnummer ……

Der Auftraggeber kann den geschlossenen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers vertragswidrig verweigert.

1.3 Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung

Der Zweck des der Datenverarbeitung können sein:

Datenimport / Datenexport
Wartung und Support (Fernzugriff)
Datenmigration
Softwareentwicklungen
Datenanalyse / -bearbeitung
Hosting von Kundendatenbanken
Installation von Software / Update / Upgrade

Der spezifische Zweck des Auftrags ergibt sich aus dem zwischen Auftraggeber und Auftragnehmer geschlossenen Auftrag mit der Nummer …….

1.4 Art der Daten

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

Personenstammdaten
Kommunikationststammdaten
Kundenhistorie
Nutzerdaten
Inhaltsdaten
Planungs- und Steuerungsdaten

1.5 Kreis der Betroffenen

Der Kreis, der durch den Umgang mit Ihren personenbezogenen Daten im Rahmen dieses Auftrags, betroffenen Personen, kann u.a. aus den Nachfolgenden bestehen:

Kunden
Lieferanten
Subunternehmen
Angestellte
Ansprechpartner

2. Rechte und Pflichten des Auftraggebers

2.1 Für die Beurteilung der Zulässigkeit der Datenerhebung / -verarbeitung / -nutzung, sowie für die Wahrung der Rechte der Betroffenen, ist allein der Auftraggeber verantwortlich.

2.2 Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und entsprechend Nr. 1.3 dieses Vertrages schriftlich festzulegen.

2.3. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen. Die schriftliche Bestätigung der mündlichen Weisungen sollte von Auftraggeber und Auftragnehmer zusammen mit der Vereinbarung so aufbewahrt werden, dass alle maßgeblichen Regelungen jederzeit verfügbar sind.

Weisungsberechtigte Personen des Auftraggebers sind:

…….
(Name, Funktion, Telefonnummer)

Weisungsberechtigte Person(en) des Auftragnehmers sind:

…….
(Name, Funktion, Telefonnummer)

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen. Falls Weisungen die unter Nr. 1. 3 dieses Vertrages getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Festlegung erfolgt.

2.4 Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen (TOM's, Punkt 5, Anlage) zu überzeugen. Der Auftraggeber trägt die Verantwortung dafür, dass das Schutzniveau den zu verarbeitenden Daten angemessen ist.

2.5 Der Auftraggeber informiert den Auftragnehmer unverzüglich in Schriftform, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

2.6 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

3. Pflichten des Auftragnehmers

3.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er hat personenbezogene Daten zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder einer Weisung verlangt. Andernfalls werden die im Rahmen des Auftrags durch den Auftraggeber erhaltenen Daten, ausgenommen Import- und Export relevante Daten, bis auf Widerruf für künftige Hilfestellungen bei technischen Anfragen, seitens des Auftraggebers, gesichert. Daten, die der Auftragnehmer im Zuge eines Imports oder Exports erhalten hat, werden nach Abschluss des Auftrages nach 4 Wochen von diesem gelöscht.
Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

3.2 An der Erstellung der Verfahrensverzeichnisse hat der Auftragnehmer mitzuwirken. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.

3.3 Daten oder Datenträger, sowie sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

3.4 Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Hierzu liegt ein Berechtigungskonzept vor.

3.5 Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

3.6 Für die Sicherheit erhebliche Veränderungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

3.7 Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis zu wahren.

3.8 Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften des BDSG bekannt sind.

Der Auftragnehmer 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 sie auf das Datengeheimnis verpflichtet. Der Auftragnehmer überwacht die Einhaltung der hier angegebenen datenschutzrechtlichen Vorschriften.

3.9 Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Ausgenommen hiervon sind Subunternehmen, gemäß Punkt 4.

4. Subunternehmer

4.1 Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind folgende hier aufgeführte Unternehmer für Teilleistungen für den Auftragnehmer tätig und Verarbeiten und oder Nutzen in diesem Zusammenhang unmittelbar die Daten des Auftraggebers.

4.2 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus dieser Vereinbarung dem Subunternehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieser Vereinbarung. Eine etwaige Prüfung durch den Auftraggeber beim Subunternehmer erfolgt nur in Abstimmung mit dem Auftragnehmer.

4.3 Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post- und Versanddienstleistungen oder Wartung. Der Auftragnehmer wird mit diesem Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

Für diese Subunternehmer gilt die Einwilligung in das Tätigwerden als erteilt:

