Data Processing Agreement

LAST UPDATED: JULY 19, 2023

This Data Processing Agreement and its Annexes (the "**DPA**") reflects the parties' agreement with respect to the processing of personal data by **REPLYCO LTD,** a company registered in England (company registration number 11124756) whose registered office is at 9 Oliver Business Park, Oliver Road, Park Royal, London, England, NW10 7JB ("**Replyco**") on behalf of you (the "**Customer**") (each a "**party**" and together the "**parties**") in connection with the provision of services by Replyco under the Terms and Conditions available at https://replyco.com/terms-and-conditions/ (the "**Agreement**") between Replyco and the Customer.

IT IS AGREED AS FOLLOWS:

1. Definitions

1.1. In this DPA, the terms in this clause shall have the following meanings:

(a) "**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in EU Data Protection Laws and UK Data Protection Laws;

(b) "**Applicable Data Protection Law**" means all worldwide data protection and privacy laws and regulations applicable to the personal data in question, including, where applicable, EU/UK Data Protection Law;

(c) "**Effective Date**" means the date the parties entered into the Agreement;

(d) "**EU Data Protection Laws**" means:

(i) all EU regulations applicable (in whole or in part) to the Processing of Personal Data (such as Regulation (EU) 2016/679 (the "**EU GDPR**"));

(ii) the national laws of each EEA member state implementing any EU directive applicable (in whole or in part) to the Processing of Personal Data (such as Directive 2002/58/EC); and

(iii) any other national laws of each EEA member state applicable (in whole or in part) to the Processing of Personal Data,

as amended or superseded from time to time.

(e) "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018;

(f) "**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the

European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**"); and

(g) "**UK Data Protection Laws**" means:

(i) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**");

(ii) the Data Protection Act 2018 (the "**DPA 2018**");

(iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003 as it continues to have effect under section 2 of the European Union (Withdrawal) Act 2018; and

(iv) any other laws in force in the UK from time to time applicable (in whole or in part) to the Processing of Personal Data;

as such may be amended or superseded from time to time.

1.2 In this DPA, unless the context otherwise requires:

(a) references to a person shall include any individual, company, unincorporated association, firm, partnership, trust, government, state or agency of a state, and any undertaking (in each case, whether or not having separate legal personality and irrespective of the jurisdiction in or under the laws of which it was incorporated or exists);

(b) references to one gender shall include all genders and references to the singular shall include the plural and vice versa;

(c) clause and other headings in this DPA are for convenience of reference only and will not constitute a part of or otherwise affect the meaning or interpretation of this DPA;

(d) the Schedules and Annexes shall be incorporated into and form part of this DPA;

(e) the Standard Contractual Clauses (when they are incorporated into this DPA by reference in accordance with its terms) will be deemed to be an integral part of this DPA to the same extent as if they had been set forth verbatim herein;

(f) any phrase introduced by the terms “including”, “include”, “in particular” or any similar expression shall be construed as illustrative and shall not limit the sense of the words introduced by those terms.

1.3 This DPA is subject to the terms of the Agreement and is incorporated into the Agreement. Interpretations and defined terms set forth in the Agreement apply to the interpretation of this DPA.

1.4 In the case of conflict or ambiguity between any of the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA will prevail.

2. Relationship of the parties

The Customer instructs Replyco to process the personal data described in Annex I of this DPA (the "**Data**") on its behalf. In respect of such processing, the Customer shall be a controller and Replyco shall be a processor. Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

3. Prohibited data

The Customer shall not disclose (and shall not permit any data subject to disclose) any special categories of Data to Replyco for processing.

4. Purpose limitation

Replyco shall process the Data as necessary to perform its obligations under the Agreement and in accordance with the documented instructions of the Customer (the "**Permitted Purpose**"), except where otherwise required by law(s) that are not incompatible with Applicable Data Protection Law. Replyco shall inform the Customer if, in its opinion or, it becomes aware that, such processing instructions infringe Applicable Data Protection Law (but without obligation to actively monitor the Customer's compliance with Applicable Data Protection Law). The Customer is solely responsible for the accuracy, quality, and legality of the Data.

5. Consent

The Customer will ensure that it has obtained or will obtain all necessary consents from data subjects, and has given or will give all necessary notices to data subjects, for the processing of Data by Replyco in accordance with Applicable Data Protection Law.

