OutboundSync

Updated: November 20, 2025

DATA PROCESSING AGREEMENT

This Data Processing Agreement, including its schedules and the Standard Contractual Clauses (the "**DPA**"), is made by and between OutboundSync, Inc. (the "**Provider**") and Customer, pursuant to the Cloud Service Agreement (the "**Agreement**").

1. Definitions

Capitalized terms not otherwise defined in this DPA shall have the meaning ascribed to them in the Agreement.

1.1 "**Account Data**" means Personal Data that relates to Customer's relationship with Provider, including to access Customer's account and billing information, identity verification, maintain or improve performance of the Services, provide support, investigate and prevent system abuse, or fulfill legal obligations.

1.2 "**Applicable Data Protection Legislation**" refers to laws and regulations applicable to Provider's processing of personal data under the Agreement, including but not limited to (a) the GDPR, (b) in respect of the UK, the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2019 ("**UK GDPR**") and the Data Protection Act 2018 (together, "**UK Data Protection Laws**"), (c) the Swiss Federal Data Protection Act and its implementing regulations ("**Swiss DPA**"), (d) CCPA & CPRA, and (e) Australian Privacy Principles and the Australian Privacy Act (1988), in each case, as may be amended, superseded or replaced.

1.3 "**CCPA**" or "**CCPA and CPRA**" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, together with any implementing regulations, each as may be amended from time to time.

1.4 "**Controller**" or "**controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. It has the meaning given to "controller" under the GDPR, UK GDPR, and other Applicable Data Protection Legislation. For U.S. state privacy laws, the role of a controller is analogous to the concept of a "Business" under the CCPA/CPRA, to the extent applicable.

1.5 "**Customer Personal Data**" means Personal Data that Provider processes as a processor on behalf of Customer.

1.6 "**Europe**" means for the purposes of this DPA the European Economic Area ("EEA"), the United Kingdom ("UK") and Switzerland, or another country which ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of Personal Data, as determined by the European Commission in the case that EU Data Protection Law applies respectively as determined by the ICO in the case that UK Data Protection Law applies.

1.7 **"Governing Member State"** means the Member State in which the data exporter is established or, where the data exporter is not established in a Member State, the Member State in which the data exporter's representative within the meaning of Article 27(1) of the GDPR is established.

1.8 "**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council 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).

1.9 "**Personal Data**" or "**personal data**" or "**personal information**" means any information, including personal information, relating to an identified or identifiable natural person ("**data subject**") or as defined in and subject to Applicable Data Protection Legislation.

1.10 "**Processor**" or "**processor**" means the entity that processes Personal Data on behalf of the Controller. It shall have the meaning ascribed to "processor" under the GDPR and other equivalent terms under other Applicable Data Protection Legislation (e.g., "Service Provider" as defined under the CCPA), as applicable.

1.11 "**Processing**" or "**processing**" (and "**Process**" or "**process**") means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

1.12 "**Restricted Transfer**" means: (i) where the GDPR applies, a transfer of Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy decision by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to a country that is not subject to adequacy regulations under Section 17A of the Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of Personal Data from Switzerland to a country that is not included on the list of jurisdictions recognized as providing adequate protection by the Swiss Federal Data Protection and Information Commissioner.

1.13 "**Security Incident**" means a breach of security leading to any accidental, unauthorized, or unlawful loss, disclosure, destruction, alteration, unauthorized disclosure of, or access to Customer Personal Data transmitted, stored, or otherwise processed by Provider. A Security Incident shall not include an unsuccessful attempt or activity that does not compromise the security of Customer Personal Data, including (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

1.14 "**Sensitive Data**" means any personal data subject to heightened protection under Applicable Data Protection Legislation, including (a) special categories of personal data under the GDPR (e.g., health, biometric, genetic, or data revealing racial or ethnic origin, political opinions, religious beliefs, or sexual orientation, as well as data on criminal convictions); (b) categories of "sensitive personal information" under U.S. laws (e.g., Social Security or government IDs, account log-in details with passwords, precise geolocation, biometric identifiers such as voiceprints, health data, or financial account information); and (c) any other data classified as sensitive or requiring enhanced safeguards under applicable law.

