



**Data Processing Agreement
for Cloud Services
[with EU Standard Contractual Clauses]**

This data processing agreement (the “Data Processing Agreement”) is by and between on the one hand **[INSERT ACCOUNT NAME]** having a principal place of business **[ADDRESS]** (“Customer”) and

For Adobe Cloud Services: **Adobe Systems Software Ireland Limited**, having a principal place of business at 4-6 Riverwalk, City West Business Campus, Saggart D24, Dublin, Ireland (“Adobe”); or

For Marketo Services: whichever of **Marketo, Inc.**, a company incorporated in the State of Delaware and **Marketo EMEA Limited**, a company registered in Ireland (“Marketo”) is the party to the Marketo Agreement; or

For Magento Services: **X.commerce, Inc. dba Magento, Inc.**, having a principal place of business of 345 Park Avenue San Jose, CA 95110 USA (“Magento”),

on the other hand.

Adobe, Marketo and Magento provide certain hosted services. This Data Processing Agreement supplements any Cloud License Agreement for such services, as applicable and is meant to ensure the parties’ compliance with the requirements imposed by the applicable data protection laws and regulations for Customer’s use of Cloud Services.

The attached Attachments supplement the terms of this Data Processing Agreement.

This Data Processing Agreement is intended to provide consistent obligations for each of Adobe, Marketo and Magento, where possible, but highlights those areas (sub-processors, technical and organizational measures) where there may be service-specific differences.

If the parties previously entered into a data processing agreement for Cloud Services, this Data Processing Agreement shall now supersede the foregoing.

1. Definitions.

The capitalized terms will have the meanings set forth below:

- a. “Cloud Services” means the collective Adobe Cloud Services, Magento Services or Marketo Services that are subject to the provisions of this Data Processing Agreement.
- b. “Cloud License Agreement” means the Adobe Agreement, Marketo Agreement or Magento Agreement, as applicable for the respective Cloud Service.
- c. “Adobe Cloud Services” means the On-demand Services or Managed Services provided by Adobe, including applicable Support Services where processing of Personal Data is expressly permitted.
- d. “Adobe Agreement” means the agreement under which Adobe, or Adobe as authorized agent of Adobe Systems Pty Ltd (Adobe Australia), supplies Customer with the Adobe Cloud Services, whether directly or indirectly.

- e. "European Data Protection Laws" means the General Data Protection Regulation (EU) 2016/679 ("GDPR"), Directive 2002/58/EC (as amended by Directive 2009/136/EC) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), any national laws or regulations implementing the foregoing Regulation and Directive, and any amendments or replacements thereto, or any successor for the GDPR associated with the withdrawal of the United Kingdom from the EU.
- f. "Instruction" means any documented instruction - written or by data input - received by Processor from Customer, including licenses granted under the Cloud License Agreement.
- g. "Magento Agreement" means any and all agreements under which Magento or Adobe, as applicable, supplies Customer with the Magento Services, including but not limited to those agreements accessible via <https://magento.com/legal/terms> (as may be amended from time to time).
- h. "Magento Services" refers to Magento Commerce (cloud), Magento Order Management, Magento Business Intelligence and Magento Support Services provided by Magento under a Magento Agreement.
- i. "Marketo Agreement" means the agreement (commonly named an end user subscription agreement, end user services agreement, master subscription and services agreement, or licensing agreement) and all related orders for Marketo Services, licensed by Marketo or Adobe.
- j. "Marketo Services" means the software as a service and Support Services under the Marketo Agreement.
- k. "Personal Data" shall have the same meaning as defined under European Data Protection Laws.
- l. "Personal Data Breach" means a confirmed unauthorized access by a third party or confirmed accidental or unlawful destruction, loss or alteration of Personal Data.
- m. "Process" or "Processing" shall have the meaning as defined under applicable European Data Protection Laws.
- n. "Processor" is either Adobe, Magento or Marketo, for the respective Cloud Services provided by that party to Customer.
- o. "Standard Contractual Clauses" means the agreement pursuant to European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of Personal Data to processors established in third countries which do not provide an adequate level of data protection, attached hereto as Attachment 1.
- p. "Support Services" means the applicable customer support services provided by Processor under the Cloud License Agreement.
- q. All other capitalized terms not defined in this Data Processing Agreement shall have the meanings ascribed to them in the respective Cloud License Agreement, as applicable.

