Privacy Policy

1. Introduction

We take your privacy extremely seriously. This policy explains the what, how, and why of the information we collect when you visit one of our websites, or when you use our Services. It also explains the specific ways we use and disclose that information.

Please read our Terms of Service and this Privacy Policy together with our Data Processing Agreement carefully, as you must agree to these documents in order to have permission to use our Service. This Privacy Policy is hereby made a part of the Terms of Service.

Please note that for the purposes of EU data protection legislation, MageMail is the data processor of personal information.

This Privacy Policy is effective with respect to any data that we have collected, or collect, about and/or from you, according to our Terms of Services.

2. Definitions

Throughout this document, we may use certain words or phrases, and it is important that you understand the meaning of them. The following is a non-exhaustive list of definitions of words and phrases found in this document:

- * “Agreement” means these Terms of Service, incorporating the Privacy Policy together with the Data Processing Agreement;
- * “Customer” or “Customers” refers to your customers purchasing products or services from you. In this definition, this includes prospects who have not yet purchased your products or services but have shown interest;
- * “MageMail” refers our Site, our Services, our company or a combination of all or some of the preceding definitions, depending on the context in which the word is used;

- * “Personal Data” or “Personal Information” means any information relating to an identified or identifiable natural person;
- * “Service” or “Services” refers to the applications, including related features and capabilities, that we provide through our Site, including our e-mail marketing services and our Site itself;
- * “Site” or “Website” refers to our website, www.magemail.co or www.getmagemail.com, and underlying applications;
- * “Store” refers to a single instance of an online store;
- * “You” or “you” refers to you, the person who is entering into this Agreement with MageMail on behalf of yourself and your company;
- * “User” or “Users” refers to anyone who uses our Service, including you and general visitors to our Site

3. Information We Collect

- * Information you voluntarily provide to us: When you sign up for and use the Services, consult with our customer service team, send us an email, post on our blog, integrate the Services with another website or service (for example, when you choose to connect your Magento account with MageMail), or communicate with us in any way, you are voluntarily giving us information that we collect. That information may include either your or your Customers’ name, physical address, email address, IP address, phone number, credit card information, as well as details including gender, occupation, location, purchase history, and other demographic information. By giving us this information, you consent to this information being collected, used, disclosed, transferred to the European Union or the United States and stored by us, as described in our Terms of Services and in this Privacy Policy.
- * Information we collect automatically: When you use the Services or browse one of our Sites, we may collect information about your visit to our Sites, your usage of the Services, and your web browsing. That information may include your IP address, your operating system, your browser ID, your browsing activity, and other information about

how you interacted with our Websites or other websites. We may collect this information as a part of log files as well as through the use of cookies or other tracking technologies. Our use of cookies and other tracking technologies is discussed more below.

- * List and email information: When you add a subscriber list, create a campaign, or create an email with the Services, we have and may access the data on your list and the information in your email. If a Customer chooses to use forward a link in an email campaign you send, it will allow the Customer to share your email content with individuals not on your subscriber list or in your campaign. When a Customer forwards an email to another person, we do not store that other person's email address.
- * Information from your use of the Service: We may receive information about how and when you use the Services, store it in log files or other types of files associated with your account, and link it to other information we collect about you. This information may include, for example, your IP address, time, date, browser used, and actions you have taken within the application. This type of information helps us to improve our Services for both you and for all of our users.
- * Cookies and tracking:We and our partners may use various technologies to collect and store information when you use our Services, and this may include using cookies and similar tracking technologies on our Site, such as pixels and web beacons, to analyze trends, administer the website, track users' movements around the website, serve targeted advertisements, and gather demographic information about our user base as a whole. Users can control the use of cookies at the individual browser level. We partner with third parties to display advertising on our website or to manage and serve our advertising on other sites. Our third party partners may use cookies or similar tracking technologies in order to provide you advertising or other content based upon your browsing activities and interests. If you wish to opt out of interest-based advertising click http://preferences-mgr.truste.com/ (or if located in the European Union click http://www.youronlinechoices.eu/). Please note you might continue to receive generic ads.

- * Web beacons and hooks:We use web beacons and hooks on our Websites and in our emails. When we send emails to Customers, we may track behavior such as who opened the emails and who clicked the links. This allows us to measure the performance of the email campaigns and to improve our features for specific segments. Reports are also available to us when we send email to you, so we may collect and review that information.