1.15 "**Standard Contractual Clauses**" or "**SCCs**" means (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries under Regulation (EU) 2016/679 ("**EU SCCs**"); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c), or (d) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office under section 119A(1) of the Data

Protection Act 2018 (version B1.0, effective 21 March 2022), as amended, updated, or replaced from time to time (the **"UK Addendum"**); and (iii) where the Swiss DPA applies, the standard data protection clauses issued, approved, or recognized by the Swiss Federal Data Protection and Information Commissioner (the "**Swiss SCCs**"), in each case, as updated, amended or superseded from time to time.

1.16 "**Sub-processor**" or "**sub-processor**" means (a) Provider, when Provider is processing Customer Personal Data and where Customer is itself a processor of such Customer Personal Data, or (b) any third-party Processor engaged by Provider or its affiliates to assist in fulfilling Provider's obligations under the Agreement and which processes Customer Personal Data. Sub-processors may include third parties or Provider affiliates, but shall exclude Provider employees, contractors, or consultants.

1.17 "**Third Party Request**" means any request, correspondence, inquiry, or complaint from a data subject, regulatory authority, or third party.

2. Applicability and Scope

2.1 Applicability. This DPA will apply only to the extent that Provider processes, on behalf of Customer, Personal Data to which Applicable Data Protection Legislation applies.

2.2 Scope. The subject matter of the data processing is the provision of the Services, and the processing will be carried out for the duration of the Agreement. Schedule A (Details of Processing) sets out the nature and purpose of the processing, the types of Personal Data Provider processes, and the categories of data subjects whose Personal Data is processed.

2.3 Provider as a Processor. Parties acknowledge and agree that regarding the processing of Customer Personal Data, Customer may act either as a controller or processor, and Provider is a processor. Provider will process Customer Personal Data in accordance with Customer's instructions as set forth in Section 3.1 (Customer Instructions).

2.4 Provider as Sub-processor. In situations where Customer is a processor of Customer Personal Data, Provider will be deemed a Sub-processor of Customer Personal Data. In such cases, Customer represents and warrants that it has entered into a data processing agreement with the relevant Controller that permits the appointment of Sub-processors, and Provider will comply with the equivalent data protection obligations imposed on Customer under such upstream agreement, as required by Article 28(4) GDPR.

2.5 Provider as a Controller of Account Data. Parties acknowledge that, regarding the processing of Account Data, Customer is a Controller, and Provider is an independent Controller, not a joint Controller with Customer, and such processing is not subject to this DPA. Provider will process Account Data as a Controller (a) in order to manage the relationship with Customer; (b) carry out Provider's core business operations; (c) in order to detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; (d) to conduct identity verification; (e) to comply with Provider's legal or regulatory obligations; and (f) as otherwise permitted under Applicable Data Protection Legislation and in accordance with this DPA, the Agreement, and the Privacy Policy.

3. Provider as Processor

3.1 Customer Instructions. Customer appoints Provider as a processor to process Customer Personal Data on behalf of, and in accordance with, Customer's instructions (a) as set forth in the Agreement, this DPA, and as otherwise necessary to provide the Services to Customer (which may include investigating security incidents, and detecting and preventing exploits or abuse); (b) as necessary to comply with applicable law, including Applicable Data Protection Legislation; and (c) as otherwise agreed in writing between Parties ("**Permitted Purpose**").

3.2 Lawfulness of Instructions. Customer will ensure that its instructions comply with Applicable Data Protection Legislation. Customer acknowledges that Provider is neither responsible for determining which laws are applicable to Customer's business nor whether Provider's Services meet or will meet the requirements of such laws. Customer will ensure that Provider's processing of Customer Personal Data, when done in accordance with Customer's instructions, will not cause Provider to violate any applicable law, including Applicable Data Protection Legislation. Provider will inform Customer if it becomes aware, or reasonably believes, that Customer's instructions violate applicable law, including Applicable Data Protection Legislation.

