

This Data Processing Addendum including its Schedules 1, 2, 3 and 4 (the “DPA”), once executed and received by MaD Reporting GmbH according to the instructions below, forms part of the Agreement between MaD Reporting GmbH and the Customer (each defined below).

The MaD Reporting GmbH party to this DPA is the MaD Reporting GmbH entity that is the MaD Reporting GmbH party to the Agreement. Only the Customer entity that is the party to the Agreement may sign this DPA. If the Customer entity signing this DPA is not a party to the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA. The Customer’s signatory represents and warrants that he or she has the legal authority to bind the Customer to this DPA.

In order for it to be effective, the Customer must (a) complete and sign the information block below with the Customer full legal entity details and signatory information and (b) sign Schedule 4 (2021 SCCs).

The Parties hereby agree from the Effective Date to be bound by the terms and conditions of this DPA.

Accepted and agreed to by MaD Reporting GmbH		Accepted and agreed to by the Customer	
<i>Name of data processor:</i>	MaD Reporting GmbH Kollergasse 6/1 1030 Vienna, Austria	<i>Customer legal name (include entity type, e.g., Inc., Ltd., etc.):</i>	
<i>Country of processor:</i>	Austria	<i>Country of customer:</i>	
<i>Name of signatory:</i>	Mag. Andreas Luger	<i>Name of signatory:</i>	
<i>Position:</i>	CEO	<i>Position:</i>	
<i>Signature:</i>		<i>Signature:</i>	
<i>Date:</i>		<i>Date:</i>	
<i>Key privacy contact:</i>	Angelika Brunner-Zorez COO info@mail-and-deploy.com	<i>Key privacy contact:</i>	

SCHEDULE 1 - DATA PROTECTION OBLIGATIONS

This DPA is an agreement between the Customer and MaD Reporting GmbH governing the Processing by MaD Reporting GmbH of Customer Personal Data in its performance of the Services. Capitalized terms used in the DPA will have the meanings given to them in Section 1 below.

1. DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity.

"Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Agreement" means either (i) the Mail & Deploy Customer Agreement or (ii) the Mail & Deploy OEM Partner Agreement, between MaD Reporting GmbH and the Customer under which MaD Reporting GmbH provides the applicable Services.

"CCPA" means the California Consumer Privacy Act, as amended, and its implementing regulations. The terms "Business" and "Service Provider" where used in this DPA addressing compliance under the CCPA will have the meanings given to them under the CCPA.

"Client-Managed Deployment" means a deployment of on-premise Mail & Deploy software managed and/or hosted by the Customer or by a Customer's third party cloud provider.

"Consulting Services" means any consulting services provided to the Customer by MaD Reporting GmbH pursuant to the Agreement.

"Customer" means the customer legal entity which is a Party to the Agreement.

"Customer Personal Data" means Personal Data which MaD Reporting GmbH Processes on behalf of the Customer in the performance of the Services, including, where applicable, Mail & Deploy SaaS Customer Content. It does not include Personal Data for which MaD Reporting GmbH is a Controller.

"Data Protection Law" means, as amended from time to time, the Australia Privacy Act, the Brazil General Data Protection Law (LGPD), the Canada Personal Information Protection and Electronic Documents Act, the EU GDPR, the Japan Act on the Protection of Personal Information, the Singapore Personal Data Protection Act, the Swiss Federal Act on Data Protection, the UK Data Protection Act 2018 and UK General Data Protection Regulation, and the general consumer (non-industry specific) data privacy laws of the United States and its states (including, where applicable, the CCPA), and in each case only to the extent applicable to the performance of either Party's obligations under this DPA.

"Effective Date" means the date on which MaD Reporting GmbH receives a validly executed DPA under the instructions above and always subject to the Customer having validly executed an Agreement.

"EEA" means, for the purpose of this DPA, the European Economic Area (including the European Union) and, for the purposes of this DPA, Switzerland.

"EEA Customer Personal Data" means Customer Personal Data that is subject to the EU GDPR.

"EU GDPR" means, in each case to the extent applicable to the Processing activities (i) Regulation (EU) 2016/679; and (ii) Regulation (EU) 2016/679 as amended by any legislation arising out of the withdrawal of the UK from the European Union.

"Party" or **"Parties"** means MaD Reporting GmbH and the Customer, individually and collectively, as the case may be.

"Personal Data" means information relating to an identified or identifiable natural person or as otherwise defined under applicable Data Protection Law.

"Personnel" means a Party's employees or other workers under their direct control.

"Mail & Deploy" means the MaD Reporting GmbH which is party to the Agreement.

"Mail & Deploy SaaS Customer Content" means information, data, media, or other content to the extent it includes Customer Personal Data that is, by or upon the instructions of the Customer, uploaded into and residing in Mail & Deploy SaaS which MaD Reporting GmbH Processes on behalf of the Customer.

"Mail & Deploy SaaS" means a subscription-based, hosted solution provided and managed by MaD Reporting GmbH under an Agreement.

