DATA PROCESSING AGREEMENT

"**CLIENT**" or "**CONTROLLER**":		"**MAPP**" or "**PROCESSOR**":
Company Name:	_____	
Address:	_____	The Mapp entity listed in Appendix 3 which is a party to the MSA.
	_____	
	_____	
Company Information:	_____	

This Data Processing Agreement ("**DPA**") forms part of the Master Services Agreement or other agreement for the purchase of Mapp's services (hereinafter referred to as the "**MSA**") between Client and Mapp.
By signing this DPA, Client enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Affiliates.
How to execute this DPA:

- If this DPA is pre-signed on behalf of Mapp, please: (1) complete the Client information above; (2) choose the Mapp entity which is a party to the MSA; (3) review Appendix 1 and edit if necessary; (4) sign the DPA; (5) and submit via email to privacy@mapp.com.
- Upon receipt of the fully executed DPA, it will become legally binding and form a part of the MSA.
- If Client makes any revisions to this DPA which were not mutually agreed upon, such revisions will be null and void. Client signatory represents to Mapp that he or she has the legal authority to bind Client. This DPA will terminate automatically upon termination of the MSA.

1. DEFINITIONS

1.1 **Affiliate** shall mean any entity which directly or indirectly owns or controls, is owned or controlled by, or is under common ownership or common control with the party in question.

1.2 **Data Protection Law(s)** means all laws, regulations and legislation that may exist in any relevant jurisdiction which are applicable to the processing of the Personal Data in question including: the European Union Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**General Data Protection Regulation**" or "**GDPR**"), 2002/58/EC, the California Consumer Privacy Act (the "**CCPA**") and any applicable associated or supplementary data protection laws or regulations, each as updated, amended or replaced from time to time.

1.3 **Data Subject** has the meaning given to it in the applicable Data Protection Law.

1.4 **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

1.5 **Services**, more fully described in Appendix 4, shall refer to the specific Mapp Service(s) Client purchased from Mapp as set forth in the MSA.

1.6 All other capitalised terms shall have the meaning given to it in the applicable Data Protection Law or the MSA.

2. DATA PROCESSING

2.1 The parties acknowledge and agree that regarding the Processing of Personal Data, Client is the Controller and Mapp is the Processor.

2.2 The parties shall each comply with their respective obligations under the Data Protection Laws. Each party shall, in its use of Mapp Services, Process Personal Data only in accordance with the requirements of Data Protection Laws.

2.3 Client's instructions for the Processing of Personal Data shall comply with Data Protection Laws. Mapp shall inform Client immediately if, in Mapp's opinion, an instruction from Client violates Data Protection Laws.

2.4 Mapp, in its role as service provider, shall only process Personal Data on behalf of and in accordance with Client's documented instructions for the business purposes of (i) Processing in accordance with the MSA; (ii) Processing initiated by Users in their use of the Services; (iii) Processing to comply with other documented reasonable instructions provided by Client; (iv) Safeguarding the confidentiality, integrity and availability of Personal Data and the Services in accordance with this agreement; and (v) Collecting non-identifiable statistics.

2.5 Mapp acts as service provider to Client and will not otherwise retain, use or disclose the Personal Data except as described in Section 2.4 above. Mapp further acknowledges that it shall not sell Personal Data collected in accordance with the Services.

2.6 Subject-matter, duration nature and purpose of the Processing and the type of Personal Data and categories of Data Subjects are defined in the MSA.

3. DATA SUBJECTS' RIGHTS REQUESTS

3.1 Mapp shall, to the extent legally permitted, promptly notify Client if Mapp receives a request from a Data Subject to exercise one or more of the Data Subject's rights as defined within the applicable Data Protection Laws ("**DSR Request**").

3.2 Taking into account the nature of the Processing, Mapp shall assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to a DSR Request under Data Protection Laws.