3.3 Additional Instructions. Additional instructions outside the scope of the Agreement or this DPA will be mutually agreed to between Parties in writing.

3.4 Purpose Limitation. Provider will process Customer Personal Data in order to provide the Services in accordance with the Agreement. Schedule A (Description of the Processing Activities / Transfer) of this DPA further specifies the nature and purpose of the processing, the processing activities, the duration of the processing, the types of Personal Data, and categories of data subjects.

3.5 Responding to Third-Party Requests. In the event any third-party request is made directly to Provider in connection with Provider's processing of Customer Personal Data, Provider will promptly inform Customer and provide details of the same, to the extent legally permitted. Provider will not respond to any third-party request without prior notice to Customer and an opportunity to object, except as legally required to do so or to confirm that such third-party request relates to Customer. Provider will cooperate with and provide reasonable assistance to Customer, at Customer's expense, in any legal response or other procedural action taken by Customer in response to a third-party request about Provider's processing of Customer Personal Data under this DPA.

3.6 Processing of Sensitive Data. Parties acknowledge that, in the course of providing the Services, the Provider may process Sensitive Data as defined in this DPA. Customer, as Controller, shall ensure that any collection or disclosure of such Sensitive Data to the Provider has a valid lawful basis under Applicable Data Protection Legislation. The Provider shall process Sensitive Data solely on documented instructions of Customer and not for its own purposes.

4. Compliance

Customer shall be responsible for ensuring that: a) all such notices have been given, and all such authorizations have been obtained, as required under Applicable Data Protection Legislation, for Provider (and its affiliates and Sub-processors) to process Customer Personal Data as contemplated by the Agreement and this DPA; b) it has complied, and will continue to comply, with all applicable laws relating to privacy and data protection, including Applicable Data Protection Legislation; and c) it has, and will continue to have, the right to transfer, or provide access to, Customer Personal Data to Provider for processing in accordance with the terms of the Agreement and this DPA.

5. Sub-processors

5.1 Authorization for Sub-processing. Customer agrees that (a) Provider may engage Sub-processors as listed on the website linked under Schedule C (the "**Sub-processor Page**"), which may be updated from time to time, and Provider affiliates; and (b) such affiliates and Sub-processors, respectively, may engage third-party processors to process Customer Personal Data on Provider's behalf. Customer provides a general authorization for Provider to engage onward sub-processors that is conditioned on the following requirements: (x) Provider will restrict the onward sub-processor's access to Customer Personal Data only to what is strictly necessary to provide the Services, and Provider will prohibit the sub-processor from processing Customer Personal Data for any other purpose. (y) Provider agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor to protect Customer Personal Data to the standard required by Applicable Data Protection Legislation; and (z) Provider will remain liable and accountable for any breach of this DPA that is caused by an act or omission of its sub-processors.

5.2 Current Sub-processors. Customer understands that effective operation of the Services may require the transfer of Customer Personal Data to Provider affiliates or to Provider's Sub-processors, see Schedule C. Customer hereby authorizes the transfer of Customer Personal Data to locations outside Europe, including to Provider affiliates and Sub-processors, subject to continued compliance with this DPA throughout the duration of the Agreement. Customer hereby provides general authorization to Provider to engage additional third-party Sub-processors to process Customer Personal Data within the Services for the Permitted Purpose, in accordance with Sections 5.1 and 5.3.

5.3 Notification of Sub-processor Additions. Provider may, by giving reasonable notice to Customer, add to the Sub-processor Page. Provider will notify Customer if it intends to add or replace Sub-processors from the Sub-processor Page at least 10 days prior to any such changes. Customer will receive this notification in the Provider's Platform. If Customer objects to the appointment of an additional Sub-processor within thirty (30) calendar days of such notice on reasonable grounds relating to the protection of Customer Personal Data, then Provider will work in good faith with Customer to find an alternative solution. In the event that Parties are unable to find such a solution, Customer may terminate the Agreement at no additional cost.

