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 („**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 DPA schließt der Kunde diesen DPA im eigenen Namen und, soweit dies nach den geltenden Datenschutzgesetzen erforderlich ist, auch im Namen und im Auftrag seiner verbundenen Unternehmen ab.
Wie dieser DPA ausgeführt wird:

- Wenn dieser DPA 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; (4) den DPA unterzeichnen; und (5) per E-Mail senden an: privacy@mapp.com.
- Mit Erhalt des vollständig ausgeführten DPA wird dieser rechtsverbindlich und Gegenstand des MSA.
- Wenn der Kunde Änderungen an diesem DPA 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 diesen DPA zu binden. Dieser DPA endet automatisch mit Beendigung des MSA.

1. DEFINITIONEN

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

1.2 **Datenschutzgesetze** sind alle Gesetze, Verordnungen und Bestimmungen, die in einer relevanten Gerichtsbarkeit bestehen können, die bei der Verarbeitung betreffender personenbezogener Daten anwendbar sind, einschließlich: die Verordnung der Europäischen Union zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (die „**Datenschutz-Grundverordnung**“ oder „**DSGVO**“), 2002/58/EG, der California Consumer Privacy Act („CCPA“) sowie alle anwendbaren zugehörigen oder ergänzenden Datenschutzgesetze oder -verordnungen, die jeweils von Zeit zu Zeit aktualisiert, geändert oder ersetzt werden.

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

1.4 **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.

1.5 **Dienstleistungen**, die in Anhang 4 ausführlicher beschrieben sind, beziehen sich auf die spezifischen Mapp-Dienstleistungen, die gemäß MSA von Mapp gekauft wurden.

1.6 Alle anderen großgeschriebenen Begriffe haben die im anwendbaren Datenschutzgesetz oder MSA festgelegte Bedeutung.

2. DATENVERARBEITUNG

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

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

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

2.4 Mapp, in seiner Rolle als Dienstleister, verarbeitet personenbezogene Daten nur im Auftrag und in Übereinstimmung mit den dokumentierten Anweisungen des Kunden für folgende geschäftliche Zwecke: (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 DPA; und (v) die Erhebung nicht identifizierbarer Statistiken.

2.5 Mapp fungiert als Dienstleister für den Kunden und wird die personenbezogenen Daten nicht anderweitig speichern, verwenden oder weitergeben, außer wie in Abschnitt 2.4 oben beschrieben. Mapp erkennt ferner an, dass es keine personenbezogenen Daten verkauft, die in Übereinstimmung mit den Dienstleistungen gesammelt wurden.

2.6 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 den anwendbaren Datenschutzgesetzen 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.

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 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 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 unter www.mapp.com/contracts zu finden ist. Diese Unterauftragsverarbeiter müssen vom Kunden angenommen und genehmigt werden. Mit der Unterzeichnung dieses DPA 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 vernünftigerweise erforderlich ist, um Unterstützung zu leisten, technische Projekte durchzuführen oder andere Arten von Dienstleistungen im Rahmen des MSA zu erbringen, jedoch vorausgesetzt, dass der Kunde in der EU ansässig ist und entweder: (i) diese Standorte von der Europäischen Kommission als angemessenen Datenschutz bietend anerkannt werden; oder (ii) Mapp die EU-Standardvertragsklauseln mit solchen verbundenen Unternehmen und/oder anderen Unterauftragsverarbeitern unterzeichnet hat.

6.2 Mapp hat mit jedem Unterauftragsverarbeiter eine schriftliche Vereinbarung getroffen, die Datenschutzverpflichtungen enthält, die keinen geringeren Schutzumfang bieten als die in diesem DPA 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 haften würde, wenn es die Dienste des jeweiligen Unterauftragsverarbeiters gemäß den

Bestimmungen dieses DPA direkt ausführen würde, 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, diesen DPA 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 der unterschiedlichen Wahrscheinlichkeit und Schwere des Risikos 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 DPA. 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 vernünftigerweise 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 dreißig (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, 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 DPA erforderlich sind, und ermöglicht Audits durch den Kunden oder einen vom Kunden beauftragten externen Auditor in Bezug auf die Verarbeitung personenbezogener Daten und trägt dazu bei, dass diese durchgeführt werden können. 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 Auditor 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 (10) Werktagen durchführen. Die Überprüfung darf nicht länger als einen (1) 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 Auditor 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 Auditoren 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.

