Data Processing Addendum (DPA)

CONTENTS

- How this DPA works
- Key Terms (Cover Page)
- Standard Terms: Sections 1 to 4
- Standard Terms: Sections 5 to 9
- Standard Terms: Sections 10 to 14
- Annex I: Details of the Processing
- Annex II: Technical and Organizational Measures
- Annex III: Sub-processors
- Annex IV: International Transfer

How this DPA works

This Data Processing Addendum ("DPA") forms part of the Cloud Service Agreement entered into between RWS Ltda. ("Provider" or "RWS") and Customer and governs the processing, by RWS, of the Personal Data contained in Customer Content. It is incorporated by reference into the Agreement through the "DPA" line of the Key Terms and applies automatically to every Order Form, with no separate signature required.

Structure of the document:

1. Key Terms: the variables of this DPA.
2. Standard Terms: obligations of the parties, sections 1 to 14.
3. Annex I: Details of the Processing.
4. Annex II: Technical and Organizational Measures.
5. Annex III: Sub-processors.
6. Annex IV: International Transfer.

Order of precedence in case of conflict: (1) standard contractual clauses of the ANPD or of the European Union, where applicable; (2) Key Terms; (3) Standard Terms and Annexes; (4) Agreement. In matters of Personal Data, this DPA prevails over the Agreement, as provided in Section 3.1 (Personal Data) of the Agreement.

Capitalized terms not defined in this DPA have the meaning given in the Agreement. This DPA is governed by Law No. 13,709/2018 (LGPD) and by the ANPD regulations.

RWS

Key Terms (Cover Page)

Variable	Value
Agreement	Cloud Service Agreement (RWS Standard Terms) and the Order Forms governed by it
Provider (Processor)	RWS Ltda, CNPJ 46.231.982/0001-23, Av. Santo Amaro, 1047, São Paulo/SP, Brazil
Customer	The legal entity identified in the Order Form
Role of Customer	Controller or, when it processes Personal Data on behalf of its End Customers or of another Controller, Processor; in that case RWS acts as Sub-processor (Section 1)
Provider Security Contact	security@rwsintegration.com
Provider Data Protection Officer (DPO)	dpo@rwsintegration.com
Customer contact for incidents and instructions	The Customer Notice Address provided for in the Agreement and the security or privacy contact indicated by Customer in the Order Form
Security Policy	The current version published at rwsintegration.com/pt-br/legal/security (English version at rwsintegration.com/en/legal/security), incorporated by reference (Annex II)
Approved Sub-processors	Annex III; current list at rwsintegration.com/pt-br/legal/subprocessors (English version at rwsintegration.com/en/legal/subprocessors)
Notice of a new Sub-processor	30 days in advance; Customer objection period of 10 days from the notice (Section 3)
Security Incident notification	Within 48 hours after RWS becomes aware (Section 6)
Processing location	AWS us-east-1 region (United States), under the safeguards of Annex IV
Authorized Data Categories	All categories in Annex I (B), including CPF, RG and bank account data, except the Restricted Data of Section 2.5
Deletion upon termination	Within 60 days after Customer request, as provided in Section 5.5 of the Agreement and Section 10 of this DPA
DPA Liability Cap	The General Cap Amount set in the Key Terms or in the Order Form of the Agreement (Section 11)
Governing Law and Jurisdiction	Laws of the Federative Republic of Brazil; Judicial District of São Paulo/SP, the same as the Agreement

Variable	Value
Competent authority	Brazilian National Data Protection Authority (ANPD)

Standard Terms: Sections 1 to 4

1. Roles of the Parties

1.1. When Customer is the Controller of the Personal Data, RWS acts as Processor. When Customer acts as Processor on behalf of its End Customers or of another Controller, RWS acts as Sub-processor, subject to Section 1.4.

1.2. For Usage Data and support data (User account records, support tickets, Product usage metrics), RWS acts as an independent Controller, under Section 1.4 of the Agreement and its Privacy Policy, and this DPA does not apply to that data. RWS is not a joint Controller with Customer.

1.3. Each party will comply with the obligations that the LGPD and the other Applicable Data Protection Laws assign to it by reason of its role.

1.4. When acting as Processor, Customer represents and warrants that: (a) it is authorized by the respective Controller to engage RWS as Sub-processor for the processing described in Annex I, including for the International Transfer described in Annex IV; (b) the instructions given to RWS are compatible with those received from the Controller and with the agreement entered into between them; (c) it will promptly pass on to the Controller the communications from RWS addressed to it; and (d) it will be the sole interlocutor of RWS before the Controller, unless the law provides otherwise. RWS may treat Customer's instructions as instructions of the Controller, without needing to confirm them with the Controller.