4. Use and Disclosure of Personal Information

We may use and disclose Personal Information only for the following purposes:

- * To promote use of our Services to you and others. For example, if we collect your Personal Information when you visit our Website and do not sign up for any of the Services, we may send you an email inviting you to sign up. If you use any of our Services and we think you might benefit from using another Service we offer, we may send you an email about that. You can stop receiving our promotional emails by following the unsubscribe instructions included in every email we send. In addition, we may use information we collect in order to advertise our Services to you or suggest additional features of our Services that you might consider using. In addition, we may use your Personal Information to advertise our Services to potential or other users like you.
- * To send you informational and promotional content in accordance with your marketing preferences. You can stop receiving our promotional emails by following the unsubscribe instructions included in every email.
- * To bill and collect money owed to us by You. This includes sending you emails, invoices, receipts, notices of delinquency, and alerting you if we need a different credit card number. We use third parties for secure credit card transaction processing, and we send billing information to those third parties to process your orders and credit card payments.

- * To send you System Alert messages. For example, we may inform you of temporary or permanent changes to our Services, such as planned outages, new features, version updates, releases, abuse warnings, and changes to our Privacy Policy.
- * To communicate with You about Your account and to provide customer support.
- * To enforce compliance with our Terms of Services and applicable law. This may include developing tools and algorithms that help us prevent violations.
- * To protect Your rights and safety as well as those of third parties and our own.
- * To meet legal requirements, including complying with court orders, valid discovery requests, valid subpoenas, and other appropriate legal mechanisms.
- * To provide information to representatives and advisors, including attorneys and accountants, to help us comply with legal, accounting, or security requirements.
- * To prosecute and defend a court, arbitration, or similar legal proceeding.
- * To respond to lawful requests by public authorities, including to meet national security or law enforcement requirements.
- * To provide, support, and improve the Services we offer. This includes our use of the data that our Members provide us in order to enable our Members to use the Services to communicate with their Subscribers. This also includes, for example, aggregating information from your use of the Services or visit to our Websites and sharing this information with third parties to improve our Services. This might also include sharing your information or the information you provide us about your Subscribers with third parties in order to provide and support our Services or to make certain features of the Services available to you. When we do have to share Personal Information with third parties, we take steps to protect your information by requiring these third parties to enter into a contract with us that requires them to use the Personal Information we transfer to them in a manner that is consistent with this policy.
- * To provide suggestions to you. This includes adding features to compare email campaigns or using data to suggest products or services that you may be interested in or that may be relevant to you or your Customers.

- * To transfer your information in the case of a sale, merger, consolidation, liquidation, reorganization, or acquisition. In that event, any acquirer will be subject to our obligations under this Privacy Policy, including your rights to access and choice. We may notify you of the change either by sending you an email or posting a notice on our Site.

Combined Information: We may combine Personal Information with other information we collect or obtain about you (such as information we source from our third party partners), to serve you specifically, such as to deliver a product or service according to your preferences or restrictions, or for advertising or targeting purposes in accordance with this Privacy Policy. When we combine Personal Information with other information in this way, we treat it as, and apply all of the safeguards in this Privacy Policy applicable to, Personal Information.

5. Data Collected for and by our Users

As you use our Services, you may import into our system Personal Information you have collected from your Customers or other individuals. We have no direct relationship with your Customers or any person other than you, and for that reason, you are responsible for making sure you have the appropriate permission for us to collect and process information about those individuals.

Consistent with the uses of Personal Information covered above, we may transfer Personal Information of you or your Customers to companies that help us promote, provide, or support our Services ("Service Providers"). All Service Providers enter into a contract with us that protects Personal Information and restricts their use of any Personal Information consistent with this policy. As part of our Services, we may use and incorporate into features information you have provided, we have collected from you, or we have collected about Customers. We may share this information, including Customer email addresses, with third parties in line with the approved uses of this Privacy Policy.

6. Commercial and Non-Commercial Communications to You

By providing information to the Site that forms the basis of communications with you, such as contact information, you waive all rights to file complaints concerning unsolicited e-mails from MageMail since, by providing such information, you agree to receive communications from us or anyone else covered under this Privacy Policy. However, you may unsubscribe from certain communications by notifying MageMail that you no longer wish to receive solicitations or information and we will endeavor to remove you from the database.