3.3 To the extent Client, in its use of the Services, does not have the ability to address a DSR Request, Mapp shall, upon Client's request, provide commercially reasonable efforts to assist Client in responding to such a DSR Request, to the extent Mapp is legally permitted to do so and the response to such DSR Request is required under Data Protection Laws. To the extent legally permitted, Client shall be responsible for any costs arising from Mapp's provision of such assistance.

4. DATA PROTECTION IMPACT ASSESSMENTS

Mapp shall provide reasonable assistance to Client with any data protection impact assessments, and prior consultations with a Supervisory Authority, required under Data Protection Laws, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, Mapp.

5. PERSONAL DATA BREACH NOTIFICATION

5.1 Mapp shall notify Client without undue delay after becoming aware of a Personal Data Breach. Mapp shall provide Client with sufficient information to allow Client to meet any obligations to notify a Supervisory Authority of the Personal Data Breach and/or communicate the Personal Data Breach to Data Subjects under the Data Protection Laws.

5.2 Mapp shall make reasonable efforts to identify the cause of a Personal Data Breach and take those steps as Mapp deems necessary and reasonable in order to remediate the cause of such a Client Data Incident to the extent the remediation is within Mapp's reasonable control.

5.3 The obligations herein shall not apply to incidents that are caused by Client.

6. SUB-PROCESSING

6.1 Mapp Affiliates and other Sub-processors used by Mapp to provide its contractual services, including their role and scope of sub-processing and the geographical area of sub-processing are published in Mapp's List of Sub-Processors available upon request and/or accessible at www.mapp.com/contracts. Such Sub-processors shall be agreed and consented to by the Client. By signing this DPA, Client agrees to the list of Sub-Processors attached hereto as Appendix 3 and hereby authorizes Mapp to transfer Personal Data to listed Mapp Affiliates and/or other Subprocessors to locations outside the European Economic Area, as is reasonably required to provide support, perform technical projects or perform other types of services under the MSA, provided that, if Client is incorporated in the EU, either: (i) such locations are recognized by the European Commission as providing adequate data protection; or (ii) Mapp has executed the EU Standard Contractual Clauses with such Affiliates and/or other Subprocessors.

6.2 Mapp has entered into a written agreement with each sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such sub-processor.

6.3 Mapp shall be liable for the acts and omissions of its sub-processors to the same extent Mapp would be liable if performing the services of each sub-processor directly under the terms of this DPA, except as otherwise set forth in the MSA.

6.4 Shall Mapp anticipate the need to change or add a sub-processor Mapp shall notify Client of any change in sub-processor and Client shall be entitled to contradict any change within a reasonable time frame. Where Client fails to contradict such change within such period of time, Client shall be deemed to have consented to such change. Where a materially important reason for such contradiction exists, and failing an amicable resolution of this matter by the parties, Client shall be entitled to terminating the DPA. Mapp will ensure that any new sub-processor is held to the same applicable standards as the previously agreed upon sub-processors.

7. SECURITY

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Mapp shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Client Data), confidentiality and integrity of Personal Data, as set forth in Mapp's Security Annex (Appendix 2) to this DPA. Mapp regularly monitors compliance with these measures. Mapp will not materially decrease the overall security of the Services during the term of the MSA. Mapp will limit the access

to Personal Data to its employees or Subprocessors for whom access to said data is reasonably necessary to fulfil Mapp's obligations to Client. Mapp shall ensure that persons authorized to Process the Personal Data are bound by the same or equivalent confidentiality obligations as Mapp or are under an appropriate statutory obligation of confidentiality. Mapp information Security Policy can be provided upon request shall Client prefer additional details regarding this section.

8. DELETION OR RETURN OF PERSONAL DATA

8.1 Mapp shall delete the Personal Data upon termination/expiry of the MSA as specified in the MSA or upon Client's reasonable request within 30 days and ensure the deleted data is unrecoverable. Mapp may retain Personal Data to the extent required by applicable laws and only to the extent and for such period as required by the applicable laws and always provided that Mapp shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

8.2 Mapp shall provide to Client, upon Client's request, written confirmation that deletion has occurred in accordance with this section 8.

