Repsly Data Processing Addendum

Last Modified: September 24, 2021

THIS DATA PROCESSING ADDENDUM (“**DPA**”) BETWEEN REPSLY, INC. AND ITS AFFILIATES (COLLECTIVELY, “**REPSLY**,” “**COMPANY**,” “**WE**,” “**US**” or “**PROCESSOR**”) AND THE LEGAL ENTITY LICENSING REPSLY’S SERVICE (“**CUSTOMER**,” “**YOU**” OR “**CONTROLLER**,” AND TOGETHER WITH REPSLY, THE “**PARTIES**”) UNDER AN APPLICABLE ORDER FORM (TOGETHER WITH ANY INCORPORATED TERMS OF SERVICE, “**THE PRINCIPAL AGREEMENT**”) GOVERNS CUSTOMER’S ACCESS AND USE OF THE SERVICE. BY EXECUTING AN ORDER FORM AND/OR PRINCIPAL AGREEMENT THAT REFERENCES THIS DPA, CUSTOMER AGREES TO THE TERMS OF THIS DPA.

This DPA is supplemental to, and forms an integral part of, the Principal Agreement. In case of any conflict or inconsistency with the terms of the Principal Agreement, this DPA will take precedence over the terms of the Principal Agreement. We update the terms of this DPA from time to time. If you have an active subscription to the Service, we will let you know when we do via email. The term of this DPA will follow the term of the Principal Agreement.

1. Definitions

In this DPA the following terms have the following meanings; terms not otherwise defined herein shall have the same meaning as in the Principal Agreement:

“**Anonymized Data**” means any Personal Information that has been anonymized such that the Data Subject to whom it relates cannot be identified, directly or indirectly, by Repsly or any other party reasonably likely to receive or access that Anonymized Data.

“**California Personal Information**” means Personal Information that is subject to the protection of the CCPA.

"**CCPA**" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018).

"**Consumer**,” "**Business**,” "**Sell**" and "**Service Provider**" will have the meanings given to them in the CCPA.

“**Controller**” means the legal entity that licenses Repsly’s Service, also referred to as “Customer.” The Controller, alone or jointly with others, determines the purposes and means of the Processing of Personal Information.

"**Customer Data**” means all information Customer submits or collects through the Service, including Content (as defined in the Principal Agreement).

“**Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the Service. "Data Breach" will not include 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.

“**Data Protection Laws**” means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Information in question under the Principal Agreement, including without limitation European Data Protection Laws, the CCPA, and the Virginia Consumer Data Protection Act; in each case as amended, repealed, consolidated or replaced from time to time.

“**Data Subject**” means the individual to whom Personal Information relates.

"**Europe**" means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

“**European Data**” means Personal Information that is subject to the protection of European Data Protection Laws.

"**European Data Protection Laws**" means data protection laws applicable in Europe, including: (i) 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) ("**GDPR**"); (ii) applicable national implementations of (i); (iii) in respect of the United Kingdom, any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union; and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance; in each case, as may be amended, superseded or replaced.

“Instructions” means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Information (including, but not limited to, depersonalizing, blocking, deletion, making available).

"**Permitted Affiliates**" means any of your Affiliates that (i) are permitted to use the Service pursuant to the Principal Agreement, but have not signed their own separate agreement with us and are not a “Customer” as defined under the Principal Agreement, (ii) qualify as a Controller of Personal Information Processed by us, and (iii) are subject to European Data Protection Laws.

“**Personal Information**” means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data, personal information or personally identifiable information under applicable Data Protection Laws.

"**Processing**" means any operation or set of operations which is performed on Personal Information, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Information. The terms "**Process**," "**Processes**" and "**Processed**" will be construed accordingly.

"**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Information on behalf of the Controller.

"**Standard Contractual Clauses**" means the standard contractual clauses for Processors approved pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 and most recently modified June 4, 2021, as may be further amended, superseded or replaced.