6. Restricted transfers

6.1 The parties agree that when the transfer of Data from the Customer to Replyco is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

(a) in relation to Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module Two will apply;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Clause 10 of this DPA;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

(vi) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this DPA;

(viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this DPA; and

(ix) Annex III of the EU SCCs shall be deemed completed with the information set out in Annex III to this DPA;

(b) in relation to Data that is protected by the UK GDPR, the UK Addendum will apply completed as follows:

(i) The EU SCCs, completed as set out above in clause 6.1(a) of this DPA shall also apply to transfers of such Data, subject to sub-clause (ii) below; and

(ii) Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out above, and the options "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this DPA.

(c) in the event that any provision of this DPA contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

7. Onward transfers

Replyco shall not participate in any other Restricted Transfers of Data (whether as an exporter or an importer of the Data) unless the Restricted Transfer is made in compliance with Applicable Data Protection Law and pursuant to Standard Contractual Clauses implemented between the relevant exporter and importer of the Data.

8. Confidentiality of processing

Replyco shall ensure that any person that it authorises to process the Data shall be subject to a duty of confidentiality (whether a contractual duty or a statutory duty).

9. Security

Replyco shall implement appropriate technical and organisational measures to protect the Data from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure or access (a "**Security Incident**"). Notwithstanding any provision to the contrary, Replyco may modify or update such technical and organisational measures at its discretion provided that such modification or update does not result in a material degradation in the protection offered by such technical and organisational measures.

10. Subprocessing

The Customer consents to Replyco engaging third party subprocessors to process the Data ("**subprocessor**") provided that: (i) Replyco provides prior notice of the addition or removal of any subprocessor, which may be given by posting details of such addition or removal at the following URL: https://replyco.com/subprocessors and the Customer is granted an opportunity to object to the appointment of each subprocessor within 14 days of notification; (ii) Replyco imposes data protection terms on any subprocessor it appoints that protect the Data, in substance, to the same standard provided for by this DPA; and (iii) Replyco remains fully liable for the subprocessors' performance of its obligations. If the Customer objects to Replyco's appointment of a subprocessor on reasonable grounds relating to the protection of the Data, then the parties will discuss the Customer's concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution is reached then Replyco, at its sole

discretion, may choose not to appoint the subprocessor and, if Replyco chooses to continue with the appointment, the Customer may elect to suspend or terminate the Agreement (but without prejudice to any fees incurred by the Customer prior to suspension or termination).

11. Cooperation and data subjects' rights

Upon the Customer's written request, Replyco shall provide reasonable assistance to the Customer (at the Customer's expense) to enable the Customer to respond to: (i) request(s) from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. If a domestic law, court or regulator (including the Commissioner) requires Replyco to process or disclose the Data to a third party, Replyco will first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic law prohibits the giving of such notice.

12. Data Protection Impact Assessment

Replyco shall provide the Customer with such reasonable assistance as the Customer may require in order to enable it to conduct a data protection impact assessment in accordance with Applicable Data Protection Law including, if necessary, to assist the Customer to consult with its relevant data protection authority.

13. Security incidents

Upon becoming aware of a Security Incident, Replyco shall inform the Customer without undue delay and shall provide such timely information and reasonable cooperation as the Customer may reasonably require, as it becomes known to Replyco or is reasonably requested by the Customer, in order for the Customer to fulfil its data breach reporting obligations under Applicable Data Protection Law.

14. Deletion or return of Data

Upon termination or expiry of the Agreement, Replyco shall (at the Customer's election) destroy or return to the Customer all Data (including all copies of the Data) in its possession or control. This requirement shall not apply to the extent that Replyco is required by any applicable law to retain some or all of the Data. Where the Customer does not notify Replyco in writing within thirty (30) days after the date of expiration or termination of the Agreement requesting Replyco to destroy or return to the Customer all Data, then Replyco shall be under no obligation to retain (and may destroy) such Data.

15. Audit

Replyco shall permit the Customer or its appointed third party auditors to audit Replyco's compliance with this DPA, and shall make available to the Customer all reasonable information, systems and staff necessary for the Customer or its third party auditors to conduct such audit. Replyco acknowledges that the Customer or its third party auditors may enter its premises for the purposes of conducting this audit, provided that the Customer gives it reasonable prior notice, and in any event no less than thirty (30) days, of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to Replyco's operations. The Customer will not exercise its audit rights more than once in any twelve (12) calendar month period, except (i) if and when required by

instruction of a competent data protection authority; or (ii) the Customer believes a further audit is necessary due to a Security Incident suffered by Replyco.