HAFTUNG

10.1 Die Haftung jeder Partei aus oder im Zusammenhang mit diesem DPA und allen Datenverarbeitungsverträgen zwischen verbundenen Unternehmen und Mapp, sei es aus Vertrag, 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 Datenverarbeitungsverträge 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 Datenverarbeitungsvertrag insgesamt für alle Ansprüche sowohl aus dem MSA als auch aus allen Datenverarbeitungsverträgen, die im Rahmen des MSA abgeschlossen wurden.

10.3 Wenn eine betroffene Person Ansprüche gegenüber einer Partei dieses DPA gemäß des anwendbaren Datenschutzgesetzes geltend macht, leistet die andere Partei bei der Abwehr solcher Ansprüche Unterstützung, soweit dies möglich ist.

Anhang 1: **Betroffene Personen und Kategorien**
Anhang 2: **Sicherheitsanhang**
Anhang 3: **Unterauftragsverarbeiter**
Anhang 4: **Beschreibung der Mapp-Dienstleistungen**

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

ANHANG 1: BETROFFENE PERSONEN UND KATEGORIEN

Betroffene Personen. Die verarbeiteten personenbezogenen Daten betreffen folgende Kategorien von betroffenen Personen:

- 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 SICHERHEITSMASSNAHMEN GEMÄß ART. 28 (3) DSGVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. a &b DSGVO und Art. 25 Abs. 1 DSGVO)