"Security Incident" means unauthorized or unlawful destruction, loss, alteration or access to, or disclosure of, Customer Personal Data that is in MaD Reporting GmbH's possession or under MaD Reporting GmbH's control in its performance of the Services. 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 Customer's or Customer Affiliate's failure to (a) control user access; (b) secure or encrypt Customer Personal Data which the Customer transmits to and from MaD Reporting GmbH during performance of the Services; and/or (c) implement security configurations to protect Customer Personal Data; or (ii) unsuccessful attempts or activities that do not or are not reasonably likely to compromise the security of Customer Personal Data, including but not limited to unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"Services" means, pursuant to an Agreement, (i) Mail & Deploy SaaS, (ii) a Mail & Deploy SaaS trial, (iii) a Mail & Deploy SaaS presales proof-of-concept performed by MaD Reporting GmbH, and/or (iv) Support Services and/or Consulting Services requiring MaD Reporting GmbH personnel to access or otherwise Process on Customer's behalf either (a) Mail & Deploy SaaS Customer Content while within or originating from Mail & Deploy SaaS and/or (b) Customer Personal Data relating to a Client-Managed Deployment, and in each case, only as it relates

to Processing by MaD Reporting GmbH of Customer Personal Data. Notwithstanding the foregoing, "Services" does not include, and accordingly, this DPA does not cover, (i) Mail & Deploy SaaS Customer Content which leaves Mail & Deploy SaaS, and/or (ii) Customer Personal Data stored in a Client-Managed Deployment, including but not limited to Customer Personal Data stored within self-hosted software.

"Support Services" means end user support provided by MaD Reporting GmbH to the Customer under the Agreement involving Processing by MaD Reporting GmbH of Customer Personal Data either by way of (i) temporary remote access or screenshare, and/or (ii) receipt by MaD Reporting GmbH of Customer files via Mail & Deploy's support portal on the Mail & Deploy Community website.

"Termination Date" means the termination or expiration of the relevant Service(s) under the Agreement between the Parties, or, in the case of a Mail & Deploy SaaS presales proof-of-concept or trial, the termination or expiration of that presales proof-of-concept or trial.

"Third Country" means a third country not deemed by the EU Commission or UK Information Commissioner, as applicable, to have an equivalent level of privacy protection to those jurisdictions.

"UK Addendum" means the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner and laid before Parliament in accordance with S119A(1) Data Protection Act 2018 on 2 February 2022 but, as permitted by Section 17 of such Addendum, the format of the information set out in Part 1 of the Addendum shall be amended as set out in Section 5.3 of this DPA.

"UK Customer Personal Data" means Customer Personal Data that is subject to the UK General Data Protection Regulation.

"2021 SCCs" means the 2021 SCCs Module Two and the 2021 SCCs Module Three, collectively or individually, as applicable, published under EU Commission Decision 2021/914/EU for EU Personal Data transfers

outside the EU to Third Countries not deemed by the EU Commission to have an equivalent level of privacy protection, included as Schedule 4. The terms “2021 SCCs Module Two” means the 2021 SCCs, module two (controller to processor), and “2021 SCCs Module Three” means the 2021 SCCs, module three (processor to processor).

“Controller”, “Data Subject”, “Processor”, “Process/Processed/Processing”, “Subprocessor” and “Supervisory Authority”, and analogous terms, will be interpreted in accordance with Data Protection Law.

2. PROCESSING BY MAD REPORTING GMBH OF CUSTOMER PERSONAL DATA

2.1 Details of Processing. The table below in this Section 2.1 sets out the Customer Personal Data MaD Reporting GmbH may Process when providing the Services:

Nature/Activities/ Purpose of Processing	Data analysis and Processing of Customer Personal Data by the Customer in Mail & Deploy SaaS and/or for Support or Consulting Services.
Frequency and Duration of Processing	From time to time during the term of the Services under the Agreement or, in the case of a Mail & Deploy SaaS presales proof-of-concept or trial, the term of that proof-of-concept or trial. Duration of Processing and retention period shall be the duration of the Services unless Customer Personal Data is deleted sooner.
Types of Personal Data	Customer Personal Data may include sensitive personal Data if provided by the Customer.
Categories of Data Subjects whose Personal Data is Processed	MaD Reporting GmbH will not be aware of what Personal Data the Customer may provide for the Services. It is anticipated that the Data Subjects may include employees, customers, prospects, business partners and vendors of the Customer. Processed Customer Personal Data uploaded to and residing in Mail & Deploy SaaS and/or otherwise Processed by MaD Reporting GmbH to provide the Services.

