



Teach your AI coding agent how to send email with Postmark Skills

[Learn more](#)



LOG IN



Data Processing Addendum

This Data Processing Addendum is for new customers who signed up on or after December 10, 2024. Existing customers who signed up on or before December 9, 2024 can find the DPA [here](#).

Data Processing Addendum - New Customers

Effective November 17, 2025

This Data Processing Addendum (“**DPA**”) supplements the **Terms of Service**, located at <https://postmarkapp.com/terms-of-service> or its successor URL (the “**Terms**”), between User and AC PM and is effective upon its incorporation into the Terms, which incorporation is specified in the Terms. All capitalized terms not otherwise defined in this DPA will have the meaning given to them in the Terms. Pursuant to the Terms, AC PM may update this DPA by posting the amended DPA to the Site and updating the “Effective” date above. The amended DPA will be effective as of the “Effective” date above but will not apply retroactively. User’s continued use of the Service after the “Effective” date above constitutes User’s acceptance of the amended DPA. In the event of any inconsistency or conflict between this DPA and the Terms or any other data processing addendum(s) executed by the same parties hereto, this DPA will govern, supersede and prevail. User and AC PM agree as follows:

1. **Personal Information.** In connection with providing the Service, AC PM will be Processing Personal Information on behalf of User. “**Personal Information**” means information relating, directly or indirectly, to an identified or identifiable person (a “**Data Subject**”), which is

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

Autoriser tous les cookies

included in Contract Data. Where required by Data Protection Laws (defined below), any information that AC PM will Process in connection with the (Scope of Processing). As between User and AC PM, all Personal Information is the sole and exclusive property of User. User will be solely responsible for the confidentiality, integrity, legality, reliability, and appropriateness of all Personal

2. **AC PM and User Responsibilities.** The parties acknowledge and agree that: (a) AC PM is a processor and/or service provider, as applicable, with respect to Personal Information under Data Protection Laws; (b) User is a controller and/or business with respect to Personal Information under Data Protection Laws; and (c) each party will comply with the obligations applicable to it under Data Protection Laws with respect to the Processing of Personal Information.

3. **AC PM Responsibilities.** “**Process**” or “**Processing**” means any operation or set of operations which is performed on Personal Information, whether or not by automated means, such as the access, collection, use, storage, disclosure, dissemination, combination, recording, organization, structuring, adaption, alteration, copying, transfer, retrieval, consultation, disposal, restriction, erasure and/or destruction of Personal Information. As a part of the Service, AC PM will:

1. Process Personal Information solely in accordance with User’s documented instructions. Without limiting the foregoing, AC PM will not: (i) retain, use, or disclose Personal Information outside of its direct business relationship with User, or for any purpose (including a commercial purpose) other than as necessary for the specific purpose of performing the Service in accordance with the Terms or as permitted by Data Protection Laws; and (ii) sell or share the Personal Information;
2. Process Personal Information in accordance with all data protection and privacy laws, rules, and regulations that apply to AC PM’s provision, and User’s use, of the Service, including the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”), the GDPR as incorporated into United Kingdom law (“**UK GDPR**”) and the California Consumer Privacy Act (“**CCPA**”) (collectively, “**Data Protection Laws**”);
3. not disclose Personal Information to any third party without first, except to the extent prohibited by Data Protection Laws, (i) notifying User of the anticipated disclosure (so as to provide User the opportunity to oppose the disclosure and obtain a protective

order or seek other relief); (ii) obtaining User's prior consent to the disclosure; or (iii) imposing contractual obligations on the third party recipient that are at least equivalent to those obligations imposed on AC PM under this DPA;

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

4. amend, correct, or erase Personal Information at User's written request and provide a copy of the Personal Information to the User; and make accurate Personal Information Processed by AC PM.
5. notify User of any third party request (by a Data Subject or otherwise) to (i) restrict the Processing of Personal Information; (ii) port Personal Information to a third party; or (iii) access, rectify, or erase Personal Information. AC PM will use commercially reasonable efforts to assist User, at User's reasonable written request, in complying with User's obligations under Data Protection Laws to respond to requests and complaints directed to User with respect to Personal Information Processed by AC PM, to the extent that User does not have access to such Personal Information through User's use of the Service;
6. at the reasonable written request of User, cooperate and assist User in conducting a data protection impact assessment, where required by Data Protection Laws;
7. ensure that AC PM personnel Processing Personal Information are subject to obligations of confidentiality; and
8. keep all Personal Information compartmentalized or otherwise logically distinct from other information of AC PM or its personnel, suppliers, customers or other third parties.

AC PM will use commercially reasonable efforts to inform User if AC PM becomes aware or reasonably suspects that User's instructions regarding the Processing of Personal Information may breach any Data Protection Laws. In addition, where AC PM's Processing of Personal Information is subject to the CCPA, AC PM will use commercially reasonable efforts to inform User if AC PM makes a determination that it can no longer meet its obligations under the CCPA. Notwithstanding the foregoing, User acknowledges and agrees that such notification(s) by AC PM will neither constitute a general obligation on the part of AC PM to monitor or interpret the laws applicable to User nor constitute legal advice to User.

