Data Processing Agreement

in accordance with Article 28 of the General Data Protection Regulation (GDPR)

Between (Client)	And (Contractor)
	SuperOffice GmbH **Phoenixseestr. 17** **44263 Dortmund**
Place, date	
_____, _____	_____, _____
_____	_____
Signed by Client	Signed by Contractor

This document can also be signed electronically

This agreement consists of 3 Annexes:

1. Annex 1 - Data Processing Agreement (DPA)
2. Annex 2 - List of pre-approved sub-processors
3. Annex 3 - Technical and Organizational Measures (TOM)

Appendix 1 – Data Processing Agreement

Datenverarbeitungsvereinbarung

Zwischen SuperOffice AS als Auftragsverarbeiter (nachfolgend “Auftragnehmer”) und einem Kunden als der für die Verarbeitung Verantwortliche (nachfolgend “Auftraggeber”)

Diese Vereinbarung ist gültig ab dem 01.05.2023. Sie finden hier die vorherige Version.

Einen Vergleich der vorherigen und aktuellen Version sowie eine Übersicht über die Änderungen, finden Sie hier.

1. Zweck und Definitionen

Zweck dieses Datenverarbeitungsvertrages ist es, die Verarbeitung personenbezogener Daten durch den Auftraggeber im Rahmen der Bereitstellung des SuperOffice CRM Online Service ("der Service"), der im SuperOffice CRM Online Abonnementrahmenvertrag (SuperOffice CRM Online Master Subscription Agreement, "MSA") näher beschrieben wird.

Diese Datenverarbeitungsvereinbarung regelt die Rechte und Pflichten des Auftragnehmers, um sicherzustellen, dass die Verarbeitung personenbezogener Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen erfolgt.

Die Verarbeitung personenbezogener Daten (wie unten definiert) unterliegt den Anforderungen und Verpflichtungen des geltenden Rechts. Wenn der Auftraggeber eine im Europäischen Wirtschaftsraum (EWR) ansässige juristische Person ist, wird das Deutsche Datenschutzgesetz und die aktuelle EU-Verordnung 2016/679 vom 27. April 2016 ("DS-GVO") gelten. Die Parteien kommen überein, diese Datenverarbeitungsvereinbarung in dem Maße zu ergänzen, wie es aufgrund der DS-GVO und der überarbeiteten Verordnung über elektronische Kommunikation ("ePrivacy") gemäß ihrer Deutsche Umsetzung erforderlich ist.

"Personenbezogene Daten" sind alle Informationen über eine identifizierte oder identifizierbare natürliche Person im Sinne des geltenden Rechts und der DS-GVO.

"Verarbeitung" personenbezogener Daten ist jede Nutzung und jeder Vorgang, die mit personenbezogenen Daten durchgeführt werden, unabhängig davon, ob diese automatisch erfasst, übertragen, gespeichert, geändert oder offengelegt werden, wie dies im anwendbaren Recht und der DS-GVO näher definiert ist.

"Drittländer" sind Länder außerhalb des EU/EWR-Raums, die nicht als Länder anerkannt sind, die einen angemessenen Schutz personenbezogener Daten bieten.

2. Verantwortlichkeit des Auftraggebers

Um auf den Dienst zugreifen zu können, muss der Auftraggeber dem Auftragnehmer bestimmte Daten zur Verfügung stellen, einschließlich des korrekten Namens, der Kontaktdaten und der E-Mail-Adresse der Benutzer. Darüber hinaus müssen die Benutzer des Dienstes dem Auftragnehmer erlauben, Informationen über die Benutzung des Dienstes durch die Verwendung von "Cookies" zu speichern und abzurufen, die notwendig sind, um die im Rahmen des Dienstes verwendeten An- und Abmeldeverfahren zu ermöglichen und sicherzustellen, dass Unbefugte keinen Zugang zu dem Dienst erhalten.

Der Auftraggeber erkennt an und akzeptiert, dass alle persönlichen Daten, die der Auftraggeber im Rahmen der Benutzung des Dienstes hochlädt, wie zum Beispiel hochgeladene persönliche Daten seiner eigenen Kunden, an einen Dritten (Unterauftragnehmer) mit Sitz im Europäischen Wirtschaftsraum (EWR) übermittelt werden können, der für das Hosting des Dienstes, einschließlich der Bereitstellung aller Hardware, Infrastruktur, Datenspeicherung und Kommunikationsleitungen sorgt. Die Pflichten des Dritten in Bezug auf personenbezogene Daten werden in einem separaten Datenverarbeitungsvertrag zwischen dem Auftragnehmer und dem Dritten im Rahmen dieses Datenverarbeitungsvertrages geregelt. Alle Daten des Dienstes werden auf Servern in Europa gespeichert.