2.2 Purpose of Processing Customer Personal Data. The Parties agree that either (a) the Customer is the Controller and MaD Reporting GmbH is a Processor, or (b) Customer is the Processor and MaD Reporting GmbH is a Subprocessor, in relation to the Customer Personal Data that MaD Reporting GmbH Processes on the Customer’s behalf in the course of providing the Services. For the avoidance of doubt, this DPA does not apply to Personal Data for which MaD Reporting GmbH is a Controller. MaD Reporting GmbH will Process the Customer Personal Data only to perform the Services for the Customer and for no other purpose. If MaD Reporting GmbH is required to Process the Customer Personal Data for any other purpose by applicable laws to which MaD Reporting GmbH is subject, MaD Reporting GmbH will, unless prohibited by such applicable laws and subject to the terms of this DPA, inform Customer of this requirement first. To the extent that the CCPA applies to the Processing of Customer Personal Data in the course of providing the Services, (i) MaD Reporting GmbH is a Service Provider and the Customer is a Business in relation to Customer Personal Data, and (ii) without limiting any other term in this DPA or in the Agreement, MaD Reporting GmbH shall not (a) sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic means, any Customer Personal Data to any third- party for monetary or other valuable consideration, (b) retain, disclose, or use any Customer Personal Data for any purpose (including any commercial purpose) other than the specific purpose of performing the Services, and/or (c) retain, use, or disclose any Customer Personal Data outside of the direct business relationship between the Customer and MaD Reporting GmbH. MaD Reporting GmbH hereby certifies that it understands the restrictions described in the previous sentence and shall comply with them.

2.3 Disclosure of Customer Personal Data. Unless otherwise provided for in this DPA, MaD Reporting GmbH will not disclose to any third party any Customer Personal Data, except, in each case, as necessary to maintain or provide the Services, or, notwithstanding Section 5.5 below, as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a

governmental body sends MaD Reporting GmbH such a demand for Customer Personal Data, MaD Reporting GmbH will attempt, where possible under relevant law, to redirect the governmental body to request that data directly from the Customer.

2.4 Customer Personal Data for Support Services. The Parties acknowledge that MaD Reporting GmbH does not ordinarily require to Process Customer Personal Data on the Customer's behalf to resolve a technical issue for Support Services. Accordingly;

2.4.1 the Customer shall use their best efforts to minimize any transfer of Customer Personal Data to MaD Reporting GmbH for Support Services. Such efforts shall include but not be limited to removing, anonymizing and/or pseudonymizing Customer Personal Data in files prior to Processing by MaD Reporting GmbH; and

2.4.2 MaD Reporting GmbH's total liability in relation to the Processing of Support Services Customer Personal Data, whether in contract, tort or under any other theory of liability, shall not exceed US\$20,000.

2.5 Obligations of MaD Reporting GmbH Personnel. MaD Reporting GmbH will ensure that MaD Reporting GmbH Personnel required to access the Customer Personal Data are subject to a binding duty of confidentiality in respect of such Customer Personal Data and take reasonable steps to ensure the reliability and competence of such MaD Reporting GmbH Personnel.

2.6 Instructions. Customer authorizes and instructs MaD Reporting GmbH to Process Customer Personal Data for the performance of the Services. The Parties agree that this DPA and the Agreement are the Customer's complete and final documented Processing instructions to MaD Reporting GmbH in relation to Customer Personal Data. The Customer shall ensure that its Processing instructions comply with applicable Data Protection Laws in relation to Customer Personal Data and that the Processing of Customer Personal Data in accordance with the Customer's instructions will not cause MaD Reporting GmbH to be in breach of any relevant law. The Customer warrants that it has the right

and authority under applicable Data Protection Law and any undertakings it may have entered into to disclose, or have disclosed, Customer Personal Data to MaD Reporting GmbH to be Processed by MaD Reporting GmbH for the Services and that the Customer has obtained all necessary consents and provided all necessary notifications required by Data Protection Law with respect to the Processing of Customer Personal Data by MaD Reporting GmbH. The Customer will not disclose Customer Personal Data to MaD Reporting GmbH or instruct MaD Reporting GmbH to Process Customer Personal Data for any purpose not permitted by applicable law, including Data Protection Law. MaD Reporting GmbH will notify the Customer if MaD Reporting GmbH becomes aware that, and in MaD Reporting GmbH's reasonable opinion, an instruction for the Processing of Customer Personal Data given by the Customer violates Data Protection Law, it being acknowledged that MaD Reporting GmbH is not under any obligation to undertake additional work, screening or legal assessment to determine whether Customer's instructions are compliant with Data Protection Law.

2.7 Assistance to the Customer. Upon a written request, MaD Reporting GmbH will provide reasonable cooperation and assistance necessary to assist the Customer, insofar as required by Data Protection Law and as it relates to Processing by MaD Reporting GmbH for the Services, in fulfilling the Customer's obligations to respond to requests from Data Subjects exercising their rights (notwithstanding the Customer's obligations in Section 7) and/or to carry out data protection impact assessments. MaD Reporting GmbH's Data Protection Officer and privacy team may be reached at info@mail-and-deploy.com.

2.8 Compliance with Data Protection Laws. Each Party will comply with the Data Protection Laws applicable to it in relation to their performance of this DPA, including, where applicable, the EU GDPR.