16. Liability

Replyco's aggregate liability arising under or in connection with this DPA or any breach or non-performance of it no matter how fundamental (including by reason of Replyco's negligence) in contract, tort or otherwise, shall be subject to the limitations and exclusions of liability set out in the Agreement and any reference to the liability of Replyco means aggregate liability of Replyco and all of its affiliates under the Agreement (including this DPA).

17. Commencement and termination

This DPA will commence on the Effective Date and will continue in full force and effect until the termination of the last of the data processing to be performed pursuant to Annex I.

18. Third party rights

Except as expressly provided for in the Standard Contractual Clauses (where these apply in accordance with any of the provisions of this DPA), this DPA does not confer any right or benefit on any person, existing now or in the future, who is not a party to it.

19. Variations

No purported amendment or variation of this DPA or any provision of this DPA shall be effective unless it is in writing and duly executed by or on behalf of each of the parties.

20. Miscellaneous

20.1 This DPA, including the Standard Contractual Clauses (when they are incorporated into this DPA by reference), the attached Schedules and Annexes, and any subsequent amendments agreed under clause 19, constitute the entire agreement between the parties pertaining to the subject matter of this DPA and supersedes all prior agreements, understandings, negotiations and discussions of the parties in relation to such subject matter.

20.2 The provisions of this DPA are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability will affect only such phrase, clause or provision, and the rest of this DPA will remain in full force and effect.

20.3 Any notice, letter or other communication contemplated by this DPA will be communicated in writing via letter to the addresses set out in the Agreement or by email to the email addresses set out in the Customer's Replyco account.

20.4 The provisions of this DPA will endure to the benefit of and will be binding upon the parties and their respective successors and assigns.

20.5 This DPA may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

20.6 This DPA will be governed by and construed in accordance with the laws of England and Wales and will be subject to the exclusive jurisdiction of the English courts, except where and to the extent otherwise required by Applicable Data Protection Law.

This DPA has been signed on behalf of each of the parties by a duly authorised signatory.

SIGNED for and on behalf of **REPLYCO LTD**:

.....

Signature

Artem Verovenko .....

Print name

CEO .....

Title

SIGNED for and on behalf of **CUSTOMER**:

.....

Signature

.....

Print name

.....

Title

Annex I

Data Processing Description

This Annex I forms part of the Agreement and describes the processing that the processor will perform on behalf of the controller.

A. LIST OF PARTIES

Controller(s) / Data exporter(s):

1.	Name:	The Customer, as defined in the Agreement
	Address:	The Customer's address, as set out in the Agreement
	Contact person's name, position and contact details:	The Customer's contact details, as set out in the Customer's Replyco account
	Activities relevant to the data transferred under these Clauses:	Processing of personal data in connection with Replyco's provision of the services under the Agreement
	Signature and date:	Signature and date can be found in the signatory page of this DPA
	Role (controller/processor):	Controller

Processor(s) / Data importer(s):

1.	Name:	Replyco Ltd
	Address:	9 Oliver Business Park Oliver Road, Park Royal, London, England, NW10 7JB
	Contact person's name, position and contact details:	Andrii Kornytskyi CTO at Replyco andrew@replyco.com +44 20 8064 0564
	Activities relevant to the data transferred under these Clauses:	Processing of personal data in connection with Replyco's provision of the services under the Agreement
	Signature and date:	Signature and date can be found in the signatory page of this DPA
	Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	Contractors, subcontractors and end users including customers, prospective customers and newsletter subscribers.
Categories of personal data transferred:	Name, phone numbers, email addresses, date of birth, ID, postal addresses, IP address, transaction history, credit card information.
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	N/A

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:	
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuously
Nature of the processing:	Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.
Purpose(s) of the data transfer and further processing:	The purpose of the transfer and further processing of personal data by the data importer is: • use of personal data to set up, operate, monitor and provide the services (including operational and technical support) • provision of consulting services • communication to authorised users • storage of personal data in dedicated data centres • upload any fixes or upgrades to the services • back up of personal data • network access to allow personal data transfer • execution of instructions of the Customer in accordance with the Agreement.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Data will be retained for the period of time necessary to provide the services to the Customer under the Agreement and/or in accordance with applicable legal requirements.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	Same as above to the extent such information is provided to subprocessors for purposes of providing the services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	Irish Data Protection Commission (DPC)

Annex II

Technical and Organisational Security Measures

Description of the technical and organisational measures implemented by the processor(s) / data importer(s) 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.

