DATENVERARBEITUNGSVERTRAG

„**KUNDE**“ oder „**VERANTWORTLICHER**“:

Name des Unternehmens: _____

Adresse: _____

_____

_____

_____

Unternehmensinformationen: _____

„**MAPP**“ oder „**VERARBEITER**“:

Das in Anhang 3 aufgeführte Unternehmen von Mapp, das Vertragspartei im MSA ist.

Dieser Datenverarbeitungsvertrag („**DVV**“ oder „**DPA**“) ist Teil des Rahmenvertrages (Master Services Agreement, MSA) oder eines anderen Vertrages über den Bezug von Dienstleistungen von Mapp (im Folgenden „**MSA**“ genannt) zwischen dem Kunden und Mapp.
Mit der Unterzeichnung dieses DVV schließt der Kunde diesen DVV im eigenen Namen und, soweit dies nach den geltenden Datenschutzgesetzen und -vorschriften erforderlich ist, auch im Namen und im Auftrag seiner verbundenen Unternehmen ab.
Ausführung des DVV:

- Wenn dieser DVV im Namen von Mapp bereits vorab unterzeichnet wird: (1) die vorstehenden Kundeninformationen vervollständigen; (2) das Unternehmen von Mapp auswählen, das Vertragspartei im MSA ist; (3) Anlage 1 überprüfen und gegebenenfalls bearbeiten; (3) den DVV unterzeichnen; (4) und per E-Mail senden an: privacy@mapp.com.
- Mit Erhalt des vollständig ausgeführten DVV wird dieser rechtsverbindlich und Gegenstand des MSA.
- Wenn der Kunde Änderungen an diesem DVV vornimmt, die nicht miteinander vereinbart wurden, sind diese Änderungen ungültig. Der Unterzeichner des Kunden erklärt Mapp gegenüber, dass er die gesetzliche Befugnis hat, den Kunden an diese Vereinbarung zu binden. Dieser DVV endet automatisch mit Beendigung des MSA.

1. DEFINITIONEN

1.1 **Datenschutzgesetze und -verordnungen** sind alle untergeordneten Gesetze und Verordnungen zur Umsetzung der Richtlinie, die anwendbar sind, sowie ab dem 25. Mai 2018 und danach die Verordnung der Europäischen Union zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (die „**Datenschutz-Grundverordnung**“ oder „**DSGVO**“) sowie alle untergeordneten Gesetze und Verordnungen zur Umsetzung der DSGVO, die anwendbar sein können.

1.2 **Datenschutzgesetzgebung** bezeichnet die europäischen Richtlinien 95/46/EG und 2002/58/EG, DSGVO (Verordnung (EU) 2016/679), alle Gesetze und/oder Verordnungen, die sie umsetzen oder auf deren Grundlage sie erlassen werden, die sie ändern, ersetzen, nachvollziehen, umsetzen, konsolidieren oder davon abweichen, sowie alle anderen anwendbaren Gesetze in Bezug auf die Verarbeitung personenbezogener Daten und den Datenschutz, die in jeder relevanten Rechtsordnung bestehen können. Dies schließt gegebenenfalls die Leitlinien und Verhaltenskodexe ein, die von Zeit zu Zeit von der Datenschutzbehörde, anderen relevanten Datenschutzaufsichtsbehörden für das gesamte Land und die gesamte Landesgruppe, die Europäische Kommission, die Artikel-29-Arbeitsgruppe und den Europäischen Datenschutzrat herausgegeben werden.

1.3 **Die betroffene Person** hat die im Datenschutzgesetz festgelegte Bedeutung.

1.4 **Richtlinie** bezeichnet die EU-Datenschutzrichtlinie 95/46/EG

1.5 **Ein verbundenes Unternehmen** ist jedes Unternehmen, das direkt oder indirekt Eigentümer ist oder die Kontrolle über die betreffende Vertragspartei ausübt, sich im Besitz oder unter der Kontrolle der betreffenden Vertragspartei befindet oder unter gemeinsamer Kontrolle steht.

1.6 **Verletzung personenbezogener Daten** bedeutet eine Verletzung der Sicherheit, die zur unbeabsichtigten oder rechtswidrigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zum Zugriff auf personenbezogene Daten führt, die übertragen, gespeichert oder anderweitig verarbeitet werden.

1.7 Alle anderen großgeschriebenen Begriffe haben die im Datenschutzgesetz oder dem MSA festgelegte Bedeutung.

2. DATENVERARBEITUNG

2.1 Die Vertragsparteien erkennen an und vereinbaren, dass bei der Verarbeitung personenbezogener Daten der Kunde der Verantwortliche und Mapp der Bearbeiter ist.

2.2 Die Vertragsparteien erfüllen ihre jeweiligen Pflichten aus den Datenschutzgesetzen und -verordnungen. Jede Vertragspartei verarbeitet personenbezogene Daten bei der Nutzung von Mapp-Dienstleistungen nur in Übereinstimmung mit den Anforderungen der Datenschutzgesetze und -verordnungen.

2.3 Die Anweisungen des Kunden zur Verarbeitung personenbezogener Daten müssen den Datenschutzgesetzen und -verordnungen entsprechen. Mapp informiert den Kunden unverzüglich, wenn nach Ansicht von Mapp eine Anweisung des Kunden gegen Datenschutzgesetze und -verordnungen verstößt.

