This Security Addendum amends the agreement between Mail & Deploy and the Customer that references this addendum and governs the use of Mail & Deploy SaaS ("Agreement"). In the event of any conflict between the Agreement and this Security Addendum regarding Mail & Deploy SaaS, this Security Addendum will prevail.

## SECURITY PROGRAM

Mail & Deploy recognizes that security is a fundamental consideration for Mail & Deploy SaaS customers and maintains a comprehensive documented security program based on ISO 27001 under which Mail & Deploy implements and maintains physical, administrative and technical safeguards designed to protect the confidentiality, integrity, availability and security of Mail & Deploy SaaS and Customer Content (the "Security Program") as set forth below. Mail & Deploy utilizes infrastructure-as-a-service cloud providers (each, a "Cloud Infrastructure Provider") and provides Mail & Deploy SaaS using storage hosted by the applicable Cloud Infrastructure Provider. Mail & Deploy regularly tests and evaluates its Security Program and may review and update its Security Program as well as this Security Addendum from time to time consistent with industry standards.

## 1. Definitions

"**Customer Content**" means information, data, media or other content provided by Customer (or any users authorized by Customer) for use with Mail & Deploy SaaS.

"**Mail & Deploy SaaS**" means a subscription-based, SaaS offering provided and managed by Mail & Deploy or its affiliate.

"**Security Incident**" means any unauthorized or unlawful destruction, loss, alteration or access to, or disclosure of, Customer Content that is in Mail & Deploy's possession or under Mail & Deploy's control. It does not include events which are either (i) caused by the Customer or Customer affiliates or their end users or third parties operating under their direction, such as the failure to (a) control user access; (b) secure or encrypt Customer Content which the Customer transmits to and from Mail & Deploy during performance of the Services; and/or (c) implement security configurations to protect Customer Content; or (ii) unsuccessful attempts or activities that do not or are not reasonably likely to compromise the security of Customer Content, including but not limited to unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

## 2. Audits and Certifications

Mail & Deploy's information security management program used to provide Mail & Deploy SaaS is assessed by 1 independent third-party auditor as described in the following audits and certifications ("Third Party Audits"), on an annual basis:

- ISO/IEC 27001:2022



MaD Reporting GmbH I 1030 Vienna I Austria I Kollergasse 6/1
FN 557097k I Commercial Court Vienna I VAT No. ATU 76904245
info@mail-and-deploy.com
www.mail-and-deploy.com

## 3. Hosting Location of Customer Content

The hosting location of Customer Content is determined by the location of the production instance of Mail & Deploy SaaS in the region selected by Customer upon initial tenant creation.

## 4. Encryption

4.1. Encryption of Customer Content. Mail & Deploy SaaS encrypts Customer Content at-rest using AES 256-bit (or better) encryption. Mail & Deploy SaaS uses Transport Layer Security (TLS) 1.2 (or better) for Customer Content in-transit over untrusted networks.

4.2. Encryption Key Management. Mail & Deploy SaaS provides per-tenant encryption keys, where the keys are updated when a customer saves changes to files within their tenant. Mail & Deploy SaaS logically separates encryption keys from Customer Content.

4.3. Customer-Managed Keys. Mail & Deploy SaaS has customer-managed key functionality, which enables Customers to create and manage their own encryption keys.

## 5. System & Network Security

5.1. Access Controls. Mail & Deploy SaaS is a no-view service where Mail & Deploy's internal network and Mail & Deploy personnel are separate from the production environment. Mail & Deploy personnel do not have direct access to Customer's Mail & Deploy SaaS Content and will not, subject to legal obligations, access Mail & Deploy SaaS Customer Content unless Customer invites Mail & Deploy into its tenant. The responsibility and access to perform operations, troubleshooting and support activity for Mail & Deploy SaaS is limited and restricted to Mail & Deploy personnel responsible for site reliability. All Mail & Deploy personnel access to Mail & Deploy SaaS is via a unique user ID, consistent with the principle of least privilege, requires a VPN, as well as multi-factor authentication and passwords.

5.2. Endpoint Controls. For access to Mail & Deploy SaaS, Mail & Deploy personnel use Mail & Deploy-issued laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) endpoint detection and response (EDR) tools to monitor and alert for suspicious activities and Malicious Code (as defined below), and (iii) vulnerability management in accordance with Section 4.7.3 (Vulnerability Management).

5.3. Separation of Environments. Mail & Deploy logically separates Mail & Deploy SaaS production environments from development environments.

5.4. Firewalls. Mail & Deploy shall protect the Mail & Deploy SaaS service using industry standard firewall with deny-all default policies to prevent egress and ingress network traffic protocols other than those that are business-required. In addition, Mail & Deploy also utilizes WAF technology.