We will retain Personal Information we process for as long as needed to provide our Services or to comply with our legal obligations, resolve disputes, prevent abuse, and enforce our agreements.

7. Public Information and Third Party Websites

Blog. We have public blogs on our Websites. Any information you include in a comment on our blog may be read, collected, and used by anyone. If your Personal Information appears on our blogs and you want it removed, contact us. If we are unable to remove your information, we will tell you why.

Social media platforms and widgets. Our Site includes social media features. These features may collect information about your IP address and which page you are visiting on our Site, and they may set a cookie to make sure the feature functions properly. Social media features and widgets are either hosted by a third party or hosted directly on our Site. We also maintain presences on social media platforms including Facebook, Twitter, and Instagram. Any information, communications, or materials you submit to us via a social media platform is done at your own risk without any expectation of privacy. We cannot control the actions of other users of these platforms or the actions of the platforms themselves. Your interactions with those features and platforms are governed by the privacy policies of the companies that provide them.

Links to third-party websites. Our Site include links to other websites, whose privacy practices may be different from ours. If you submit Personal Information to any of those sites, your

information is governed by their privacy policies. We encourage you to carefully read the privacy policy of any website you visit.

8. Third Parties

Service Providers. Sometimes, we share your information with our third party Service Providers, who help us provide and support our Services. For example, if it is necessary to provide you something you have requested then we may share your and/or your Customer's Personal Information with a Service Provider for that purpose. Just like with the other third parties we work with, these third party Service Providers enter into a contract that requires them to use your Personal Information only for the provision of services to us and in a manner that is consistent with this policy. Examples of Service Providers include payment processors, hosting services, and content delivery services.Without limiting the generality of the foregoing, you authorize us to collect, share, store, and otherwise use your information in conjunction with the entities listed in our Third-Party Sub-Processors page.

Advertising partners. We may partner with third party advertising networks and exchanges to display advertising on our Site or to manage and serve our advertising on other sites and may share Personal Information with them for this purpose. All third parties with which we share this information are required to use your Personal Information in a manner that is consistent with this policy. We and our third party partners may use cookies and other tracking technologies, such as pixels and web beacons, to gather information about your activities on our Site and other sites in order to provide you with targeted advertising based on your browsing activities and interests.

9. Content of Email Campaigns

When you send an email marketing campaign, it bounces from server to server as it crosses the Internet. Along the way, server administrators can read what you send. Email was not built for confidential information. Please do not use MageMail to send confidential information.

10. Your Subscriber Lists and Campaigns

A Subscriber List and related Campaigns can be created in a number of ways, including by importing contacts, such as through csv or directly from Magento. Magento is the system of record for your Subscriber Lists, and we sync subscribes and unsubscribes. Data is stored on a secure MageMail server. We do not, under any circumstances, sell your Subscriber Lists. Only authorized employees have access to view Subscriber Lists. You may export (download) your Subscriber Lists from MageMail at any time.

We do not, under any circumstances, sell your Subscriber Lists. We will use and disclose the information in your Subscriber Lists only for the legal and regulatory reasons. We will not use and disclose the information in your Subscriber Lists to:

- * bill or collect money owed to us;
- * send you informational and promotional content.

If we detect abusive or illegal behavior related to your Subscriber List, we may share your Subscriber List or portions of it with affected ISPs or anti-spam organizations.

11. Notice of Breach of Security

If a security breach causes an unauthorized intrusion into our system that materially affects you or people on your Subscriber Lists, then MageMail will notify you as soon as possible and later report the action we took in response.

12. Safeguarding Your Information

We take reasonable and appropriate measures to protect Personal Information from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the risks involved in the processing and the nature of the Personal Information.

Our credit card processing vendor uses security measures to protect your information both during the transaction and after it is complete. Our vendor is certified as compliant with card association security initiatives, including the Visa Cardholder Information Security and Compliance (CISP), MasterCard® (SDP), and Discovery Information Security and Compliance (DISC). If you have any questions about the security of your Personal Information, you may contact us at hello@magemail.co.