4. **Sub-processors.** AC PM will not engage another processor to Process Personal Information on behalf of User for the purpose of fulfilling AC PM's obligations with respect to the provision of the Service under the Terms (a "**Sub-processor**") without authorization from User. AC PM will be responsible to User for any material failure of a Sub-processor to fulfill AC PM's data

protection obligations as set forth in this DPA. User hereby provides its general written authorization for AC PM to engage Sub-processors. AC PM will notify User of the appointment of any new Sub-processors by way of updating AC PM's Sub-processor webpage located

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

at <https://costmarl.com/en/privacy#sub-processors> (or such successor URL as discretion) (the "**Sub-processor Webpage**"). In addition, User will subscribe to receive email notifications from AC PM about the appointment of any new Sub-processors by completing the form available via the Sub-processor Webpage. If within 7 days of AC PM notifying User, User does not notify AC PM in writing of any objections (on reasonable grounds relating to the protection of Personal Information) to the appointment, it will be deemed that User has consented to the appointment.

5. Data Transfers. Where required by Data Protection Law, AC PM will not transfer any Personal Information from one country to another without User's prior written consent, which User shall not unreasonably withhold, and which User hereby provides as required for AC PM's provision of Service under the Terms. Where User consents to such transfer, the transfer will be in accordance with Data Protection Laws and with the following:

1. AC PM has certified its compliance to the EU-U.S. Data Privacy Framework Principles, including as applied under the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework Principles (collectively, the "**DPF Principles**") with the U.S. Department of Commerce (the "**Department**") in respect of the Processing of Personal Information received from the European Economic Area, the United Kingdom or Switzerland. Where required by Data Protection Laws and at User's written request, AC PM will provide commercially reasonable assistance to User in responding to requests from the Department or other applicable data protection regulators in the U.S., the European Economic Area, the United Kingdom and Switzerland related to compliance with the DPF Principles. Upon request of the Department, AC PM may disclose the terms of this DPA to the Department.
2. Alternatively, where required by Data Protection Laws, any regulated data transfer to a country not subject to an adequacy decision will be conducted pursuant to the Standard Contractual Clauses promulgated by the European Commission Decision 2021/914/EU under Module Two (transfer controller to processor) (the "**Standard Contractual Clauses**"), the International Data Transfer Addendum issued by the United Kingdom Information Commissioner under section 119(A)(1) of the Data Protection Act 2018 (the "**UK Addendum**") and/or the Standard Contractual Clauses approved by the Brazilian National Data Protection Authority pursuant to Resolution CD/ANPD No. 19/2024 (the "**Brazil SCCs**"), which will, as applicable, be deemed entered into (and incorporated into this DPA by reference) and completed as follows:

1. User will be referred to as the “data exporter” and AC PM will be referred to as the “data importer” in the Standard Contractual Clauses, the UK Addendum and/or the Brazil SCCs;

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

2. Annexes, and II of the Standard Contractual Clauses, Tables 1 to 3 of the UK Addendum and Options I and III of the Brazil SCCs will be deemed completed with the relevant information set out in Schedules 1 and 2 of this DPA and the Sub-processor Webpage;
3. The optional Clause 7 (Docking Clause) will not be included in the Standard Contractual Clauses;

4. In Clause 9(a) of the Standard Contractual Clauses, Option 2 will apply, as per the time period set out in Section 4 of this DPA;
5. In Clause 11 of the Standard Contractual Clauses, the optional language will not apply;
6. In Clause 17 of the Standard Contractual Clauses, Option 1 will apply and the Standard Contractual Clauses will be governed by Irish law;
7. In Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before the courts of Ireland;
8. In Table 4 of the UK Addendum, both the data importer and the data exporter may end the UK Addendum in accordance with the terms of the UK Addendum;
9. In Clause 3 of the Brazil SCCs, Option B will apply, with onward transfers permitted in accordance with Section 4 of this DPA;
10. In Clause 4 of the Brazil SCCs, Option A will apply and the data exporter will be responsible for complying with the obligations set out in Clause 4.1(a)-(c);
11. Schedule 3 of this DPA will be attached as Appendix 2 to the Standard Contractual Clauses and by this reference incorporated into the Standard Contractual Clauses;
12. Schedule 4 of this DPA will be included in Section IV of the Brazil SCCs as an additional annex and by this reference incorporated into the Brazil SCCs; and
13. If there is any conflict between, on one hand, the Standard Contractual Clauses, the UK Addendum or the Brazil SCCs and, on the other hand, the terms of this DPA or the Terms, the Standard Contractual Clauses, the UK Addendum or the Brazil SCCs (as applicable) will prevail.

3. If an alternative transfer mechanism for legitimizing regulated data transfers not described in this DPA (an “**Alternative Transfer Mechanism**”) becomes available during the term of this DPA and AC PM adopts the Alternative Transfer Mechanism, the

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

Alternative Transfer Mechanism will automatically apply instead of the mechanisms described in this DPA only to the extent such Alternative Transfer Mechanism complies with Data Protection Law).

6. **Security Safeguards.** AC PM will implement and maintain the technical and organizational measures set out in Schedule 2 of this DPA. User has reviewed such measures and agrees that, as to the Service, the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the Processing of Personal Information.