2.4 Mapp verarbeitet personenbezogene Daten nur im Auftrag und in Übereinstimmung mit den dokumentierten

Anweisungen des Kunden für (i) die Verarbeitung in Übereinstimmung mit dem MSA; (ii) die Verarbeitung, die von den Benutzern bei der Nutzung der Dienstleistungen ausgelöst wurde; (iii) die Verarbeitung zur Einhaltung anderer dokumentierter angemessener Anweisungen des Kunden; (iv) die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten und der Dienstleistungen in Übereinstimmung mit dieser Vereinbarung; und (v) die Erhebung nicht identifizierbarer Statistiken.

2.5 Gegenstand, Dauer und Zweck der Verarbeitung sowie die Art der personenbezogenen Daten und Kategorien der betroffenen Personen sind im MSA festgelegt.

3. ANTRÄGE ZU DEN RECHTEN BETROFFENER PERSONEN

3.1 Mapp benachrichtigt den Kunden, wenn Mapp von einer betroffenen Person einen Antrag zur Ausübung eines oder mehrerer der in Kapitel III DSGVO (33–36) festgelegten Rechte der betroffenen Person erhält („**RBP-Antrag**"), soweit gesetzlich zulässig.

3.2 Unter Berücksichtigung der Art der Verarbeitung unterstützt Mapp den Kunden durch geeignete technische und organisatorische Maßnahmen, sofern dies möglich ist, bei der Erfüllung seiner Verpflichtung zur Beantwortung eines RBP-Antrags gemäß den Datenschutzgesetzen und -verordnungen.

3.3 Wenn der Kunde bei der Nutzung der Dienstleistungen nicht in der Lage ist, einen RBP-Antrag zu beantworten, ergreift Mapp auf Wunsch des Kunden wirtschaftlich angemessene Maßnahmen, um den Kunden bei der Beantwortung eines solchen RBP-Antrags zu unterstützen, soweit Mapp dies gesetzlich erlaubt ist und die Beantwortung eines solchen RBP-Antrags gemäß den Datenschutzgesetzen und -verordnungen erforderlich ist. Soweit gesetzlich zulässig, trägt der Kunde alle Kosten, die sich aus der Bereitstellung dieser Unterstützung durch Mapp ergeben.

4. FOLGENABSCHÄTZUNGEN ZUM DATENSCHUTZ

Mapp unterstützt den Kunden angemessen bei allen nach den Datenschutzgesetzen und -verordnungen erforderlichen Folgenabschätzungen zum Datenschutz und vorherigen Rücksprachen mit einer Aufsichtsbehörde, in jedem Fall ausschließlich in Bezug auf die Verarbeitung personenbezogener Daten durch Mapp und unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen.

5. BENACHRICHTIGUNG ÜBER DIE VERLETZUNG PERSONENBEZOGENER DATEN

5.1 Mapp benachrichtigt den Kunden unverzüglich nach Kenntniserlangung von einer Verletzung personenbezogener Daten. Mapp stellt dem Kunden ausreichende Informationen zur Verfügung, damit er seinen Verpflichtungen nachkommen kann, eine Aufsichtsbehörde über die Verletzung personenbezogener Daten zu informieren und/oder die Verletzung personenbezogener Daten an betroffene Personen im Rahmen der Datenschutzgesetze weiterzugeben.

5.2 Mapp unternimmt angemessene Anstrengungen, um die Ursache einer Verletzung personenbezogener Daten zu ermitteln und die von Mapp für notwendig und angemessen erachteten Maßnahmen zu ergreifen, um die Ursache eines solchen Vorfalls von Kundendaten zu beheben, soweit die Behebung in der angemessenen Kontrolle von Mapp liegt.

5.3 Die hierin enthaltenen Verpflichtungen gelten nicht für Vorfälle, die vom Kunden verursacht werden.

6. UNTERAUFTRAGSVERARBEITUNG

6.1 Verbundene Unternehmen von Mapp und andere Unterauftragsverarbeiter, die von Mapp zur Erbringung seiner vertraglichen Dienstleistungen verwendet werden, einschließlich ihrer Rolle und ihres Umfangs bei der Unterauftragsverarbeitung und des geografischen Bereichs der Unterauftragsverarbeitung, werden in der Liste der Unterauftragsverarbeiter von Mapp veröffentlicht, die auf Anfrage erhältlich und/oder zugänglich ist unter www.mapp.com/contracts. Diese Unterauftragsverarbeiter müssen vom Kunden angenommen und genehmigt werden. Mit der Unterzeichnung dieses Datenverarbeitungsvertrags stimmt der Kunde der Liste der Unterauftragsverarbeiter zu, die als Anhang 3 beigefügt sind, und ermächtigt Mapp hiermit, personenbezogene Daten an aufgelistete verbundene Unternehmen von Mapp und/oder andere Unterauftragsverarbeiter an Orte außerhalb des Europäischen Wirtschaftsraums zu übertragen, sofern dies angemessen erforderlich ist, um Unterstützung zu leisten, technische Projekte durchzuführen oder andere Arten von Dienstleistungen im Rahmen des MSA zu erbringen, sofern der Kunde in der EU ansässig ist, entweder: (i) die Standorte werden von der Europäischen Kommission als angemessenen Datenschutz bietend anerkannt oder (ii) Mapp hat die EU-Standardvertragsklauseln mit solchen verbundenen Unternehmen und/oder anderen Unterauftragsverarbeitern unterzeichnet.