6. Impact Assessment.

Provider shall, to the extent required by Applicable Data Protection Legislation, provide Customer with reasonable assistance (at Customer's cost and expense) with data protection impact assessments or prior consultations with data protection authorities that Customer is required to carry out under such legislation.

7. Security

7.1 Security Measures. Provider has in place and will maintain throughout the term of this Agreement appropriate technical and organizational measures designed to protect Customer Personal Data against Security Incidents. These measures shall, at a minimum, comply with applicable law and include the measures identified in Schedule B (Technical and Organizational Security Measures). Customer acknowledges that the security measures are subject to technical progress and development and that Provider may update or modify the security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by Customer.

7.2 Staff. Provider will ensure that any person authorized to process Customer Personal Data (including its staff, agents, and subcontractors) shall be subject to a duty of confidentiality.

7.3 Security Incident. Upon becoming aware of a Security Incident involving Customer Personal Data processed by Provider on behalf of Customer under this DPA, Provider shall notify Customer without undue delay, but no later than 72 hours after becoming aware of the Security Incident, and shall provide such information as Customer may reasonably require, including to enable Customer to fulfil its data breach reporting obligations under Applicable Data Protection Legislation. Provider's notification of or response to a Security Incident shall not be construed as an acknowledgement by Provider of any fault or liability with respect to the Security Incident.

7.4 Customer's Responsibility. Customer is solely responsible for its use of the Services, including (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of Customer Personal Data; (b) securing the account authentication credentials, systems, and devices Customer uses to access the Service; and (c) backing up Customer Personal Data.

8. Return or Deletion.

Upon termination or expiry of this Agreement, Provider will (at Customer's election) delete or return to Customer all Customer Personal Data (including copies) in its possession or control as soon as reasonably practicable and within a maximum period of 30 days of termination or expiry of the Agreement, save that this requirement will not apply to the extent that Provider is required by applicable law to retain some or all of Customer Personal Data, or to Customer Personal Data it has archived on back-up systems, which Customer Personal Data Provider will securely isolate and protect from any further processing, except to the extent required by applicable law.

9. Audits

9.1 Acknowledgment. Parties acknowledge that when Provider is acting as a processor on behalf of Customer, Customer must be able to assess Provider's compliance with its obligations under Applicable Data Protection Legislation and this DPA.

9.2 Previous Audits. Upon written request and at no additional cost to Customer, Provider shall provide Customer, or its appropriately qualified third-party representative (collectively, the "**Auditor**"), access to reasonably requested documentation evidencing Provider's compliance with its obligations under this DPA in the form of the relevant audits or certifications.

9.3 Customer Audit. Parties intend to ordinarily rely on the provision of documentation, certifications, and/or third-party audit reports (such as ISO 27001, SOC 2 Type II, or HITRUST, as applicable) to demonstrate the Provider's compliance with this DPA and Applicable Data Protection Legislation. Upon Customer's written request, the Provider shall make available such documentation or reports that are reasonably sufficient to demonstrate compliance. Where such documentation is not reasonably sufficient, Provider shall permit Customer or its Auditor to carry out an audit, at Customer's cost and expense, (including, without limitation, the costs and expenses of Provider), of Provider's processing of Customer Personal Data under the Agreement upon Customer's written request for an audit, subject to the terms of this Section 9.3. Following Provider's receipt of such a request, Provider and Customer shall mutually agree

in advance on the details of the audit, including the reasonable start date, scope, and duration of any such audit. Any such audit shall be subject to Provider's security and confidentiality terms and guidelines and may only be performed once in any twelve (12) month period, unless otherwise required by a competent supervisory authority or applicable law. Where the Auditor is a third-party, Provider may object in writing to such Auditor, if in Provider's reasonable opinion, the Auditor is not suitably qualified or is a direct competitor of Provider. Any such objection by Provider will require Customer to either appoint another Auditor or conduct the audit itself. Any expenses incurred by an Auditor in connection with any review of reports or an audit shall be borne exclusively by the Auditor. For clarity, the exercise of audit rights under the SCCs or other applicable transfer mechanisms shall be as described in and subject to the terms of this Section 9.3 of this DPA.