MageMail accounts require a username and password to log in. You must keep your username and password secure, and never disclose it to a third party. Because the information in your Subscriber Lists is sensitive, account passwords are encrypted, which means we cannot see your passwords.

13. Operations

Our headquarter offices are located in Sweden, so your information may be transferred to, stored, or processed in Sweden. While the data protection, privacy, and other laws of the European Union might not be as comprehensive as those in your country, we take many steps to protect your privacy, including offering a data processing addendum. By using our Site, you understand and consent to the collection, storage, processing, and transfer of your information to our facilities in the European Union and the United States and those third parties with whom we share it as described in this policy.

14. Users Located in Australia

If you are a Member who lives in Australia, this Section applies to you. We are subject to the operation of the Privacy Act 1988 ("**Australian Privacy Act**"). Here are the specific points you should be aware of:

Where we say we assume an obligation about Personal Information, we are also requiring our subcontractors to undertake a similar obligation, where relevant.

We will not use or disclose Personal Information for the purpose of our direct marketing to you unless: you have consented to receive direct marketing; you would reasonably expect us to use your personal details for the marketing; or we believe you may be interested in the material but it is impractical for us to obtain your consent. You may opt out of any marketing materials we send to you through an unsubscribe mechanism or by contacting us directly. If you have requested not to receive further direct marketing messages, we may continue to provide you with messages that are not regarded as “direct marketing” under the Australian Privacy Act, including changes to our terms, system alerts, and other information related to your account.

Our servers are primarily located in the United States and the European Union. In addition, we or our subcontractors, may use cloud technology to store or process Personal Information, which may result in storage of data outside Australia. It is not practicable for us to specify in advance which country will have jurisdiction over this type of off-shore activity. All of our subcontractors, however, are required to comply with the Australian Privacy Act in relation to the transfer or storage of Personal Information overseas.

If you think the information we hold about you is inaccurate, out of date, incomplete, irrelevant or misleading, we will take reasonable steps, consistent with our obligations under the Australian Privacy Act, to correct that information upon your request.

If you are unsatisfied with our response to a privacy matter then you may consult either an independent advisor or contact the Office of the Australian Information Commissioner for additional help. We will provide our full cooperation if you pursue this course of action.

15. Accuracy and Retention of Data

We do our best to keep your data accurate and up to date, to the extent that you provide us with the information we need to do so. If your data changes (for example, if you have a new email address), then you are responsible for notifying us of those changes. Upon request, we will provide you with information about whether we hold, or process on behalf of a third party, any of your Personal Information. We will retain your information for as long as your account is active

or as long as needed to provide you with our Services. We may also retain and use your information in order to comply with our legal obligations, resolve disputes, prevent abuse, and enforce our Agreements.

16. Access

We will give an individual, either you or a Subscriber, access to any Personal Information we hold about them within 30 days of any request for that information. Individuals may request to access, correct, amend or delete information we hold about them by contacting us. Unless it is prohibited by law, we will remove any Personal Information about an individual, either you or a Subscriber, from our servers at your or their request. There is no charge for an individual to access or update their Personal Information.

17. Amendments

We may amend this Privacy Policy from time to time. When we amend this Privacy Policy, we will e-mail you to inform you of the amendments. Your continued use of our Service shall constitute your acceptance of any such amendments.

If you have any questions or comments, or if you want to update, delete, or change any Personal Information we hold, or you have a concern about the way in which we have handled any privacy matter, please contact us by postal mail or email at: hello@magemail.co or BOX 7609, 103 94 Stockholm, Sweden.

Data Processing Agreement

Last updated: August 25, 2020

This Data Processing Agreement (“DPA”) is an addendum to the Customer Terms of Service and Privacy Policy (“Agreement”) between MageMail and the Customer. This DPA includes and incorporates by reference the annexes and addenda referenced at the bottom of this document. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

Customer enters into this DPA on behalf of itself and, to the extent required under Data Protection Laws, in the name and on behalf of its Authorized Affiliates (defined below).

The parties agree as follows:

1. Definitions

"Affiliate" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

"Authorized Affiliate" means any of Customer Affiliate(s) permitted to or otherwise receiving the benefit of the Services pursuant to the Agreement.

"Control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term **"Controlled"** shall be construed accordingly.

"Controller" means an entity that determines the purposes and means of the processing of Personal Data.