6.2 Mapp hat mit jedem Unterauftragsverarbeiter eine schriftliche Vereinbarung getroffen, die Datenschutzverpflichtungen enthält, die keinen geringeren Schutzumfang bieten als die in diesem Datenverarbeitungsvertrag festgelegten Datenschutzverpflichtungen in Bezug auf den Schutz personenbezogener Daten, soweit dies auf die Art der von diesem Unterauftragsverarbeiter bereitgestellten Dienste anwendbar ist.

6.3 Mapp haftet für die Handlungen und Unterlassungen seiner Unterauftragsverarbeiter in demselben Umfang, in

dem Mapp haftet, wenn die Dienstleistungen eines jeden Unterauftragsverarbeiters direkt gemäß den Bestimmungen dieses DVV ausgeführt werden, sofern im MSA nichts anderes festgelegt ist.

6.4 Erwartet Mapp die Notwendigkeit einer Änderung oder Hinzufügung eines Unterauftragsverarbeiters, so benachrichtigt Mapp den Kunden über jede Änderung in Bezug auf den Unterauftragsverarbeiter und der Kunde ist berechtigt, Änderungen innerhalb eines angemessenen Zeitraums zu widersprechen. Widerspricht der Kunde dieser Änderung nicht innerhalb dieser Frist, so wird davon ausgegangen, dass er dieser Änderung zugestimmt hat. Wenn ein wesentlicher Grund für einen solchen Widerspruch vorliegt und die Parteien diesbezüglich keine einvernehmliche Lösung finden, ist der Kunde berechtigt, den Datenverarbeitungsvertrag zu kündigen. Mapp stellt sicher, dass alle neuen Unterauftragsverarbeiter denselben geltenden Standards unterliegen wie die zuvor vereinbarten Unterauftragsverarbeiter.

7. SICHERHEIT

Unter Berücksichtigung des Stands der Technik, der Kosten für die Durchführung und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie des Risikos unterschiedlicher Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen unterhält Mapp angemessene technische und organisatorische Maßnahmen zum Schutz der Sicherheit (einschließlich des Schutzes vor unbefugter oder rechtswidriger Verarbeitung und vor unbeabsichtigter oder rechtswidriger Zerstörung, Verlust, Änderung oder Beschädigung, unbefugter Weitergabe von oder Zugriff auf Kundendaten), der Vertraulichkeit und Integrität personenbezogener Daten gemäß Mapps Sicherheitsanhang (Anhang 2) zu diesem Datenverarbeitungsvertrag. Mapp überwacht regelmäßig die Einhaltung dieser Maßnahmen. Mapp wird die Gesamtsicherheit der Dienstleistungen während der Laufzeit des MSA nicht wesentlich verringern. Mapp beschränkt den Zugriff auf personenbezogene Daten auf seine Mitarbeiter oder Unterauftragsverarbeiter, für die der Zugriff auf diese Daten zur Erfüllung der Verpflichtungen von Mapp gegenüber dem Kunden angemessen erforderlich ist. Mapp stellt sicher, dass Personen, die zur Verarbeitung der personenbezogenen Daten berechtigt sind, denselben oder gleichwertigen Geheimhaltungspflichten unterliegen wie Mapp oder einer entsprechenden gesetzlichen Geheimhaltungspflicht unterliegen. Die Datensicherheitsrichtlinien von Mapp können auf Anfrage bereitgestellt werden, wenn der Kunde zusätzliche Details zu diesem Abschnitt wünscht.

8. LÖSCHUNG ODER RÜCKGABE PERSONENBEZOGENER DATEN

8.1 Mapp löscht die personenbezogenen Daten nach Beendigung/Ablauf des MSA wie im MSA festgelegt oder auf begründete Anfrage des Kunden innerhalb von 30 Tagen und stellt sicher, dass die gelöschten Daten nicht wiederherstellbar sind. Mapp darf personenbezogene Daten im gesetzlich vorgeschriebenen Umfang und nur in dem Umfang und für den Zeitraum aufbewahren, der gesetzlich vorgeschrieben ist und stets vorausgesetzt, dass Mapp die Vertraulichkeit all dieser personenbezogenen Daten gewährleistet und sicherstellt, dass solche personenbezogenen Daten nur soweit verarbeitet werden, wie es für die Zwecke erforderlich ist, die in den geltenden Gesetzen festgelegt sind, in denen die Speicherung vorgeschrieben ist, und für keinen anderen Zweck.

8.2 Mapp wird dem Kunden auf dessen Anfrage eine schriftliche Bestätigung über die Löschung gemäß diesem Abschnitt 8 vorlegen.

8.3 Mapp sendet dem Kunden personenbezogene Daten gemäß dem im MSA festgelegten Verfahren und Zeitrahmen zurück.

9. AUDITS UND KONTROLLEN

9.1 Mapp stellt dem Kunden alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses Datenverarbeitungsvertrags erforderlich sind, und ermöglicht Audits durch den Kunden oder einen vom Kunden beauftragten externen Auditor in Bezug auf die Verarbeitung personenbezogener Daten und leistet einen Beitrag dazu. Auf schriftliche Anfrage des Kunden füllt Mapp höchstens einmal pro Jahr einen angemessenen Fragebogen zur Informationssicherheit in Bezug auf die Datenschutz- und Informationssicherheitspraktiken und -richtlinien von Mapp aus, der vom Kunden bereitgestellt wird.