3. SECURITY

3.1 Security of Data Processing. MaD Reporting GmbH will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data against unauthorized

or unlawful Processing and against accidental or unlawful loss, destruction, alteration or damage, and against unauthorized disclosure or access. These measures will be appropriate to the harm, which might result from any unauthorized or unlawful Processing, accidental loss, destruction, damage or theft of the Customer Personal Data and having regard to the nature of the Customer Personal Data which is to be protected. At a minimum, these will include the measures set out in Schedule 2.

3.2 Notification of a Security Incident. Upon becoming aware of a Security Incident, MaD Reporting GmbH will notify the Customer without undue delay 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 MaD Reporting GmbH's reasonable control. A notification by MaD Reporting GmbH to the Customer of a Security Incident under this DPA is not and will not be construed as an acknowledgement by MaD Reporting GmbH of any fault or liability of MaD Reporting GmbH with respect to the Security Incident.

3.3 Notification Mechanism. Security Incident notifications, if any, will be delivered to Customer by any means MaD Reporting GmbH selects, including via email. It is the Customer's responsibility to ensure that it provides MaD Reporting GmbH with accurate contact information and secure transmission at all times.

4. SUBPROCESSORS

4.1 Authorized Subprocessors. The Customer agrees that MaD Reporting GmbH may use its Affiliates and other Subprocessors to fulfil its contractual obligations under this DPA or to provide certain Services on its behalf. The MaD Reporting GmbH website lists Subprocessors that are currently engaged by MaD Reporting GmbH to carry out Processing activities on Customer Personal Data.

4.2 Subprocessor Obligations. Where MaD Reporting GmbH uses a Subprocessor as set forth in this Section 4, MaD Reporting GmbH will (i) enter into a written agreement with the Subprocessor and will impose on the Subprocessor contractual obligations not less protective on an aggregate basis than the overall obligations that MaD Reporting GmbH has

provided under this DPA, including but not limited to, where applicable, incorporating the 2021 SCCs and/or the UK Addendum; and (ii) restrict the Subprocessor's access to and use of Customer Personal Data only to provide the Services. For the avoidance of doubt, where a Subprocessor fails to fulfil its obligations under any subprocessing agreement or any applicable Data Protection Law with respect to Customer Personal Data, MaD Reporting GmbH will remain liable, subject to the terms of this DPA, to the Customer for the fulfilment of MaD Reporting GmbH's obligations under this DPA.

4.3 Appointing a New Subprocessor. At least thirty (30) days before MaD Reporting GmbH engages any new Subprocessor to carry out Processing activities on Customer Personal Data, MaD Reporting GmbH will provide notice of such update to the Subprocessor list through the applicable website. If the Customer is entitled to do so under applicable Data Protection Law and as it relates to the Processing of Customer Personal Data by the Subprocessor, the Customer may make reasonable objections in writing to info@mail-and-deploy.com within the 30-day period regarding the appointment of the new Subprocessor. After receiving such written objection MaD Reporting GmbH will either: (i) work with the Customer to address the Customer's objections to its reasonable satisfaction, (ii) instruct the Subprocessor not to Process Customer Personal Data, provided that the Customer accepts that this may impair the Services (for which MaD Reporting GmbH shall bear no responsibility or liability), or (iii) notify the Customer of an option to terminate this DPA and the applicable order form for Services which cannot be provided by MaD Reporting GmbH without the use of the objected-to new subprocessor. If MaD Reporting GmbH does not receive an objection from the Customer within the 30-day objection period, the Customer will be deemed to have consented to the appointment of the new Subprocessor.

5. EEA/UK THIRD COUNTRY DATA TRANSFERS

5.1 Transfers of EEA Customer Personal Data. For transfers of EEA Customer Personal Data by the Customer to MaD Reporting GmbH, where the MaD Reporting GmbH party to this DPA is in a Third Country not deemed under EEA Data

Protection Law to provide an equivalent level of privacy protection to that in the EEA;

5.1.1 where the Customer is the Controller and MaD Reporting GmbH a Processor of such EEA Customer Personal Data, such transfer(s) are subject to the 2021 SCCs Module Two; and/or 5.1.2 where the Customer is the Processor and MaD Reporting GmbH a Subprocessor of such EEA Customer Personal Data (i.e., where the EEA Customer Personal Data contains EEA Personal Data of the Customer's customers where the Customer is a Processor), such transfer(s) are subject to the 2021 SCCs Module Three; in each case, the 2021 SCCs Module Two and 2021 SCCs Module Three, as applicable, shall apply as set out in Schedule 4 and subject to the provisions of this DPA.

5.2 Particulars regarding the 2021 SCCs. The 2021 SCCs are particularized in Schedule 4. The Parties agree that, to the fullest extent permitted under the 2021 SCCs, (a) the aggregate liability of MaD Reporting GmbH to the Customer under or in connection with the 2021 SCCs will be limited as set out in sections 2.4 and 8.3 of this DPA, and (b) any rights to audit pursuant to Clause 8.9 of the 2021 SCCs will be exercised in accordance with section 6 below.