7. **Audits.** Where required by Data Protection Law, AC PM will make available to User such records and information as is necessary to demonstrate its compliance with this DPA (“**Audit Information**”). In addition, where AC PM’s Processing of Personal Information is subject to the CCPA, AC PM agrees that User has the right, upon prior written notice to AC PM, to take reasonable and appropriate steps to ensure that User uses the Personal Information in a manner consistent with User’s obligations under the CCPA, and to stop and remediate any unauthorized use by AC PM of the Personal Information. User acknowledges and agrees that User will exercise its audit rights under this DPA by instructing AC PM to comply with the audit measures described in this Section. To request Audit Information, User must identify in writing the information requested and underlying legal requirement for the request. User may request Audit Information up to once per year. Within a reasonable time after AC PM has received and reviewed such request, the parties will discuss and work in good faith towards agreeing on a plan to determine the details of how the request can be addressed. The parties agree to use the least intrusive means for AC PM to verify its compliance with this DPA, taking into account the applicable legal requirements, the nature of the Service, and the urgency of the matter, as well as the need for AC PM to maintain the security of its facilities, maintain uninterrupted business operation, protect itself and its customers from risk, and prevent disclosure of its (or its customers’) confidential information. The parties must have a separate non-disclosure agreement in place which protects the Audit Information as AC PM’s confidential information prior to the disclosure of any Audit Information. User will be responsible for all costs associated with any such audits.

8. **Security Breach.** If AC PM becomes aware of any actual Security Breach (defined below), AC PM will take commercially reasonable efforts to, without undue delay: (a) notify User of the Security Breach and any third-party legal processes relating to the Security Breach; and (b) help User investigate, remediate, and take any action required under Data Protection Laws

regarding the Security Breach. “**Security Breach**” means a breach of security leading to any unlawful or accidental loss, destruction, alteration, or unauthorized Processing of Personal Information under AC PM’s possession or control, that is notifiable under Data Protection

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

Laws. The obligations in this Section do not apply to incidents that are caused by User or unsuccessful attempts or activities that do not compromise the security of Personal Information, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems. AC PM’s obligation to notify a Security Breach under this Section is not and will not be construed as an acknowledgement by AC PM of any fault or liability of AC PM with respect to such Security Breach. Prior to making any Security Breach notification that names AC PM or from which AC PM’s identity could reasonably be determined, User agrees to timely provide AC PM with a draft for discussion on the content of its intended Security Breach notification and this draft will be discussed in a timely fashion and in good faith between the parties, provided however that User will not be required to prejudice its obligations under Data Protection Law.

9. **Return or Destruction of Personal Information.** Upon termination of the Terms and written request by User, AC PM will return all Personal Information to User or destroy all Personal Information and all copies thereof (excluding any backup or archival copies which will be deleted in accordance with AC PM’s data retention schedule), except to the extent that AC PM is required or allowed by Data Protection Laws to keep a copy of Personal Information for a specified period of time.
10. **DISCLAIMER.** AC PM MAKES NO REPRESENTATION OR WARRANTY THAT THIS DPA IS LEGALLY SUFFICIENT TO MEET USER’S NEEDS UNDER DATA PROTECTION LAWS, INCLUDING THE GDPR, UK GDPR, CCPA, LGPD AND AUSTRALIAN PRIVACY ACT. AC PM EXPRESSLY DISCLAIMS ALL REPRESENTATIONS OR WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, THROUGH A COURSE OF DEALING, OR OTHERWISE THAT THIS DPA WILL COMPLY WITH OR SATISFY ANY OF USER’S OBLIGATIONS UNDER DATA PROTECTION LAWS, INCLUDING THE GDPR, UK GDPR, CCPA, LGPD AND AUSTRALIAN PRIVACY ACT. USER FULLY UNDERSTANDS THAT IT IS SOLELY RESPONSIBLE FOR COMPLYING WITH ALL OF ITS OBLIGATIONS IMPOSED BY DATA PROTECTION LAWS. THE PARTIES AGREE THAT THERE WILL BE NO PRESUMPTION THAT ANY AMBIGUITIES IN THIS DPA WILL BE CONSTRUED OR INTERPRETED AGAINST THE DRAFTER.

SCHEDULE 1

Scope of Processing

Subject Matter of Processing: The context for the Processing of Personal Information is AC PM's provision of the Service under the Terms.

Duration of Processing: The duration of the Processing of Personal Information is subject to the terms of the DPA and the Terms. The DPA will terminate simultaneously and automatically with the termination of the Terms.

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

Nature and Purpose of Processing: The purpose of the Processing is to allow User to reliably deliver application emails to their email recipients using the Service. Application emails sent through the Service are categorized as transactional or broadcast electronic messages.

Transactional emails are primarily functional, high-priority messages sent to a single recipient, like password resets or receipts/invoices. Broadcast emails are sent to multiple recipients at once, like announcements of product updates or revised terms of service. The nature of the Processing relates to facilitating the sending and receiving such email messages, including hosting/storage of contact lists and message content, and analytics services, on a continuous basis in accordance with the instructions of User. AC PM does not make any decisions itself as to the use, updating, or deletion of Personal Information.

Types of Personal Information: The Personal Information may concern the following categories of data, which are determined by User in its sole discretion: metadata, email address, message content and other Personal Information collected and provided by User in connection with User's use of the Service. Message content may also include name and other information decided and added by User, like attachments. User also has the option to enable open/link tracking and other analytics/tracking of recipient actions, which could include IP address, location, operating system, browser, device, email client and spam complaints.

Categories of Data Subjects: The Personal Information concerns the following categories of data subjects: customers and prospective customers of User and other email recipients determined by User in connection with User's use of the Service.

SCHEDULE 2

Technical and Organizational Measures

Summary

AC PM hosts its servers in SOC 2 certified data centres. The Service supports opportunistic TLS for all outbound email, ensuring messages are encrypted in transit to remote mail servers and ISPs who

support TLS. Combining this with full HTTPS and TLS support on AC PM's SMTP and API endpoints provides safe passage for messages flowing through the Service. AC PM's systems are regularly tested using both automated systems and manual audits from respected security firms.