9.2 Der Kunde oder ein vom Kunden beauftragter externer Wirtschaftsprüfer kann auf Kosten des Kunden und höchstens einmal pro Jahr eine Überprüfung der Datenschutz- und Informationssicherheitspraktiken und -richtlinien von Mapp vor Ort mit einer angemessenen schriftlichen Vorankündigungsfrist von mindestens zehn Werktagen durchführen. Die Überprüfung darf nicht länger als einen Tag während der normalen Geschäftszeiten von Mapp nach einem einvernehmlichen Zeitplan stattfinden, der die Auswirkungen des Audits auf die Geschäftstätigkeit von Mapp auf ein Mindestmaß beschränkt. Der Kunde oder ein vom Kunden beauftragter externer Prüfer muss die Sicherheitsanforderungen von Mapp in Bezug auf die Durchführung der Überprüfung erfüllen. Aufgrund von Vertraulichkeits- und Sicherheitsanforderungen schließen solche Überprüfungen Vor-Ort-Überprüfungen von Multi-Tenant-Umgebungen (wie von Mapp verwendete IaaS-Rechenzentren) aus. Vor-Ort-Untersuchungen solcher Umgebungen können durch detaillierte Unterlagen zu den jeweils ergriffenen Datenschutz- und Sicherheitsmaßnahmen und spezifischen Zertifizierungen ersetzt werden, die von seriösen externen Prüfern ausgestellt wurden und von Mapp auf Wunsch des Kunden bereitgestellt werden.

9.3 Der Kunde muss Mapp unverzüglich über alle bei einem solchen Audit/einer solchen Überprüfung festgestellten Verstöße informieren.

10. HAFTUNG

10.1 Die Haftung jeder Partei aus oder im Zusammenhang mit diesem Datenverarbeitungsvertrag und allen Datenverarbeitungsverträgen zwischen verbundenen Unternehmen und Mapp, sei es vertraglich festgelegt, aus unerlaubter Handlung oder aufgrund einer anderen Haftungstheorie, unterliegt der im MSA vereinbarten Haftungsbeschränkung, und jeglicher Verweis in diesem Abschnitt auf die Haftung einer Partei bedeutet den gesamten Haftungsumfang dieser Partei und aller ihrer verbundenen Unternehmen im Rahmen des MSA und aller DVV zusammen.

10.2 Um Zweifel auszuschließen, gilt der gesamte Haftungsumfang von Mapp für alle Ansprüche des Kunden und aller seiner verbundenen Unternehmen aus oder im Zusammenhang mit dem MSA und jedem DVV für alle Ansprüche sowohl aus dem MSA als auch aus allen gemäß diesem Vertrag unterzeichneten DVV.

10.3 Wenn ein Datensubjekt Ansprüche gegenüber einer Partei dieses DVV gemäß Art. 82 DSGVO geltend macht, leistet die andere Partei bei der Abwehr solcher Ansprüche Unterstützung, soweit dies möglich ist.

Anhang 1: **Datensubjekte und Kategorien**
Anhang 2: **Sicherheitsanhang**
Anhang 3: **Liste der verbundenen Unternehmen von Mapp und Subunternehmer**

VERANTWORTLICHER		**VERARBEITER**	
Unterschrift:		Unterschrift:	
Name in Druckbuchstaben, Titel:		Name in Druckbuchstaben, Titel:	Steven Warren, CEO
Datum:		Datum:	

ANHANG 1: DATENSUBJEKTE UND KATEGORIEN

Datensubjekte. Die verarbeiteten personenbezogenen Daten betreffen folgende Kategorien von Datensubjekten:

- Kunden des Kunden,
- Interessenten des Kunden,
- Website-Besucher des Kunden,
- Mitarbeiter des Kunden,

Datenkategorien. Die verarbeiteten personenbezogenen Daten betreffen folgende Datenkategorien:

- E-Mail-Adressen,
- Handynummer,
- Festnetznummer,
- Nachname, Vorname,
- Anschrift,
- Geburtsdatum,
- Öffnen empfangener E-Mails,
- Klicks auf Links innerhalb der empfangenen E-Mails,
- IP-Adressen,
- Nutzungsverhalten auf der Website,