5.3 Transfers of UK Customer Personal Data. For transfers of UK Customer Personal Data by the Customer to MaD Reporting GmbH where the MaD Reporting GmbH party to this DPA is in a Third Country not deemed under UK Data Protection Law to provide an equivalent level of privacy protection to that in the UK, the Parties agree that the provisions of the UK Addendum shall apply to such transfers. In particular:

5.3.1 the Customer will be the data exporter, and MaD Reporting GmbH the data importer;

5.3.2 the start date for transfers in Table 1 of the UK Addendum shall be the Effective Date unless otherwise agreed between the Parties;

5.3.3 the details of the Parties and their key contacts in Table 1 of the UK Addendum shall be as set out at the commencement of this DPA, and with no requirement for additional signature;

5.3.4 for the purposes of Table 2, the UK Addendum shall be appended to the 2021 SCCs

as incorporated by reference into this DPA (including the selection of modules as specified in Section 5.1, the particulars as specified in Section 5.2 of this DPA and the selection and disapplication of optional clauses as set out in Schedule 4);

5.3.5 the appendix information listed in Table 3 of the UK Addendum is set out at the commencement of this DPA (List of Parties), in Section 2 (Description of Transfer) and in Schedule 2 to this DPA (Technical and Organizational Measures); and

5.3.6 for the purposes of Table 4, neither Party may end the UK Addendum as set out in Section 19 thereof.

5.4 Alternative Lawful Transfer Mechanisms. The Customer acknowledges that MaD Reporting GmbH's obligations under the 2021 SCCs and/or the UK Addendum under this DPA may be replaced by obligations under any successor or alternate EEA/UK Third Country lawful transfer mechanism adopted by MaD Reporting GmbH which is recognized by the relevant EEA/UK authorities. In such instances, the Parties shall not be required to re-execute this DPA as they have already agreed to such measures, and such obligations will be deemed automatically included in this DPA.

5.5 EEA/UK-US Transfers. In response to the Court of Justice of the European Union's decision in Schrems II, Case No. C-311/18, and related guidance from Supervisory Authorities, the Parties acknowledge that supplemental measures may be needed with respect to EEA/UK-U.S. data transfers where Customer Personal Data may be subject to government surveillance. The Customer and MaD Reporting GmbH agree that Customer's EEA/UK operations involve ordinary commercial services, and any EEA/UK-U.S. transfers of EEA Customer Personal Data contemplated by this DPA involve ordinary commercial information, such as employee data, which is not the type of data that is of interest to, or generally subject to, surveillance by U.S. intelligence agencies. Accordingly, MaD Reporting GmbH agrees that it will not provide access to Customer Personal Data of an EEA/UK Customer transferred under this DPA to any government or intelligence agency, except where its legal counsel has

determined it is strictly relevant and necessary to comply with the law or a valid and binding order of a government authority (such as pursuant to a court order). If a law enforcement agency or other government authority provides MaD Reporting GmbH with a demand for access to such Customer Personal Data, MaD Reporting GmbH will attempt to redirect the law enforcement agency to request the Customer Personal Data directly from the Customer. If compelled by law to provide access to such Customer Personal Data to a law enforcement agency or other government authority, and only after a determination of such is made by legal counsel, then MaD Reporting GmbH will, unless MaD Reporting GmbH is legally prohibited from doing so: (1) give Customer notice of the demand no later than five (5) days after such demand is received to allow Customer to seek recourse or other appropriate remedy to adequately protect the privacy of EEA/UK Data Subjects, and MaD Reporting GmbH shall provide reasonable cooperation in connection with the Customer seeking such recourse; and (2) in any event, provide access only to such Customer Personal Data as is strictly required by the relevant law or binding order (having used reasonable efforts to minimize and limit the scope of any such access). This Section 5.5 does not overwrite Clause 15 (where applicable) of the 2021 SCCs or the equivalent protection under the UK Addendum.

5.6 EEA Mail & Deploy SaaS Storage Capability. For the avoidance of doubt, although the Customer may select (where available) the region in which its Mail & Deploy SaaS Customer Content resides, including the EU, the ability to retain Mail & Deploy SaaS Customer Content (including Customer Personal Data) solely in-region is subject to how the Customer's users of Mail & Deploy SaaS share and use applications and other technical particulars.

6. AUDITS

6.1 Audit Requests. MaD Reporting GmbH will give to the Customer on written request (where such requests shall occur no more than once every 12 months) reasonable information necessary to determine MaD Reporting GmbH's compliance with this DPA and will discuss in good faith any audits reasonably required by the

Customer, conducted by a third party agreed to by the Parties. Such audits, if agreed, must be carried out at the Customer's cost, be conducted in a manner undistruptive to the business of MaD Reporting GmbH and its Affiliates, be conducted subject to the terms of an applicable non-disclosure agreement, and not prejudice other confidential information (including but not limited to Personal Data) of MaD Reporting GmbH, its Affiliates or its other customers.