"**Sub-Processor**" means any Processor engaged by us or our Affiliates to assist in fulfilling our obligations with respect to the provision of the Service under the Principal Agreement. Sub-Processors may include third parties or our Affiliates but will exclude any Repsly employee or consultant.

2. Customer Responsibilities

a. Compliance with Laws. Within the scope of the Principal Agreement and in your use of the Service, you will be responsible for complying with all requirements that apply to you under applicable Data Protection Laws with respect to its Processing of Personal Information and the Instructions your issue to us.

In particular but without prejudice to the generality of the foregoing, you acknowledge and agree that you will be solely responsible for: (i) the accuracy, quality, and legality of Customer Data and the means by which you acquired Personal Information; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Information, including obtaining any necessary consents and authorizations (particularly for use by Customer for marketing purposes); (iii) ensuring you have the right to transfer, or provide access to, the Personal Information to us for Processing in accordance with the terms of the Principal Agreement (including this DPA); (iv) ensuring that your Instructions to us regarding the Processing of Personal Information comply with applicable laws, including Data Protection Laws; and (v) complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent or managed through the Service, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices. You will inform us without undue delay if you are not able to comply with its responsibilities under this sub-section (a) or applicable Data Protection Laws.

b. Controller Instructions. The parties agree that the Principal Agreement (including this DPA), together with your use of the Service in accordance with the Principal Agreement, constitute your complete Instructions to us in relation to the Processing of Personal Information, and additional instructions outside the scope of the Instructions shall require prior written agreement between us and you.

3. Repsly's Obligations

a. Compliance with Instructions. We will only Process Personal Information for the purposes described in this DPA or as otherwise agreed within the scope of your lawful Instructions, except where and to the extent otherwise required by applicable law. We are not responsible for compliance with any Data Protection Laws applicable to you or your industry that are not generally applicable to us.

b. Conflict with Law. If we become aware that we cannot Process Personal Information in accordance with your Instructions due to a legal requirement under any applicable law, we will (i) promptly notify you of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Information) until such time as you issue new Instructions with which we are able to comply. If this provision is invoked, we will not be liable to you under the Principal Agreement for any failure to perform the applicable Service until such time as you issue new lawful Instructions with regard to the Processing.

c. Security. We will implement appropriate technical and organizational measures to protect and safeguard processed Personal Information The measures shall at least reach a level of security equivalent of what is prescribed by Data Protection Laws, relevant supervisory authorities' applicable regulations and guidelines regarding security of Personal Information and what is otherwise appropriate to the risk of the processing of Personal Information against Data Breaches.

Minimal security requirements are described in Annex 2.

d. Confidentiality. We will ensure that any personnel whom we authorize to Process Personal Information on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Information.

e. Data Breaches. We will notify you without undue delay after we become aware of any Data Breach and will provide timely information relating to the Data Breach as it becomes known or reasonably requested by you. At your request, we will promptly provide you with such reasonable assistance as necessary to enable you to notify relevant Data Breaches to competent authorities and/or affected Data Subjects, if you are required to do so under Data Protection Laws.

f. Deletion or Return of Personal Information. We will delete or return all Customer Data, including Personal Information (including copies thereof) Processed pursuant to this DPA, on termination or expiration of your Service in accordance with the procedures and timeframes set out in the Principal Agreement, save that this requirement shall not apply to the extent we are required by applicable law to retain some or all of the Customer Data, or to Customer Data we have archived on back-up systems, which data we will securely isolate and protect from any further Processing and delete in accordance with its deletion practices.

4. Data Subject Requests

Repsly shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of processing, erasure, data portability, or to object to processing, each a "**Data Subject Request**." Repsly will advise the Data Subject to submit their request to you and will not otherwise respond to any such requests unless authorized to do so by Customer (unless required to do so under Data Protection Laws or under the instructions of a competent authority). Customer will be solely responsible for responding substantively to any such Data Subject Requests or communications involving Personal Information.