Physische Zugangskontrolle	**Implementierung**
Mapp unterhält geeignete Maßnahmen, um zu verhindern, dass Unbefugte Zugang zu den Datenverarbeitungsanlagen erhalten, in denen die personenbezogenen Daten verarbeitet oder genutzt werden.	- Eingerichtete Sicherheitsbereiche mit geschützten Ein-/Ausreisepunkten. - Berechtigungsverfahren für Mitarbeiter und Dritte. - Besuchermanagementverfahren, um eine ordnungsgemäße Authentifizierung und Überwachung zu gewährleisten. - CCTV-Überwachung für alle Rechenzentren und primären Bürostandorte, die alle Ein- und Ausgänge überwachen. - Für den Zugriff auf Rechenzentrumsgeräte sind mindestens zwei verschiedene Authentifizierungsfaktoren erforderlich. - Die Geräte sind so angeordnet, dass sie effektiv vor unbefugter Offenlegung von Informationen geschützt sind. - Sicherheitsalarmsysteme für Rechenzentren und primäre Bürostandorte. - Bemannte Empfangs- und/oder Sicherheitspersonal in Rechenzentren. - Verfahren für die sichere Schlüsselkartenzuweisung und/oder biometrische Registrierung. - Elektronisches Zugangssystem, das alle Zugriffe auf Rechenzentren und primäre Bürostandorte protokolliert.
Systemzugriffskontrolle	**Implementierung**
Mapp wird geeignete Maßnahmen ergreifen, um zu verhindern, dass seine Systeme zur Verarbeitung personenbezogener Daten von Unbefugten genutzt werden.	- Richtlinie betreffend Zugriffskontrolle wird gewahrt. - Verfahren zur Verwaltung von Benutzer- und privilegierten Konten entsprechend dem Beschäftigungslebenszyklus auf der Grundlage eines zentralen Verzeichnisses. - Multi-Faktor-Authentifizierung ist für privilegierten Zugriff auf die Infrastruktur erforderlich. - Passwortrichtlinie, die technisch mindestens 8 Zeichen erfordert; das Passwort muss mindestens drei der folgenden vier Elemente enthalten: Großbuchstabe(n), Kleinbuchstabe(n), Zahl(en), Symbol(e); ein Passwort, das sich von den 8 zuvor verwendeten Passwörtern unterscheidet; interne Benutzerkennwörter werden nach Ablauf und möglicher Kompromittierung zurückgesetzt. Administrator- und Dienstkonten haben eine Passwortmindestlänge von 14 Zeichen. Benutzer müssen die anfänglichen Kennwörter bei der ersten Anmeldung ändern. - Option zum Aktivieren der Multi-Faktor-Authentifizierung oder des einmaligen Anmeldens über eine benutzerdefinierte Identitätsquelle, um die Sicherheit des Kundenzugriffs zu erhöhen (gilt für Mapp Engage, Mapp Intelligence und Mapp Acquire). - Die Mitarbeiter sind zur Einhaltung der Clean Desk-Richtlinien verpflichtet. Bildschirme werden nach mehr als 15 Minuten Inaktivität automatisch gesperrt. - Der Zugriff auf das interne Netzwerk von Mapp ist auf autorisierte Unternehmensgeräte beschränkt. - Anti-Malware-Systeme sind auf allen Windows-Systemen und Linux-Servern installiert, die anfällig für Malware-Infektionen sind. - Überwachung von Sicherheitsereignissen im Zusammenhang mit internen und Mapp Cloud-Produktionssystemen. - Keine Datenverarbeitung auf mobilen Endgeräten wie Mobiltelefonen oder Tablets. - Richtlinie, die die Übertragung von Daten auf Wechselmedien verbietet. - Der Kunde bleibt für den Schutz der GUI- und API-Anmeldeinformationen unter seiner Kontrolle verantwortlich. - Prozess für das technische Schwachstellenmanagement, einschließlich der Härtung der physischen und virtuellen Serverinfrastruktur, statischer Codeanalyse, regelmäßiger interner Schwachstellenbewertungen, 3rd-Party-Penetrationstests und rechtzeitiger Befreiung von Sicherheitsschwachstellen nach einem risikobasierten Ansatz. Kunden können in Absprache mit Mapp eigene technische Bewertungen durchführen. - Sichere Codierungsprinzipien nach OWASP Top 10, zu denen die Mapp-Softwareentwickler regelmäßig geschult werden. - Physische und virtuelle Produktionsnetzwerke werden streng kontrolliert, effektiv getrennt und durch Firewalls geschützt. Keine Datenspeicherung in der Präsentationszone eines Netzwerks. - Netzwerkbasiertes Intrusion Detection- und/oder Prevention-System vorhanden und überwacht (gilt für Mapp Engage und Mapp Intelligence). - Host-basiertes Intrusion Detection-System an Ort und Stelle und überwacht (gilt für Mapp Engage).
Datenzugriffskontrolle	**Implementierung**
Mapp trifft geeignete Maßnahmen, um unbefugte Lese-, Kopier-, Änderungs- oder Löschvorgänge innerhalb von Informationssystemen zu verhindern.	- Verfahren zur Verwaltung von Mapp-Benutzer- und privilegierten Zugriffsrechten entsprechend dem Beschäftigungslebenszyklus basierend auf einem zentralen Verzeichnis. - Zugriff auf Daten ist auf autorisierte Gruppen beschränkt. - Die Vergabe privilegierter Zugriffsrechte folgt dem Least-Privilege-Prinzip. - Für Mapp Cloud implementiertes abgestuftes Rollen- und Berechtigungsmodell, um die Anpassung des Kundenzugriffs nach dem Erforderlichkeitsprinzip zu ermöglichen. - Die zentralen Mapp-Verzeichniskonten werden halbjährlich überprüft. - Mapp überprüft privilegierte Konten und Berechtigungen mit Zugang zur Infrastruktur mindestens halbjährlich. - Benutzer- und privilegierte Kontoaktivitäten sowie andere sicherheitsrelevante Ereignisse werden protokolliert und vor Verlust und Manipulation geschützt. - Mapp überprüft die Aktivitäten privilegierter Konten regelmäßig, manuell und/oder automatisch. - Der Kunde bleibt für anwendungsspezifische Zugriffsprüfungen, die Richtigkeit der Zugriffskontrollliste und den Schutz der zugewiesenen Anmeldeinformationen verantwortlich. - Speichersysteme wenden Dateisystem- oder Objektverschlüsselung mit AES-256 (oder gleichwertig) an (gilt für Mapp Engage und Mapp Acquire). - Verwendung von verschlüsselten Dateisystemen auf Firmenlaptops. - Verwendung von Wechselmedien ist technisch eingeschränkt.