6.2 Subprocessor Audits. If the Customer's request for information relates to a Subprocessor, or information held by a Subprocessor which MaD Reporting GmbH cannot provide to the Customer itself, MaD Reporting GmbH will promptly submit a request for additional information in writing to the relevant Subprocessor(s). The Customer acknowledges that information about the Subprocessor's previous independent audit reports is subject to agreement from the relevant Subprocessor, and that MaD Reporting GmbH cannot guarantee access to that Subprocessor's audit information at any particular time, or at all.

7. ACCESS AND DELETION OF CUSTOMER PERSONAL DATA

7.1 Access and Deletion of Mail & Deploy SaaS Customer Content during the Agreement. Customer is responsible for any data minimization before inputting Customer Personal Data and for executing any requests to access, retrieve, correct and/or delete Mail & Deploy SaaS Customer Content (including any Customer Personal Data therein). MaD Reporting GmbH will, as necessary to enable the Customer to meet its obligations under Data Protection Law, provide the Customer via availability of Mail & Deploy SaaS with the ability to access, retrieve, correct and delete through to the Termination Date its Mail & Deploy SaaS Customer Content in Mail & Deploy SaaS. The Customer acknowledges that such ability may from time to time be limited due to temporary service outage for maintenance or other updates to Mail & Deploy SaaS. To the extent that the Customer, in its fulfilment of its Data Protection Law obligations, is unable to access, retrieve, correct or delete Customer Personal Data in Mail & Deploy SaaS due to prolonged unavailability of Mail & Deploy SaaS due to an issue within MaD Reporting GmbH's control (for example,

exceeding 10 working days), upon written request from the Customer, MaD Reporting GmbH will where possible use reasonable efforts to provide, correct or delete such Customer Personal Data. The Customer acknowledges that MaD Reporting GmbH may maintain backups of Mail & Deploy SaaS Customer Content, which would remain in place for approximately third (30) days following a deletion in Mail & Deploy SaaS. The Customer remains solely responsible for the deletion, correction and accuracy of its Mail & Deploy SaaS Customer Content and will be solely responsible for retrieving such Mail & Deploy SaaS Customer Content to respond to Data Subject access requests or similar requests relating to Customer Personal Data. If MaD Reporting GmbH receives any such Data Subject request, MaD Reporting GmbH will use commercially reasonable efforts to redirect the Data Subject to the Customer.

7.2 Access and Deletion of Customer Personal Data on Termination of the Agreement. By the Termination Date, the Customer will have deleted all Mail & Deploy SaaS Customer Content Personal Data, unless prohibited by law, or the order of a governmental or regulatory body. Notwithstanding the foregoing, after the Termination Date and upon the Customer's written request MaD Reporting GmbH will provide reasonable assistance to the Customer to securely destroy or return any remaining Customer Personal Data. The Customer acknowledges that Customer Personal Data may be stored by MaD Reporting GmbH after the Termination Date in line with MaD Reporting GmbH's data retention rules and back-up procedures until it is eventually deleted. To the extent that any portion of Customer Personal Data remains in the possession of MaD Reporting GmbH following the Termination Date, MaD Reporting GmbH's obligations set forth in this DPA shall survive termination of the Agreement with respect to that portion of the Customer Personal Data until it is eventually deleted.

8. MISCELLANEOUS

8.1 Entire Agreement. This DPA and the Agreement, where referenced, contain the entire agreement regarding the subject matter thereof and supersede any other data protection/privacy agreements and communications between the

Parties concerning the Processing by MaD Reporting GmbH of Customer Personal Data in MaD Reporting GmbH's performance of the Services.

8.2 Effect of this DPA. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the Parties, including the Agreement and this DPA, the terms of this DPA will control as it relates to Processing of Customer Personal Data. If the Parties have entered into a Business Associate Agreement, that Business Associate Agreement shall govern with respect to U.S. "PHI" as defined thereunder. In the event of a conflict between this DPA and the applicable 2021 SCCs (Modules Two or Three) and/or the UK Addendum, the relevant 2021 SCCs and/or the UK Addendum will prevail. This DPA is effective from the Effective Date and only if and for so long as MaD Reporting GmbH provides Services under the Agreement. This DPA will terminate, unless otherwise terminated by the Parties, on the Termination Date.

8.3 Liability. Subject to Section 2.4.2, the total combined liability of either Party towards the other Party, whether in contract, tort or under any other theory of liability, shall be limited to that set forth in the Agreement as well as any disclaimers contained therein. Any reference in such section to the liability of a Party means the aggregate liability of that Party under the Agreement and this DPA.

8.4 Third Party Rights. This DPA shall not confer any rights or remedies to any other person or entity other than the Parties except as to enable the Data Protection Law rights of Data Subjects of Customer Personal Data under this DPA.

8.5 Updates to this DPA. MaD Reporting GmbH may modify the terms of this DPA, such as to account for future changes in Data Protection Law to enable the continued Processing of Customer Personal Data to carry out the Services and shall do so by way of updating the DPA terms on www.mail-and-deploy.com.