ANHANG 2: SICHERHEITSANHANG

TECHNISCHE UND ORGANISATORISCHE INFORMATION SICHERHEITSMASSNAHMEN VERSION 5.0, 23.05.2019

1. Vertraulichkeit (Art. 32 Abs. 1 lit. a & b DSGVO und Art. 25 Abs. 1 DSGVO)	
Physische Zugangskontrolle	**Implementierung**
Mapp ergreift geeignete Maßnahmen, um zu verhindern, dass unbefugte Personen Zugang zu den Datenverarbeitungsgeräten erhalten, in denen die personenbezogenen Daten verarbeitet oder genutzt werden.	Die Maßnahmen werden gemäß ISO 27001:2013, insbesondere A.11.1.x bis A.11.6.x, konzipiert, angewandt und überwacht. Diese schließen ein: - Etablierte Sicherheitsbereiche mit geschützten Ein- und Ausgangspunkten. - Genehmigungsverfahren für Mitarbeiter und Dritte. - Verfahren zur Besucherverwaltung, um eine ordnungsgemäße Authentifizierung und Überwachung sicherzustellen. - CCTV-Überwachung für alle Rechenzentren und Hauptbürostandorte, die alle Eingangs- und Ausgangspunkte abdeckt. - Für den Zugriff auf Rechenzentrumsgeräte sind mindestens zwei unterschiedliche Authentifizierungsfaktoren erforderlich. - Die Geräte sind so aufgestellt, dass sie effektiv vor unbefugter Offenlegung von Informationen geschützt sind. - Sicherheitsalarmsysteme für Rechenzentren und Hauptbürostandorte. - Personal am Empfang und/oder Sicherheitspersonal in Rechenzentren. - Verfahren für die sichere Zuweisung von Schlüsselkarten und/oder die biometrische Registrierung. - Elektronisches Zugangssystem, das den gesamten Zugang zu Rechenzentren und Hauptbürostandorten protokolliert. - Zusätzliche Sicherheitskontrollen gemäß den Richtlinien für die Informationssicherheit von Mapp.
Systemzugriffskontrolle	**Implementierung**
Mapp ergreift geeignete Maßnahmen, um zu verhindern, dass seine Systeme zur Verarbeitung personenbezogener Daten von unbefugten Personen verwendet werden.	Die Maßnahmen werden gemäß ISO 27001:2013, insbesondere A.6.2.1, A.9.1.x, A.9.2.x, A.9.3.x, A.10.1.x, A.11.2.8-.9, A.12.2.1, A.12.4.1, A.12.6.1, A.14.2.x und A.18.2.3, konzipiert, angewandt und überwacht. Diese schließen ein: - Beibehaltung der Richtlinie zu Zugriffskontrollen. - Vorgehensweise zum Verwalten von Benutzer- und privilegierten Konten in Übereinstimmung mit dem Beschäftigungszyklus auf der Grundlage eines zentralen Verzeichnisses. - Für den privilegierten Zugriff auf die Infrastruktur ist eine Multi-Faktor-Authentifizierung erforderlich. - Kennwortrichtlinie, die technisch mindestens 8 Zeichen erfordert; umfassen mindestens drei der folgenden vier Elemente: Großbuchstabe(n), Kleinbuchstabe(n), Zahl(en), Symbol(e); ein anderes Kennwort als die 8 zuvor verwendeten; interne Benutzerkennwörter laufen nach 90 Tagen ab; und eine Mindestlänge für Administrator- und Servicekonten von 14 Zeichen. Benutzer müssen die anfänglichen Kennwörter bei der ersten Anmeldung ändern. - Die Mitarbeiter sind verpflichtet, die Clean-Desk-Richtlinie einzuhalten. Die Bildschirme werden automatisch nach nicht mehr als 15 Minuten Inaktivität gesperrt. - Der Zugriff auf das interne Netzwerk ist auf autorisierte Firmengeräte beschränkt. - Auf allen Windows-Systemen und Linux-Servern, die für Malware-Infektionen anfällig sind, sind Anti-Malware-Systeme installiert. - Überwachung von Sicherheitsereignissen in Bezug auf interne und Produktionssysteme. - Es erfolgt keine Datenverarbeitung auf mobilen Geräten wie Handys oder Tablets. - Eine Richtlinie, die die Übertragung von Daten auf Wechselmedien verbietet. - Der Kunde bleibt für den Schutz der von ihm kontrollierten Anmeldeinformationen verantwortlich. - Ein Prozess für das technische Schwachstellenmanagement, einschließlich statischer Code-Analyse, regelmäßiger interner Schwachstellenbewertungen und Penetrationstests von Drittanbietern. Kunden können ihre eigenen technischen Bewertungen in Absprache mit Mapp durchführen. - Sichere Codierungsprinzipien gemäß OWASP Top 10, die regelmäßig an Softwareentwickler weitergegeben werden. - Produktionsnetzwerke werden effektiv durch Firewalls getrennt und geschützt. Keine Datenspeicherung in der Präsentationszone eines Netzwerks. - Ein hostbasiertes Einbruchmeldesystem ist vorhanden und wird überwacht (gilt für Mapp Engage). - Ein netzwerkbasiertes System zur Erkennung und Verhinderung von Eindringlingen ist vorhanden und wird überwacht (gilt für Mapp Engage). - Zusätzliche Sicherheitskontrollen gemäß den Informationssicherheitsrichtlinien von Mapp.
Datenzugriffskontrolle	**Implementierung**
Keine unbefugten Lese-, Kopier-, Änderungs- oder Löschvorgänge innerhalb von Informationssystemen	Die Maßnahmen werden gemäß ISO 27001:2013, insbesondere A.6.2.1, A.8.3.2, A.9.1.x, A.9.2.x, A.10.1.1-.2 und A.11.2.7, konzipiert, angewandt und überwacht. Diese schließen ein: - Vorgehensweise zum Verwalten von Benutzer- und privilegierten Zugriffsrechten in Übereinstimmung mit dem Beschäftigungszyklus auf der Grundlage eines zentralen Verzeichnisses. - Der Zugriff auf Daten ist auf autorisierte Gruppen beschränkt. - Die Vergabe privilegierter Zugriffsrechte erfolgt nach dem Prinzip der geringsten Rechte. - Es wurde ein integriertes Rollen- und Berechtigungsmodell implementiert, um die Anpassung des Kundenzugriffs nach dem Prinzip „Kenntnis nur, wenn nötig“ (Need-to-Know-Prinzip) zu ermöglichen. - Zentrale Verzeichniskonten werden halbjährlich überprüft. - Privilegierte Konten mit Zugang zur Infrastruktur werden mindestens halbjährlich überprüft. - Aktivitäten von Benutzern und privilegierten Konten sowie andere sicherheitsrelevante Ereignisse werden protokolliert und die Protokolle werden vor Verlust und Manipulation geschützt. - Privilegierte Kontoprotokolle werden regelmäßig manuell und/oder automatisch überprüft. - Der Kunde bleibt für anwendungsspezifische Zugriffsüberprüfungen verantwortlich.