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre <https://aws.amazon.com/security/>

AWS also has a dedicated Compliance Program which include certifications and accreditations like CSA, ISO, SOC and more, as listed on their website here: <https://aws.amazon.com/compliance/programs>.

Deft (formerly known as ServerCentral) details

A DuPont Fabros facility, the Deft data center is SOC 2 Type 2 accredited and includes keycard protocols, biometric scanning protocols and round-the-clock surveillance. Deft's environment is colocated, meaning it has full control of the physical environment and only its policies affect the access and use of the hardware, network and software. Deft provides multiple levels of backups and redundancy to ensure uptime and peace of mind. Data transferred to Deft's servers is encrypted via SSL that is configured to meet or exceed all industry standards. Cold data at rest is encrypted with 2048-bit RSA. Deft uses technical and physical controls designed to prevent unauthorized access to personal data that it processes on behalf of controllers. Deft restricts access to personal data only to its employees, contractors and agents who need to know this information in order to operate, develop or improve its service, and whom are bound by confidentiality obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations.

App security

All access to the Postmark interface is secured over SSL (HTTPS), ensuring the information is encrypted. AC PM's SSL configurations are regularly and automatically scanned to ensure AC PM can quickly remediate any vulnerabilities discovered, such as Heartbleed. Additionally, AC PM provides both TLS and HTTPS connections to the Postmark SMTP and API services, ensuring emails

sent to the service are encrypted. AC PM offers a method to recycle API keys at anytime in the Postmark interface.

Security that User can implement

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre [Politique de confidentialité](#) et the Service allows for detailed user permissions so that User can easily and efficiently control who has access to each of its servers. AC PM also fully supports and encourages use of email standards like DKIM, SPF, and DMARC, giving User control over its domain's reputation and reducing the risk of email spoofing.

SCHEDULE 3

Appendix 2 to the Standard Contractual Clauses

Where these Clauses apply pursuant to Section 5 of the DPA, then this Appendix 2 forms part of these Clauses and sets out the Parties' interpretations of their respective obligations under specific provisions within these Clauses, as identified below. Where a Party complies with the interpretations set out in this Appendix 2, that Party shall be deemed by the other Party to have complied with its commitments under these Clauses.

Nothing in the interpretations below is intended to vary or modify these Clauses or conflict with either Party's rights or responsibilities under these Clauses and, in the event of any conflict between the interpretations below and these Clauses, these Clauses shall prevail to the extent of such conflict. Notwithstanding this, the Parties expressly agree that any claims brought under these Clauses shall be exclusively governed by the limitations on liability set out in the Terms. For the avoidance of any doubt, in no event shall any Party limit its liability with respect to any data subject rights under these Clauses.

Clause 8.3: Obligations of the data exporter regarding non-disclosure requirements

The data exporter agrees that the terms of these Clauses constitute the data importer's confidential information and may not be disclosed by the data exporter to any third party without the data importer's prior agreement (other than to a data subject pursuant to Clause 8.3, with the exception of any business secrets or other confidential information, including the measures described in Annex II and personal data, as consistent with the Parties' obligations in that Clause).

Clause 8.9: Audits

The Parties agree that the audit described in Clause 8.9 will be performed in accordance with Section 7 of the DPA. Should a supervisory authority finally determine that such mechanism is not legally sufficient under these Clauses:

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

audit pursuant to Clause 8.9 will be: (i) scoped to only the Audit Information, as provided by the data importer to the data exporter under Section 7 of the DPA, unless a supervisory authority determines that the scope of such audit is not legally sufficient to enable the data importer to comply with its obligations under Clause 8.9; and (ii) conducted no more than annually unless (a) the data exporter reasonably believes the data importer is failing to fulfil its obligations under these Clauses or (b) there has been a confirmed personal data breach, in which case the data exporter may perform an audit at the data exporter's request provided that it makes such request known to the data importer in writing within 30 days after being notified of the personal data breach or the occurrence of any facts giving rise to the belief that the data importer is failing to fulfil its obligations under these Clauses.

2. The data exporter will provide the data importer with reasonable advance written notice of its intent to conduct an audit and to cooperate reasonably with data importer in scheduling such audit. The data exporter will conduct such audit during the data importer's standard business hours and in such a manner to minimise any business disruption to the data importer. To request an audit, the data exporter must submit a detailed audit plan at least 90 days in advance of the proposed audit date describing the proposed scope, duration, and start date of the audit.
3. Any audit will be conducted at the data exporter's expense and the data importer may charge reasonable day rates for any support that it provides to the data exporter in connection with such audit (such rates to be agreed with the data importer in advance or, if no such agreement, then at the data importer's normal professional day rates).
4. Any auditor, whether internal to the data exporter or a third party appointed by the data exporter, must execute a non-disclosure agreement in a form reasonably acceptable to the data importer prior to accessing the data importer's facilities or otherwise receiving confidential information from the data importer in connection with such audit.

Clause 9(a): Use of sub-processors

For the avoidance of any doubt, the data exporter acknowledges and expressly agrees to the data importer's engagement of sub-processors in accordance with Section 4 of the DPA. Such authorization is conditional on the data importer's compliance with the following requirements:

1. the data importer must restrict the sub-processor's access to personal data only to what is strictly necessary to perform its subcontracted data processing services to the data importer (which shall be consistent with the instructions issued to the data importer by the data exporter); and

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

the data importer shall prevent the sub-processor from processing the personal data for any other purpose.