8.3 Mapp shall return Personal Data to Client in accordance with the procedure and timeframe specified in the MSA.

9. AUDITS AND INSPECTIONS

9.1 Mapp shall make available to Client all information necessary to demonstrate compliance with this DPA and shall allow for and contribute to audits by Client or a third-party auditor mandated by Client in relation to the Processing of Personal Data. Upon Client's written request, Mapp shall, not more than once per year, accurately complete a reasonable information security questionnaire provided by Client regarding Mapp's data protection and information security practices and policies.

9.2 Client or a third-party auditor mandated by Client may, at Client's expense and not more than once per year, perform an on-site inspection of Mapp's data protection and information security practices and policies with written notice reasonably, at least ten business days, in advance. The inspection shall take place over not more than one day during Mapp's normal business hours on a mutually agree schedule that will minimize the audit's impact on Mapp's operations. Client or a third-party auditor mandated by Client shall comply with Mapp's security requirements related to the performance of the inspection. Due to confidentiality and security requirements, such inspections shall exclude on-site inspections of multi-tenant environments (such as IaaS data centres used by Mapp). On-site examinations of such environments can be substituted by detailed documentation regarding the respective data protection and security measures taken and specific certifications issued by reputable third-party auditors, provided by Mapp upon Client's request.

9.3 Client shall promptly notify Mapp of any non-compliance discovered during such an audit/inspection.

10. LIABILITY

10.1 Each party's liability arising out of or related to this DPA and all DPAs between Affiliates and Mapp, whether in contract, tort or under any other theory of liability, is subject to the limitation of liability section agreed under the MSA, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the MSA and all DPAs together.

10.2 For the avoidance of doubt, Mapp's total liability for all claims from the Client and all of its Affiliates arising out of or related to the MSA and each DPA shall apply in the aggregate for all claims under both the MSA and all DPAs established under this Agreement.

10.3 Where a Data Subject asserts any claims against a party to this DPA in accordance in accordance with the applicable Data Protection Law, the other party shall support in defending against such claims, where possible.

Appendix 1: Data Subjects and Categories
Appendix 2: Security Annex
Appendix 3: Subprocessor List
Appendix 4: Description of Mapp Services

CONTROLLER		**PROCESSOR**	
Signature:		Signature:	
Printed Name, Title:		Printed Name, Title:	Steven Warren, CEO
Date:		Date:	

APPENDIX 1: DATA SUBJECTS & CATEGORIES

Data subjects. The personal data processed concern the following categories of data subjects:

- Client's customers,
- Client's prospects,
- Client's website visitors,
- Client's employees,

Categories of data. The personal data processed concern the following categories of data:

- Email addresses,
- Mobile number,
- Landline number,
- Last name, first name,
- Postal address,
- Date of birth,
- Opening of received emails,
- Clicks of links within the received emails,
- IP addresses,
- Website usage behaviour,