Name des Subunternehmens	Anschrift des Subunternehmens	Teilleistung
Marketcircle, INC.	30 Centurian Drive, Suite 201 Markham, Ontario L3R8B8 Kanada	CRM Provider
TeamViewer GmbH	Jahnstraße 30 73037 Göppingen Deutschland	Fernwartungsdienst
Skalio GmbH	Hongkongstraße 7 20457 Hamburg Deutschland	Datentransfer
HONDS IT GmbH	Von-Coels-Str. 390 52080 Aachen Deutschland	Hosting
ALL-INKL.COM	Hauptstrasse 68 02742 Friedersdorf Deutschland	E-Mail Provider
SparkPost, Inc.	301 Howard St. Suite 1330 San Francisco, CA 94105 USA	E-Mail Provider
Atlassian, Inc. (JIRA)	1098 Harrison St, San Francisco, CA 94103 USA	Webanwendung Fehlerbehebung Software
Zoom Video Communications, INC.	55 Almaden Boulevard, Suite 600 San Jose, CA 95113 USA	Tool Online-Videokonferenz (Kunden-Produktschulung, Kunden-Support)
LogMeIn Ireland Limited (GoToWebinar / GoToMeeting)	Bloodstone Building Block C 70 Sir John Rogerson's Quay Dublin Irland	Tool Online-Videokonferenz (Kunden-Produktschulung, Kunden-Support)
Dropbox International Unlimited Company	One Park Place, Floor 5 Upper Hatch Street, Dublin 2 Irland	Dokumentenspeicherung
Starface GmbH	Stephanienstr. 102 76133 Karlsruhe Deutschland	IP-Telefonanlagen
Slack Technologies, INC.	155 5th Street 6th Floor San Francisco, CA 94103 USA	Chat
SEVENIT GmbH	Hauptstraße 40 77652 Offenburg Deutschland	Faktura-Software
Simple Sign International AB	Mäster Samuelsgatan 36 111 57 Stockholm Schweden	E-Signaturen Service
Webinaris GmbH	Bussardstr. 5 82166 Gräfelfing Deutschland	Online-Webinare

Auftraggeber

……..

……..

……..

Vertreten durch: (Vor- und Nachname, Position)

……

…….. ……..
Ort, Datum Unterschrift

Auftragnehmer

iOSXpert Business auf Mac & iPhone GmbH
Brauereistrasse 2-20
56170 Bendorf

Vertreten durch den Geschäftsführer:

Alf Ruppert

…….. ……..
Ort, Datum Unterschrift

5 Technische und organisatorische Maßnahmen (TOM) nach Art. 32 DSGVO

5.1 Das als Anlage beigefügte Datensicherheitskonzept (mit den Festlegungen entsprechend der Anlage zu Art. 32 DSGVO) des Auftragnehmers wird als verbindlich festgelegt.

5.2 Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

5.3. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.

5.4 Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

5.5 Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Informationspflichten des Auftraggebers nach § 42 a BDSG. Der Auftragnehmer sichert zu, den Auftraggeber bei seinen Pflichten nach § 42 a BDSG zu unterstützen.

5.6. Datenschutz auf Mitarbeiterebene

- Interne Schulungen zum Thema Datenschutz
- Regelung betrieblicher E-Mail- / Internetnutzung
- Verpflichtung zur Vertraulichkeit / Verschwiegenheitserklärung

5.7 Archivierung, Löschung und Einschränkung

- Es liegt ein Archivierungskonzept mit festgelegten Zuständigkeiten vor
- Es liegt ein Löschkonzept mit festgelegten Zuständigkeiten vor
- Es liegt ein Berechtigungs- und Zugriffskonzept vor

5.8 Wahrung der Betroffenenrechte

- Es liegt ein Konzept vor, das die Wahrung der Rechte der Betroffenen (Auskunft, Korrektur, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet.

5.9 Notfallkonzept

- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten gewährleistet.

5.10 Zutrittskontrolle

- Sicherheitsschlösser
- kontrollierte Schlüsselvergabe / Schlüsselregelung
- Videoüberwachung der Zugänge
- Beaufsichtigung von Aushilfen / Praktikanten
- Besucherkontrolle, -begleitung und -abholung durch Mitarbeiter
- Regelung für Gäste besteht

5.11 Zugriffskontrolle

- Nutzung der aktuellen Softwareversionen
- Trennung von Berechtigungsbewilligung und -vergabe
- Berechtigungs- und Zugriffskonzept
- Automatische Bildschirmsperre nach festgelegtem Zeitraum
- Sichere Passwortvergabe und regelmäßige Änderung dieser
- Ausgeschiedene Mitarbeiter werden umgehend gesperrt

5.12 Weitergabekontrolle

- Verschlüsselte Verbindung bei Datenübertragung
- Dokumentation der Empfänger von Daten
- Zugriffskontrolle durch Berechtigungskonzept
- Verpflichtung aller Mitarbeiter des Auftragnehmers auf das Datengeheimnis

5.13 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Nachvollziehbarkeit von Eingabe und Löschung von Daten durch individuelle Benutzernamen

5.14 Verfügbarkeitskontrolle / Integrität

- ständig kontrolliertes Backup- und Recoverykonzept
- Feuerlöschgeräte im Serverraum
- Unterbrechungsfreie Stromversorgung
- Notfallkonzept
- Rauchmelder im Serverraum
- Software zur Überwachung der Serverleistung
- Software zur Überwachung der Integrität der Serverfestplatten

5.15 Gewährleistung des Zweckbindungs- / Trennungsgebotes

- Trennung von Produktiv- und Testsystemen
- Berechtigungs- und Zugriffskonzept
- Logische Mandantentrennung
- Festlegung von Datenbankrechten