"Customer Data" means any data that MageMail and/or its Affiliates processes on behalf of the Customer in the course of providing the Services under the Agreement.

"Data Protection Laws" means all data protection and privacy laws and regulations applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.

"EU Data Protection Law" means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (**"GDPR"**); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (in each case, as may be amended, superseded or replaced).

“Personal Data” means any Customer Data relating to an identified or identifiable natural person to the extent that such information is protected as personal data under applicable Data Protection Law.

“Processor” means an entity that processes Personal Data on behalf of the Controller.

“Processing” has the meaning given to it in the GDPR and **“process”**, **“processes”** and **“processed”** shall be interpreted accordingly.

“Security Incident” means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data.

“Services” means any product or service provided by MageMail to Customer pursuant to and as more particularly described in the Agreement.

“Standard Contractual Clauses” means the standard contractual clauses issued pursuant to the European Commission Decision of February 5, 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC.

“Sub-processor” means any Processor engaged by MageMail or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or any MageMail Affiliate.

2. Scope and Applicability of this DPA

2.1 This DPA applies where and only to the extent that MageMail processes Personal Data on behalf of the Customer in the course of providing the Services and such Personal Data is subject to Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom. The parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

2.2 Role of the Parties. As between MageMail and Customer, Customer is the Controller of Personal Data and MageMail shall process Personal Data only as a Processor on behalf of

Customer. Nothing in the Agreement or this DPA shall prevent MageMail from using or sharing any data that MageMail would otherwise collect and process independently of Customer's use of the Services.

2.3 Customer Obligations. Customer agrees that (i) it shall comply with its obligations as a Controller under applicable Data Protection Laws in respect of its processing of Personal Data and any processing instructions it issues to MageMail; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under these Data Protection Laws for MageMail to process Personal Data and provide the Services pursuant to the Agreement and this DPA.

2.4 MageMail Processing of Personal Data. As a Processor, MageMail shall process Personal Data only for the following purposes: (i) processing to perform the Services in accordance with the Agreement; (ii) processing to perform any steps necessary for the performance of the Agreement; and (iii) to comply with other reasonable instructions provided by Customer to the extent they are consistent with the terms of this Agreement and only in accordance with Customer’s documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer’s complete and final instructions to MageMail in relation to the processing of Personal Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and MageMail.

2.5 Nature of the Data. MageMail handles Customer Data provided by Customer. Such Customer Data may contain special categories of data depending on how the Services are used by Customer. The Customer Data may be subject to the following process activities: (i) storage and other processing necessary to provide, maintain and improve the Services provided to Customer; (ii) to provide customer and technical support to Customer; and (iii) disclosures as required by law or otherwise set forth in the Agreement.

2.6 MageMail Data. Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that MageMail shall have a right to use and disclose data relating to and/or obtained in connection with the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support,

product development and sales and marketing. To the extent any such data is considered personal data under Data Protection Laws, MageMail shall process such data in compliance with applicable Data Protection Laws.

3. Subprocessing

3.1 Authorized Sub-processors. Customer agrees that MageMail may engage Sub-processors to process Personal Data on Customer's behalf. The Sub-processors currently engaged by MageMail and authorized by Customer are available upon request.

3.2 Sub-processor Obligations. MageMail shall: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Personal Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause MageMail to breach any of its obligations under this DPA.

3.3 Changes to Sub-processors. MageMail shall provide Customer reasonable advance notice (for which email shall suffice) if it adds or removes Sub-processors.

3.4 Objection to Sub-processors. Customer may object in writing to MageMail's appointment of a new Sub-processor on reasonable grounds relating to data protection by notifying MageMail promptly in writing within five (5) calendar days of receipt of MageMail's notice in accordance with Section 3.3. Such notice shall explain the reasonable grounds for the objection. In such event, the parties shall discuss such concerns in good faith with a view to achieving commercially reasonable resolution. If this is not possible, either party may terminate the applicable Services that cannot be provided by MageMail without the use of the objected-to-new Sub-processor.

4. Security

4.1 Security Measures. MageMail shall implement and maintain appropriate technical and organizational security measures to protect Personal Data from Security Incidents and to preserve the security and confidentiality of the Personal Data, in accordance with MageMail's security standards described in Annex B.