2. Applicability.

- a. The provisions of this Data Processing Agreement are applicable to the Processing of Personal Data by the respective Processor, to the extent the Processing and use of such Personal Data is permitted under the Cloud License Agreement.
 - i. In case of discrepancies between this Data Processing Agreement and the applicable Cloud License Agreement, the provisions of this Data Processing Agreement shall prevail. If there are any discrepancies between this Data Processing Agreement and the Standard Contractual Clauses, where the Customer, as data exporter, has entered into the Standard Contractual Clauses for the purposes of this Data Processing Agreement, in which case, the Standard Contractual Clauses shall prevail.

3. Processing and Categories of Personal Data.

- a. Details of Processing of Personal Data. The subject matter, nature and purpose and details of the data processing and the details of the type of Personal Data and categories of data subjects are as set out in Appendix 1 to Attachment 1.
- b. Locations of Processing.
 - i. Adobe Processes Personal Data in the locations described in the Adobe Privacy Center website: www.adobe.com/go/processing
 - ii. Magento Processes Personal Data in one of the available European hosting locations, selected by Customer.
 - iii. Marketo Processes Personal Data in one of the available European hosting locations, selected by Customer.

4. Data Controller.

In accordance with all applicable data protection laws, Customer shall be the data controller.

5. Processor's Responsibility.

Processor will only Process Personal Data within the scope of Customer's Instructions for the applicable Cloud Services. Processor shall notify Customer promptly if it considers that an Instruction from Customer is in breach of European Data Protection Law, and Processor shall be entitled, but not obliged, to suspend execution of the Instructions concerned, until Customer confirms such Instructions in writing. Notwithstanding the foregoing, Processor may process the Personal Data if it is required under law to which it is subject. In this situation, Processor shall inform the Customer of such a requirement before Processor Processes the data unless the law prohibits this on important grounds of public interest.

6. Technical and Organization Measures and Security of Processing.

- a. 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, Processor has implemented and maintains technical and

organizational measures to ensure a level of security of the processing of Personal Data appropriate to the risk of the respective Cloud Service.

- i. Technical and Organizational Measures for Adobe Cloud Services are accessible here: <https://www.adobe.com/go/CloudSvcTOSM>. Adobe has obtained the third-party certifications and audits listed on Adobe's Trust Center website (also accessible via <https://www.adobe.com/security/compliance.html>).
 - ii. Technical and Organizational Measures for Magento Services set forth in Magento's Security, Privacy and Architecture Guide, are available here: www.adobe.com/go/magento-security-guide.
 - iii. Technical and Organizational Measures for Marketo Services are accessible here: www.adobe.com/go/marketo-dpa.
- b. Processor's Technical and Organisational Measures are subject to technical progress and further development. Accordingly, Processor reserves the right to modify the Technical and Organisational Measures provided that the functionality and security of the Cloud Services are not degraded.

7. Personal Data Breach

In the case of a Personal Data Breach, Processor will notify Customer without undue delay after Processor becomes aware of the Personal Data Breach via the email address specified by Customer in Clause 15 or as may be provided in the Cloud Services user interface and, as required by Article 33 of the General Data Protection Regulation, Processor shall supply Customer with information regarding the Personal Data Breach (to the extent that such information is available to Processor) to enable Customer to comply with its notification requirements to the supervisory authority (and, if necessary, the relevant data subjects) under European Data Protection Laws. Processor will, promptly, commence a forensic investigation of a Personal Data Breach and take appropriate remedial steps to prevent and minimize any possible harm. For the avoidance of doubt, Personal Data Breaches will not include unsuccessful attempts to, or activities that do not, compromise the security of Personal Data including, without limitation, unsuccessful log in attempts, denial of service attacks and other attacks on firewalls or networked systems.

8. Further Obligations

- a. Taking into account the nature of the Processing under this Data Processing Agreement, Processor shall take all reasonable steps to assist Customer in meeting Customer's obligations under Articles 30, and 32 to 36 of GDPR. Processor and Customer agree that, for the purposes of Article 30 GDPR, the Cloud License Agreement and this Data Processing Agreement constitute the record of all categories of Processing activities carried out by Processor on behalf of Customer.
- b. Processor will, at the choice of the Controller, delete or return to the Controller all Personal Data after the end of the applicable Cloud License Agreement, unless applicable law requires continued storage of Personal Data.

