MARKETO

TECHNICAL AND ORGANIZATIONAL MEASURES FOR DATA PROTECTION

This document describes Marketo's technical and organizational security measures implemented to protect the security and privacy of Customer Data. All such measures are assessed in light of the varying risks posed to the privacy rights of natural persons whose personal data may be processed as a part of Customer Data.

Security Audits

- Marketo employs reputable third parties to conduct regular security audits, including SOC 2 Type 2 or equivalent audits on an annual basis. Upon written request and pursuant to confidentiality contract terms and/or a non-disclosure agreement, Marketo will provide its most current security audit report to Marketo customers, which may supplement or clarify the measures set forth herein.
- Marketo also conducts vulnerability testing and internal penetration testing for every new software release, including at least one annual third party penetration test.

Data Protection Policies and Governance

- Marketo bases its security process on identifying the risks associated with the loss of confidentiality, integrity and/or availability of information that are posed to Customer and Data Subject rights.
- Marketo oversees and manages the implementation of the various aspects of the privacy and security programs in written policies and procedures and routinely reassesses risk.
- Documented information security and privacy policies and procedures have been approved by management, published, and communicated to all relevant employees and external parties utilizing appropriate document management processes.
- Information security and privacy policies and procedures are reviewed at least annually, or if significant changes occur, to ensure their continuing suitability, adequacy, and effectiveness.
- All information security roles and responsibilities are defined, with risk owners identified.
- Confidentiality terms and non-disclosure agreements reflecting the organization's needs for the protection of information are regularly reviewed and updated as necessary.

- Marketo's approach to managing data protection and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) are reviewed independently at least annually and when significant changes to the security implementation occur.
- Information assets are inventoried and classified; asset owners are assigned, and procedures defined for acceptable data use, labelling, and handling.
- Management ensures that information security policies and objectives are set, integrated, compatible with the organization's strategic direction, and achieve desired outcomes.

Employee Risk Governance

Marketo takes appropriate measures to ensure that persons who have demonstrated traits averse to data protection are not employed by Marketo as well as to ensure that all employees receive data protection training. Such measures include:

- background verification on all candidates for employment are carried out in accordance with applicable laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks;
- training of employees on applicable security and privacy policies, laws and issues (including GDPR, HIPAA, data security), as well as recurring security awareness campaigns.
- all employees are subject to confidentiality provisions in employment agreements that prohibit the misappropriation and misuse of Customer Data and company proprietary information.

Security Measures

Confidentiality and Integrity Controls

Marketo implements appropriate measures to prevent its data processing systems from being used by unauthorized persons and ensures that Customer Data is only processed in accordance with documented instructions of its customers. Marketo also implements appropriate measures to ensure that it can establish whether and by whom Customer Data has been input into or removed from data processing systems as outlined below:

Systems Access Controls

The measures that protect access to all Marketo systems include, at a minimum, the following:

- encryption of all remote sessions (including mobile, remote and portable devices) to Marketo SaaS applications using industry standard algorithms utilizing Hypertext Transfer Protocol Secure (HTTPS) and/or Transport Layer Security (TLS 1.2);

- provision of network intrusion detections systems (IDS) and intrusion prevention systems (IPS) by enhanced firewall modules or separate IPS devices;
- maintaining system administrators' access logs for at least six months and keeping them secure, accurate and unmodified;
- audit of system administrators' activities to assess compliance with assigned tasks, the instructions received by Marketo and applicable laws;
- log of system administrators' identification details (*e.g.*, name, surname, function or organizational area) and tasks assigned;
- adoption of suitable measures to register system administrators' access logs and keep them secure, accurate and unmodified for at least six months;
- logging, tracking, and monitoring of all data transmissions to and from systems;
- logging of user ID log-in events (monitoring of break-in-attempts);
- formal systems for user registration and de-registration to enable access right assignment and processes for authenticating users and revoking access;
- secure log-on procedures used to authenticate user access to systems;
- utilization of user codes (passwords) of at least eight characters or the system maximum permitted number and modification at first use and thereafter at least every 90 days;
- policy requiring all employees with access to personal data processed for Marketo customers to reset their passwords at least once in a 180-day period;
- automatic workstation session timeouts of no more than 15 minutes;
- automatic lock-out of the user ID to systems after several erroneous passwords are entered;
- deactivation of user authentication credentials (such as user IDs) in case the person is disqualified from accessing personal data or in case of non-use for a substantial period of time (at least six months), except for those authorized solely for technical management;
- authentication of the authorized personnel, including individual authentication credentials such as user IDs that cannot be reassigned to another person once registered (including subsequently), as well as two-factor authentication.
- enforcement of role-based and ‘need-to-know’ access to Customer Data;
- enforcement of policies restricting and limiting employee access rights to personal data, informing employees about their obligations and the consequences of any violations of such obligations, to