4.2 Confidentiality of Processing. MageMail shall ensure that any person who is authorized by MageMail to process Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

4.3 Security Incident Response. Upon becoming aware of a Security Incident, MageMail shall notify Customer without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer.

4.4 Updates to Security Measures. Customer acknowledges that the Security Measures are subject to technical progress and development and that MageMail may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

5. Security Reports and Audits

5.1 MageMail shall maintain records of its security standards. Upon Customer's written request, MageMail shall provide (on a confidential basis) documentation reasonably required by Customer to verify MageMail's compliance with this DPA. MageMail shall further provide written responses (on a confidential basis) to all reasonable requests for information made by Customer (acting reasonably) considered necessary to confirm MageMail's compliance with this DPA, provided that Customer shall not exercise this right more than once per year.

5.2 To the extent the Standard Contractual Clauses apply and the Customer reasonably argues and establishes that the above documentation is not sufficient to demonstrate compliance with the obligations laid down in this DPA, the Customer may execute an audit as outlined under Clause 5 lit.f) of the Standard Contractual Clauses accordingly, provided that in such an event, the parties agree: (a) Customer is responsible for all costs and fees relating to such audit

(including for time, cost and materials expended by MageMail); (b) a third party auditor must be mutually agreed upon between the parties to follow industry standard and appropriate audit procedures; (c) such audit must not unreasonably interfere with MageMail's business activities and must be reasonable in time and scope; and (d) the parties must agree to a specific audit plan prior to any such audit, which must be negotiated in good faith between the parties. For avoidance of doubt, nothing in this Section 5.2 modifies or varies the Standard Contractual Clauses, and to the extent a competent authority finds otherwise or any portion of Section 5.2 is otherwise prohibited, unenforceable or inappropriate in view of the Standard Contractual Clauses, the relevant portion shall be severed and the remaining provisions hereof shall not be affected.

6. International Transfers

6.1 Processing Locations. MageMail may transfer and process Customer Data in the European Union and anywhere in the world where MageMail, its Affiliates and/or its Sub-processors maintain data processing operations. MageMail shall implement appropriate safeguards to protect the Personal Data, wherever it is processed, in accordance with the requirements of Data Protection Laws.

7. Return or Deletion of Data

7.1 Upon deactivation of the Services, all Personal Data shall be deleted, save that this requirement shall not apply to the extent MageMail is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which such Personal Data MageMail shall securely isolate and protect from any further processing, except to the extent required by applicable law.

8. Cooperation

8.1 To the extent that Customer is unable to independently access the relevant Personal Data within the Services, MageMail shall (at Customer's expense) taking into account the nature of

the processing, provide reasonable cooperation to assist Customer by appropriate technical and organizational measures, in so far as is possible, to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to MageMail, MageMail shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If MageMail is required to respond to such a request, MageMail shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

8.2 To the extent MageMail is required under applicable Data Protection Law, MageMail shall (at Customer's expense) provide reasonably requested information regarding MageMail's processing of Personal Data under the Agreement to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

9. Miscellaneous

9.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

9.2 This DPA is a part of and incorporated into the Agreement so references to "Agreement" in the Agreement shall include this DPA.

9.3 In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

9.4 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

Annex A – Standard Contractual Clauses

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The Customer under the MageMail DPA accepting the clauses (the “data exporter”)

and

MageMail

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

For the purposes of the Clauses:

Clause 1

Definitions

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter*' means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to

a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on

the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the

Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of

protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[1]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

1 Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

    (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

    (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter.

Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter

The data exporter is the entity defined as the data exporter above.

Data importer

The data importer is MageMail.

Data subjects

Data subjects, if any, are within the control of the data exporter and may include individuals about whom data is provided to data importer by or at the direction of the data exporter pursuant to applicable terms of service between them.

Categories of data

The categories of personal data, if any, are within the control of the data exporter and may include data relating to individuals to the extent provided to data importer by or at the direction of the data exporter pursuant to applicable terms of service between them.

Processing operations

The processing operations are the Services (as defined in the Data Processing Agreement between the parties) that are used by the data exporter and described in respective documentation.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The description of technical and organisational security measures implemented by the data importer are described in Annex B to the Data Processing Agreement executed between the parties.

Annex B - Security Measures

Available upon request