9. Responsibilities of the Data Controller.

- a. Instructions. Customer shall give Instructions to Processor as agreed by the Parties in the Cloud License Agreement.
- b. Information Duty. If Customer becomes aware of any breaches of, or other irregularities with, the requirements of all applicable data protection laws, if required by applicable law, Customer shall promptly notify and provide Processor with Instructions detailing the Processing activities Processor must take to ensure the protection of Personal Data, or avoid non-compliance with applicable data protection laws.

10. Costs.

In the event that Customer instructs Processor to provide assistance which goes beyond the standard functionality of the Service(s), then Processor may charge Customer for any costs beyond the agreed upon license fees to the extent it is not commercially reasonable for Processor to provide such assistance without charge (considering relevant factors such as volume of requests, complexity of Instructions and timescale requested). This shall include, without limitation, costs incurred by Processor in executing Customer's Instructions relating to the erasure, additional storage and/or retention of Customer's Personal Data, and compliance with any subject access request received by Customer in accordance with Clause 11.

11. Access and Data Deletion.

Data Subject Requests. Processor will promptly inform Customer of any data subject requests it receives in connection with the Cloud Services licensed by Customer. Customer is responsible for ensuring such requests are handled in accordance with European Data Protection Laws. Processor will implement appropriate technical and organizational measures to assist Customer with its obligations in connection with such data subject requests.

12. Audit

- a. Customer may audit Processor's compliance with the terms of this Data Processing Agreement up to once per year (either for itself or on behalf of a regulatory body to which it is subject and only pursuant to a formal request for information from such regulator) ("Audit").
- b. Customer agrees that its right to audit set out above means that it shall be entitled to exercise the following process:
 - i. Customer will be able to review the output of the formal annual independent review of Processor's Technical and Organisational Measures conducted by a reputable qualified third party ("Compliance Report").
 - ii. Upon review of the Compliance Report if Customer identifies areas that have not been covered that is it lawfully under this Data Processing Agreement permitted to audit, then Customer will submit an additional list of reasonably specific and detailed questions to Processor in writing. ("Audit Questions").

1. Within a reasonable timeframe, Processor will respond to the Audit Questions (“Responses”) to Customer (or its Regulator if so Instructed by Customer).
 2. Customer agrees that upon receipt of the responses to the Audit Questions Customer will have completed its Audit, unless Customer can objectively demonstrate that the Responses do not adequately demonstrate Processor’s compliance with its statutory obligations and this Data Processing Agreement. Under such an event, Customer may then be entitled to invoke the process set out below.
- iii. Subject to compliance with i. and ii. above, Customer shall be entitled to request a formal audit of Processor’s compliance with this Data Processing Agreement concerning the Audit Questions not already covered by the documentation provided by Processor (“Gap Audit”). To do so Customer must submit a detailed audit plan to Processor at least two weeks in advance of the proposed audit date. The audit plan must describe the proposed scope, duration, and start date of the Gap Audit. Processor will review the audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Processor security, privacy, employment or other relevant policies), and work with Customer to agree on a final audit plan.
1. The Gap Audit will at all times be subject to the following:
 - a. It must be conducted during normal business hours at the applicable facility, subject to Processor policies with respect to on-site visitors and may not unreasonably interfere with Processor business activities;
 - b. The parties agree to use the least intrusive means to verify Processor's, compliance with obligations under this Data Processing Agreement;
 - c. The Parties agree to respect the need for Processor to maintain the security of facilities and uninterrupted business operation, protect themselves and customers from risk and to prevent disclosure of information that would jeopardize the confidentiality of Processor or Processor’s customers’ information.
 - d. If Customer appoints a third party is to conduct the Gap Audit, the third party must be mutually agreed to by Customer and Processor and must execute a written confidentiality agreement acceptable to Processor before conducting the Gap Audit.
 - e. Where Customer is conducting a Gap Audit as a result of a regulator’s requests, and if Processor and/or Processor’s sub-processor believe that it is not possible to meet a specific time frame set by the regulator, Processor and/or its sub-processor will assist Customer to explain this to the relevant regulator. Customer acknowledges that access to the sub-processor's facilities is subject to agreement from the relevant sub-processor, and that Processor cannot guarantee access to that sub-processor's facilities at any particular time.