Der Auftraggeber bestätigt, dass er:

- über eine ausreichende Rechtsgrundlage für die Verarbeitung personenbezogener Daten verfügt;
- das Recht hat, den Auftragnehmer mit der Verarbeitung der persönlichen Daten zu beauftragen;
- die Verantwortung für die Richtigkeit, die Integrität, den Inhalt, die Zuverlässigkeit und die Rechtmäßigkeit der persönlichen Daten hat;
- im Hinblick auf die Benachrichtigung und Genehmigung der zuständigen Behörden das geltende Recht einhält;
- die betroffene Person gemäß geltendem Recht informiert hat

Der Auftraggeber muss:

- auf Anfragen der Betroffenen antworten bezüglich der Verarbeitung personenbezogener Daten gemäß dieser Datenverarbeitungsvereinbarung;
- die Notwendigkeit spezifischer Maßnahmen gemäß diesem Datenverarbeitungsvertrag gemäß Art. 3.3.2 und Art. 3.3.4 beurteilen und diese Maßnahmen beim Auftragnehmer einfordern.

Der Auftraggeber trifft ausreichende technische und organisatorische Maßnahmen, um die Einhaltung der DS-GVO ab dem Zeitpunkt ihres Inkrafttretens in Norwegen sicherzustellen und nachzuweisen.

Der Auftraggeber ist verpflichtet, Verstöße gegen personenbezogene Daten den zuständigen Behörden und, falls erforderlich, den Betroffenen gemäß geltendem Recht unverzüglich mitzuteilen.

3. Verantwortlichkeit des Auftragnehmers

3.1 Compliance

Der Auftragnehmer hält sich an alle Bestimmungen zum Schutz personenbezogener Daten, die in diesem Vertrag über die Verarbeitung personenbezogener Daten und in den geltenden Datenschutzgesetzen mit Relevanz für die Verarbeitung personenbezogener Daten festgelegt sind. Der Auftragnehmer unterstützt den Auftraggeber dabei sicherzustellen und zu zu dokumentieren, dass der Auftraggeber seine Anforderungen gemäß den geltenden Datenschutzbestimmungen erfüllt.

Der Auftragnehmer hat die Weisungen und Abläufe des Auftraggebers in Bezug auf die Verarbeitung personenbezogener Daten einzuhalten.

3.2 Beschränkungen der Nutzung

Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Weisung des Auftraggebers. Der Auftragnehmer darf personenbezogene Daten nicht ohne vorherige schriftliche Zustimmung des Auftraggebers oder ohne schriftliche Weisungen des Auftraggebers verarbeiten, die über das hinausgehen, was zur Erfüllung seiner Verpflichtungen gegenüber dem Auftraggeber im Rahmen der Vereinbarung erforderlich ist.

3.3 Informationssicherheit

3.3.1 Pflicht zur Informationssicherung

Der Auftragnehmer gewährleistet durch geplante, systematische, organisatorische und technische Maßnahmen eine angemessene Informationssicherheit in Bezug auf Vertraulichkeit, Integrität und Zugänglichkeit im Zusammenhang mit der Verarbeitung personenbezogener Daten gemäß den Bestimmungen der geltenden Datenschutzgesetze.

Die Maßnahmen und die Dokumentation, die der internen Kontrolle des Auftragnehmers dienen, sind dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

3.3.2 Bewertung von Maßnahmen

Bei der Entscheidung, welche technischen und organisatorischen Maßnahmen durchgeführt werden sollen, berücksichtigt der Auftragnehmer in Absprache mit dem Auftraggeber:

- Den Stand der Technik
- Die Kosten der Implementierung
- Art und Umfang der Verarbeitung
- Kontext und Zweck der Verarbeitung,
- Die Schwere der Risiken, die die Verarbeitung personenbezogener Daten für die Rechte und Freiheiten der betroffenen Person mit sich bringt.

Der Auftragnehmer prüft in Absprache mit dem Auftraggeber:

- Die Implementierung der Pseudonymisierung und Verschlüsselung von personenbezogenen Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Verarbeitungssystemen und -diensten kontinuierlich zu gewährleisten;
- die Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Ereignisses rechtzeitig wiederherzustellen;
- ein Verfahren zur laufenden regelmäßigen Überprüfung, Kontrolle, Bewertung und Beurteilung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

3.3.3 Anfragen der Betroffenen

In Anbetracht der Art der Verarbeitung trifft der Auftragnehmer geeignete technische und organisatorische Maßnahmen, um den Auftraggeber bei seiner Pflicht zu unterstützen, auf Anfragen bezüglich der Ausübung der Rechte der betroffenen Personen zu reagieren.

3.3.4 Unterstützung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung des anwendbaren Rechts, einschließlich der Unterstützung des Auftraggebers bei:

- Der Durchführung der oben genannten technischen und organisatorischen Maßnahmen;

- der Einhaltung der Meldepflicht gegenüber Aufsichtsbehörden und Betroffenen im Falle eines Verstoßes gegen personenbezogene Daten;
- der Durchführung von Datenschutzfolgenabschätzungen;
- der Durchführung vorheriger Konsultationen mit den Aufsichtsbehörden, wenn eine Folgenabschätzung zum Schutz der Privatsphäre dies erforderlich macht;
- der Mitteilung an den Auftraggeber, wenn der Auftragnehmer der Meinung ist, dass eine Anweisung des Auftraggebers nicht den geltenden Datenschutzbestimmungen entspricht.

Die vorstehenden Unterstützungshandlungen durch den Auftragnehmer sind unter Berücksichtigung ihrer Notwendigkeit auszuführen. Dabei sind die Bedürfnisse des Auftraggebers, die Art der Verarbeitung und die dem Auftragnehmer zur Verfügung stehenden Informationen zu berücksichtigen.