	- Verfahren für die sichere Entsorgung von Geräten und die nicht wiederherstellbare Löschung von Daten während des Offboardings des Kunden.
Trennungskontrolle	**Implementierung**
Mapp unterhält geeignete Maßnahmen, um die Verarbeitung von Daten, die für verschiedene Zwecke erhoben wurden, zu trennen.	- Logische Trennung von Mandantendaten in Produktions- und Serviceumgebungen entweder auf Datenmodell- oder Datenbankschemaebene. - Entwicklungs- und Testsysteme sind von Produktionsumgebungen getrennt. - Produktionsdaten werden nicht zu Testzwecken verwendet.
Pseudonymisierung / Anonymisierung	**Implementierung**
Verarbeitung personenbezogener Daten in einer Weise, die die Zuordnung von Daten zu einer bestimmten Person ohne zusätzliche Informationen, die durch geeignete technische oder organisatorische Maßnahmen getrennt aufbewahrt werden, unmöglich macht.	- Die Entwicklungsverfahren umfassen Designprinzipien für Datenminimierung, Sammlungsbeschränkung und Privacy by default, einschließlich der Anforderung einer Pseudonymisierung, wo dies möglich ist. - Verhaltensdaten werden in pseudonymisierter Form und nach Möglichkeit getrennt vom entsprechenden Kontaktprofil gespeichert (gilt für Mapp Engage). - Online-Tracking ist standardmäßig pseudonym, mit der Möglichkeit zur Pseudonymisierung und Anonymisierung gesammelter benutzerdefinierter Attribute z.B. durch Hashing oder Kürzung (gilt für Mapp Acquire und Mapp Intelligence). - Systemprotokolle werden soweit möglich anonymisiert. - Wenn die Servicefunktionalität datengesteuerte Analysen und Vorhersagen umfasst, werden die Daten effektiv anonymisiert, bevor die erforderlichen Berechnungen und Verarbeitungen ausgeführt werden.
2. Integrität (Art. 32 Abs. 1 lit.b DSGVO)	
Übergangskontrolle	**Implementierung**
Mapp trifft geeignete Maßnahmen, um unbefugte Lese-, Kopier-, Änderungs- oder Löschvorgänge während der Übermittlung oder des Transports zu verhindern.	- Daten, die über öffentliche Datenübertragungsnetze übertragen werden, werden durch bewährte Industriestandards 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 gibt es sichere elektronische Nachrichtenfunktionen. Mapp gestattet keine Übertragung von Daten (die im Rahmen dieser DPA verarbeitet werden) per E-Mail. Wenn Kunden Daten per E-Mail senden oder Mapp dazu anweisen, ist der Kunde für mögliche Folgen verantwortlich. - Option zum Schutz der Integrität von E-Mail-Domänen mit DMARC (gilt für Mapp Engage).
Eingabekontrolle	**Implementierung**
Mapp unterhält geeignete Maßnahmen, um festzustellen, ob personenbezogene Daten in Informationssysteme eingegeben, geändert oder gelöscht wurden.	- 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). - Host-basiertes Intrusion Detection-System an Ort und Stelle und überwacht (gilt für Mapp Engage). - Netzwerkbasiertes Intrusion Detection- und/oder Prevention-System vorhanden und überwacht (gilt für Mapp Engage und Mapp Intelligence). - Prozess für das technische Schwachstellenmanagement, einschließlich der Härtung der physischen und virtuellen Serverinfrastruktur, statischer Codeanalyse, regelmäßiger interner Schwachstellenbewertungen, 3rd-Party-Penetrationstests und rechtzeitiger Befreiung von Sicherheitsschwachstellen nach einem risikobasierten Ansatz. Kunden können in Absprache mit Mapp eigene technische Bewertungen durchführen. - Anti-Malware-Systeme, die auf allen Windows-Systemen und Linux-Servern installiert sind, die anfällig für Malware-Infektionen sind.
3. Verfügbarkeit und Ausfallsicherheit (Art. 32 Abs. 1 lit.b & c DSGVO)	
Verfügbarkeitskontrolle	**Implementierung**
Mapp unterhält geeignete Maßnahmen zum Schutz vor versehentlichem oder vorsätzlichem Verlust oder Zerstörung.	- Erkennungs- und Unterdrückungssysteme werden in Rechenzentren implementiert, um Risiken im Zusammenhang mit Feuer und Wasser zu minimieren. Diese werden mindestens einmal jährlich gewartet und getestet. - Die Geräte ist so aufgestellt, dass sie wirksam gegen Umweltschäden oder Sabotage geschützt sind. - Implementierte Sicherheitsmechanismen und Redundanzen, um Geräte vor Ausgängen von Versorgungsunternehmen zu schützen. Batteriesysteme und Dieselgeneratoren mit mindestens 24h Kraftstoffversorgung werden mehrmals im Jahr implementiert und getestet, um eine unterbrechungsfreie Stromversorgung zu gewährleisten. - Kritische Systemkomponenten (z.B. Webserver oder Load Balancer) sind redundant ausgelegt, um Single Points of Failure zu vermeiden. - Daten werden täglich repliziert und relationale Daten gesichert. - Prozess für das technische Schwachstellenmanagement, einschließlich der Härtung der physischen und virtuellen Serverinfrastruktur, statischer Codeanalyse, regelmäßiger interner Schwachstellenbewertungen, 3rd-Party-Penetrationstests und rechtzeitiger Befreiung von Sicherheitsschwachstellen nach einem risikobasierten Ansatz. Kunden können in Absprache mit Mapp eigene technische Bewertungen durchführen. - Planung und Überwachung der Rechen-, Speicher- und Netzwerkkapazität. - Überwachung des Systemzustands und der Verfügbarkeit. - Verfahren für das Änderungsmanagement während des normalen Betriebs und in Notfällen.