Measure	Description
Measures of pseudonymisation and encryption of personal data	Data at rest is encrypted using secure Windows Server algorithms, data in transit is encrypted with SHA-256 certificates, and database backups are additionally encrypted using AES-256.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Confidentiality: • Access controls and authentication mechanisms to ensure that only authorized individuals can access sensitive data. • Encryption techniques to protect data from unauthorized access, both at rest (when stored) and in transit (when being transmitted). • Regularly monitoring and auditing access logs to detect and prevent any unauthorized access attempts. Integrity: • Regularly backing up data and verifying the integrity of backups to ensure data can be restored accurately. Availability: • Load balancing techniques to distribute traffic and prevent overloading of systems. • Conducting regular maintenance, updates, and testing to identify and address any potential vulnerabilities or performance issues. Resilience: • Incident response plans to effectively handle and mitigate security incidents or breaches. • Backing up data regularly and storing backups in separate locations to ensure data can be restored in case of a disaster or system failure. • Regular risk assessments and vulnerability scans to identify and address potential weaknesses in systems and services.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	• Regular Data Backups • Disaster Recovery Plan • Testing and Simulation • Incident Response Team
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	• Vulnerability Assessments and Penetration Testing • Employee Training and Awareness Programs
Measures for user identification and authorisation	• Usernames and Passwords • Two-Factor Authentication (2FA) • Secure Authorization and Session Refresh Tokens • Role-Based Access Control (RBAC)
Measures for the protection of data during transmission	• Encryption • Virtual Private Networks (VPNs) • Firewalls and Intrusion Detection Systems (IDS)
Measures for the protection of data during storage	• Encryption • Access Controls • Secure Storage Facilities • Data Backup and Disaster Recovery • Regular Security Audits and Monitoring
Measures for ensuring physical security of locations at which personal data are processed	• N/A as Amazon's secured data centre is used
Measures for ensuring events logging	• Logging Framework • Secure Log Storage • Retention Policies • Real-time Monitoring and Alerts • Regular Log Reviews and Analysis
Measures for ensuring system configuration, including default configuration	• Standard Configuration Baseline • Configuration Management Tools • Removal of Unnecessary Services and Features • Strong Authentication and Access Controls • Patch and Update Management

Measures for internal IT and IT security governance and management	• IT Policies and Procedures • IT Security Awareness Training • Incident Response Planning
Measures for certification/assurance of processes and products	• Measures for certification/assurance of processes and products • Product Lifecycle Management • Continuous Monitoring and Improvement • Customer Satisfaction and Feedback (NPS)
Measures for ensuring data minimisation	• Purpose Limitation • Data Retention and Deletion Policies • Access Controls • Employee Training and Awareness
Measures for ensuring data quality	• Data Validation and Verification • Data Cleansing and Deduplication • Continuous Monitoring and Data Audits • User Training and Awareness
Measures for ensuring limited data retention	• Data Retention Policies • Data Minimization • Automated Deletion or Archiving • Data Backup and Recovery • Secure Data Destruction
Measures for ensuring accountability	• Clearly Defined Roles and Responsibilities • Access Controls and Authentication • Logging and Audit Trails • Training and Awareness Programs
Measures for allowing data portability and ensuring erasure	• Standardized APIs • Secure Data Transmission • Data Erasure Mechanisms • Data Retention and Deletion Policies • Employee Training and Awareness

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller (and, for transfers from a processor to a sub-processor, to the data exporter).

Measure	Description
Measures for a (sub-) processor to take to provide assistance to the controller and ensure secure transfers	• Data Protection Policies and Procedures • Secure Data Transfers • Data Minimization and Purpose Limitation • Regular Security Audits and Assessments

Annex III

Subprocessors

The list of our subprocessors can be found on at the following URL:
https://replyco.com/subprocessors