APPENDIX 2: SECURITY ANNEX

TECHNICAL AND ORGANIZATIONAL INFORMATION SECURITY MEASURES PER ART. 28 (3) GDPR

1. Confidentiality (Art. 32 Sect. 1 lit. a & b GDPR, and Art. 25 Abs. 1 GDPR)	
Physical access control	**Implementation**
Mapp shall maintain suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the personal data is processed or used.	- Established security areas with protected entry/exit points. - Authorization procedures for employees and third parties. - Visitor management procedures to ensure proper authentication and supervision. - CCTV monitoring for all data centers and primary office locations covering all entry and exit points. - Access to data center equipment requires two different authentication factors at a minimum. - Equipment is sited to protect it effectively against unauthorized information disclosure. - Security alarm systems for data centers and primary office locations. - Manned reception and/or security guards in data centers. - Procedures for secure key card assignment and/or biometric enrollment. - Electronic access system which logs all access to data centers and primary office locations.
System access control	**Implementation**
Mapp shall maintain suitable measures to prevent its personal data processing systems from being used by unauthorized persons.	- Access control policy maintained. - Procedure for managing user and privileged accounts in line with the employment lifecycle based on a central directory. - Multi-factor authentication required for privileged access to the infrastructure. - Password policy which technically requires at least 8 characters; include at least three of the following four elements: Capital letter(s), Lower-case letter(s), Number(s), Symbol(s); a password different from the 8 previously used ones; internal user passwords are reset upon expiry and potential compromise; and a minimum length for administrator and service accounts of 14 characters. Users are required to change initial passwords upon first login. - Option to enable multi-factor authentication or single sign-on via custom identity source to increase customer access assurance (applies to Mapp Engage, Mapp Intelligence, and Mapp Acquire). - Employees are required to follow clean desk policy. Screens are locked automatically after no more than 15 minutes of inactivity. - Access to the Mapp internal network restricted to authorized company devices. - Anti-malware systems installed on all Windows systems and Linux servers that are susceptible to malware infections. - Monitoring of security events related to internal and Mapp Cloud production systems. - No data processing on mobile devices such as mobile phones or tablets. - Policy prohibiting transfer of data to removable media. - Customer remains responsible for protecting GUI and API credentials under his/her control. - Process for technical vulnerability management including the hardening of the physical and virtual server infrastructure, static code analysis, periodic internal vulnerability assessments, 3rd party penetration tests, and timely patching of security weaknesses following a risk-based approach. Customers may conduct their own technical assessments in agreement with Mapp. - Secure coding principles in accordance with OWASP Top 10, which are regularly trained to Mapp software developers. - Physical and virtual production networks are tightly controlled, effectively segregated, and protected by firewalls. No data storage in a network's presentation zone. - Network-based intrusion detection and/or prevention system in place and monitored (applies to Mapp Engage and Mapp Intelligence). - Host-based intrusion detection system in place and monitored (applies to Mapp Engage).

Data access control	**Implementation**
Mapp shall maintain suitable measures in order to prevent unauthorized read, copy, change or delete operations within information systems.	- Procedure for managing Mapp user and privileged access rights in line with the employment lifecycle based on a central directory. - Access to data restricted to authorized groups. - Assignment of privileged access rights follows the least privilege principle. - Grained role and permission model implemented for Mapp Cloud to allow customization of customer access according to the need-to-know principle. - Central Mapp directory accounts are reviewed half-annually. - Mapp privileged accounts and entitlements with access to the infrastructure are reviewed at least half-annually. - User and privileged account activity, as well as other security-related events are logged, and logs protected from loss and manipulation. - Mapp privileged account logs are regularly reviewed, manually and/or automatically. - Customer remains responsible for application-specific access reviews, the accuracy of the access control list and the protection of assigned credentials. - Storage systems apply filesystem or object-level encryption using AES-256 (or equivalent) (applies to Mapp Engage and Mapp Acquire). - Use of encrypted filesystems on company laptops. - Use of removable media technically limited. - Procedures for secure disposal of equipment and unrecoverable deletion of data during client off-boarding.
Separation control	**Implementation**
Mapp shall maintain suitable measures in order to separate processing of data that has been collected for different purposes.	- Logical segregation of tenant data in production and service environments either on the data model or database schema level. - Development and test systems are segregated from production environments. - Production data is not used for testing purposes.
Pseudonymization / Anonymization	**Implementation**
Processing of personal data in a way that prevents the association of data to a certain individual without additional information which is kept separately by appropriate technical or organizational measures.	- Development procedures include design principles for data minimization, collection limitation and privacy by default, including the requirement for pseudonymization where feasible. - Behavioral data is stored in pseudonymized form and separate from the corresponding contact profile where feasible (applies to Mapp Engage). - Online tracking by default pseudonymous, option to pseudonymize and anonymize collected custom attributes e.g. via hashing or truncation (applies to Mapp Acquire and Mapp Intelligence). - System logs are anonymized where feasible. - Where service functionality involves data-driven analytics and predictions, data is effectively anonymized before running required calculation and processing.
2. Integrity (Art. 32 Sect. 1 lit. b GDPR)	
Transfer control	**Implementation**
Mapp shall maintain suitable measures in order to prevent unauthorized read, copy, change or delete operations during	- Data transferred over public data-transmitting networks is effectively protected using industry good practice standards and algorithms such as TLS or SSH with secure configurations. - Data is not transferred physically, neither on paper nor on mobile storage devices. - Secure electronic messaging capabilities are in place for internal and external communication, but we do not permit the transfer of data (processed under this DPA) via email. In case