3.3.5 Vergütung

Die Unterstützung durch den Auftragnehmer, wie sie in diesem Datenverarbeitungsvertrag festgelegt ist, sowie die Unterstützung in Bezug auf spezifische Abläufe und Weisungen des Auftraggebers werden vom Auftragnehmer gemäß den regulären Bedingungen und Preisen des Auftraggebers vergütet.

3.4 Meldung von Verletzungen des Schutzes personenbezogener Daten und sonstiger Abweichungen

Jegliche Nutzung der Informationssysteme und der persönlichen Daten, die nicht mit den festgelegten Abläufen und Weisungen des Auftraggebers oder den geltenden Datenschutzgesetzen übereinstimmen, sowie jegliche Sicherheitsverletzungen werden als Abweichung behandelt.

Der Auftragnehmer muss über Abläufe und systematische Verfahren zur Nachvollziehung von Abweichungen verfügen, die die Wiederherstellung des normalen Zustands, die Beseitigung der Ursache der Abweichung und die Verhinderung ihres Wiederauftretens umfassen.

Der Auftragnehmer wird den Auftraggeber unverzüglich über jeden Verstoß gegen diese Datenverarbeitungsvertrag oder über versehentlichen, unrechtmäßigen oder unbefugten Zugriff auf personenbezogene Daten, deren Verwendung oder Offenlegung oder darüber informieren, dass die personenbezogenen Daten möglicherweise gefährdet sind oder die Integrität der personenbezogenen Daten verletzt wurde. Der Auftraggeber stellt dem Auftragnehmer alle erforderlichen Informationen zur Verfügung, damit dieser die geltenden Datenschutzvorschriften einhalten und alle Anfragen der zuständigen Datenschutzbehörden beantworten kann. Es liegt in der Verantwortung des Auftraggebers, die zuständige Datenschutzbehörde über die Verletzung des Schutzes personenbezogener Daten und sonstiger Abweichungen in Übereinstimmung mit dem geltenden Recht zu informieren.

3.5 Vertraulichkeit

Der Auftragnehmer ist verpflichtet, alle persönlichen Daten und andere vertrauliche Informationen vertraulich zu behandeln. Der Auftragnehmer stellt sicher, dass jeder Mitarbeiter des Auftragnehmers, unabhängig davon, ob er Angestellter oder Leiharbeiter ist, Zugang zu oder an der Verarbeitung personenbezogener Daten im Rahmen der MSA beteiligt ist, (i) sich zur

Vertraulichkeit verpflichtet hat und (ii) über die Verpflichtungen aus dieser Datenverarbeitungsvereinbarung informiert wird und diese einhält. Die Geheimhaltungspflicht gilt auch nach Beendigung des MSA oder dieses Vertrages über die Datenverarbeitung.

3.6 Sicherheitskontrollen

Der Auftragnehmer führt regelmäßig Sicherheitsaudits für Systeme und ähnliches durch, die für die Verarbeitung personenbezogener Daten, die unter diese Datenverarbeitungsvereinbarung fallen, relevant sind. Berichte, die die Sicherheitsaudits dokumentieren, müssen dem Auftraggeber zur Verfügung stehen.

Der Auftraggeber hat das Recht, Sicherheitsaudits durch einen unabhängigen Dritten zu verlangen gewählt von dem Auftragnehmer. Der Dritte stellt dem Auftraggeber auf Anfrage einen Bericht zur Verfügung. Der Auftraggeber akzeptiert, dass der Auftragnehmer eine Entschädigung für die Durchführung der Prüfung verlangen kann.

3.7 Subunternehmer (Unterauftragnehmer)

Der Auftragnehmer ist berechtigt, Unterauftragnehmer einzusetzen und der Auftraggeber akzeptiert den Einsatz von Unterauftragnehmern. Eine Liste der vorab genehmigten Unterauftragnehmer ist im SuperOffice Trust Center verfügbar. Der Auftragnehmer stellt durch schriftliche Vereinbarung mit einem Unterauftragnehmer sicher, dass die Verarbeitung personenbezogener Daten durch den Unterauftragnehmer denselben Verpflichtungen und Beschränkungen unterliegt, die dem Auftragnehmer gemäß dieser Datenverarbeitungsvereinbarung auferlegt werden.

Beabsichtigt der Auftragnehmer, Unterauftragnehmer auszuwechseln oder einen neuen Unterauftragnehmer einzusetzen, so hat der Auftragnehmer dies dem Auftraggeber 4 Monate vor jeder Verarbeitung durch den neuen Unterauftragnehmer schriftlich mitzuteilen, und der Auftraggeber kann innerhalb eines Monats nach der Benachrichtigung über den Wechsel der Unterauftragnehmer widersprechen. Widerspricht der Auftraggeber dem Wechsel, kann er den Vertrag mit einer Frist von 3 Monaten kündigen. Soweit der Auftraggeber den Vertrag nicht kündigt, gilt der Wechsel des Unterauftragnehmers als akzeptiert.