- f. Customer will provide Processor any Gap Audit reports generated under this section, unless prohibited by law. Customer may use the Gap Audit report only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this Data Processing Agreement.
- g. The Gap Audit report is Confidential Information of the parties under the terms of the Cloud License Agreement.
- iv. With exception of the Compliance Reports, any Audits and any related costs incurred by Processor (e.g. damages caused by Customer or its auditors to facilities or data held therein) are at the Customer's expense.

13. Sub-processors

- a. Customer agrees that Processor shall be entitled to use sub-processors for the respective Cloud Service listed as follows:
 - i. For Adobe Cloud Services: <http://www.adobe.com/go/processing>;
 - ii. For Magento Services: www.adobe.com/go/magento-subprocessors; and,
 - iii. For Marketo Services www.adobe.com/go/marketo-subprocessors.
- b. Processor has entered into agreements with the applicable sub-processors which ensure that such sub-processors shall be obliged to meet equivalent obligations as those set out in this Data Processing Agreement. Where the Standard Contractual Clauses are applicable and where the sub-processor is located in a third country which does not provide adequate protection for Personal Data, for the purposes of Clause 11(1) of the Standard Contractual Clauses, Processor has entered into the Standard Contractual Clauses with such sub-processors. Where Processor's sub-processor fails to fulfil its data protection obligations, Processor will remain responsible.
- c. Adding Sub-processors. At least 14 days prior to authorizing any new sub-processor to access Personal Data, Processor will update the respective Processor Website for the Cloud Service and such update will serve as notice to Customer. Customer may subscribe to (i) receive email notifications for updates to the Adobe Processor Website via the link on the site or (ii) the RSS feed for notification available on the respective Marketo and Magento Sub-processor websites. If Customer wishes to object to the approval of the new sub-processor it must provide such objection in writing to Processor promptly after receipt of Processor's notice. In the event that Customer objects to such new sub-processor then Customer may terminate the applicable Cloud Service without penalty by providing written notice of termination that includes an explanation on the grounds for non-approval.
- d. Sub-processor Agreements. Where the Standard Contractual Clauses are applicable, the parties agree that the obligation at Clause 11(1) to seek approval for sub-processors is met by the process outlined above and that the copies of sub-processor agreements that must be sent to data exporter by data importer pursuant to Clause 5(j) of the Standard Contractual Clauses may have

all commercial information removed by the data importer, and that such copies will be provided by data importer only upon request.

14. Adequate Data Transfer Mechanism to the US.

Standard Contractual Clauses. For transfers of Personal Data from the European Economic Area to the US, Customer (as data exporter) and each of Adobe Inc., Magento, and Marketo, Inc. (as data importers, as relevant) enter into the terms of the Standard Contractual Clauses in Attachment 1 for the transfer of Personal Data to the relevant data importer.

15. Contact Information and Notifications:

a. For Processor:

Data Protection Officer - Adobe
Adobe Systems Software Ireland Limited
4-6 Riverwalk,
City West Business Campus
Dublin 24
Ireland
Email: dpo@adobe.com

Data Protection Officer – Marketo
Marketo EMEA Limited
4-6 Riverwalk,
City West Business Campus
Dublin 24
Ireland
Email: privacyofficer@marketo.com

Data Protection Officer – Magento
X.commerce, Inc. d/b/a Magento, Inc.
345 Park Avenue
San Jose, CA 95110
USA
Email: magprivc@magento.com

b. For Customer:

Customer Data Protection Officer:

Insert name

Insert email

Customer Representative:

Insert name

Insert email

Insert name

Insert email

Customer Representative:

Insert name

Insert email

16. Miscellaneous.

No amendment, change or suspension of this Data Processing Agreement shall be valid unless agreed upon in writing between Customer and Adobe and unless this Data Processing Agreement is expressly referred to.

17. Independent Parties.

Adobe, Magento and Marketo are independent parties and the processing activities with respect to each Processor under this Data Processing Agreement are solely the responsibility of that Processor for their respective Cloud Services.

Adobe Systems Software Ireland Limited
4-6 Riverwalk, City West Business Campus, Dublin 24
Ireland

[CUSTOMER NAME]
[INSERT ACCOUNT BILLING ADDRESS]

Authorized Signature

Authorized Signature

Print Name

Print Name

Title

Title

Date

Date

Adobe Systems Software Ireland Limited
4-6 Riverwalk, City West Business Campus, Dublin 24
Ireland

Legal Entity Name
Account Name
Account Billing Address

Authorized Signature

Authorized Signature

Print Name

Print Name

Title

Title

Date

Date

Authorized Signature

X.commerce, Inc. d/b/a Magento, Inc.

