MojoHost Security & Privacy Practices

Last Updated: April 1, 2022

1. Security Practices. MojoHost is responsible for the security measures set out in the Agreement and shall maintain and implement the following technical and organizational measures concerning the security of the Customer Configuration.

1.1 Physical Security - Data Centers. The following physical security controls apply to Customer Data residing in a data center or office premises either owned or leased by Easy Online Solutions, Ltd. d/b/a MojoHost or its Affiliate for providing Services to Customer (and expressly excludes third-party hosting Services):

(a) Servers and devices dedicated to Customer's use as part of the Customer Configuration provided by MojoHost will be located in a controlled-access data center (or part of it) either operated by or dedicated to use by MojoHost or its Affiliate.

(b) MojoHost operates or audits the use of an electronic access control system that logs access to physical facilities managed by a professional security guard force in line with its current processes.

(c) Access to the raised production floor of the data halls will be restricted to MojoHost employees or its agents who need access to provide the Services. Access within data center facilities is in zones and provisioned based on physical access rights required by a given individual. Access to designated "meet me" rooms will be available to customers, subject to data center escort policies.

(d) The data center will be staffed 24/7/365 and will be monitored by video surveillance, recording to a centralized location, and viewed by the onsite security force.

(e) MojoHost limits access to physical facilities to authorized individuals by proximity-based access cards and biometric hand scanners or other approved security authentication methods.

(f) Except as specifically stated in the Agreement, MojoHost will not relocate the Customer Configuration from a MojoHost data center to a data center in another country without Customer's express written permission.

(g) After the termination of the Agreement or a Customer Configuration, MojoHost will wipe data from those hard drives and storage devices dedicated to Customer use before re-use.

1.2 Security Controls Audits & Reporting. MojoHost shall engage qualified third-party auditors to perform examinations of its systems and services according to the best practice recommendations of ISO 27001 to audit MojoHost's compliance with SSAE 18 compliance frameworks and the AT 101 compliance framework (based on select Trust Services Principles) or equivalent industry standards or both. MojoHost's annual SOC report(s) or suitable equivalent standard(s) as specified by MojoHost is available to Customer on Customer's request subject to MojoHost's SOC distribution requirements. Not all MojoHost Services are included in the scope of the SOC report(s) or audits described in this section 1.2; for details, Customer should contact the MojoHost account manager.

1.3 Administrative Controls.

(a) Screening. MojoHost will perform pre-employment background screening of its employees who have access to Customer's account and is committed to employee supervision, training, and management.

(b) MojoHost Access. MojoHost will restrict the use of administrative access codes for Customer's account to its employees and other agents who need the access codes to provide the Services. MojoHost personnel who use access codes will be required to log on using an assigned username and password.

(c) Customer Access. As the primary system administrator, Customer is responsible for managing their account, including creation, change management, termination, and enforcement of related remote working and password controls.

1.4 PCI-DSS. For the security of cardholder data, as that term is defined in the Payment Card Industry-Data Security Standard, which MojoHost might possess or otherwise store, process, or transmit on Customer's behalf, MojoHost will provide (a) those physical, technical, and administrative safeguards described in the Agreement and (b) the Services selected by Customer and described in the Agreement, except that Customer remains responsible for ensuring all PCI-DSS requirements are met for that cardholder data. MojoHost maintains PCI-DSS Service Provider, or equivalent, accreditation for dedicated hosting services (excluding managed virtualization services).

1.5 Reports of and Response to Security Breach. MojoHost will report to Customer as soon as reasonably practicable in writing and under law, of a material breach of the security of the Customer Configuration that results in unauthorized access to Customer Data resulting in the destruction, loss, unauthorized disclosure, or alteration of Customer Data of which MojoHost becomes aware. On request, MojoHost will promptly provide to Customer all relevant information and documentation that MojoHost has available to MojoHost regarding the Customer Configuration for any such event. MojoHost is not obligated to notify routine security alerts about the Customer Configuration (including pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing, or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers, or similar incidents) except as otherwise specifically set out in the Agreement.

1.6 Customer Data.

(a) Customer remains the primary system and account administrator and is responsible for the integrity, security, maintenance, and protection of Customer Data, including Sensitive Data, by: (i) selecting, buying, and properly configuring appropriate Services; (ii) implementing adequate controls to maintain appropriate security, protection, and deletion of Customer Personal Data (which shall include encryption and logical access measures); (iii) ensuring that MojoHost is not provided with any access to Customer Data, except as otherwise explicitly set out in the Agreement; and (iv) using the data integrity controls to allow Customer to restore the availability of Customer Personal Data in a timely manner (which shall include routine backups and archiving of Customer Personal Data in an environment separate from the Customer Configuration). Customer Data is, and at all times will remain, Customer's exclusive property. MojoHost will only back up data if stated on a Service Order, and MojoHost will not use or disclose Customer Data except as materially required to perform the Services or as required by law.

(b) Unless otherwise specified in the Service Order, the Services enable Customer to retrieve, correct, and delete Customer Data. Customer's access to the Customer Configuration or Customer Data may be restricted during a suspension or after the termination of the Services or the Agreement. Customer is responsible for retrieving a copy of Customer Data before the termination of the Agreement. MojoHost may delete Customer Data at any time after Agreement termination.

(c) Customer will cooperate with the investigation and resolution of outages and security incidents. MojoHost is not responsible to Customer or any nonparty for unauthorized access to Customer Data or for unauthorized use of the Services that is not solely caused by MojoHost's failure to meet its security obligations under the Agreement.

2. Privacy Practices. Customer and MojoHost will comply with laws concerning their collection and processing of any Sensitive Data in providing and using the Services.

2.1 Data Processing Addendum. If Applicable Data Protection Law applies to the Processing of Personal Data (as each of those terms are defined in the Data Processing Addendum), the Data Processing Addendum will form part of this Agreement.

2.2 CCPA. If the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq. ("**CCPA**") applies to the processing of Personal Information (as defined in the CCPA), the Consumer Privacy Protection Act Addendum will form part of this Agreement.