	- Auf allen Windows-Systemen und Linux-Servern, die anfällig für Malware-Infektionen sind, Anti-Malware-Systeme installiert. - Netzwerkbasiertes Intrusion Detection- und/oder Prevention-System ist vorhanden und wird überwacht (gilt für Mapp Engage und Mapp Intelligence).
Wiederherstellungsfähigkeit	**Implementierung**
Mapp unterhält geeignete Maßnahmen, um die Fähigkeit zur Wiederherstellung innerhalb eines angemessenen Zeitrahmens nach einem störenden Ereignis aufrechtzuerhalten.	- Business Continuity Pläne für Rechenzentren und Software-Services werden gepflegt und regelmäßig getestet. - USV- und Dieselgeneratoren werden in Rechenzentren implementiert, um Stromausfälle von mindestens 24 Stunden zu überstehen. Diese werden mindestens einmal jährlich gewartet und getestet. - Daten werden repliziert und relationale Daten täglich an entfernten Standorten gesichert. Backup-Recovery-Verfahren werden regelmäßig getestet.

4. Verfahren zur regelmäßigen Überprüfung der Wirksamkeit von Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 & 2 DSGVO)	
Datenschutz-Management	**Implementierung**
Mapp verfolgt beim Management des Datenschutzes einen systematischen Ansatz.	- 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 Pflege und Kommunikation von Richtlinien, interne und externe Compliance-Bewertungen, Managementberichte und -überprüfungen sowie die Verfolgung kontinuierlicher Verbesserungen. - Informationssicherheits- und Datenschutzbewusstseinsprogramm, einschließlich obligatorischer Neueinstellungen und jährlichen Auffrischungsschulungen sowie zusätzlicher Sensibilisierungsmaßnahmen. - Jährliche unabhängige Prüfung des Informationssicherheits- und Datenschutzmanagementsystems
Vorfallreaktions-Management	**Implementierung**
Mapp verfolgt einen systematischen Ansatz für das Management von Vorfällen.	- Verfahren zur Meldung von Vorfällen, wird allen Mitarbeitern über eine Schulung vermittelt. - Verfahren für die Reaktion auf Sicherheitsvorfälle, einschließlich Überprüfung, Einstufung, Eindämmung, Tilgung und Wiederherstellung; Playbooks, die für ausgewählte Arten von Vorfällen verwaltet werden. - Meldeverfahren gemäß den gesetzlichen und vertraglichen Anforderungen. - Post-Mortem-Analyse für signifikante Vorfälle erforderlich. - Zusätzliche Sicherheitskontrollen gemäß den Informationssicherheitsrichtlinien von Mapp.
Standardmässiger Datenschutz	**Implementierung**
Mapp unterhält geeignete Maßnahmen, um sicherzustellen, dass die Einhaltung des data-Schutzes während des gesamten Lebenszyklus von Technologien und Verfahren eingebettet ist.	- Die Entwicklungsverfahren umfassen standardmäßig Planungsgrundsätze für Datenminimierung, Sammlungsbeschränkung und Datenschutz. Unsere Software-Services /Anwendungen sind bis zu einem gewissen Grad anpassbar. Optionen zur Konfiguration finden Sie in der jeweiligen Online-Hilfe. - Die Kunden bleiben für die rechtmäßige und datenschutzfreundliche Nutzung der Softwaredienste von Mapp verantwortlich. Darüber hinaus gilt die Richtlinie zur akzeptablen Nutzung: https://mapp.com/acceptable-use-policy/
Auftragskontrolle (Art. 28 DSGVO)	**Implementierung**
Mapp ergreift geeignete Maßnahmen, um eine Datenverarbeitung ohne Weisung des Verantwortlichen zu verhindern.	- Mapp verarbeitet Daten nur auf Grundlage der Anweisungen des Kunden, d.h. auf der Grundlage vertraglicher Vereinbarungen, Bestellungen oder zusätzlicher Anweisungen. Weisungen sollten Kunden nur in schriftlicher Form erteilen oder schriftlich bestätigen, wenn sie mündlich erfolgen. - Mapp wird auf Anfragen der betroffenen Person nicht antworten, sondern diese an den Kunden weiterleiten. - Verfahren für die sichere Entsorgung von Geräten und die nicht wiederherstellbare Löschung von Daten während des Offboardings des Kunden. - Effektive Einschränkung der Verarbeitung von Daten, die aus rechtlichen Gründen aufbewahrt werden, durch Verschlüsselung von Sicherungsdateien, Verschlüsselung von Dateisystemen, strenge Zugriffskontrollen, Audit-Protokollierung und ticketbasierte Wiederherstellungsverfahren.