3.8 Übermittlung von persönlichen Daten an Drittländer

Wenn der Auftragnehmer Unterauftragnehmer außerhalb des EU/EWR-Raums für die Verarbeitung personenbezogener Daten einsetzt, muss diese Verarbeitung im Einklang mit dem EU-Standard-Vertragsklauseln für die Übermittlung in Drittländer oder einer anderen ausdrücklich genannten gesetzlichen Grundlage für die Übermittlung personenbezogener Daten in ein Drittland stehen. Im Zweifel gilt das Gleiche, wenn die Daten in der EU/EWR gespeichert sind, aber von Orten außerhalb der EU/EWR abgerufen werden können.

Sollte der Auftraggeber einer solchen Übermittlung personenbezogener Daten zustimmen, ist er verpflichtet, mit dem Auftragnehmer zusammenzuarbeiten, um eine konforme Übermittlung zu gewährleisten. Beruht die Übertragung auf den EU-Standardvertragsklauseln für Auftragsverarbeiter, so ermächtigt der für die Verarbeitung Verantwortliche den Datenverarbeiter, im Auftrag des für die Verarbeitung Verantwortlichen in solche EU-Standardvertragsklauseln mit dem Unterauftragnehmer einzutreten.

4. Haftung, Verstöße

Im Falle eines Verstoßes gegen diese Datenschutzvereinbarung oder eines Verstoßes gegen die Verpflichtungen nach dem anwendbaren Recht über die Verarbeitung personenbezogener Daten gelten die einschlägigen Bestimmungen zum Vertragsbruch des MSA.

Ansprüche der einen Partei wegen Nichteinhaltung des Datenverarbeitungsvertrages durch die andere Partei unterliegen den gleichen Beschränkungen wie im MSA. Bei der Beurteilung, ob die Haftungsbeschränkung im MSA erreicht ist, sind die Ansprüche wegen Vertragsbruchs aus diesem Datenverarbeitungsvertrag und dem MSA gemeinsam zu berücksichtigen, wobei die Begrenzung im MSA als Gesamtbegrenzung anzusehen ist.

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er Grund zu der Annahme hat, dass er seinen Verpflichtungen aus dieser Datenschutzvereinbarung nicht nachkommen kann.

5. Laufzeit und Kündigung der Datenschutzvereinbarung, Änderungen

Diese Datenverarbeitungsvereinbarung gilt ab dem Datum ihrer Unterzeichnung durch beide Parteien und bis zur Beendigung der Verpflichtungen des Auftragnehmers in Bezug auf die Erbringung von Dienstleistungen in Übereinstimmung mit dem MSA, mit Ausnahme der Bestimmungen des MSA und der Datenverarbeitungsvereinbarung, die auch nach einer solchen Beendigung weiterhin gelten.

Nach Beendigung dieser Datenverarbeitungsvereinbarung werden die personenbezogenen Daten/Daten in einem standardisierten Format und Medium zusammen mit den notwendigen Anweisungen zurückgegeben, um die weitere Verwendung der personenbezogenen Daten/Daten durch den Auftraggeber zu erleichtern. Der Auftragnehmer wird zunächst alle personenbezogenen Daten und andere Daten zurückgeben und anschließend löschen. Der Auftragnehmer (und seine Unterauftragnehmer) werden die Verarbeitung personenbezogener Daten ab dem von dem Auftraggeber festgelegten Datum unverzüglich einstellen.

Als Alternative zur Rückgabe der personenbezogenen Daten (oder anderer Daten) kann der Auftraggeber nach eigenem Ermessen den Auftragnehmer schriftlich anweisen, dass die personenbezogenen Daten (oder andere Daten) ganz oder teilweise vom Auftragnehmer gelöscht werden, es sei denn, der Auftragnehmer ist durch zwingende Rechtsvorschriften daran gehindert, die personenbezogenen Daten zu löschen.

Der Auftragnehmer hat kein Recht, eine Kopie der von dem Auftraggeber im Zusammenhang mit der MSA oder dieser Datenschutzvereinbarung bereitgestellten Daten in irgendeinem Format aufzubewahren, und alle physischen und logischen Zugriffe auf diese personenbezogenen Daten oder andere Daten werden gelöscht.

Der Auftragnehmer stellt dem Auftraggeber eine schriftliche Erklärung zur Verfügung, in der er garantiert, dass alle oben genannten personenbezogenen Daten oder andere Daten gemäß den Anweisungen des Auftraggebers zurückgegeben oder gelöscht wurden und dass der Auftragnehmer keine Kopie, keinen Ausdruck oder Speicherung der Daten auf einem Datenträger vorgenommen hat.

Die Verpflichtungen nach Ziffer 3.5 und 4 gelten auch nach der Kündigung fort. Ferner gelten die Bestimmungen des Datenverarbeitungsvertrages in vollem Umfang für alle personenbezogenen Daten, die vom Auftragnehmer unter Verstoß gegen diesen Abschnitt 5 aufbewahrt werden.

Die Parteien werden diese Datenschutzvereinbarung bei relevanten Änderungen des anwendbaren Rechts anpassen.