	- Speichersysteme wenden die Verschlüsselung auf Dateisystem- oder Objektebene mit AES-256 (oder einem gleichwertigen Verfahren) an. - Verwendung von verschlüsselten Dateisystemen auf Unternehmens-Laptops. - Die Verwendung von Wechselmedien ist technisch eingeschränkt. - Verfahren zur sicheren Entsorgung von Geräten und zur unwiederbringlichen Löschung von Daten beim Offboarding von Kunden. - Zusätzliche Sicherheitskontrollen gemäß den Informationssicherheitsrichtlinien von Mapp.
Trennungskontrolle	**Implementierung**
Separate Verarbeitung von Daten, die für verschiedene Zwecke gesammelt wurden.	Die Maßnahmen werden gemäß ISO 27001:2013, insbesondere A.9.4.1, A.12.1.4 und A14.3.1, konzipiert, angewandt und überwacht. Diese schließen ein: - Logische Trennung von Mieterdaten in Produktions- und Serviceumgebungen. - Entwicklungs-, Test- und Produktionsumgebung sind getrennt. - Keine Verwendung von Produktionsdaten zu Testzwecken. - Zusätzliche Sicherheitskontrollen gemäß den Informationssicherheitsrichtlinien von Mapp.
Pseudonymisierung	**Implementierung**
Die Verarbeitung personenbezogener Daten erfolgt so, dass die Zuordnung von Daten zu einer bestimmten Person ohne zusätzliche Informationen, die durch geeignete technische oder organisatorische Maßnahmen getrennt aufbewahrt werden, verhindert wird.	Die Maßnahmen werden gemäß ISO 27001:2013, insbesondere A.6.1.5, A.14.1.1, A.14.2.1 und A.14.2.8, konzipiert, angewandt und überwacht. Diese schließen ein: - Die Entwicklungsverfahren umfassen Planungsgrundsätze für die Minimierung von Daten, die Einschränkung der Erhebung und den standardmäßigen Datenschutz, einschließlich der Forderung nach Pseudonymisierung, wo dies möglich ist. - Verhaltensdaten werden in pseudonymisierter Form gespeichert und, soweit möglich, vom entsprechenden Kontaktprofil getrennt (gilt für Mapp Engage). - Das Online-Tracking ist standardmäßig pseudonym (gilt für Mapp Acquire). - Systemprotokolle werden soweit möglich anonymisiert. - Zusätzliche Sicherheitskontrollen gemäß den Informationssicherheitsrichtlinien von Mapp.
2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)	
Übertragungskontrolle	**Implementierung**
Keine unbefugten Lese-, Kopier-, Änderungs- oder Löschvorgänge während der Übertragung oder des Transports.	Die Maßnahmen werden gemäß ISO 27001:2013, insbesondere A.8.3.3, A.9.1.x und A.10.1.1-2, konzipiert, angewandt und überwacht. Diese schließen ein: - Daten, die über öffentliche Datenübertragungsnetze übertragen werden, werden durch branchenübliche Standards und Algorithmen wie TLS oder SSH mit sicheren Konfigurationen wirksam geschützt. - Daten werden weder auf Papier noch auf mobilen Speichergeräten physisch übertragen. - Für die interne und externe Kommunikation sind sichere elektronische Nachrichtenfunktionen vorhanden. Wir gestatten jedoch nicht die Übertragung von (unter diesem DVV verarbeiteten) Daten per E-Mail. Wenn Kunden Daten per E-Mail senden oder Mapp dazu anweisen, wird der Kunde zur Rechenschaft gezogen. - Zusätzliche Sicherheitskontrollen gemäß den Informationssicherheitsrichtlinien von Mapp.
Eingabekontrolle	**Implementierung**
Es wird festgestellt, ob personenbezogene Daten in Informationssystemen eingegeben, geändert oder gelöscht wurden.	Die Maßnahmen werden gemäß ISO 27001:2013, insbesondere A.12.2.1, A.12.4.1-.4 und A.12.6.1, konzipiert, angewandt und überwacht. Diese schließen ein: - Benutzer- und privilegierte Konten sind eindeutig und identifizierbar, sofern dies technisch machbar ist. Ausnahme: Root-Konten, die streng kontrolliert werden. - Der Zugriff auf Daten auf Anwendungs- und Datenbankebene wird umfassend protokolliert und die Protokolle vor Verlust und Manipulation geschützt. - Protokollquellen verwenden eine synchronisierte Zeitquelle (NTP). - Ein hostbasiertes Einbruchmeldesystem ist vorhanden und wird überwacht (gilt für Mapp Engage). - Ein netzwerkbasiertes System zur Erkennung und Verhinderung von Eindringlingen ist vorhanden und wird überwacht (gilt für Mapp Engage). - Ein Prozess für das technische Schwachstellenmanagement, einschließlich statischer Code-Analyse, regelmäßiger interner Schwachstellenbewertungen und Penetrationstests von Drittanbietern. Kunden können ihre eigenen technischen Bewertungen in Absprache mit Mapp durchführen. - Auf allen Windows-Systemen und Linux-Servern, die für Malware-Infektionen anfällig sind, sind Anti-Malware-Systeme installiert. - Zusätzliche Sicherheitskontrollen gemäß den Informationssicherheitsrichtlinien von Mapp.
3. Verfügbarkeit und Ausfallsicherheit (Art. 32 Abs. 1 lit. b & c DSGVO)	
Verfügbarkeitskontrolle	**Implementierung**
Schutz vor versehentlichem oder vorsätzlichem Verlust oder Zerstörung.	Die Maßnahmen werden gemäß ISO 27001:2013, insbesondere A.12.1.2, A.12.1.3, A.12.2.1, A.12.3.1, A.12.4.1, A.12.6.1, A.17.1.x und A.17.2.1, konzipiert, angewandt und überwacht. Diese schließen ein: - Erkennungs- und Unterdrückungssysteme werden in Rechenzentren implementiert, um Risiken im Zusammenhang mit Feuer und Wasser zu minimieren. Diese werden mindestens jährlich gewartet und getestet. - Die Geräte sind so aufgestellt, dass sie wirksam gegen Umweltschäden oder Sabotage geschützt sind. - Wichtige Systemkomponenten (z. B. Webserver oder Load Balancer) werden redundant ausgelegt, um einzelne Fehlerquellen zu vermeiden. - Die Daten werden täglich repliziert und relationale Daten werden täglich gesichert. - Ein Prozess für das technische Schwachstellenmanagement, einschließlich statischer Code-Analyse, regelmäßiger interner Schwachstellenbewertungen und Penetrationstests von Drittanbietern. Kunden können ihre eigenen technischen Bewertungen in Absprache mit Mapp durchführen. - Planung und Überwachung der Rechen-, Speicher- und Netzwerkkapazität. - Überwachung des Systemzustands und der Systemverfügbarkeit. - Verfahren für das Änderungsmanagement im normalen Betrieb und in Notfällen. - Auf allen Windows-Systemen und Linux-Servern, die für Malware-Infektionen anfällig sind, sind Anti-Malware-Systeme installiert.