10. Transfers

10.1 Authorization. Customer agrees that Provider may transfer Customer Personal Data outside the EEA, the United Kingdom, or other relevant geographic territory as necessary to provide the Service. If Provider transfers Customer Personal Data to a territory for which the European Commission or other relevant supervisory authority has not issued an adequacy decision, Provider will implement appropriate safeguards for the transfer of Customer Personal Data to that territory consistent with Applicable Data Protection Legislation.

10.2 Transfer Mechanism. Parties agree that when the transfer of personal data from Customer (as "**data exporter**") to Provider (as "**data importer**") is a Restricted Transfer, Applicable Data Protection Legislation requires that appropriate safeguards be put in place. For the purposes of such Restricted Transfers from Customer to Provider, Parties rely on Provider's certification under the EU-US Data Privacy Framework, the Swiss-US Data Privacy Framework, and the UK-US Data Privacy Framework (together, the "**DPF**") operated by the U.S. Department of Commerce. To the extent that the DPF is invalidated or ceases to be an appropriate safeguard under Article 46 GDPR for transfers to the United States, then, such transfer shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form part of this DPA, as follows: In relation to transfers of Customer Personal Data that is protected by the GDPR, the EU SCCs shall apply, completed as follows:

10.3 Module Two (Controller to Processor) of the EEA SCCs apply when Customer is a Controller and Provider is processing Customer Personal Data on behalf of Customer as a Processor.

10.4 Module Three (Processor to Sub-Processor) of the EEA SCCs apply when Customer is a Processor and Provider is Processing Customer Personal Data on behalf of Customer as a Sub-processor.

10.5 For each module, the following applies (when applicable):

10.5.1 The optional docking clause in Clause 7 does not apply;

10.5.2 In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of Sub-processor changes is 10 business days;

10.5.3 In Clause 11, the optional language does not apply;

10.5.4 All square brackets in Clause 13 are removed;

10.5.5 In Clause 17 (Option 1), the EEA SCCs will be governed by the laws of the Governing Member State;

10.5.6 In Clause 18(b), disputes will be resolved in the courts of the Governing Member State; and

10.5.7 This DPA contains the information required in Schedule 1 of the EEA SCCs.

10.6 UK Transfers. To the extent Customer Personal Data is transferred from the United Kingdom to Provider in the United States, and such transfer is covered by the UK Extension to the EU–U.S. Data Privacy Framework ("**UK DPF**"), the parties agree that Provider's participation in the UK DPF constitutes the applicable transfer safeguard under the UK GDPR. If, at any time, the UK DPF is (i) invalidated, (ii) suspended, or (iii) no longer recognized as an appropriate safeguard under the UK GDPR, then, without requiring any further action by the parties, the following shall automatically apply:

10.6.1 The International Data Transfer Addendum to the EU Commission Standard Contractual Clauses is incorporated into and forms part of this DPA.

10.6.2 The UK Addendum applies to all Restricted Transfers from the United Kingdom to Provider, and is completed as follows:

10.6.2.1 Table 2 of the UK Addendum (SCC selection and modules) is completed with the information set out in Schedule A of this DPA.

10.6.2.2 Table 4 of the UK Addendum is modified as follows: Neither party may terminate the UK Addendum under Section 19. If the ICO issues a revised Approved Addendum under Section 18, the parties will work in good faith to update this DPA accordingly.

10.6.2.3 Schedules A and B to this DPA contain the information required by Annex 1A, Annex 1B, Annex II, and Annex III of the UK Addendum.

10.6.3 For clarity, the parties agree that the fallback to the UK Addendum under this Section 10.6 applies immediately upon such invalidation or suspension of the UK DPF, ensuring that all UK-protected Personal Data continues to be transferred under a valid and compliant safeguard in accordance with the UK GDPR.