6. Gerichtsstand und anwendbares Recht

Dieser Vertrag über die Datenverarbeitung unterliegt den anwendbaren Gesetzen des jeweiligen Landes des SuperOffices, mit dem der Kunde einen Vertrag abschließt:

Wohnort	**Vertragspartner**	**Mitteilungen sind zu richten an:**	**Anwendbares Recht ist:**	**Die ausschließliche Gerichtszuständigkeit liegt in:**
Dänemark	SuperOffice Danmark A/S	Islands Brygge 41, 3.sal, DK-2300 København, Danmark	Dänisch	Kopenhagen, Dänemark
Finnland und Schweden	SuperOffice Sweden AB	Sveavägen 159, SE-113 46 Stockholm, Sverige	Schwedisch	Stockholm, Schweden
Norwegen	SuperOffice Norge AS	Wergelandsveien 27 NO-0167 Oslo, Norge	Norwegisch	Oslo, Norwegen
Deutschland	SuperOffice GmbH	Phoenixseestr. 17, D-44263 Dortmund, Germany	Deutsch	Dortmund, Deutschland
Großbritannien und Irland	SuperOffice Norge AS	Wergelandsveine 27, NO-	UK	Milton Keynes, Großbritannien

		0167 Oslo, Norge		
Schweitz	SuperOffice AG	Uferstrasse 90, 4057 Basel, Switzerland	Schweit-zerisch	Basel, Schweitz
Nieder-lande, Belgien und-Luxem-burg	SuperOffice Benelux B.V.	Emmasingel 29.41, 5611 AZ Nether-lands	Nieder-ländisch	Oost-Brabant, lo-catie Eindhoven, Niederlande

Die in der obigen Tabelle genannten Rechtsordnungen stellen keine Ausnahme von den Bestimmungen über den territorialen Geltungsbereich des Artikels 3 des BIPR oder anderer anwendbarer Rechtsvorschriften dar und ist auch nicht dazu bestimmt.

Lister der vorab genehmigten Subunternehmer (Unter-Auftragnehmer)

Gemäß Klausel 3.7 dieser Vereinbarung wird SuperOffice eine Liste der vorab genehmigten Unternauftragnehmer bereit halten-. Diese Liste ist im SuperOffice Trust Center verfügbar.

Appendix 2 – List of pre-approved Sub-processors

List of pre-approved sub-Processors

in SuperOffice CRM Online

This list is valid from June 2, 2025.

You can see the previous version here.

According to clause 3.7 in the Data Processing Agreement between Customer (Controller) and SuperOffice (Processor), SuperOffice shall maintain a list of pre-approved sub-processors (Sub-Contractors).

Content:

A. SuperOffice AS is the provider of the CRM Online cloud service

Company name	**SuperOffice AS**, Wergelandsveien 27, 0167 Oslo, Norway
SuperOffice Affiliates	Norway, Sweden, Denmark, The Netherlands, Germany, United Kingdom, Switzerland and Lithuania. Entities details are listed in the “CRM Online Terms of Service” available in SuperOffice Trust Center.
Description of Service	SuperOffice CRM Online offers a broad set of CRM (Customer Relationship Management) functionality. The functionality includes a customer database as well as functions for i.e. marketing, sales and service processes. SuperOffice CRM Online is available as a cloud service hosted by SuperOffice AS

The Personal Data to be Processed concerns the following categories of Data Subjects (Persons):	As a Processor SuperOffice stores the complete CRM Online Database for the Controller. Data Subjects and categories of Personal Data registered in the Database is defined by the Controller.
Processing of data	Data entered by the Controller into the CRM Online service are processed by sub-processors listed in this document.
Sensitive personal Data (if relevant)	SuperOffice is not aware or notified if the Controller enters sensitive data into the CRM Online Database. Categories of Personal Data that requires special protection, must be protected by configurations and settings in the CRM Online Application by the Controller.
Additional information regarding Privacy and Security Governance	Penetration Test Reports (Pentest) is available on request to privacy@superoffice.com

B. Pre-approved Sub-processors

The following sub-processors are pre-approved by SuperOffice AS (these are listed below):

1. Visma IT & Communications AS
2. Mailgun Technologies Inc.
3. InfoBridge B.V.
4. Microsoft Corporation
5. Userflow Inc.
6. Amplitude

In addition, the use of Third-Party Services (Applications) must be observed.

1. Visma IT & Communications AS

Entity Company Name	**Visma IT & Communications AS,** Karenslyst Allé 56, 0277 Oslo, Norway
Company website	www.visma.com
Entity Country	Norway
Processing Country	Norway
Entity Type and description of Service	Hosting Provider. Hosting and operations of all servers, and infrastructure for SuperOffice CRM Online. Visma also stores the complete CRM database for the Controller.
The Personal Data to be Processed concerns the following categories of Data Subjects (Persons):	Personal Data entered into Controllers CRM Database.
Categories of Personal Data	Personal Data entered into Controllers CRM Database.
Sensitive personal Data (if relevant)	Personal Data entered into Controllers CRM Database
The Personal Data will be subject to the following Processing activities.	Storage of data in the CRM Database. Back up and restoring of data when requested.

	Monitoring and incident-related activities. Access control and logging.
Additional information regarding Privacy and Security Governance.	ISO Certificates for ISO9001 and ISO27001. Security audit Report ISAE3402 is available on request.