	- Ein netzwerkbasiertes System zur Erkennung und Verhinderung von Eindringlingen zum Schutz vor Denial-of-Service-Angriffen ist vorhanden und wird überwacht (gilt für Mapp Engage). - Zusätzliche Sicherheitskontrollen gemäß den Informationssicherheitsrichtlinien von Mapp.
Wiederherstellungsfähigkeit	**Implementierung**
Fähigkeit zur Wiederherstellung innerhalb eines angemessenen Zeitraums nach einem störenden Ereignis.	Die Maßnahmen werden gemäß ISO 27001:2013, insbesondere A.12.3.1, A.17.1.x und A.17.2.1, konzipiert, angewandt und überwacht. Diese schließen ein: - Geschäftskontinuitäts- und Notfallwiederherstellungspläne für Rechenzentren und Softwaredienste werden beibehalten und regelmäßig getestet. - USV- und Dieselgeneratoren werden in Rechenzentren implementiert, um Stromausfälle von mindestens 24 Stunden zu überstehen. Diese werden mindestens jährlich gewartet und getestet. - Die Daten werden täglich repliziert und relationale Daten werden täglich gesichert. Wiederherstellungsverfahren für Sicherungskopien werden regelmäßig getestet. - Zusätzliche Sicherheitskontrollen gemäß den Informationssicherheitsrichtlinien von Mapp.
4. Verfahren zur regelmäßigen Überprüfung der Wirksamkeit von Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abschn. 1 & 2 DSGVO)	
Datenschutzmanagement	**Implementierung**
Systematischer Ansatz für das Datenschutzmanagement.	Betrieb eines Informationssicherheits- und Datenschutzmanagementsystems gemäß ISO 27001:2013, ISO 27002:2013 und ISO 27018:2014. Dies beinhaltet: - Klar definierte und kommunizierte Rollen und Verantwortlichkeiten in Bezug auf Informationssicherheit und Datenschutz, einschließlich, aber nicht beschränkt auf: Informationssicherheitsbeauftragter und Datenschutzbeauftragter. - Governance-Verfahren für das Informationsrisikomanagement, die Aufrechterhaltung und Kommunikation von Richtlinien, interne und externe Compliance-Bewertungen, Managementberichterstattung und -prüfung sowie die Nachverfolgung kontinuierlicher Verbesserungen. - Informationssicherheits- und Datenschutzaufklärungsprogramm mit obligatorischen Neueinstellungen und jährlichen Auffrischungsschulungen sowie zusätzlichen Aufklärungsmaßnahmen. - Jährliche unabhängige Prüfung des Informationssicherheits- und Datenschutzmanagementsystems. - Zusätzliche Sicherheitskontrollen gemäß den Informationssicherheitsrichtlinien von Mapp.
Vorfallreaktions-Management	**Implementierung**
Systematischer Ansatz für die Verwaltung von Vorfällen.	Die Maßnahmen werden gemäß ISO 27001:2013, insbesondere A.16.1.x, konzipiert, angewandt und überwacht. Diese schließen ein: - Das Verfahren zur Meldung von Vorfällen wird allen Mitarbeitern über eine Schulung vermittelt. - Verfahren zur Reaktion auf Vorfälle, einschließlich Überprüfung, Klassifizierung, Eindämmung, Beseitigung und Wiederherstellung; Beispielszenarios für ausgewählte Arten von Vorfällen. - Meldeverfahren gemäß den gesetzlichen und vertraglichen Bestimmungen. - Post-Mortem-Analyse für bedeutsame Vorfälle erforderlich. - Zusätzliche Sicherheitskontrollen gemäß den Informationssicherheitsrichtlinien von Mapp.
Standardmäßiger Datenschutz	**Implementierung**
Die Einhaltung des Datenschutzes sollte über den gesamten Lebenszyklus von Technologien und Verfahren hinweg gewährleistet sein.	Die Maßnahmen werden gemäß ISO 27001:2013, insbesondere A.8.1.3, A.13.2.1 und A.14.2.5, konzipiert, angewandt und überwacht. Diese schließen ein: - Zu den Entwicklungsverfahren gehören standardmäßig Planungsgrundsätze für die Minimierung von Daten, die Einschränkung der Erhebung und der Datenschutz. Unsere Software-Dienstleistungen sind in hohem Maße anpassbar. Konfigurationsmöglichkeiten finden Sie in der jeweiligen Online-Hilfe. - Die Kunden bleiben verantwortlich für die gesetzliche und datenschutzfreundliche Nutzung der Software-Dienstleistungen von Mapp. Darüber hinaus gelten folgende Nutzungsbedingungen: https://mapp.com/acceptable-use-policy/
Auftragskontrolle (Art. 28 DSGVO)	**Implementierung**
Ohne Anweisung des Verantwortlichen erfolgt keine Datenverarbeitung.	Die Maßnahmen werden gemäß ISO 27001:2013, insbesondere A.8.3.2, A.11.2.7, A.13.2.1 und A.18.1.1, konzipiert, angewandt und überwacht. Diese schließen ein: - Mapp verarbeitet Daten nur gemäß den Anweisungen des Kunden, d. h. basierend auf vertraglichen Vereinbarungen, Aufträgen oder zusätzlichen Anweisungen. Kunden sollten Anweisungen nur in schriftlicher Form erteilen oder schriftlich bestätigen, sofern sie in mündlicher Form erfolgt sind. - Verfahren zur sicheren Entsorgung von Geräten und zur unwiederbringlichen Löschung von Daten beim Offboarding von Kunden. - Wirksame Einschränkung der Verarbeitung von Daten, die für rechtliche Zwecke aufbewahrt werden durch Verschlüsselung von Sicherungsdateien, Verschlüsselung von Dateisystemen, strenge Zugriffskontrollen, Audit-Protokollierung und ticketbasierte Wiederherstellungsverfahren.