Clause 9(c): Disclosure of sub-processor agreements

1. The Parties agree that the copies of the sub-processor agreements that must be provided by the data importer to the data exporter pursuant to Clause 9(c) may have all business secrets or other confidential information, or provisions unrelated to these Clauses, removed by the data importer beforehand and that such copies will be provided by the data importer, in a manner to be determined in its discretion, only upon request by the data exporter.
2. The Parties agree that all copies of the sub-processor agreements, and information related thereto, that the data importer provides to the data exporter will constitute the data importer's confidential information and may not be disclosed by the data exporter to any third party without the data importer's prior agreement.

Clause 12: Liability

Any claims brought under these Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Terms or other written or electronic agreement for the data exporter's use and purchase of the data importer's products and services. In no event shall any Party limit its liability with respect to any data subject rights under these Clauses.

Clause 14(a): Supplementary Measures

The Parties acknowledge that it is the responsibility of the data exporter to verify whether the safeguards employed by the data importer (which include the technical and organizational measures set out in Schedule 2 of the DPA) are sufficient to meet its obligations under Data Protection Laws, including with respect to the provision of adequate safeguards necessary to secure the transfer of personal data through these Clauses.

Clauses 14(f), 16(b) and 16(c): Suspension of data transfers and termination

1. If the data exporter intends to suspend the transfer of personal data and/or terminate the contract, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("Cure Period").

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

2. If, after the Cure Period, the data importer has not or cannot cure the non-compliance then the data exporter shall terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clauses 8.5 and 16(d): Obligation after the termination of personal data processing services

1. The data importer will fulfil its obligations pursuant to Clauses 8.5 and 16(d) by complying with Section 9 of the DPA.
2. Certification of deletion of personal data will be provided upon the data exporter's written request.

SCHEDULE 4

Section IV of the Brazil SCCs – Additional Annex

Where these Clauses apply pursuant to Section 5 of the DPA, then this Annex forms part of these Clauses and sets out the Parties' interpretations of their respective obligations under specific provisions within these Clauses, as identified below. Where a Party complies with the interpretations set out in this Annex, that Party shall be deemed by the other Party to have complied with its commitments under these Clauses.

Nothing in the interpretations below is intended to vary or modify these Clauses or conflict with either Party's rights or responsibilities under these Clauses and, in the event of any conflict between the interpretations below and these Clauses, these Clauses shall prevail to the extent of such conflict. Notwithstanding this, the Parties expressly agree that any claims brought under these Clauses shall be exclusively governed by the limitations on liability set out in the Terms. For the avoidance of any doubt, in no event shall any Party limit its liability with respect to any Data Subject's rights under these Clauses.

Clause 3: Onward Transfers to Sub-processors

For the avoidance of any doubt, the Exporter acknowledges and expressly agrees to the Importer's engagement of Sub-processors as third-party recipients in accordance with Section 4 of the DPA.

Such authorization is conditional on the Importer's compliance with the following requirements:

1. the Importer must restrict the Sub-processor's access to Personal Data only to what is strictly necessary to perform its subcontracted data processing services to the Importer (which shall be issued to the Importer by the Exporter); and
- Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre
- purpose.

Clause 14: Obligations of the Exporter regarding non-disclosure requirements

The Exporter agrees that the terms of these Clauses, as executed, constitute the Importer's confidential information and may not be disclosed by the Exporter to any third party without the Importer's prior agreement (other than to a Data Subject pursuant to item 14.3, with the exception of any business secrets or other confidential information, including the measures described in Section III and Personal Data, as consistent with the Parties' obligations in item 14.3).

Clause 17: Liability and damages compensation

Any claims brought under these Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Terms in effect as of the date of execution of these Clauses or other written or electronic agreement for the Exporter's use and purchase of the Importer's products and services. In no event shall any Party limit its liability with respect to any Data Subjects' rights under these Clauses.

Clauses 20: Obligations of the Importer regarding the deletion of data

Without limiting its rights to store personal data for the authorized purposes set out in item 20.1, the Importer will fulfil its obligations pursuant to Clause 20 by complying with Section 9 of the DPA.

Clauses 21 and 22: Obligations of the Exporter and the Importer regarding data processing security and legislation of country of destination

The Parties acknowledge that it is the responsibility of the Exporter to verify whether:

1. the safeguards employed by the Importer are sufficient to meet its obligations under Data Protection Laws, including with respect to the provision of adequate safeguards necessary to secure the International Data Transfer and Onward Transfers through these Clauses; and
2. the legislation of the country of destination, including any laws and administrative practices, prevents the Importer from complying with the obligations under these Clauses.

The Importer will fulfil its obligations pursuant to Clause 22 by using commercially reasonable efforts to inform the Exporter if the Importer makes a determination that it can no longer meet its obligations under these Clauses. Notwithstanding the foregoing, the Exporter acknowledges and agrees that such notification by the Importer will neither constitute a general obligation on the part of the Importer nor constitute a waiver of the laws applicable to the Exporter nor legal advice to the Exporter.

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

Clause 23: Suspension of the International Data Transfer and termination

1. If the Exporter intends to suspend the International Data Transfer and/or terminate the contract pursuant to item 23.2, it shall endeavour to provide notice to the Importer and provide the Importer with a reasonable period of time to cure the non-compliance ("Cure Period").
2. If after the Cure Period, the Importer has not or cannot cure the non-compliance then the Exporter may suspend or terminate the International Data Transfer immediately. The Exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to Data Subjects or their Personal Data.