2. Mailgun Technologies Inc.

Entity Company Name	**Mailgun Technologies Inc.** 535 Mission St. San Francisco, CA94105, US
Company website	www.mailgun.com
Entity Country	US
Processing Country	Frankfurt, Germany in EU
Entity Type and description of Service	Email service provider. Mailgun is 1) sending mass emails generated from SuperOffice CRM and 2) receiving and sending replies related to service-tickets in SuperOffice Service. Emails are stored by Mailgun for max. 72 hours for resending purposes. Individual emails sent from the customer's own email service (i.e. exchange, gmail) is not sent to Mailgun.
The Personal Data to be Processed concerns the following categories	Email recipients in e-marketing campaigns and customer service tickets. Senders and recipients of email messages.

of Data Subjects (Persons):	
Categories of Personal Data	The personal data processed includes name, email, IP address and personal data included in message content
Sensitive personal Data (if relevant)	None.
The Personal Data will be subject to the following Processing activities.	Receipt of email addresses from SuperOffice Mailservice. Sending email messages to the selected emailadresses. Receiving and sending replies related to service-tickets in SuperOffice Service. Storage in max 72 hours for the purpose of resending mails in fault situations.
Additional information regarding Privacy and Security Governance.	Sub-processor agreement in place requiring adequate privacy and information security measures
Sinch (Mailgun) Trust Center	Access Security policies, certificates and audit reports. https://trust.sinch.com/

3. InfoBridge B.V.

Entity Company Name	**InfoBridge B.V.,** Europalaan 24F, 5232 BC 's-Hertogenbosch, Netherlands InfoBridge B.V. is a 100% owned subsidiary of SuperOffice AS.

Company website	www.infobridge.com
Entity Country	The Netherlands
Processing Country	The Nederlands
Entity Type and description of Service	Calendar synchronization Service between SuperOffice CRM and various Calendaring Systems (Microsoft 365 and Google G-Suite). No personal data is stored in the InfoBridge Service itself, only in SuperOffice CRM Online and Microsoft 365 / Google G-Suite.
The Personal Data to be Processed concerns the following categories of Data Subjects (Persons):	Users of SuperOffice CRM Online.
Categories of Personal Data	Usernames, Calendar item data incl. basic company and person data fields. Unstructured text entered into the calendar item.
Sensitive personal Data (if relevant)	None.

The Personal Data will be subject to the following Processing activities.	Calendar entries in the SuperOffice Calendar will be synchronized (inserted/updated/deleted) in the Microsoft 365/Google calendar. Calendar entries in the Microsoft 365/Google calendar will be synchronized (inserted/updated/deleted) in the SuperOffice Calendar. Invitations coming via email in MS365/Google will be inserted into the SuperOffice Calendar if accepted.
Additional information regarding Privacy and Security Governance.	Sub-processor agreement in place requiring adequate privacy and security measures

4. Microsoft Corporation

Entity Company Name	**Microsoft Corporation,** One Microsoft Way, Redmond, WA 98052-6399, US
Company website	www.microsoft.com
Entity Country	US
Processing Country	The Netherlands and Ireland

Entity Type and description of Service	Document Storage Provider. All documents stored in SuperOffice CRM Online is stored in a Microsoft Azure service.

	Documents are stored as separate files. No Personal Data (or any other metadata) is stored in connection with the document. The document itself may contain unstructured personal data.
The Personal Data to be Processed concerns the following categories of Data Subjects (Persons):	Potentially Personal Data contained in a document stored by the Controller.
Categories of Personal Data	Potentially Personal Data contained in documents.
Sensitive personal Data (if relevant)	Potentially Personal Data contained in documents.
The Personal Data will be subject to the following Processing activities.	Structured personal data is not stored in Azure, only the document itself. Documents may be containing unstructured personal data. Documents are stored, backed-up and restored when requested.
Additional information regarding Privacy and Security Governance.	https://www.microsoft.com/en-us/trustcenter/cloudservices/azure

Entity Type and description of Service	SuperOffice AI Services – 3 language analytics services: 1. Ticket categorization 2. Language detection and translation 3. Sentiment detection

	The services are licenced as separate addon services.
The Personal Data to be Processed concerns the following categories of Data Subjects (Persons):	Potentially Personal Data contained in service requests (tickets) and submitted to SuperOffice CRM Online.
Categories of Personal Data	Potentially Personal Data contained in service tickets.
Sensitive personal Data (if relevant)	Potentially Personal Data contained in service tickets.
The Personal Data will be subject to the following Processing activities.	The content of the service tickets will be sent to a set of Azure Sservices and processed to provide AI – based language services.
Additional information regarding Privacy and Security Governance.	Data Residency in Azure | Microsoft Azure https://azure.microsoft.com/en-us/global-infrastructure/data-residency/#overview

5. Userflow Inc.

Entity Company Name	**Userflow Inc.,** 548 Market St. PMB 69598, San Fransisco, CA94194-5401, US
Company website	www.userflow.com
Entity Country	US

Processing Country	US
Entity Type and description of Service	User onboarding and activation software that works with SuperOffice CRM delivering in-product communication. Including tooltips, onboarding tours, resource centers with contextual help, and customer surveys.
The Personal Data to be Processed concerns the following categories of Data Subjects (Persons):	Licensed users of SuperOffice CRM Cloud.
Categories of Personal Data	The personal data processed includes: - User ID - Customer ID - Role and department - Page views and clicks in SuperOffice and Userflow (usage). Does not include any data-input.
Sensitive personal Data (if relevant)	None
The Personal Data will be subject to the following Processing activities.	Based on usage data and preferences, the user gets targeted and personalized communication.
Additional information regarding Privacy and Security Governance.	Sub-processor DPA in place requiring adequate privacy and information security measures. SOC 2 Type II certification.