10.7 Alternative Transfer Mechanism. For Personal Data transfers where Swiss law (and not the law in any EEA member state or the United Kingdom) applies to the international nature of the transfer, references to the GDPR in Clause 4 of the EEA SCCs are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority will include the Swiss Federal Data Protection and Information Commissioner

11. Cooperation and Data Subject Rights

11.1 Data Subject Rights. Provider provides Customer with a number of self-service features via the Services, including the ability to delete, obtain a copy of, or restrict use of Customer Personal Data. Customer may use such self-service features to assist in complying

with its obligations under Applicable Data Protection Legislation with respect to responding to Third Party Requests from data subjects via the Services at no additional cost. Upon Customer's request, Provider shall, taking into account the nature of the processing, provide reasonable assistance to Customer where possible and at Customer's cost and expense, to enable Customer to respond to requests from a data subject seeking to exercise their rights under Applicable Data Protection Legislation. In the event that such a request is made directly to Provider, if Provider can, through reasonable means, identify Customer as the controller of Customer's personal data of a data subject, Provider shall promptly inform Customer of the same. As between Parties, Customer shall have sole discretion and responsibility in responding to the rights asserted by any individual in relation to Customer Personal Data.

11.2 Cooperation. In the event that either party receives (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Legislation or (b) any third-party request relating to the processing of Account Data or Customer Personal Data conducted by the other party, such party will promptly inform the other party in writing. Parties agree to cooperate, in good faith, as necessary to respond to any third-party request and fulfill their respective obligations under Applicable Data Protection Legislation.

12. Limitation of Liability

12.1 Liability Caps and Damages Waiver. To the maximum extent permitted under Applicable Data Protection Legislation, each party's total cumulative liability to the other party arising out of or related to this DPA will be subject to the waivers, exclusions, and limitations of liability stated in the Agreement.

12.2 Related-Party Claims. Any claims made against Provider or its Affiliates arising out of or related to this DPA may only be brought by the Customer entity that is a party to the Agreement.

12.3 Exceptions. This DPA does not limit any liability to an individual regarding the individual's data protection rights under Applicable Data Protection Legislation. This does not create unlimited liability between Parties.

13. No Sale or Sharing

13.1 To the extent that the processing of Customer Personal Data is subject to U.S. data protection laws, Provider is prohibited from: (a) selling Customer Personal Data or otherwise making Customer Personal Data available to any third party for monetary or other valuable consideration; (b) sharing Customer Personal Data with any third party for cross-behavioral advertising; (c) retaining, using, or disclosing Customer Personal Data for any purpose other than for the business purposes specified in this DPA or as otherwise permitted by U.S. data protection laws; (d) retaining, using or disclosing Customer Personal Data outside of the direct business relationship between Parties, and; (e) except as otherwise permitted by U.S. data protection laws, combining Customer Personal Data with personal data that Provider receives from or on behalf of another person or persons, or collects from its own interaction with the data subject. Provider will notify Customer promptly if it makes the determination that it can no longer meet its obligations under applicable U.S. data protection laws.

14. Miscellaneous

14.1 If there is a conflict between the Agreement and this DPA, the terms of this DPA will prevail. The order of precedence will be: (a) this DPA; (b) the Agreement; and (c) the

Privacy Policy. To the extent there is any conflict between the Standard Contractual Clauses, and any other terms in this DPA, the Agreement, or the Privacy Policy, the provisions of the Standard Contractual Clauses will prevail.

14.2 Parties agree that this DPA shall replace and supersede any prior data processing addendum that Provider and Customer may have previously entered into in connection with the Services.

14.3 Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

14.4 In no event does this DPA restrict or limit the rights of any data subject or of any competent supervisory authority.

14.5 In the event (and to the extent only) of a conflict (whether actual or perceived) among Applicable Data Protection Legislation, Parties (or relevant party as the case may be) shall comply with the more onerous requirement or standard, which shall, in the event of a dispute in that regard, be solely determined by Provider.