ANHANG 3: UNTERAUFTRAGSVERARBEITER

	Unterauftragsverarbeiter und Adressen	Verarbeitungsort und geeignete Garantien (Art. 46 DSGVO, falls zutreffend)	Zweck /Anwendungsbereich
MAPP ENTITIES	**Mapp Digital Germany GmbH** Sandstr. 3, München, Deutschland	Europäische Union (Deutschland)	Entwicklung & Softwarewartung, Support & Dienstleistungen
	Mapp Digital France S.A.S. 33 rue Lafayette, 75009 Paris, Frankreich	Europäische Union (Frankreich)	Support & Dienstleistungen
	Mapp Digital Italy SrL Via Pietro Orseolo, 12, Mailand, Italien	Europäische Union (Italien)	Support & Dienstleistungen
	Webtrekk GmbH Robert-Koch-Platz 4, Berlin, Deutschland	Europäische Union (Deutschland & Italien)	Entwicklung & Softwarewartung, Support & Dienstleistungen
	Mapp Digital Poland sp. z.o.o. ul. Kamienskiego 47, Krakau, Polen	Polen	Entwicklung & Softwarewartung
	Mapp Digital Netherlands B.V. Lichttoren 32, BJ Eindhoven, Niederlande	Niederlande	Entwicklung & Softwarewartung
	Mapp Digital UK Ltd 6th Floor, 95 Gresham Street, London, Großbritannien	Großbritannien (Angemessenheitsentscheidung)	Support & Dienstleistungen
	Mapp Digital US, LLC 3655 Nobel Dr Suite 500, San Diego, Kalifornien, USA	USA (Standardvertragsklauseln)	Support & Dienstleistungen [optional für Europäische Kunden]
EXTERNE DRITTE	**Global Access Internet Services GmbH** Potsdamer Str. 3, München, Deutschland	Europäische Union (Deutschland)	Rechenzentrumsinfrastruktur
	IP Exchange GmbH Am Tower 5, Nürnberg, Deutschland	Europäische Union (Deutschland)	Rechenzentrumsinfrastruktur
	Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, Luxemburg	Europäische Union (Deutschland & Irland)	Rechenzentrumsinfrastruktur
	Amazon Web Services, Inc. 410 Terry Ave N, Seattle, Washington, USA	USA (Standardvertragsklauseln)	Rechenzentrumsinfrastruktur [nur Mapp Empower]
	Google Cloud EMEA Ltd 70 Sir John Rogerson's Quay, Dublin, Irland	Europäische Union (Belgien, Irland)	Rechenzentrumsinfrastruktur [nur Mapp Acquire]
	Google Cloud EMEA Ltd 70 Sir John Rogerson's Quay, Dublin, Irland	Europäische Union (Belgien, Irland) USA (Standardvertragsklauseln) Singapur (Standardvertragsklauseln)	Rechenzentrumsinfrastruktur [nur Mapp Acquire, gilt nicht, wenn die Option "EU-only tracking" gewählt wurde]
	Sinch Sweden AP (zuvor genannt: CLX Networks AB) Lindhagensgatan 74, Stockholm, Schweden	Europäische Union	SMS-Nachrichten [nur Mapp Engage, optional]
	R&D Communication Srl Via dei Castagni 9, Verona,	Europäische Union	SMS-Nachrichten [nur Mapp Engage, optional]