Data Processing Addendum - Existing Customers

Effective May 3, 2022

This Data Processing Addendum, including the Standard Contractual Clauses (as defined below) attached hereto (collectively, the "DPA"), is made and entered into as of the effective date (the "Effective Date") of the applicable customer's ("Customer") acceptance of the Terms of Service between AC PM LLC ("AC PM") and Customer to which this DPA is attached and incorporated (the "Agreement"). All capitalized terms not otherwise defined in this DPA will have the meaning given to them in the Agreement. Under the Agreement, AC PM provides certain Services to Customer that may involve AC PM processing Customer's data, which may include Personal Information (as defined below).

This DPA forms part of the Agreement and contains certain terms and conditions relating to data protection, privacy and security to include certain requirements of the General Data Protection Regulation (EU) 2016/679 (the "GDPR"), including the GDPR as saved into United Kingdom law by

virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"), and the California Consumer Privacy Act of 2018 (Cal. Civ. Code, Title 1.81.5 comprising §§ 1798.100 – 1798.198 (as amended)) (the "CCPA"), where applicable. In the event (and to the extent

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

1. Definitions.

a. "Controller", "Personal Data," "Process," "Processed," "Processing," and "Processor" have the same meanings as in the GDPR. With respect to the CCPA, AC PM and Customer hereby agree that Customer is a "Business" and AC PM is the "Service Provider," as defined under the CCPA and with respect to Personal Information (as defined below).

b. "Customer Data" means any content, data, information or other materials (including Personal Information) submitted or shared by or for Customer to or through the Service.

c. "Data Protection Laws" means all data privacy or data protection laws and regulations that apply to the Processing of Personal Information under the Agreement, including the GDPR and the CCPA, in each case, as amended from time to time.

d. "Data Subject" means (i) an identified or identifiable natural person who is in the EEA or whose rights are protected by EU Data Protection Laws; or (ii) a "Consumer" as the term is defined in the CCPA.

e. "Personal Information" means information relating to a living individual or household who is, relates to, describes or can be, reasonably identified or linked, directly or indirectly from information, either alone or in conjunction with other information, within AC PM's or Customer's control and which is stored, collected, Processed or submitted to or via the Service as Customer Data. Personal information includes Personal Data.

f. "Standard Contractual Clauses" means (i) where the GDPR applies, the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries approved by the European Commission Decision of 4 June 2021, as attached to this DPA; or (ii) where the UK GDPR applies, the Standard Contractual Clauses (controller to processor) promulgated by the European Commission Decision 2010/87/EU.

2. Scope and Application. This DPA applies to the processing of Personal Information subject to Data Protection Laws within the scope of the Agreement. Insofar as AC PM Processes Personal Information subject to Data Protection Laws in the course of performance of the Agreement the

terms of this DPA shall apply. In the context of the GDPR, Customer may act as "controller" and AC PM may act as "processor" with respect to the Personal Information. In the context of the CCPA, Customer may act as "Business" and AC PM may act as "Service Provider" with respect to the Personal Information. Customer shall act as the "data exporter" and AC PM shall act as the "data importer" with respect to the Standard Contractual Clauses.

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

3. Data Processing. AC PM will process Personal Information only in accordance with Customer's lawful instructions the Agreement, and AC PM will not process Personal Information for any purpose other than to provide the Service. This DPA and the Agreement consist of Customer's written instructions to AC PM for the Processing of Personal Information and AC PM must comply with any further reasonable written instructions from Customer for the processing of Personal Information. AC PM will access, collect, retain, use, disclose, and otherwise Process Customer's Personal Information solely to fulfill its obligations to Customer under the Agreement and this DPA, and on Customer's behalf, and for no other purposes. Furthermore, AC PM shall not "sell" (as defined in the CCPA) Personal Information. Each party will comply in all respects with applicable Data Protection Laws in any country where the Service is used, provided or delivered.

4. Cross-Border Transfer Mechanisms for International Data Transfers.

- a. To the extent that Customer's use of the Service requires a transfer of Personal Information outside the EEA or the United Kingdom (the "UK"), AC PM and Customer will take such measures as are necessary to ensure the transfer is in compliance with applicable Data Protection Laws.
- b. AC PM and Customer will only transfer Personal Information from the EEA or the UK to countries outside the EEA or the UK (i) that are recognized by the European Commission as providing an adequate level of protection for Personal Information; (ii) that are covered by a suitable framework recognized by the European Commission as providing an adequate level of protection for Personal Information; or (iii) through the use of other legally recognized validation methods such as Standard Contractual Clauses or Binding Corporate Rules.
- c. AC PM currently transfers personal data from the EEA or the UK to countries outside the EEA as follows: AC PM has adopted and hereby incorporates by reference the Standard Contractual Clauses. The parties further agree that the Standard Contractual Clauses will apply to Personal Information that is transferred via the Service from the EEA or the UK, either directly or via onward transfer, to any country or recipient not recognized by the European Commission as providing an adequate level of protection for personal data.
- d. The parties hereby agree that as new Standard Contractual Clauses are approved by the European Commission or other competent authority and become available for data controller to

data processor transfers, this DPA will be updated to replace the existing Standard Contractual Clauses with the updated and approved Standard Contractual Clauses, if any.

e. Each party agrees to the attached Standard Contractual Clauses under the following Module(s),
Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

f. Audits. The parties agree that the following supplemental terms shall apply in the event of an audit pursuant to Section 8.9 of the attached Standard Contractual Clauses:

(i) If Customer chooses to conduct an independent audit rather than rely on a current SOC 2 Report or current third party audit, if applicable and available, or if Customer makes such choice because a current SOC 2 Report or current third party audit is not available, Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit. AC PM will provide Customer with further details of any applicable costs or fees, and the basis of its calculation, in advance of any such review or audit.