6. Amplitude

Entity Company Name	**Amplitude,** 201 3rd Street 200, San Francisco, CA 94103, USA
Company website	www.amplitude.com
Entity Country	US
Processing Country	Frankfurth, Germany
Entity Type and description of Service	Analytics to see
The Personal Data to be Processed concerns the following categories of Data Subjects (Persons):	Licensed users of SuperOffice CRM Cloud.
Categories of Personal Data	The personal data processed includes: - User ID (anonymized) - Customer ID (anonymized) - Page views and clicks. No data input is recorded or transferred.
Sensitive personal Data (if relevant)	None
The Personal Data will be subject to the following Processing activities.	Usage statistics to improve the performance and behaviour of the product
Additional information regarding Privacy and Security Governance.	Sub-processor DPA in place requiring adequate

	privacy and information security measures. SOC 2 Type II certification.

C. SuperOffice App Store Partners (Third Party Services)

The table below is a general description of Software Partners in the SuperOffice App Store. SuperOffice AS has signed sub-processor DPA's with all Software Partners. In addition to this, a specific DPA has to be signed between Customer (Controller) and Software Partner (Processor).

Entity Company Name	**SuperOffice App Store partners**
Company website	App Store partner website
Entity Country	App Store partner location
Processing Country	App Store partner processing localtion
Entity Type and description of Service	SuperOffice offers 3rd parties to integrate other solutions with the CRM Online service. Partners are using APIs available in the CRM Online Platform to build integrated standard Apps as well as customized solutions. These APIs provide access to customer data. SuperOffice certifies each individual App regarding security, privacy and proper technical and operational use of our API's. Each partner sign a sub-processor Data Processing Agreement with SuperOffice. The integration is not activated until a formal Data Processing Agreement is signed between the Partner and the Customer and presented to SuperOffice. It is the Customer's responsibility to sign a DPA directly with the Partner.

The Personal Data to be Processed concerns the following categories of Data Subjects (Persons):	Must be described in the DPA between Customer and Partner.
Categories of Personal Data	Must be described in the DPA between Customer and Partner.
Sensitive personal Data (if relevant)	Must be described in the DPA between Customer and Partner.
The Personal Data will be subject to the following Processing activities.	Must be described in the DPA between Customer and Partner.
Additional information regarding Privacy and Security Governance.	Must be described in the DPA between Customer and Partner.

D. Integration to Identify Providers

SuperOffice offers technology that enables integration between SuperOffice and industry standard Identity providers like Google Identity and Microsoft Azure AD based on OpenID Connect. However it is the sole responsibility of the Customer to sign DPA's and other relevant agreements with the providers of the Identity Provider.

Company Names of Identity Providers	Microsoft Corporation Inc. and Google LLC
Entity Type and description of Service	SuperOffice offers standard integration to Identity Services provided by the companies listed above. Additional standard integrations might be launched in the future. The Identity Providers handles following data:

	• Username and password (hash) • In addition, User Management will require additional organizational information related to Persons. It is the SCIM standard that enables this feature. SuperOffice supports the industry standard SCIM protocol.
The Personal Data to be Processed concerns the following categories of Data Subjects (Persons):	Must be described in the DPA between Customer and Partner.
Categories of Personal Data	Must be described in the DPA between Customer and Partner.
Sensitive personal Data (if relevant)	Must be described in the DPA between Customer and Partner.
The Personal Data will be subject to the following Processing activities.	Must be described in the DPA between Customer and Partner.
Additional information regarding Privacy and Security Governance.	Must be described in the DPA between Customer and Partner.

Appendix 3 – Technical and Organizational measures

In compliance with the requirements of Art. 32 GDPR, the contractor has implemented the following technical and organizational measures (TOM) to ensure a level of protection appropriate to the risk for the personal data processed by the client on behalf of the contractor. These measures are regularly reviewed and updated as necessary (see also information in our Trust Centre). In detail:

- **Access control (physical security):**

  The servers and systems on which the service operates are located in highly secure data centres. Access to the buildings and systems of the hosting partner (Visma IT & Communications, see Appendix 2) is strictly regulated. Unauthorised persons are physically denied access: access control systems (electronic badges, individual access gates) ensure that only authorised persons can enter the server rooms. Video surveillance is used at building entrances and in sensitive areas. Visitors or external technicians are only granted access after prior authorisation and when accompanied by authorised staff. The data centres are also equipped with advanced alarm systems and a 24/7 security service.

- **Access Control (System Access):**

  Unauthorized individuals must not be able to use the contractor's IT systems. Access to the service infrastructure is protected by multi-factor authentication. External attack attempts are blocked by firewalls and intrusion prevention systems. Data transmission between the customer and the service is encrypted (at least TLS/SSL). Users of the CRM Online Services log in with individual credentials (username/password); for enhanced security, two-factor authentication (2FA) is supported (e.g., via Office 365 or Google Workspace integration). Password management includes complexity requirements and regular expiration intervals according to current best practices. Error messages and login attempts are logged, and in case of suspicious patterns (e.g., brute-force attacks), countermeasures are automatically triggered (e.g., temporary account lockout).