2. Processing of Personal Data

2.1. Details of the processing. The subject matter, nature, purpose and duration of the processing, and the categories of Data Subjects and of Personal Data processed, are described in Annex I.

2.2. Instructions. RWS will process Personal Data only in accordance with Customer's documented instructions, which comprise: (a) the Agreement and this DPA; (b) the configuration of the Integrations, including connectors, credentials, field mappings, transformation rules, schedules and destinations, made by Customer or its Users in the Product, or by RWS at Customer's request in the provision of implementation or support services; and (c) additional written instructions, sent from Customer's Notice Address or by administrator Users of Customer's account and confirmed by RWS. If RWS believes that an

instruction violates the LGPD or another Applicable Law, or that it cannot comply with it due to a legal requirement, it will inform Customer and suspend the affected processing (except secure storage) until Customer confirms, modifies or revokes the instruction. A good-faith suspension does not constitute a breach of the Agreement and does not give rise to discounts, credits or penalties provided for in it. RWS is not required to perform a legal analysis of Customer's instructions, and the absence of a response from RWS does not amount to a statement as to the lawfulness of the instruction.

2.3. Customer obligations. Customer is solely responsible for: (a) defining the legal basis and the purpose of the processing (arts. 7 and 11 of the LGPD); (b) ensuring the accuracy, lawfulness and origin of the Personal Data submitted to the Product; (c) providing Data Subjects with the information required by the LGPD, including about the use of processors and about the international transfer described in Annex IV; and (d) configuring the Integrations so as to transmit only the fields necessary for each purpose (necessity principle, art. 6, III, of the LGPD). When Customer acts as Processor, it will also comply with the agreement entered into with its Controller.

2.4. Authorized data. Notwithstanding the definition of Prohibited Data in the Agreement, Customer is authorized to submit to the Product the Authorized Data Categories of the Key Terms, including identification numbers (CPF, RG, CNH, PIS, CTPS), bank account data for payroll, payment and reconciliation purposes, and Sensitive Personal Data when necessary for the Integration (for example, union membership, occupational health or benefits data in HR and payroll integrations). Customer is responsible for the specific legal basis for Sensitive Personal Data (art. 11 of the LGPD).

2.5. Restricted Data. It remains prohibited to submit to the Product: (a) full payment card data (card number, security code, and magnetic stripe or chip data), as they require specific PCI DSS certification of the Provider; and (b) any data whose processing is subject to a sector-specific regulatory regime that requires specific certification or authorization of the Provider. RWS will not be liable for the processing of Restricted Data submitted in violation of this Section and may, upon notice to Customer, suspend the affected Integration or delete the Restricted Data held in its systems, to the extent necessary to end the violation.

2.6. Purpose limitation. RWS will not use Personal Data from Customer Content for its own purposes and will not sell it or share it with third parties, except authorized Sub-processors.

2.7. Artificial intelligence and service improvement. For the purposes of Section 1.6 (Machine Learning) of the Agreement, RWS will only use data derived from Customer Content to develop, train or improve models after anonymizing it under art. 12 of the LGPD, so that it cannot be reversed by reasonable and available means, and will not attempt to re-identify it.

Personal Data that has not been anonymized will not be used for those purposes. This clause prevails over Section 1.6 of the Agreement as to Personal Data.

2.8. Notification channels. Execution and error notifications, which may contain payload excerpts with Personal Data, are sent only upon activation by Customer, to: (a) a Slack channel shared between the RWS workspace and Customer's workspace (Slack Connect), or a channel in the RWS workspace with guest users from Customer, in which case Slack acts as Sub-processor (Annex III); or (b) a webhook or other destination indicated by Customer, which is a system of Customer or of a third party engaged by it and whose provider is not a Sub-processor of RWS. In both cases, the activation constitutes an instruction of Customer under Section 2.2, and Customer is responsible for defining who has access to the channel and for assessing the suitability of the destination for the processing of Personal Data.

2.9. Content monitoring. RWS has no duty to monitor or review the content of the Personal Data passing through the Integrations, except to the extent necessary for the provision of the Cloud Service, for support requested by Customer, for the security of the Cloud Service or for compliance with the law. If it becomes aware that Customer submits Personal Data manifestly excessive for the purpose of the Integration, or Restricted Data, RWS will notify Customer, who will be responsible for taking the appropriate steps, including reconfiguring the Integration and deleting the data.