14.6 Notwithstanding anything else to the contrary in the Agreement, Provider reserves the right to make any modification to this DPA as may be required to comply with Applicable Data Protection Legislation.

14.7 Notwithstanding anything in the Agreement or any order form entered in connection therewith, Parties acknowledge and agree that Provider's access to Customer Personal Data does not constitute part of the consideration exchanged by Parties in respect of the Agreement.

14.8 In no event shall this DPA benefit or create any right or cause of action on behalf of a third party (including a third-party Controller), but without prejudice to the rights or remedies available to Data Subjects under Data Protection Laws or this DPA (including the DPF and SCCs).

OutboundSync

Updated: November 20, 2025

Schedule A
Description of the Processing Activities / Transfer

Schedule A (1) — List of Parties

Data Exporter	Data Importer
Name: The Customer signing the DPA	**Name:** OutboundSync, Inc.
Address: As identified in the Agreement or Order Form	**Address:** 131 Continental Dr Ste 305, Newark, Delaware 19713, USA
Contact details: As identified in the Agreement or Order Form	**Contact details:** Harris Kenny, President — As identified in the Agreement
Activities relevant to the transfer: See Schedule A(2)	**Activities relevant to the transfer:** See Schedule A(2)
Role: Controller	**Role:** Processor

Schedule A (2) — Description of Transfer

Field	Description
Categories of data subjects:	• Prospective customers and leads included in outbound sales campaigns. • CRM contacts, companies, and related entities maintained by the Customer. • Customer's employees or authorized users who configure or use the integration. • Customer's end users or customers whose Personal Data enters the CRM through outbound activity.
Categories of personal data:	• Full name • Business email address • Job title • Company name • Contact information (email, phone number, or address) • Engagement metadata (e.g. email subject lines, reply indicators, open/click/bounce events, social media activity, telephony) • CRM identifiers and attributes • User activity information (device data, session identifiers, IP address)
Sensitive data:	OutboundSync does not intentionally collect or process special categories of data under GDPR Article 9. No sensitive data is required for the Services.
Frequency of the transfer:	Continuous transfer and synchronization, based on Customer system activity.

Nature and subject matter of processing:	• Receiving and ingesting engagement signals (opens, clicks, replies, bounces). • Normalizing, structuring, and mapping engagement metadata to CRM objects (contacts, leads, companies, deals). • Creating CRM timeline activities and updating fields. • Managing blocklists to prevent duplicate outreach. • Synchronizing updates between Customer systems and CRM records. • Storage, organization, retrieval, and secure transmission of Personal Data. • Returning, deleting, or correcting Personal Data as instructed by Customer. • Technical support, troubleshooting, and security monitoring.
Purpose(s) of the data transfer and further processing:	• To synchronize outbound engagement activity into CRM systems. • To maintain CRM accuracy, hygiene, attribution, and reporting integrity. • To prevent duplicate outreach and manage domain/email blocklists. • To support Customer-configured workflows and outbound operations. • To perform processing strictly on Customer's documented instructions.
Duration of the processing:	Processing Term: for the duration of the Customer's Agreement with OutboundSync and until all Customer Personal Data has been returned or deleted in accordance with the DPA.
Retention period (or criteria):	OutboundSync retains Personal Data only as necessary to perform the Services or comply with applicable law. Upon termination, Personal Data is deleted or returned as required by the DPA.

Schedule A (3): Competent supervisory authority

The supervisory authority will be the supervisory authority of the data exporter, as determined in accordance with Clause 13 of the EEA SCCs or the relevant provision of the UK Addendum.

OutboundSync

Updated: November 20, 2025

Schedule B
Technical and Organizational Measures

The technical and organizational measures implemented by Provider (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context, and purposes of the processing, and the risks for the rights and freedoms of natural persons, is accessible at: https://trust.outboundsync.com/.

Further detail on these measures and the current SOC 2 Type II report is available to customers under a confidentiality agreement.

OutboundSync

Updated: November 20, 2025

Schedule C
Approved Sub-processors

List of approved Sub-processors is accessible at: https://trust.outboundsync.com/