Any future changes to this DPA published by MaD Reporting GmbH on its website will become effective once published and shall supersede any previous DPA between the Parties,

insofar and only to the extent that those changes (i) are to account for changes under Data Protection Law, which may include to account for revised guidance from a Supervisory Authority, or (ii) to enable an EEA/UK Third Country lawful transfer mechanism, as contemplated under Section 5.2, or (iii) are not less favorable to the

Customer (for example, to permit further data types of Customer Personal Data to be uploaded to Mail & Deploy SaaS). The Customer is therefore encouraged to keep up to date with these DPA terms at www.mail-and-deploy.com.

FOR REVIEW ONLY

SCHEDULE 2 - TECHNICAL AND ORGANIZATIONAL MEASURES

MaD Reporting GmbH shall undertake appropriate technical and organizational measures for the availability and security of Customer Personal Data and to protect it against unauthorized or unlawful Processing and against accidental or unlawful loss, destruction, alteration or damage, and against unauthorized disclosure or access. These measures, listed below, shall take into account the nature, scope, context and purposes of the Processing, available technology as well as the costs of implementing the specific measures and shall ensure a level of security appropriate to the harm that might result from a Security Incident. Some of the measures below apply to MaD Reporting GmbH's general IT infrastructure/practices and may not necessarily apply to Mail & Deploy SaaS. While MaD Reporting GmbH may alter its measures in line with evolving security practices and risks, and with due regard to the nature of the Processing, MaD Reporting GmbH will not materially decrease the overall protections of the Customer Personal Data below the aggregate standard of the measures in this Schedule 2. Customers should stay up to date with MaD Reporting GmbH's security measures by visiting its security resources available at www.mail-and-deploy.com.

- 1. Access Controls to Premises and Facilities.** MaD Reporting GmbH maintains technical and organizational measures to control access to premises and facilities, particularly to check authorization, utilizing various physical security controls such as ID cards, keys, alarm systems, surveillance systems, entry/exit logging and door locking to restrict physical access to office facilities.
- 2. Access Controls to Systems and Data.** MaD Reporting GmbH operates technical and organizational measures for user identification and authentication, such as logs, policies, assigning distinct usernames for each employee and utilizing password complexity requirements for access to on-premises and cloud-based platforms. In addition, user access is established on a role basis and requires user management, system or HR approval, depending on use. Second-layer authentication may be employed where relevant by way of multi-factor authentication. User access for sensitive platforms is subject to periodic review and testing. MaD Reporting GmbH's IT control environment is based upon industry-accepted concepts, such as multiple layers of preventive and detective controls, working in concert to provide for the overall protection of MaD Reporting GmbH's computing environment and data assets. To strengthen access control, a centralized identity and access management solution is used to manage application access. MaD Reporting GmbH uses on-boarding and off-boarding processes to regulate access by MaD Reporting GmbH Personnel.
- 3. Disclosure Controls.** MaD Reporting GmbH maintains technical and organizational measures to transport, transmit and communicate or store data on data media (manual or electronic). For certain data transfers, bearing in mind the risk and sensitivity of the data, MaD Reporting GmbH may employ encrypted network or similar transfer technologies. Personnel must utilize a dedicated or local VPN network to access internal resources and/or industry-standard authentication and secure communication mechanisms to access cloud-based systems. Logging and reporting are utilized for validation and review purposes. Third party Subprocessors are subject to privacy and security risk assessments and contractual commitments.

4. **Input Controls.** MaD Reporting GmbH maintains measures in its general IT systems for checking whether relevant data has been entered, changed or removed (deleted), and by whom, such as by way of application-level data entry and validation capabilities. and reporting is utilized for validation and review purposes. For Mail & Deploy SaaS Customer Content, other than as provided for under this DPA, the Customer is solely responsible for entry, alteration and removal (deletion) of any of its Mail & Deploy SaaS Customer Content in Mail & Deploy SaaS and, to respect the security and integrity of the Customer Personal Data, MaD Reporting GmbH does not monitor Mail & Deploy SaaS Customer Content for regular entries, alterations or removals (deletion) by the Customer or its users in its use of the Services.
5. **Job Controls.** MaD Reporting GmbH uses technical (e.g., access controls) and organizational (e.g., policies) measures to delineate, control and protect data for which the MaD Reporting GmbH is the Controller or the Processor. MaD Reporting GmbH records and delineates the data types for which it is a Controller or a Processor in its record of processing activities under Article 30 (2) EU GDPR.
6. **Separation Controls.** MaD Reporting GmbH uses segregation standards and protocols between production, testing and development environments of sensitive platforms. Additionally, segregation of data is further supported through user access role segregation.
7. **Availability Controls.** MaD Reporting GmbH maintains measures to assure data availability such as local and/or cloud-based back-up mechanisms involving scheduled and monitored backup routines, and local disaster recovery procedures. MaD Reporting GmbH may supplement these with additional security protections for its business, for example malware protection. Additionally, data centers of a critical nature are required to submit to periodic 3rd party evaluation of operating effectiveness for significant controls ensuring data availability. Relevant systems and data center locations are protected through the use of industry-standard firewall capabilities.
8. **Other Security Controls.** MaD Reporting GmbH maintains (i) regular control evaluation and testing by audit (internal and/or external), on an as-needed basis, (ii) individual appointment of system administrators, (iii) user access by enterprise IDP, (iv) binding policies and procedures for MaD Reporting GmbH's Personnel, and (v) regular security and privacy training. Policies will clearly inform Personnel of their obligations (including confidentiality and associated statutory obligations) and the associated consequences of any violation.