3. Sub-processors

3.1. Customer authorizes RWS to engage the Approved Sub-processors listed in Annex III and published at rwsintegration.com/pt-br/legal/subprocessors (English version at rwsintegration.com/en/legal/subprocessors) to process Personal Data in the provision of the Cloud Service.

3.2. Before allowing a new Sub-processor to process Personal Data, RWS will update the published list and notify Customer by email at least 30 days in advance. Customer may object, in writing, within 10 days from the notice, provided that the objection is based on a reasonable ground related to data protection and is accompanied by the objective reasons why it believes the Sub-processor does not offer adequate guarantees of security or of compliance with the Applicable Data Protection Laws. In the absence of an objection within that period, the Sub-processor is deemed approved.

3.3. In case of objection, RWS will use commercially reasonable efforts to offer an alternative that avoids the processing by the new Sub-processor. If no viable alternative is found within 30 days, either party may terminate the affected Order Form upon written notice, without penalty, with a prorated refund of Fees prepaid for the unused period, which will be Customer's sole remedy in the event of an objection to a Sub-processor.

3.4. RWS will enter into a written agreement with each Sub-processor imposing data protection obligations no less protective than those of this DPA, to the extent applicable to the service provided, and will remain fully liable to Customer for the acts and omissions of its Sub-processors as if they were its own.

3.5. Where the replacement of a Sub-processor is necessary to contain or prevent a Security Incident, preserve the continuity of the Cloud Service or comply with a legal requirement, and it is not feasible to observe the period in Section 3.2, RWS may carry it out immediately, notifying Customer as soon as possible, with an indication of the reason. In that case, the objection period will run from the notice.

3.6. Customer acknowledges that providers of cloud infrastructure and of standardized software contract under their own uniform terms, which satisfy Section 3.4 provided that they observe the standard set out in it.

4. International Transfer

4.1. The Cloud Service is hosted and operated in the AWS us-east-1 region, in the United States. Customer acknowledges that location and authorizes and instructs RWS, as exporter, to transfer Personal Data to AWS and to the other Sub-processors indicated on the Sub-processors page, as importers, in the countries indicated there, exclusively for the provision of the Cloud Service.

4.2. The transfer is carried out on the basis of art. 33, II, of the LGPD, through the standard contractual clauses approved by the ANPD (Resolution CD/ANPD No. 19/2024) entered into between RWS and AWS, as detailed in Annex IV. For as long as there is no ANPD adequacy decision for the destination country, RWS will maintain that or another mechanism provided for in art. 33 of the LGPD.

4.3. RWS will indicate to Customer, upon request, where to consult the standard clauses incorporated into the AWS contractual terms or will provide a copy of them, with commercial information unrelated to data protection redacted, together with the information necessary for Customer to fulfill its transparency duties before Data Subjects and the ANPD regarding the transfer.

4.4. RWS will not transfer Personal Data to another country or Sub-processor outside Brazil without observing Section 3 and without a valid mechanism under art. 33 of the LGPD.

4.5. If the processing is subject to the GDPR or the UK GDPR, item 5 of Annex IV applies.

Standard Terms: Sections 5 to 9

5. Security

5.1. RWS will adopt technical and administrative measures capable of protecting Personal Data from unauthorized access and from accidental or unlawful destruction, loss, alteration, communication or dissemination (art. 46 of the LGPD), taking into account the state of the art, the nature of the data and the risks involved. The measures adopted are those described in the Security Policy, incorporated into this DPA by reference as provided in Annex II.

5.2. RWS may update the Security Policy, provided that it does not materially reduce the general level of protection during the Subscription Period.

5.3. RWS will provide Customer with reasonable cooperation so that Customer can fulfill its own security obligations, taking into account the nature of the processing and the information available to RWS.

5.4. The obligations of RWS under this Section are obligations of means, and the occurrence of a Security Incident does not, by itself, constitute a breach of this DPA.

6. Security Incidents

6.1. Notification. RWS will notify Customer, through the contacts indicated in the Key Terms, within 48 hours after becoming aware of a Security Incident affecting Customer's Personal Data. Awareness is deemed to occur when RWS confirms, with a reasonable degree of certainty, the occurrence of the incident. This period was set to allow Customer, as Controller, to meet the deadline for communication to the ANPD and to Data Subjects provided for in art. 48 of the LGPD and in the ANPD regulations on incident communication.