(ii) Before the commencement of any such on-site audit, Customer and AC PM shall mutually agree upon the scope, timing, and duration of the audit.

(iii) Customer shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to AC PM's premises, equipment, personnel and business while Customer's personnel are on those premises in the course of such an audit or inspection.

5. General.

a. This DPA will terminate automatically upon termination of the Agreement.

b. In the event of a conflict between the Agreement (excluding this DPA) and this DPA, the terms of this DPA will take precedence to the extent of the conflict. In the event of a conflict between the Standard Contractual Clauses and the remaining terms of this DPA, the Standard Contractual Clauses will take precedence to the extent of the conflict. Nothing in this DPA modifies the Standard Contractual Clauses or affects any third party's rights under the Standard Contractual Clauses.

STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

SECTION 1

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

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

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

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. Clause 8 - Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
- iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
- iv. Clause 12 - Modules Two and Three: Clause 12(a), (d) and (f);
- v. Clause 13;
- vi. Clause 15.1(c), (d) and (e);
- vii. Clause 16(e);
- viii. Clause 18 - Modules Two and Three: Clause 18(a) and (b).

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 - Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c. 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.

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

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 - Optional - Docking clause

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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 organisational 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.

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

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 organisational 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 risk of a personal data breach, 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 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 organisational 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 authorised 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 implement the specific restrictions and/or additional safeguards described in Annex I B.

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

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 defence 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 regular intervals or if there are indications of non-compliance. In deciding on a review or audit, 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.
- 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 the data subject's personal information, including personal data, the data exporter 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 organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised 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 controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational 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 authorised 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 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

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

The data importer shall not disclose 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 (6) (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 defence 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 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 account relevant certifications held by the data importer.

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

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. GENERAL WRITTEN AUTHORISATION. The data importer has the data exporter's general authorisation 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 fourteen (14) 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. 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 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.

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.

MODULE THREE: Transfer processor to processor

a. GENERAL WRITTEN AUTHORISATION. The data importer has the controller's general authorisation 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

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

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 authorised 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 organisational 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 authorised 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 organisational 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 authorised to handle complaints. It

shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

b. If a dispute arises between the 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, organisation 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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 its 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 Regulation (EU) 2016/679 in accordance with its Article 3(2) without prejudice to the supervisory authority pursuant 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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 authorising 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 geographic sector in which the transfer occurs; the storage location of the data transferred;

ii. the laws and practices of the country of destination— including those requiring the disclosure of data to public authorities or authorising 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 organisational 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). [For Module Three: The data exporter shall forward the notification to the controller.]

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 organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:; if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] 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

MODULE TWO: Transfer controller to processor

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

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.

[For Module Three: The data exporter shall forward the notification to the controller.]

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.). [For Module Three: The data exporter shall forward the information to the controller.]

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

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it requests the data importer to disclose the data requested by a 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. [For Module Three: The data exporter shall make the assessment available to the controller.]

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;

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

ii. the data importer fails to comply with a 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 [for Module Three: and the controller] 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18 - Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

- Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre
- a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b. The Parties agree that they shall submit to the courts of Ireland.
- 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.

APPENDIX

ANNEX I

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

A. LIST OF PARTIES

Data exporter:

Name: Customer, as defined in the Data Processing Addendum to the Agreement. Contact person's name, position and contact details: As specified in the Agreement. Activities relevant to the data transferred under these Clauses: As described under Section B.

Signature and date: The parties agree that execution of the Agreement by the data importer and the data exporter shall constitute execution of these Clauses by both parties on the Effective Date of the Agreement.

Role: Controller/Processor

Data importer:

Name: AC PM LLC

Address: 1 N Dearborn Street, Suite 500, Chicago, IL 60602

Contact person's name, position and contact details: As specified in the Agreement. Activities relevant to the data transferred under these Clauses: As described under Section B.

Signature and date. The parties agree that execution of the Agreement by the data importer and the data exporter shall constitute execution of these Clauses by both parties on the Effective Date

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data subjects are the recipients of emails the data exporter sends using our Services – typically their customers. Where the data exporter is a processor, data subjects are their customers and end users.

Note: We also transfer the personal data of the (representatives of the) data exporter, those who enter into this agreement with us (our customers) and anyone they allow to access their account (users, for example employees, contractors, collaborators). For this processing and transfer of personal data, we are the Controller and our Privacy Policy applies.

Categories of personal data transferred

The categories of personal data transferred relates to the sending and receiving of email messages (and which constitutes personal data). At a minimum, this includes metadata, email address and message content. Message content may also include name and other information decided and added by the sender, like attachments. The data exporter also has the option to enable open/link tracking and other analytics/tracking of recipient actions, which could include IP address, location, operating system, browser, device, email client and spam complaints.

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not applicable.

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

The frequency of transferring the personal data is *continuous*, until the agreement comes to an end.

Nature of the processing

Application emails sent through Postmark are categorized as *transactional* or *broadcast* electronic messages. Transactional emails are primarily functional, high-priority messages sent to a single recipient, such as account creation, password resets, or invoices. Broadcast emails are sent to multiple recipients at a time, such as newsletters, promotional offers, or revised terms of service. The nature of the processing relates to facilitate sending and receiving such email messages, including hosting/storage of contact lists and message content, and analytics services.