We will provide commercial reasonable assistance to Customer by taking appropriate technical and organizational measures for the fulfilment of Customer's obligation to respond to requests for exercising the Data Subjects' rights as laid down by Data Protection Laws. Unless prohibited under the Data Protection Laws, Customer will reimburse Repsly with any costs and expenses related to Repsly's provision of such assistance.

5. Sub-Processors

You agree that we may engage Sub-Processors to Process Personal Information on your behalf. We have currently appointed, as Sub-Processors, Repsly Affiliates and third parties listed at www.repsly.com/legal. We will notify you if we add or remove Sub-Processors on this list prior to any such changes.

Where we engage Sub-Processors, we will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Information as those in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the Service provided by such Sub-Processors. We will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of its obligations under this DPA.

6. Data Transfers

You acknowledge and agree that we may access and Process Personal Information on a global basis as necessary to provide the Service in accordance with the Principal Agreement, and in particular that Personal Information will be transferred to and Processed by Repsly in the United States and to other jurisdictions where Repsly Affiliates and Sub-Processors have operations. We will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

7. Additional Provisions for European Data

a. Scope of Section 7. This "Additional Provisions for European Data" section shall apply only with respect to European Data.

b. Roles of the Parties. When Processing European Data in accordance with your Instructions, the parties acknowledge and agree that you are the Controller of European Data and we are the Processor.

c. Instructions. If we believe that your Instruction infringes European Data Protection Laws (where applicable), we will inform you without delay.

d. Notification and Objection to New Sub-Processors. We will notify you of any changes to Sub-processors by updating our Sub-Processor list at www.repsly.com/legal and will give you the opportunity to object to the engagement of the new Sub-Processor on reasonable grounds relating to the protection of Personal Information within 30 days after this list. If you do notify us of such an objection, the parties will discuss your concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, we will, at our sole discretion, either not appoint the new Sub-Processor, or permit you to suspend or terminate the affected Service in accordance with the termination provisions of the Principal Agreement without liability to either party (but without prejudice to any fees incurred by you prior to suspension or termination).

e. Data Protection Impact Assessments and Consultation with Supervisory Authorities. To the extent that the required information is reasonably available to us, and you do not otherwise have access to the required information, we will provide reasonable assistance to you with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by European Data Protection Laws.

f. Transfer Mechanisms for Data Transfers.

(A) Repsly shall not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Information (within the meaning of applicable European Data Protection Laws), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Information, to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws, or to a recipient that has executed the Standard Contractual Clauses.

(B) You acknowledge that in connection with the performance of the Service, Repsly is a recipient of European Data in the United States. The parties acknowledge and agree the following:

(a) **Standard Contractual Clauses**: Repsly shall execute the Standard Contractual Clauses (and/or any successor standard contractual clauses issued by the EU Commission) in the event that Customer's Personal Information is transferred to: (i) the United States or (ii) other countries outside the EEA that are not recognized by the EU Commission as providing adequate protection pursuant to Article 45 of the GDPR.

(b) The parties agree that (i) purely for the purposes of the descriptions in the Standard Contractual Clauses, Repsly will be deemed the "**data importer**" and Customer will be deemed the "**data exporter**" (notwithstanding that you may yourself be located outside Europe and/or be acting as a processor on behalf of third party controllers), and (ii) if and to the extent the Standard Contractual Clauses (where applicable) conflict with any provision of this DPA, the Standard Contractual Clauses will prevail to the extent of such conflict.

Appendix 1 to such Standard Contractual Clauses shall be populated as set forth in Annex 1 attached hereto.