6.2. Content. The initial notification will contain the information available at that time and will be supplemented as the investigation progresses, including: (a) a description of the nature of the incident; (b) the categories and approximate number of Data Subjects and of Personal Data affected, where possible; (c) the likely risks and consequences; (d) the measures adopted or recommended to contain and mitigate the effects; and (e) the RWS contact for clarifications.

6.3. Cooperation. RWS will take reasonable measures to contain, investigate and remediate the incident, to the extent within its control, and will support Customer in the communications to the ANPD and to Data Subjects. The assessment of relevant risk or damage and the communications to the ANPD and to Data Subjects are the Controller's responsibility, and RWS will not make them on Customer's behalf, except where required by law or agreed in writing between the parties. Customer will coordinate with RWS the content of public communications that mention RWS. When Customer acts as Processor, it is responsible for passing the notification on to its Controller.

6.4. Limits. An incident notification does not constitute an acknowledgment of fault or liability by RWS. The obligations of this Section do not apply to incidents caused by the action or

omission of Customer, of its Users or of the systems of Customer and of its End Customers, including the compromise of credentials in Customer's custody, although RWS will inform Customer of events of that nature of which it becomes aware.

7. Data Subject Rights and Cooperation

7.1. Data Subject requests. If RWS directly receives a request from a Data Subject relating to Customer's Personal Data (art. 18 of the LGPD), it will inform Customer within 5 business days, direct the Data Subject to Customer, and will not respond to the request without Customer's authorization, except where required by law. Customer is responsible for responding to Data Subjects.

7.2. Assistance. Taking into account the nature of the processing, RWS will provide reasonable assistance to Customer in responding to Data Subject requests when Customer cannot do so through the functionalities of the Product, including locating, correcting, blocking or deleting Personal Data in RWS custody.

7.3. Authorities. RWS will inform Customer, unless legally prohibited, of requests from public authorities involving Customer's Personal Data and will cooperate with Customer in prior consultations or proceedings before the ANPD.

7.4. Impact report. RWS will provide the information reasonably necessary for Customer to prepare a Personal Data Protection Impact Report (art. 38 of the LGPD) related to the Cloud Service, to the extent Customer does not have that information.

7.5. Costs. The assistance provided for in this Section and in Section 8 is provided at no cost when limited to the delivery of existing documentation and to reasonable efforts. Requests requiring significant additional work will be quoted in advance and charged upon Customer's approval.

8. Audits and Reports

8.1. Documentation. Upon written request to the Security Contact and under confidentiality, RWS will make available to Customer: (a) previous versions of the Security Policy, where necessary to verify the contracted period; (b) the Site-to-Site Connection Compliance Document, where applicable; (c) the reference to AWS public certifications and reports; and (d) responses to a security questionnaire, limited to one per year, except in case of a material change to the Service or an incident.

8.2. Security testing. Customer may engage an independent company to perform security tests on the RWS services, at its own expense, upon RWS's prior written authorization as to scope, window, environment and method. The tests may not involve denial-of-service attacks, social engineering against RWS staff or access to other customers' data, and

Customer will be liable for any damages arising from them. The results will be reviewed jointly by the parties, classified by risk level and addressed by RWS within the agreed time frames, and constitute Confidential Information of RWS.

8.3. Audit. Customer may audit RWS's compliance with this DPA in the following cases: (a) proven insufficiency of the documentation in Section 8.1; (b) a requirement of the ANPD, of another competent authority or of the law; or (c) the occurrence of a Security Incident affecting Personal Data. The audit will be carried out at most once every 12 months, except in cases (b) and (c), and will observe: (i) 30 days' prior notice, reduced to 10 business days in cases (b) and (c) or to the period set by the authority, accompanied by an audit plan with scope, duration and date; (ii) performance preferably by documentary or remote means, with on-site audits admitted only when those means prove insufficient; (iii) performance during business hours, without undue interference with RWS's activities; (iv) conduct by an independent auditor approved by RWS, which will not withhold approval without reasonable grounds, provided that the auditor is not a competitor of RWS and is bound by a confidentiality undertaking; and (v) full costs borne by Customer. RWS may restrict access to information of other customers, to trade secrets, to information whose disclosure would compromise the security of the Cloud Service and to data protected by a legal duty of secrecy. The verification of Sub-processors will be based on their reports and certifications, and this DPA does not grant Customer the right to audit or inspect Sub-processor facilities.