Purpose(s) of the data transfer and further processing

The purpose of transferring the personal data is to allow the data exporter to reliably deliver application emails to their users/customers.

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

We process personal data on behalf of the data exporter for as long as they remain customers of ours. When the data exporter terminate their use of the Services, we delete their user/customer data within 30 days of the account termination.

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

We rely on some sub-processors when delivering our application email services. The subject matter pertains mainly to infrastructure hosting. The nature of the processing relates to facilitating sending and receiving email messages, including hosting/storage of contact lists and message content, and analytics services. We also use sub-processors for content distribution, logging and similar operations that are strictly necessary for delivering our services. The duration of processing is for as long as the data exporter remains a customer, after which their data is deleted within 30 days.

Current sub-processors are specified in Annex III.

C. COMPETENT SUPERVISORY AUTHORITY

The Data Protection Commission of Ireland.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

We host our servers in highly secure, SOC 2 certified data centers and use the latest security practices to protect our customers' data. Out of the box, the Postmark service supports opportunistic TLS for all outbound email, ensuring messages are encrypted in transit to remote mail servers and ISPs who support TLS. Combining this with full HTTPS and TLS support on our SMTP and API endpoints provides safe passage for messages flowing through Postmark. Our systems are regularly tested using both automated systems and manual audits from respected security firms.

Amazon Web Services (AWS) details

All personal data is stored in highly secure AWS data centers. AWS regularly achieves third-party validation for thousands of global compliance requirements that they continually monitor to help their customers meet security and compliance standards. AWS supports security standards and compliance certifications like PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2 and NIST 800-171. For a detailed overview of all security and privacy measures, see the AWS Cloud Security page (<https://aws.amazon.com/security>)

AWS also has a dedicated Compliance Program which include certifications and accreditations like CSA, ISO, SOC and more, as listed on their website here: <https://aws.amazon.com/compliance/programs>.

Deft (formerly known as ServerCentral) details

A DuPont Fabros facility, the Deft data center is SOC 2 Type 2 accredited and includes keycard protocols, biometric scanning protocols and round-the-clock surveillance. Our environment is colocated, meaning we have full control of the physical environment and only our policies affect the access and use of the hardware, network and software. We provide multiple levels of backups and redundancy to ensure uptime and peace of mind. Data transferred from our customers to our servers is encrypted via SSL that is configured to meet or exceed all industry standards. Cold data at rest is encrypted with 2048-bit RSA. We use technical and physical controls designed to prevent unauthorized access to personal data we process on behalf of controllers. We restrict access to personal data only to our employees, contractors and agents who need to know this information in order to operate, develop or improve our service, and whom are bound by confidentiality

obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations.

App security

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre [privacy policy](#).

All information sent to and from our servers is secured over SSL (HTTPS), ensuring the information is encrypted. Our SSL configurations are regularly and automatically scanned to ensure we can quickly remediate any vulnerabilities discovered, such as Heartbleed. Additionally, we provide both TLS and HTTPS connections to the Postmark SMTP and API services, ensuring emails sent to the service are encrypted. Account passwords are encrypted in the Postmark database, preventing even our own staff from viewing them. We offer a method to recycle API keys at anytime in the Postmark interface.

Security the controller can implement

Further, our customers (the controllers) can enable 2FA on their account and we allow for detailed user permissions so they can easily and efficiently control who has access to each of their servers. We also fully support and encourage use of email standards like DKIM, SPF, and DMARC, giving them control over their domain's reputation and reducing the risk of email spoofing.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors, as found on the data importer's website here: <https://postmarkapp.com/eu-privacy#sub-processors>. Use of sub-processors, including any addition or replacement of sub-processors, will be in accordance with Clause 9.

Product

[Pricing](#)

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

[Referral Partner Program](#)

[🔔 Latest Updates](#)

Features

[Email API](#)

[Bulk API](#)

[SMTP Service](#)

[Message Streams](#)

[Transactional Email](#)

[Email Delivery](#)

[Templates](#)

[Inbound Email](#)

[Analytics & Retention](#)

[Integrations](#)

[Webhooks](#)

[Security](#)

[Email Experts](#)

[Rebound](#)

Postmark For

[Agencies](#)

[Startups](#)

[Enterprise](#)

[Bootstrapped Startups](#)

[Side Projects](#)

[Developers](#)

Postmark vs.

[SendGrid](#)

[SparkPost](#)

[Mailgun](#)

[Amazon SES](#)

[Mandrill](#)

[Resend](#)

Resources

[Blog](#)

[API Documentation](#)

[API Explorer](#)

[Getting Started](#)

[Email Guides](#)

[Email Comic](#)

[Videos](#)

[Podcast](#)

[DMARC Digests](#)

[Webinars](#)

[Labs](#)

[Migration Guides](#)

[Newsletter](#)

[Glossary](#)

Help

Support Center

Contact Support

Nous, ainsi que nos partenaires, utilisons des cookies pour fournir nos services et vous proposer des publicités. En utilisant notre site web, vous acceptez l'utilisation de cookies comme décrit dans notre

Visit ActiveCampaign for:

Autonomous Marketing

Email Marketing

CRM & Sales Automation

WhatsApp Automation

SMS Automation

Forms & Landing Pages

Made with  at [ActiveCampaign](#) >

[Privacy Policy](#) ↗

[Terms of Service](#)

[EU Data Protection](#)

[Cookie Policy](#)

Paramètres des cookies

© ActiveCampaign, LLC, 2026.