SCHEDULE 3 - SUBPROCESSORS

Third Party Subprocessors:

- Amazon Web Services
- Microsoft
- Freshworks
- Microsoft Azure
- GitHub

FOR REVIEW ONLY

SCHEDULE 4 - 2021 SCCs

Controller to Processor (Module 2) or Processor to Processor (Module 3)

SECTION I**Clause 1- Purpose and scope**

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) for the transfer of personal data to a third country.
- (b) The Parties: (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 - Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3- Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) 8.9(a), (c), (d) and (e);
 - (iii) Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e); and
 - (viii) Clause 18(a) and (b).
 - (ix) [If the data exporter is a controller:] Clause 8.1(b)
 - (x) [If the data exporter is a processor:] Clause 8.1(a), (c) and (d) and Clause 8.9 (f) and (g);
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4- Interpretation

- (c) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (d) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (e) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5- Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 - Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - [not used]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 - Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract. (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout

the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where
- (i) possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

- (a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
- (b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

- (c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
- (d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during

transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

- (b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain
 - (i) the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

- (a) The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:
 - (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
 - (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

- (iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
 - (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.
- (b) Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.
- (c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
- (d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into
 - (a) account relevant certifications held by the data importer.
- (e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
- (f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 - Use of sub-processors*MODULE TWO: Transfer controller to processor*

- (a) The data importer has the data exporter's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8.
- (a) The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (b) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (c) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (d) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

- (a) The data importer has the controller's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 - Data subject rights*MODULE TWO: Transfer controller to processor*

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

- (a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorized to do so by the controller.
- (b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter

Clause 11 – Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 – Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on

behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 – Supervision

- (a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant
- (a) to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 - Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the

fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
 - iii. any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the data importer in case of access by public authorities

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data

- transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
- (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
 - (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
 - (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
 - (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses. In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.
- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 - Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18 - Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Austria.

- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

FOR REVIEW ONLY

ANNEX I**A. LIST OF PARTIES**

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Data exporter(s):

Name: The Customer, as defined in the Agreement.

Address: The address of Customer specified in the Agreement, DPA and/or applicable order form(s) as applicable.

Contact person's name, position, and contact details: The name, position, and contact details of the Customer's contact person specified in the table at the commencement of this DPA.

Activities relevant to the data transferred under these Clauses: transfer of Customer Personal Data, as defined in the DPA, for Processing by the data importer.

Signature and date: [insert signature and date]

Role: controller (module two) or processor (module three).

Data importer(s):

Name: MaD Reporting GmbH, as defined in the Agreement.

Address: Kollergasse 6/1, 1030 Vienna, Austria

Contact person's name, position, and contact details: Mag. Andreas Luger, CEO, info@mail-and-deploy.com

Activities relevant to the data transferred under these Clauses: Processing of Customer Personal Data, as defined in the DPA, on behalf of the data exporter.

Signature and date: [insert signature and date]

Role: processor (module two) or subprocessor (module three).

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See the Details of Processing table at the commencement of this DPA.

Categories of personal data transferred

Customer Personal Data as defined in the DPA. See the Details of Processing table at the commencement of the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

See the Details of Processing table at the commencement of the DPA. Applied restrictions or safeguards are set out in the DPA.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

See the Details of Processing table at the commencement of the DPA.

Nature of the processing

See the Details of Processing table at the commencement of the DPA.

Purpose(s) of the data transfer and further processing

For the purposes of enabling the data exporter to use the Services in accordance with the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

In accordance with any retention periods controlled by the Customer, or if such retention periods are controlled by MaD Reporting GmbH, in accordance with the Agreement and the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

MaD Reporting GmbH's Subprocessor details are set out at Schedule 3 to the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The Competent Supervisory Authority of the EU Member State in which the data exporter is established, based on the list available at https://edpb.europa.eu/about-edpb/about-edpb/members_en. In case of ambiguity, this will be the Competent Supervisory Authority of Austria:

Österreichische Datenschutzbehörde
Barichgasse 40-42
1030 Wien

Tel. +43 1 52 152-0
Email: dsb@dsb.gv.at
Website: <http://www.dsb.gv.at/>

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

These are as listed in Schedule 2 of the DPA.

ANNEX III

LIST OF SUB-PROCESSORS

The data exporter has authorized the use of the sub-processors listed in Schedule 3 of the DPA, as updated from time to time