transmission or transport.	customers send data via email or instruct Mapp to do this, the customer will remain responsible for any possible consequences. - Option to protect email domain integrity with DMARC (applies to Mapp Engage)
Input control	**Implementation**
Mapp shall maintain suitable measures in order to determine whether personal data was entered to, changed, or deleted from information systems.	- User and privileged accounts are unique and identifiable where technically feasible; exception: root accounts which are strictly controlled. - Access to data at the application and database level is comprehensively logged, and logs protected from loss and manipulation. - Log sources use a synchronized time source (NTP). - Host-based intrusion detection system in place and monitored (applies to Mapp Engage). - Network-based intrusion detection and/or prevention system in place and monitored (applies to Mapp Engage and Mapp Intelligence). - Process for technical vulnerability management including the hardening of the physical and virtual server infrastructure, static code analysis, periodic internal vulnerability assessments, 3rd party penetration tests, and timely patching of security weaknesses following a risk-based approach. Customers may conduct their own technical assessments in agreement with Mapp. - Anti-malware systems installed on all Windows systems and Linux servers that are susceptible to malware infections.
3. Availability and Resilience (Art. 32 Sect. 1 lit. b & c GDPR)	
Availability control	**Implementation**
Mapp shall maintain suitable measures in order to protect against accidental or intentional loss or destruction.	- Detection and suppression systems are implemented in data centers to minimize the risk related to fire and water. These are maintained and tested at least annually. - Equipment is sited to protect it effectively against environmental damage or sabotage. - Security mechanisms and redundancies implemented to protect equipment from utility service outages. Battery systems and diesel generators with at least 24h fuel supply are implemented and tested several times a year to ensure uninterrupted power. - Critical system components (e.g. web servers or load balancers) are laid out redundantly to avoid single points of failure. - Data is replicated and relational data backed-up daily. - Process for technical vulnerability management including the hardening of the physical and virtual server infrastructure, static code analysis, periodic internal vulnerability assessments, 3rd party penetration tests, and timely patching of security weaknesses following a risk-based approach. Customers may conduct their own technical assessments in agreement with Mapp. - Planning and monitoring of computing, storage, and network capacity. - System health and availability monitoring. - Procedures for change management during normal operations and emergencies. - Anti-malware systems installed on all Windows systems and Linux servers that are susceptible to malware infections. - Network-based intrusion detection and/or prevention system in place and monitored (applies to Mapp Engage and Mapp Intelligence).
Ability of recovery	**Implementation**
Mapp shall maintain suitable measures in order to sustain the ability to recovery within an appropriate timeframe after a disruptive event.	- Business continuity plans for data centers and software services are maintained and tested regularly. - UPS and diesel generators are implemented in data centers to survive power outages of at least 24 hours. These are maintained and tested at least annually. - Data is replicated and relational data backed-up daily to remote locations. Backup recovery procedures are regularly tested.
4. Process for regular assessment of the effectiveness of measures (Art. 32 Sect. 1 lit. d GDPR; Art. 25 Sect. 1 & 2 GDPR)	