- **Access Rights Control (Data Access Permissions):**

  Within the service, it is ensured that authorized users can only access data relevant to their roles. The customer independently manages users and their permission levels (admin, standard user, restricted roles, etc.). The system supports fine-grained access controls, so that, for example, sales users can only view their own customer records, while administrators have broader access. The contractor only accesses personal customer data in exceptional cases and with the customer's prior approval (e.g., in support cases), and even then only through dedicated, logged support accounts. Employees with administrative access to the system level are carefully selected and monitored (server-level administrative access is limited to a small group of authorized personnel).

- **Data Transfer Control (Transmission Security):**

  When transmitting personal data—whether within the internal network or over the internet—appropriate encryption methods are used. All communication between the customer and the service is conducted via HTTPS (TLS). Data transfers between internal server components or to subcontractors are also protected (e.g., TLS communication between the service and Mailgun email servers). Backups are stored encrypted and, if transferred to external systems or locations, are always transmitted via secure, encrypted tunnels (VPN). Decommissioned data carriers are subject to a documented deletion or destruction process (e.g., physical destruction of hard drives) to ensure data cannot be recovered. If personal data is transported via mobile

storage devices in exceptional cases, this is only done in encrypted form and by authorized personnel.

- **Input Control (Activity Logging):**

  All relevant access and modifications to personal data in the system are logged. In particular, each user read/write access to the database is recorded in log files and/or the database history, including user ID, timestamp, type of action, and—where applicable—the affected records. Administrative access by the contractor (e.g., by technicians during troubleshooting) is also logged. Log data is securely stored and regularly evaluated to detect unauthorized access or anomalies. Changes to security-related settings (e.g., permission changes, password updates) are only possible for authorized admin users and are specially monitored. Sensitive actions (such as bulk data exports) may require additional confirmations or approvals. Log data is subject to internal evaluation policies and can be made available to the customer upon request during audits.

- **Processing Control (Separation for Different Purposes):**

  The contractor processes data exclusively in accordance with this agreement and the instructions of the customer. The system design ensures strict separation of data belonging to different customers (multi-tenant architecture). Each customer's data is stored logically separated (e.g., separate databases or schema-level separation), preventing any intermingling. Test or development environments are separated from the production environment; live customer data is not used for testing without control. If subcontractors are used, the contractor has concluded data processing agreements with them in accordance with Art. 28 GDPR, ensuring purpose-specific data processing. Data will not be shared with third parties (who are not subcontractors under this agreement) unless explicitly authorized by the customer.

- **Availability Control (Data Backup and Fault Tolerance):**

  The contractor's systems are designed to ensure high availability and to protect data against loss. All servers are connected to redundant power supplies; uninterruptible power supplies (UPS) and backup generators protect against outages. Climate control and fire protection are redundantly available (e.g., fire suppression systems, smoke detectors). A detailed disaster recovery plan is in place. Critical components are redundant, so the failure of a single system does not lead to data loss. The contractor performs regular backups of all customer data—typically once a day (usually overnight). Databases are backed up daily with point-in-time recovery, allowing data restoration to any point in the past 30 days. Additionally, monthly full backups are kept for at least 12 months, and yearly archival backups for up to 10 years (where applicable). Backups are stored encrypted. Documents/files uploaded into the CRM are continuously mirrored (synchronously replicated) between two data center locations. Deleted files are retained in backups for at least 90 days to allow recovery of accidental deletions. Backup data is stored in separate, secure environments. Regular restoration tests ensure that backups can be successfully recovered when needed. The contractor informs the customer of planned maintenance or service interruptions (e.g., for updates) with appropriate lead time—usually at least 24 hours in advance.

- **Organizational Measures:**

  In addition to technical measures, the contractor has implemented organizational procedures to ensure data protection and security. These include binding employee policies (e.g., password policy, clean desk policy), regular data protection training, a role and authorization concept within the organization, and defined procedures for handling data protection incidents (incident response plan). An internal data protection management system is in place, and compliance is regularly reviewed both internally and externally. A Data Protection Officer (contact details above) has been appointed and oversees the procedures. Additionally, the contractor conducts annual external audits: for example, security audits according to ISAE 3402 Type II by independent auditors (e.g., EY), with corresponding reports being generated. Regular penetration tests of the application and infrastructure are also conducted by external experts; the results are evaluated and feed into continuous improvements. Relevant reports (audit summaries, pentest reports) can be provided to the customer upon request.

- **Certifications and Standards:**

  The technical and organizational measures (TOMs) implemented by Visma IT & Communications (Visma ITC) are based on internationally recognized standards to ensure the highest levels of quality, environmental management, and information security. This is demonstrated by the following certifications:

  - **ISO 9001:2015:** This certification confirms the implementation of an effective quality management system, based on principles such as customer focus, process orientation, and continuous improvement.

  - **ISO 14001:2015:** This certification attests to the establishment of an environmental management system that helps organizations systematically manage their environmental responsibilities and promote sustainable practices.

  - **ISO/IEC 27001:2013:** This certification confirms the implementation of an Information Security Management System (ISMS) designed to protect sensitive data through strict security controls.