Appendix 2 to such Standard Contractual Clauses shall be populated as follows:

> *"Technical and organisational measures including technical and organisational measures to ensure the security of the data are described in the Annex 2 of the Data Processing Addendum, available at* https://www.repsly.com/legal*."*

g. Demonstration of Compliance. We will make all information reasonably necessary to demonstrate compliance with this DPA available to you and allow for and contribute to audits, including inspections by you in order to assess compliance with this DPA. You acknowledge and agree that you will exercise your audit rights under this DPA by instructing us to comply with the audit measures described in this sub-section (g). You acknowledge that the Service is hosted by our data center partners who have not agreed to permit such audit rights. At your written request, we will provide written responses (on a confidential basis) to all reasonable requests for information made by you necessary to confirm our compliance with this DPA, provided that you will not exercise this right more than once per calendar year.

8. Additional Provisions for California Personal Information

a. Scope of Section 8. The "Additional Provisions for California Personal Information" section of this DPA will apply only with respect to California Personal Information.

b. Roles of the Parties. When processing California Personal Information in accordance with your Instructions, the parties acknowledge and agree that you are a "Business" and we are a "Service Provider" for the purposes of the CCPA.

c. Responsibilities. The parties agree that we will Process California Personal Information as a Service Provider strictly for the purpose of performing the Service and Consulting Services under the Principal Agreement (the "**Business Purpose**") or as otherwise permitted by the CCPA, including as described in the "Data Practices and Machine Learning" section of our Product Specific Terms.

9. Anonymous Data

Customer acknowledges and agrees that Repsly may create and derive, from Processing under the Agreement, Anonymized Data. Repsly shall be freely able to use and disclose Anonymized Data for Repsly's own business purposes without restriction.

10. Liability Limitation

Repsly's total liability for any action, proceeding, liability, loss, damage, cost, claim, fine, expense and/or demand incurred by Customer arising from Repsly's breach of its obligations under this Data Processing Addendum is limited to the total amount Repsly received from you during the twelve (12) months preceding the claim.

11. New or Amended Privacy Laws

Repsly agrees and warrants that it will implement such policies and commitments as Customer may reasonably request in connection with compliance with applicable new or amended privacy laws, including without limitation undertaking reasonable commitments to otherwise address new or amended privacy laws, with regard to which Customer and Repsly agree and warrant that they will work together in good faith to agree upon and to amend this Data Processing Addendum accordingly before the applicable effective dates such laws. If the parties cannot reach agreement on how to address such laws, Customer may terminate the Principal Agreement, subject to a transition period designated by Customer during which Repsly will continue to provide the Services and assist in transitioning the Services to a new provider, and Customer shall only be responsible for fees and costs on a pro rata basis through the post-transition termination date.

12. General Provisions

a. Amendments. Notwithstanding anything else to the contrary in the Principal Agreement and without prejudice to the "Compliance with Instructions" or "Security" sections of this DPA, we reserve the right to make any updates and changes to this DPA and the terms that apply in the "Amendment; No Waiver" section of the Master Terms will apply.

b. Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

c. Governing Law. The parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

Annex 1

Data exporter

Data Exporter is the legal entity that has executed the Standard Contractual Clauses as a Data Exporter established within the European Economic Area (EEA) and/or Switzerland that have purchased Covered Services on the basis of one or more order document(s).

Data importer

Repsly, which processes personal data upon the instruction of the data exporter in accordance with the terms of the Principal Agreement.

Data subjects

Data exporter may submit Personal Data to the Covered Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

☒ Prospects, customers, business partners and vendors of data exporter (who are natural persons)

☒ Employees or contact persons of data exporter's prospects, customers, business partners and vendors

☒ Employees, agents, advisors, freelancers of data exporter (who are natural persons)

☒ Data exporter's Users authorized by data exporter to use the Covered Services

Categories of data

Data exporter may submit Personal Data to the Covered Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data as listed in table A below in this Annex.

Special categories of personal data (if appropriate)

Special categories of personal data are not systematically processed under this DPA. However, data exporter may submit special categories of personal data to the Covered Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation:

Processing operations

Repsly Inc. will provide real-time insights on retail execution and sales performance, smart merchandising, promotion, and sales execution tools to the Customer through the online service.