Data Protection Management	**Implementation**
Mapp shall follow a systematic approach to the management of data protection.	- Clearly defined and communicated roles and responsibilities with regards to information security and privacy, including but not limited to: Information Security Officer and Data Protection / Privacy Officer. - Governance procedures for information risk management, maintenance, and communication of policies, internal and third party compliance assessments, management reporting and review, and tracking of continuous improvement. - Information security and privacy awareness program including mandatory new hire and annual refresher trainings as well as additional awareness measures. - Annual independent audit of the information security and data protection management system.
Incident Response Management	**Implementation**
Mapp shall follow a systematic approach to the management of incidents.	- Procedure for incident reporting, trained to all employees. - Procedure for incident response including verification, classification, containment, eradication and recovery; playbooks maintained for selected types of incidents. - Procedure for notification in line with legal and contractual requirements. - Post-mortem analysis required for significant incidents. - Additional security controls as per Mapp's information security policies.
Privacy by default	**Implementation**
Mapp shall maintain suitable measures to ensure that data protection compliance is embedded throughout the entire life cycle of technologies and procedures.	- Development procedures include design principles for data minimization, collection limitation and privacy by default. Our software services /applications are customizable to a certain extent. Options for configuration are available in the respective online help. - Customers remain responsible for the lawful and privacy-friendly use of Mapp's software services. Moreover, the Acceptable Use Policy applies: https://mapp.com/acceptable-use-policy/
Order control (Art. 28 GDPR)	**Implementation**
Mapp shall maintain suitable measures in order to prevent data processing without the controller's instruction.	- Mapp processes data only based on the Customer's instructions, i.e. based on contractual agreements, orders, or additional instructions. Customers should provide instructions only in written form or confirm in written form when done verbally. - Mapp will not respond to data subject requests but forward them to the Customer. - Procedures for secure disposal of equipment and unrecoverable deletion of data during client off-boarding. - Effective restriction of the processing of data retained for legal purposes via encryption of backup files, encryption of file systems, strict access controls, audit logging, and ticket-based restore procedures.

APPENDIX 3: SUBPROCESSOR LIST

	Legal Entity and Address	Processing Location(s) and Legal Safeguards (Art.46 EU GDPR, if applicable)	Purpose/Applicability
MAPP ENTITIES	**Mapp Digital Germany GmbH** Sandstr. 3, München, Germany	European Union (Germany)	Development & Maintenance Support and Professional Services
	Mapp Digital France S.A.S. 33 rue Lafayette, 75009 Paris, France	European Union (France)	Support and Professional Services
	Mapp Digital Italy SrL Via Dante 7, Milan, Italy	European Union (Italy)	Support and Professional Services
	Webtrekk GmbH Schönhauser Allee 148, Berlin, Germany	European Union (Germany & Italy)	Development & Maintenance Support and Professional Services
	Mapp Digital Poland sp. z.o.o. ul. Kamienskiego 47, Krakow, Poland	European Union (Poland)	Development & Maintenance
	Mapp Digital Netherlands B.V. Lichttoren 32, BJ Eindhoven, Netherlands	European Union (Netherlands)	Development & Maintenance
	Mapp Digital UK Ltd 6th Floor, 95 Gresham Street, London, UK	United Kingdom (Adequacy Decision)	Support and Professional Services
	Mapp Digital US, LLC 3655 Nobel Dr Suite 500, San Diego, CA, US	United States (Standard Contractual Clauses)	Support and Professional Services (optional for European customers)
EXTERNAL THIRD PARTIES	**Global Access Internet Services GmbH** Potsdamer Str. 3, München, Germany	European Union (Germany)	Data center infrastructure
	IP Exchange GmbH Am Tower 5, Nürnberg, Germany	European Union (Germany)	Data center infrastructure
	Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, Luxembourg	European Union (Germany & Ireland)	Data center infrastructure
	Amazon Web Services, Inc. 410 Terry Ave N, Seattle, WA, US	United States (Standard Contractual Clauses)	Data center infrastructure (Mapp Empower only)
	Google Cloud EMEA Ltd 70 Sir John Rogerson's Quay, Dublin, Ireland	European Union (Belgium, Ireland)	Data center infrastructure (Mapp Acquire only)
	Google Cloud EMEA Ltd 70 Sir John Rogerson's Quay, Dublin, Ireland	European Union (Belgium, Ireland) United States (Standard Contractual Clauses) Singapore (Standard Contractual Clauses)	Data center infrastructure (Mapp Acquire only, does not apply when EU-only tracking option is selected)
	Sinch Sweden AP (previously CLX Networks AB) Lindhagensgatan 74, Stockholm, Sweden	European Union (Ireland & France)	SMS Message Delivery (Mapp Engage only, optional service)
	R&D Communication Srl Via dei Castagni 9, Montorio V.se , Italy	European Union	SMS Message Delivery (Mapp Engage only, optional service)