ANHANG 3: DIGITALE LISTE DER VERBUNDENEN UNTERNEHMEN VON MAPP UND SUBUNTERNEHMER

Unterauftragsverarbeiter	Verarbeitungsort (und rechtliche Schutzbestimmungen, falls außerhalb des EWR)	Zweck
Mapp Digital Germany GmbH	Deutschland	Intern: Support & Dienstleistungen, F & E
Mapp Digital France S.A.S.	Frankreich	Intern: Support & Dienstleistungen
Mapp Digital Italy SrL.	Italien	Intern: Support & Dienstleistungen
Mapp Digital UK Ltd	Vereinigtes Königreich*	Intern: Support & Dienstleistungen
Mapp Digital Poland sp. z.o.o.	Polen	Intern: F & E
Mapp Digital Netherlands B.V.	Niederlande	Intern: F & E
Mapp Digital US, LLC	USA (EU-Standardvertragsklauseln & Zertifiziert nach dem EU-US-Datenschutzschild)	Intern: Support & Dienstleistungen, F & E [Nur Mapp Empower]
Aprimo/MEMO Marketing Operations Philippines Inc	Philippinen (Standardvertragsklauseln)	Intern: Support & Dienstleistungen
Aprimo Australia Pty Ltd	Australien (Standardvertragsklauseln)	Intern: Support
Pythian Group Inc.	Kanada (Angemessenheitsentscheidung)	Extern: F & E [Nur Mapp Empower]
Amazon Web Services, Inc.	Deutschland & Irland	Extern: Rechenzentrumsinfrastruktur
Amazon Web Services, Inc.	USA (Standardvertragsklauseln)	Extern: Rechenzentrumsinfrastruktur [Nur Mapp Empower]
Google, LLC.	Hauptverarbeitung und Datenspeicherung in Belgien. Weltweit verteilte Sammlung technisch erforderlich aufgrund der Art der Dienstleistungen (Standardvertragsklauseln)	Extern: Rechenzentrumsinfrastruktur [Nur Mapp Acquire]
Global Access Internet Services GmbH	Deutschland	Extern: Rechenzentrumsinfrastruktur
CLX Networks AB	Schweden & USA (Standardvertragsklauseln)	Extern: SMS-Nachrichten [Mapp Engage, optional]
R & D Communications SrL	Italien	Extern: SMS-Nachrichten [Mapp Engage, optional]
Mitto AG	Deutschland & Schweiz (Angemessenheitsentscheidung)	Extern: SMS-Nachrichten [Mapp Engage, optional]
WebTrekk GmbH	Deutschland & Italien	Intern: Mapp Intelligence
Webtrekk Analytics SL	Spanien	Intern: Mapp Intelligence

*Für den Fall, dass Großbritannien im Zuge des Brexit ein Drittland wird, führt Mapp Standardvertragsklauseln aus, um die künftige Einhaltung der grenzüberschreitenden Übermittlung personenbezogener Daten sicherzustellen.

ZUSÄTZLICHE ANBIETER KÖNNEN FÜR BESTIMMTE DIENSTLEISTUNGEN ODER KUNDEN MIT ERHÖHTEN SUPPORT-ANFORDERUNGEN NOTWENDIG SEIN. DIESE ANBIETER WERDEN IN DER FÜR DIESE DIENSTLEISTUNGEN ANWENDBAREN LEISTUNGSBESCHREIBUNG BENANNT.