Authorized Signature

Print Name

Title

Date

Marketo EMEA Ltd.

Authorized Signature

Print Name

Title

Date

Marketo Inc.

Authorized Signature

Jonathan Vaas

Print Name

Title

Date

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 protection

The entity identified as “Customer” on the Data Processing Agreement for Cloud Services (with EU Standard Contractual Clauses are attached) (the “data exporter”)

AND

- (1) In respect of Adobe Cloud Services, Adobe Inc., 345 Park Avenue, San Jose, CA 95110, USA;
- (2) In respect of Marketo Services, Marketo Inc., 901 Mariners Island Boulevard, Suite #500, San Mateo CA 94404, USA;
- (3) In respect of Magento Services, X.commerce, Inc. d/b/a Magento, Inc., 345 Park Avenue San Jose, CA 95110 USA

(each, the “data importer”, in respect of the applicable services only)

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 the Data Processing Agreement and subject to data permitted under the applicable Cloud License Agreement.

Clause 1

Definitions

For the purposes of the Clauses:

- (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 sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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 organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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 sub-processor 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 sub-processor 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 organizational 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, unauthorized 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 sub-processor 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 sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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

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 organizational 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 unauthorized access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized 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;
- (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 sub-processing, 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor 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 or 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor 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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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**Sub-processing**

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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor 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 sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing 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 sub-processing 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 sub-processor 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 sub-processor 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.

On behalf of the data exporter:

Legal Entity Name
Account Name
Account Billing Address

Authorized Signature

Print Name

Title

Date

On behalf of the data importer:

Adobe Inc.
345 Park Avenue San Jose, CA 95110-2704
USA

Authorized Signature

Print Name

Title

Date

X.commerce, Inc. d/b/a Magento, Inc.

Authorized Signature

Print Name

Title

Date

Marketo Inc.

Authorized Signature

Print Name

Title

Date

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter

The data exporter is identified as “Customer” in the Cloud License Agreement to which these Standard Contractual Clauses refer.

Data importer

The data importer is the provider of software and services to the data exporter.

Data subjects

Data subjects may include the data exporter’s end users, customers, prospects, business partners, vendors, contractors, employees, agents, and advisors.

Categories of data

For Adobe Cloud Services:

The subject matter, nature and purpose and details of the data processing and the details of the type of Personal Data and categories of data subjects are determined by the exporter in their use of the Adobe Services in accordance with, and subject to the limits of, the Agreement and as described here: www.adobe.com/go/processing.

For Marketo Services:

The subject matter, nature and purpose and details of the data processing and the details of the type of Personal Data and categories of data subjects are determined by the exporter in their use of the Marketo Services are in accordance with, and subject to the limits of, the Marketo Agreement and as more specifically described in the applicable documentation available here:

- <https://docs.marketo.com/display/public/DOCS/Product+Docs> and
- <https://docs.marketo.com/display/public/DOCS/Using+the+Person+Detail+Page>.

For Magento Services:

The subject matter, nature and purpose and details of the data processing and the details of the type of Personal Data and categories of data subjects are determined by the exporter in their use of the Magento Service in accordance with, and subject to the limits of, the terms of the Magento Agreement(s) and the product documentation applicable to the Magento version:

- Personal Information Reference for [Magento 1.x](#)
- Personal Information Reference for [Magento 2.x](#)

Sensitive data

The personal data transferred may include the following categories of sensitive data, as determined at the sole discretion of the data exporter and as permitted by the Cloud License Agreement:

- Sexual preferences
- Medical or health information
- Political Opinions
- Religious beliefs

- Trade union membership
- Racial or ethnic origin

Purposes of the transfer / Processing operations

The personal data transferred will be subject to the following basic processing activities:

The processing of the personal data by data importer shall be to enable (1) the performance of the Cloud Services; (2) to provide any technical and customer support as requested by data exporter; and, (3) to fulfil all other obligations under the Cloud License Agreement.

SAMPLE

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

The data importer has implemented and will maintain appropriate technical and organizational measures to protect the Personal Data, against misuse and accidental loss or destruction as set forth in Section 6 of the Data Processing Agreement (with EU Standard Contractual Clauses), and which are hereby incorporated into this Appendix 2 by reference.

SAMPLE