ensure that employees will only access Customer Data and resources required to perform their job duties;

- removal of all access rights of all employees, contractors and third party users to information and information processing facilities upon termination of their employment, contract or agreement -- or adjustment upon change of status;
- requirement that all employees, contractors and third party users return all of the organization's assets in their possession upon termination of their employment, contract or agreement;
- quarterly audits of employee access accounts to all systems;
- maintaining a formal system for user registration and de-registration to enable access right assignment and processes for authenticating users and revoking access;
- secure log-on procedures are used to authenticate user access to information and application systems;

Data Access Controls

In addition to the above System Access Controls, the measures that apply to Customer Data entrusted to Marketo include, at a minimum, the following:

- requirement of identification and password to reopen closed user terminals for devices allowing access to Customer Data;
- logging, tracking and monitoring of accesses to all Customer Data;
- logging, tracking, and monitoring of all Customer Data transmissions;
- enforcement of role-based and 'need-to-know' access to Customer Data;
- destruction of Customer Data within 30 days of termination of Subscription Services;
- secure disposal of media on which Customer Data is stored when it is no longer required;
- an authorization policy and protective measures for the input of Customer Data into memory, as well as for the reading, alteration and deletion of stored data;
- provision of customers with the option of data at-rest encryption for Customer Data;
- the use of automated handshake protocols as well as manual monitoring of the completeness and correctness of the transfer of Customer Data (end-to-end check);
- antivirus checks and blocking of potentially unsafe files performed on all files uploaded into the customer's Marketo instance;

Premises Access Controls

The measures taken to ensure the security of premises controlled or owned by Marketo include the following, with respect to Data Centers and Business Offices.

Data Centers

Marketo's Data Centers where Customer Data is hosted or stored (physical premises housing data storage equipment) implement ISO 27001-certified measures in order to prevent unauthorized persons from gaining access to the data processing equipment. This is accomplished by at least the following measures:

- utilizing unmarked facilities;
- security check-in process required for all visitors to all facilities;
- 24-hour security service, including security alarms, video surveillance and security guards at all facilities;
- logging, monitoring, and tracking all access to the Data Centers;
- A mandatory color-coded, photo ID badge system that identifies employees uniquely;
- Two-factor authentication required to gain access to sensitive areas of the Data Center and mandatory two-factor authentication for all access to business applications;
- Biometric access to devices, including fingerprint or three-dimensional facial recognition where feasible;
- Closed circuit video surveillance on the interior and exterior of all entrance points; and
- Restricted physical access to Marketo servers within the raised floor of the Data Center limited to authorized personnel only.

Business Offices

Marketo does not store Customer Data in its Business Offices (registered locations where Marketo employees conduct business other than at Data Centers). Marketo implements appropriate physical security measures at its offices, including, a minimum, the following:

- 24-hour security service provided by property owner, including security alarms, video surveillance and security guards;
- securing data processing equipment;
- personal access controlled with photo ID badges;

- electronic card-keys;
- Clean Desk policy;
- secure destruction of paper waste through third party shredding service.

Availability Controls

Marketo implements measures to ensure that Customer Data are protected from accidental destruction or loss. This is accomplished through at least the following measures:

- each network device relied upon by Marketo, including firewalls, switches and intrusion detection has a failover backup to ensure maximum uptime;
- dedicated routers and switches feature redundant power and connectivity to the internet;
- internet redundancy is achieved using multiple physical connections with multiple peering point providers;
- all Customer Data is backed up on network storage subsystems across the infrastructure;
    - For critical information in U.S. jurisdiction Data Centers, near-line backups are mirrored over secure links and stored in remote Marketo Data Centers within the same jurisdiction;
    - The Europe region backups are performed daily and stored offsite in a third party system that meets the same standards and is within the same jurisdiction;
    - The Australia region Data Center is mirrored and stored in an alternate location within Australia;
- redundant lines of communication to telecommunication providers providing customers with failover communication paths in the event of data communications interruption;
- implementation of sensors to detect environmental hazards, including smoke detectors, floor water detectors and fire detection and suppression systems;
- raised floors to protect equipment from water damage;
- uninterruptible power supplies (UPS) to mitigate the risk of short-term utility power failures and fluctuations;
    - the UPS power subsystem is at least n+1 redundant with instantaneous failover in the event of a primary UPS failure;
    - the UPS systems are inspected and/or serviced at least annually by a third party contractor;

- diesel generators to mitigate the risk of long-term utility power failures and fluctuations; generators are tested at least every 120 days and serviced at least annually by a third party contractor to maintain appropriate operability in the event of an emergency;

- any detected physical security incident is recorded, alongside the followed data recovery procedures, and the identification of the person who carried them out.

Application Design Data Protection Measures

At a minimum, the following controls are implemented to protect Customer Data through the design of the Marketo applications:

- adherence to a software development process that follows the OWASP standards for building secure applications, including stringent code reviews, integration and regression testing, and full internal and external security testing for vulnerabilities;

- access to data is logically separated for only appropriate users;

- each customer Marketo instance is stored on a separate database with Marketo's corporate instance separated from the customer environment;

- at the database level, data is stored in different data sets, logically separated per module or function they support;

- interactive processes, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately;

- granular permissions for various roles, design functions, campaign execution and person/lead database actions;

- Privacy by Design program to protect Data Subject privacy rights.

Application Confidentiality and Integrity Control Features

Personal data entry is managed by the Customer through the Marketo application user interface, where at least the following security features are available to the Customer:

- adherence to a software development process that follows the OWASP standards for building secure applications, including stringent code reviews, integration and regression testing, and full internal and external security testing for vulnerabilities;

- access to data is logically separated for only appropriate users;

- each customer Marketo instance is stored on a separate database with Marketo's corporate instance separated from the customer environment;

- at the database level, data is stored in different data sets, logically separated per module or function they support;
- interactive processes, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately;
- granular permissions for various roles, design functions, campaign execution and person/lead database actions;
- Privacy by Design program to protect Data Subject privacy rights.

Third Party (Sub-processor) Control and Management

Marketo takes appropriate measures to ensure that it remains accountable for onward transfers of Customer Data to third party Sub-processors that process personal data on Marketo's behalf as part of the subscription services. At a minimum, such measures include identifying the risks to Customer and Data Subject rights based upon nature, scope and context of processing; reviewing the security and data protection controls implemented by the Sub-processor to protect Customer Data (including SOC 2 Type 2 audit reports and/or ISO 27001 certificates as applicable); imposing data protection contractual terms that protect personal data to the same standard Marketo is obligated to provide its customers (including valid cross border transfer mechanisms, sub-processor management, and compliance programs); requiring the Sub-processor to only process Customer Data on behalf of Marketo and its customers and, limiting its processing of Customer Data to the scope of Marketo's instructions.

Data Protection Measures Specific to Certain Marketo Affiliates or Applications

The following data protection measures are in *addition* to, or a *modification* of, measures introduced in the general section.

Marketo Sales Engage/ToutApp

Audited Standards

The Marketo Sales Engage/ToutApp organization adheres to the same standards as the rest of the Marketo family of affiliated companies and also employs reputable third parties to conduct regular security audits, including SOC 2 Type 1 or equivalent audits on an annual basis. Upon written request, Marketo will provide the most current security audit report applicable to Marketo Sales Engage/ToutApp.

Bizible

Audited Standards

The Bizible organization adheres to the same standards as the rest of the Marketo family of affiliated companies and also employs reputable third parties to conduct regular security audits including SOC 2 Type 1 or equivalent audits on an annual basis. Upon written request, Marketo will provide the most current security audit report specific to Bizible.

Data Access Controls

- All data is encrypted at rest by default, without being specifically referenced in the applicable Order for Subscription Services.

Availability Controls

- Bizible maintains 30 days of point-in-time backups on Microsoft Azure Cloud, utilizing geo-replication features in North America.