	Mitto AG Bahnhofstrasse 21 · 6300 Zug, Switzerland	European Union & Switzerland (Adequacy Decision)	SMS Message Delivery (Mapp Engage only, optional service)
	Pure Bros Mobile Srl Via Barletta 29, Roma, Italy	European Union	SMS Message Delivery (Mapp Engage only, optional service)
	Kenscio Digital Marketing Pvt Ltd 2-2A Maltings Place, 169 Tower Bridge Road, London SE1 3JB, UK	India (Standard Contractual Clauses)	Professional Services (optional)
	Gerniks doo 6/31, Belgrad, Serbia	Serbia (Standard Contractual Clauses)	Development, Maintenance & Support (optional)
	Pythian Group Inc 319 McRae Ave, Suite 700 Ottawa, Ontario, Canada, Canada	Canada (Adequacy Decision)	Development & Maintenance (Mapp Empower only)
	Fresh Relevance Ltd 2-2A, Maltings Place, Tower Bridge Rd, London SE1 3JB	Ireland, United Kingdom (Adequacy Decision)	Services [eCommerce Plus only]

ADDITIONAL PROVIDERS MAY BE NECESSARY FOR CERTAIN SERVICES OR THOSE CUSTOMERS WITH ELEVATED SUPPORT DEMANDS. THESE PROVIDERS SHALL DE DESIGNATED IN THE APPLICABLE SOW FOR THESE SERVICES.

APPENDIX 4: DESCRIPTION OF MAPP SERVICES

Mapp Cloud includes the following services, which can be purchased separately:

Mapp Engage

Mapp Engage is a cloud-based solution for creating, planning and delivering advertising campaigns and other customer and prospect communications across email, app, social and web channels. The comprehensive target group segmentation capabilities are based on the captured user interactions and attributes in the supported channels. For a data-driven working style, graphical dashboards are also available to monitor success and further optimize communication activities.

Mapp Intelligence

Mapp Intelligence is a cloud solution for collecting, analyzing and activating first-party data. Data is collected on the company's own websites, apps and other digital channels using tracking libraries (SDK) developed in-house. Various analysis tools are available to evaluate this data, which enables the visualization of long-term trends, anomalies and other findings. The data and insights gained can be made available to other products within the Mapp Cloud, but also to external systems, for communication and marketing purposes.

Mapp Acquire

The cloud solution Mapp Acquire enables the collection of first-party data on websites and mobile apps. The collection of data can be configured as desired and includes user attributes, interactions with the website or app and transactions. The data is used to personalize customer communications and is made available to the other products in the Mapp Cloud for this purpose. Optionally, data can be used in third channels, for example for retargeting purposes in the advertising networks of Google and Facebook.

Mapp Empower

Mapp Empower is an e-mail marketing solution for sending customer and prospect communication via e-mail. For this purpose, e-mail addresses and other optional user attributes such as name and gender are stored. This data is used for a personalized approach to customers and prospects.

PRODUCT DATA LOCATIONS (data may still be accessed from other locations in accordance with the DPA)	
PRODUCT	**DATA HOSTING LOCATION**
Mapp Engage	Germany
Mapp Acquire	Belgium
Mapp Intelligence	Germany
Mapp Empower	USA