	Italien		
	Mitto AG Bahnhofstrasse 21, Zug, Schweiz	Europäische Union & Schweiz (Angemessenheitsentscheidung)	SMS-Nachrichten [nur Mapp Engage, optional]
	Pure Bros Mobile Srl Via Barletta 29, Rom, Italien	Europäische Union	SMS-Nachrichten [nur Mapp Engage, optional]
	Kenscio Digital Marketing Pvt Ltd 2-2A Maltings Place, 169 Tower Bridge Road, London SE1 3JB, Großbritannien	Indien (Standardvertragsklauseln)	Dienstleistungen [optional]
	Gerniks doo 6/31, Belgrad, Serbien	Serbien (Standardvertragsklauseln)	Entwicklung & Softwarewartung [nur Mapp Empower]
	Pythian Group Inc 319 McRae Ave, Suite 700 Ottawa, Ontario, Kanada	Kanada (Angemessenheitsentscheidung)	Entwicklung & Softwarewartung [nur Mapp Empower]

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.

ANHANG 4: BESCHREIBUNG DER MAPP-DIENSTLEISTUNGEN

Mapp Cloud enthält die folgenden Dienstleistungen, die separat erworben werden können:

Mapp Engage

Mapp Engage ist eine Cloud-basierte Lösung zum Erstellen, Planen und Bereitstellen von Werbekampagnen und anderen Kunden- und Interessentenkommunikationen über E-Mail-, App-, Social- und Web-Kanäle. Die umfassenden Zielgruppensegmentierungsfunktionen basieren auf den erfassten Benutzerinteraktionen und -attributen in den unterstützten Kanälen. Für einen datengesteuerten Arbeitsstil stehen auch grafische Dashboards zur Verfügung, um den Erfolg zu überwachen und die Kommunikationsaktivitäten weiter zu optimieren.

Mapp Intelligence

Mapp Intelligence ist eine Cloud-Lösung zum Sammeln, Analysieren und Aktivieren von Daten von Erstanbietern. Die Datenerfassung auf firmeneigenen Websites, Apps und anderen digitalen Kanälen erfolgt über eigens entwickelte Tracking Libraries (SDK). Zur Auswertung dieser Daten stehen verschiedene Analysewerkzeuge zur Verfügung, mit denen langfristige Trends, Anomalien und andere Ergebnisse visualisiert werden können. Die gewonnenen Daten und Erkenntnisse können für Kommunikations- und Marketingzwecke anderen Produkten in der Mapp Cloud, aber auch externen Systemen zur Verfügung gestellt werden.

Mapp Acquire

Die Cloud-Lösung Mapp Acquire ermöglicht die Erfassung von First-Party-Daten auf Websites und mobilen Apps. Die Datenerfassung kann beliebig konfiguriert werden und umfasst Benutzerattribute, Interaktionen mit der Website oder App sowie Transaktionen. Die Daten werden zur Personalisierung der Kundenkommunikation verwendet und zu diesem Zweck den anderen Produkten in der Mapp Cloud zur Verfügung gestellt. Optional können Daten in dritten Kanälen verwendet werden, beispielsweise für Retargeting-Zwecke in den Werbenetzwerken von Google und Facebook.

Mapp Empower

Mapp Empower ist eine E-Mail-Marketinglösung zum Versenden von Kunden- und Interessentenkommunikation per E-Mail. Zu diesem Zweck werden E-Mail-Adressen und andere optionale Benutzerattribute wie Name und Geschlecht gespeichert. Diese Daten werden für eine personalisierte Ansprache von Kunden und Interessenten verwendet.

PRODUKTDATENSTANDORTE (Der Zugriff auf Daten von anderen Standorten ist gemäß DPA weiterhin möglich.)	
PRODUKT-	**DATEN-HOSTING-STANDORT**
Mapp Engage	Deutschland
Mapp Acquire	Belgien
Mapp Intelligence	Deutschland
Mapp Empower	USA