5.5. Hardening. Mail & Deploy SaaS is hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in this Security Addendum.



MaD Reporting GmbH I 1030 Vienna I Austria I Kollergasse 6/1
FN 557097k I Commercial Court Vienna I VAT No. ATU 76904245
info@mail-and-deploy.com
www.mail-and-deploy.com

5.6. Monitoring & Logging

5.6.1. Infrastructure Logs. Monitoring tools or services, such as network-based IDS, are utilized to log certain activities and changes within Mail & Deploy SaaS. These logs are further monitored, analysed for anomalies and are securely stored to prevent tampering for at least one year.

5.6.2. User Logs. Customer tenant user logs of certain user activities and changes within their Mail & Deploy Cloud tenant are available to Customer for preservation and analysis.

5.7. Vulnerability Detection & Management

5.7.1. Anti-Virus & Vulnerability Detection. Mail & Deploy SaaS leverages industry standard threat detection tools with daily signature updates, which are used to monitor and alert for suspicious activities, potential malware, viruses and/or malicious computer code (collectively, "Malicious Code"). Mail & Deploy does not monitor Customer Content for Malicious Code.

5.7.2. Penetration Testing & Vulnerability Detection. Mail & Deploy works with an independent third party to conduct penetration tests of Mail & Deploy SaaS at least once annually. Mail & Deploy also runs weekly vulnerability scans for Mail & Deploy SaaS using updated vulnerability databases.

5.7.3. Vulnerability Management. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to Mail & Deploy SaaS. To assess whether a vulnerability is 'critical', 'high', or 'medium', Mail & Deploy leverages the National Vulnerability Database's (NVD) Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-Cert rating.

## 6. Administrative Controls

6.1. Personnel Security. Mail & Deploy conducts background checks on Mail & Deploy personnel as part of our standard hiring process, subject to local laws and regulations.

6.2. Personnel Training. Mail & Deploy maintains a documented security awareness and training program for Mail & Deploy personnel. Mail & Deploy personnel are also required to acknowledge and comply with key Mail & Deploy security policies.

6.3. Mail & Deploy Risk Management & Threat Assessment. Mail & Deploy's risk management process is modelled on ISO 27001. Mail & Deploy conducts an annual risk assessment, which includes Mail & Deploy SaaS, to review material changes in the threat environment and to identify potential control deficiencies in order to make recommendations for new or improved controls and threat mitigation strategies.

6.4. External Threat Intelligence Monitoring. Mail & Deploy reviews external threat intelligence, including US-Cert vulnerability announcements and other trusted sources of vulnerability reports. U.S.-Cert announced vulnerabilities rated as critical or high are prioritized for remediation in accordance with Section 5.7.3 (Vulnerability Management).



MaD Reporting GmbH I 1030 Vienna I Austria I Kollergasse 6/1
FN 557097k I Commercial Court Vienna I VAT No. ATU 76904245
info@mail-and-deploy.com
www.mail-and-deploy.com

6.5. Vendor Risk Management. Mail & Deploy maintains a vendor risk management program for vendors that process Customer Content designed to ensure each vendor maintains security measures consistent with Mail & Deploy's obligations in this Security Addendum. A list of these sub processor vendors may be found here.

## 7. Physical & Environmental Controls

7.1. Cloud Environment Data Centers. To ensure the Mail & Deploy SaaS Infrastructure Provider has appropriate physical and environmental controls for its data centers hosting the SaaS Service, Mail & Deploy regularly reviews those controls as audited under the Cloud Infrastructure Provider's third-party audits and certifications. Each Cloud Infrastructure Provider shall have a SOC 2 Type II annual audit and ISO 27001 certification, or industry recognized equivalent frameworks. Such controls, shall include, but are not limited to, the following:

7.1.1. Physical access to the facilities is controlled at building ingress points;
7.1.2. Visitors are required to present ID and are signed in;
7.1.3. Physical access to servers is managed by access control devices;
7.1.4. Physical access privileges are reviewed regularly;
7.1.5. Facilities utilize monitor and alarm response procedures;
7.1.6. Use of CCTV;
7.1.7. Fire detection and protection systems;
7.1.8. Power back-up and redundancy systems; and
7.1.9. Climate control systems.

7.2. Mail & Deploy Development Locations. While Customer Content is not hosted at Mail & Deploy offices, Mail & Deploy's technical, administrative and physical controls for its development locations are covered by its ISO 27001 certification and includes the following:

7.2.1. Physical access is controlled at office ingress points;
7.2.2. Badge access is required for all personnel and badge privileges are reviewed regularly;
7.2.3. Visitors are required to sign in;
7.2.4. Inventory of Mail & Deploy-issued laptops and network assets;
7.2.5. Fire detection and sprinkler systems; and
7.2.6. Climate control systems

## 8. Incident Detection & Response

8.1. Security Incident. Upon becoming aware of a Security Incident, Mail & Deploy will notify the Customer and take reasonable steps to identify, prevent and mitigate the effects of the Security Incident and to remedy the Security Incident to the extent such remediation is within Mail & Deploy's reasonable control.