As an integral part of the agreed service provisioning Users (typically customers' employees) manually and automatically fill the information needed for the service provisioning including the following data which can be directly or indirectly connected to a physical person and will be processed for the described purposes:

Personal data processed	Purpose of processing
• **Information entered by the service users** (users', customers' suppliers' and other contact information, such as: Users Contact Data, Calendar Data, Geolocation Data, Work Activity Data, Photos. • **information about the service usage collected from the users' devices** (Geolocation data, Logs…) • **Automatically generated information about the user** (User IDs, Activity logs, Service usage tracking information, Message IDs …)	• WEB application Service provisioning • Mobile application Service provisioning • Geolocation based services provisioning • Mobile App data synchronization • Customers' Data storage service • Providing API integration/connectivity service • Insights Dashboards provisioning • Customer e-mail communication • User messaging services
• **Any information manually exchanged with users required for identification, troubleshooting, and providing other support services** • **automatically collected information about service usage** (activity logs, service usage tracking information…)	• Providing customer support

Table A

Retention Periods

Controller is responsible for providing instructions to Processor regarding the retention of Personal Information it processes hereunder, following termination of the Principal Agreement. If such instructions are not provided, Processor will retain Personal Information for up to three (3) years based on the Repsly’s legitimate interest in simplifying the process of future contract renewals.

Annex 2
Minimal Security Requirements

1. To ensure ongoing **confidentiality, integrity, availability, and resilience**, Repsly is responsible to:
    a. implement and maintain strong authentication and authorisation controls to ensure access to customer data will only be granted where this is required for providing the agreed service,
    b. establish and maintain a list of people and organizations with access to data processed as a part of providing the service,
    c. use encryption for data in rest and during transfers,
    d. implement and maintain appropriate input data validation controls across the provided service,
    e. design its systems on the high availability principles, introducing redundant servers, load balancers, automated backups, and appropriate business continuity plans.
    f. ensure data processing facilities are adequately protected from unauthorised physical and logical access, fire, flood, earthquake, power outages and have efficient and reliable HVAC systems.
    g. regularly educate its staff accessing personal data about their responsibilities with regards to privacy protection and information security.
    h. ensure all **data transfers** over public networks are encrypted using the secure encryption algorithms and key lengths in accordance with the industry best practices.
2. To comply with data **minimization principles** Repsly is responsible:
    a. only to collect information required to provide the agreed service,
    b. not to create or keep copies of the personal data which are not necessary for providing the agreed service,
    c. to delete or anonymize personal data after the retention period expiration,
    d. to make sure all sub-processors delete personal data after the retention period expiration as well,
    e. to ensure, personal data used for statistical and reporting purposes where personally identifiable information is not absolutely required is **anonymized**,
3. Repsly is responsible for regular (at least on the annual basis) **information security risk assessment and mitigation** by updating and/or introducing new appropriate security controls.
4. Repsly is responsible to **scan systems and code for vulnerabilities** at least before deploying new versions of the Repsly service, and ensure related risk is acceptable (will not result in a negative impact to the customer and data subject whose personal data is processed by Repsly).
5. Repsly is responsible to ensure, critical systems and applications are configured to generate sufficient **logs** for forensics investigations in case of the data breach. Such logs must be protected from unauthorised access and modification.
6. Repsly is responsible to implement adequate **information security and privacy policies** and procedures to ensure people involved in the data processing understand their tasks and responsibilities.
7. Repsly is responsible to ensure for all staff and sub-processors accessing customers' data, sign an NDA or other enforceable document with confidentiality clause and understand their confidentiality responsibilities.
8. To ensure the accountability, Repsly must:
    a. establish and keep records proving the efficiency of the security controls,
    b. conduct an independent security audit at least on a annual basis,

c. establish and keep records providing an evidence top management is aware of the information security risk and continuously support effective risk management.