8.2. Investigation. In the event of a Security Incident as described above, Mail & Deploy shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. Any logs determined to be relevant to a Security Incident, shall be preserved for at least one year.



MaD Reporting GmbH I 1030 Vienna I Austria I Kollergasse 6/1
FN 557097k I Commercial Court Vienna I VAT No. ATU 76904245
info@mail-and-deploy.com
www.mail-and-deploy.com

8.3. Communication and Cooperation. Security Incident notifications, if any, will be delivered to Customer by any means Mail & Deploy selects, including via email. It is the Customer's responsibility to ensure that it provides Mail & Deploy with accurate contact information and secure transmission at all times. Mail & Deploy shall provide Customer timely information about the Security Incident to the extent known to Mail & Deploy, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by Mail & Deploy to mitigate or contain the Security Incident, the status of Mail & Deploy's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because Mail & Deploy personnel may not have visibility to the content of Customer Content, it may be unlikely that Mail & Deploy can provide information as to the particular nature of the Customer Content impacted, or where applicable, the identities, number, or categories of affected data subjects. Communications by or on behalf of Mail & Deploy with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Mail & Deploy of any fault or liability with respect to the Security Incident.

## 9. Business Continuity and Disaster Recovery

9.1 Business Continuity Plan/Disaster Recovery Plan. As it relates to Mail & Deploy SaaS, Mail & Deploy is prepared to handle large business disruptions with its corporate business continuity program, which is driven by a Business Continuity Policy (BC Policy) and a Business Continuity Plan (BCP). BCP's are reviewed on an annual basis to confirm they are in accordance with the established policies and procedures. Mail & Deploy maintains a disaster recovery plan (DRP) to help ensure continued availability. The DRP is tested at least annually -date. Data backups are managed by a Cloud Infrastructure Provider to ensure redundancy. Primary and secondary backups are daily incremental and are encrypted in transit (SSL/TLS 1.2) and at rest (AES-256). Backups are retained in accordance with Mail & Deploy's internal Data Retention Policy.

## 10. Deletion of Customer Content

10.1. By Customer. Mail & Deploy SaaS provides Customer controls for the deletion of Customer Content.

10.2. By Mail & Deploy. Subject to applicable provisions of the Agreement and deletion of primary data by Customer, upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination "retrieval period" set forth in the Agreement, Mail & Deploy shall regularly delete backups of Customer Content.

## 11. Customer Rights & Shared Security Responsibilities

11.1. Customer Audit and Inquiry Rights.

11.1.1. Upon written request and at no additional cost to Customer, Mail & Deploy shall provide Customer, and/or its appropriately qualified third-party representative (collectively, the "Auditor"), access to reasonably requested documentation evidencing Mail & Deploy's compliance with its obligations under this Security Addendum in the form of, as applicable, (i) Mail & Deploy's ISO 27001 certificate, (ii) Mail & Deploy's most recently completed industry standard security questionnaire, such



MaD Reporting GmbH I 1030 Vienna I Austria I Kollergasse 6/1
FN 557097k I Commercial Court Vienna I VAT No. ATU 76904245
info@mail-and-deploy.com
www.mail-and-deploy.com

as a SIG or CAIQ, and (iii) architecture and technical overview documentation for the Service (collectively, "Audit Reports"). Audit Reports are considered Mail & Deploy's Confidential Information.

11.2. Shared Security Responsibilities. Without diminishing Mail & Deploy's commitments in this Security Addendum, Customer agrees:

11.2.1. Mail & Deploy has no obligation to assess the content or accuracy of Customer Content, including to identify information subject to any specific legal, regulatory or other requirement.

11.2.2. Customer is responsible for managing and protecting its user roles and credentials, including but not limited to (i) ensuring that all users keep credentials confidential and not share such information with unauthorized parties, (ii) promptly reporting to Mail & Deploy any suspicious activities related to Customer's account (e.g., a user credential has been compromised), (iii) appropriately configuring ser and role-based access controls, including scope and duration of User access, taking into account the nature of its Customer Content, and (iv) maintaining appropriate authentication, password and logging controls; 11.2.3. To appropriately manage and protect any Customer-managed encryption keys to ensure the integrity, availability, and confidentiality of the key and Customer Content encrypted with such key.

11.2.4. Customer is responsible for the security of any and all third-party software or applications installed and utilized by the Customer in conjunction with Mail & Deploy SaaS.



MaD Reporting GmbH I 1030 Vienna I Austria I Kollergasse 6/1
FN 557097k I Commercial Court Vienna I VAT No. ATU 76904245
info@mail-and-deploy.com
www.mail-and-deploy.com