8.4. Customer will provide RWS with a copy of the reports produced, which constitute Confidential Information of RWS and may only be used to verify compliance with this DPA and to meet regulatory requirements. RWS will keep records of compliance with this DPA for 3 years after its termination.

9. Personnel and Confidentiality

9.1. RWS will limit access to Personal Data to the employees and contractors who need it to perform the Agreement, with individual, named accounts, multi-factor authentication and the least privilege principle.

9.2. All persons with access to Personal Data are bound by confidentiality obligations no less protective than those of Section 10 of the Agreement and receive information security and data protection training upon joining and periodically.

9.3. RWS has appointed a Data Protection Officer, whose contact is in the Key Terms, as the channel with Data Subjects, with the ANPD and with Customer for matters relating to this DPA.

Standard Terms: Sections 10 to 14

RWS

10. Retention, Return and Deletion

10.1. During the term. The Cloud Service is an integration platform, not a storage platform. Personal Data passes through RWS queues and processing until delivery to the destination system. Execution logs and backups are retained for the periods defined in the Security Policy, encrypted and with restricted access, exclusively for diagnostics, support and continuity.

10.2. During the term, Customer may delete or correct Personal Data through the functionalities of the Product or by request to RWS, as provided in Section 7.

10.3. Upon termination. Once the Agreement has ended, RWS will delete Customer Content, including Personal Data, within 60 days after Customer's written request, as provided in Section 5.5 of the Agreement. In the absence of a request, deletion will occur at the end of the retention periods of the Security Policy. Before deletion, Customer may request in writing, within 30 days after the end of the Agreement, an export of Customer's Integration schemas, which RWS will make available in a format defined by RWS within 15 business days of the request, at no additional cost.

10.4. Data in encrypted backups will be deleted in the normal backup expiration cycle and will remain protected by this DPA until then. RWS may retain Personal Data where required by Applicable Law, limiting the processing to secure storage for the legal period.

10.5. Upon request, RWS will confirm in writing that the deletion has been completed.

10.6. Given the nature of the Cloud Service, RWS will not be required to return Personal Data already delivered to the destination systems or not held by the Cloud Service, with the export functionalities and the provisions of the Agreement applying to the remaining data. The deletion provided for in this Section does not cover the data delivered by the Integrations to the systems of Customer, of its End Customers or of third parties, nor the messages sent to webhooks or other destinations indicated by Customer.

11. Liability

11.1. Each party's total liability for DPA Claims will not exceed the DPA Liability Cap, which corresponds to the General Cap Amount set in the Agreement. This is a single, cumulative cap for the Agreement and for this DPA: DPA Claims count toward that cap, and the same event does not give rise to double recovery under the Agreement, this DPA or any Order Form. To the extent not modified by this Section, the exclusions and conditions of Section 8 (Limitation of Liability) of the Agreement apply.

11.2. Nothing in this DPA limits a party's liability toward Data Subjects or toward the ANPD under arts. 42 to 45 of the LGPD, which is governed by law, nor establishes joint and several

liability between the parties beyond the cases provided for by law. The party that causes the damage, by breaching this DPA, the Applicable Data Protection Laws or the lawful instructions of the Controller, will reimburse the other for the amounts the latter is compelled to pay to Data Subjects, by reason of a court decision or of a settlement previously approved by the reimbursing party, or to the ANPD, by reason of a final administrative decision, in proportion to its share in the harmful event (art. 42, paragraph 4, of the LGPD) and subject to the DPA Liability Cap. If the decision is reversed or annulled, the reimbursed amounts will be returned.

11.3. RWS will not be liable for damages arising from, and to the extent they arise from: (a) Customer's instructions, including the configuration of the Integrations by Customer or at its request; (b) data submitted without a legal basis or Restricted Data; (c) acts or omissions of Customer, of its Users, of its End Customers or of its suppliers, including the compromise of credentials in Customer's custody; (d) security failures in the systems of Customer and of its End Customers or in the destinations indicated by it; or (e) the cases provided for in art. 43 of the LGPD.

11.4. Only the Customer entity that entered into the Agreement may bring claims against RWS under this DPA, including on behalf of its Affiliates and of its End Customers.

11.5. The DPA Liability Cap does not apply: (a) to Customer's obligations to pay the Fees; (b) to Customer's indemnification obligations under items (a) and (b) of Section 11.6; and (c) to damages caused by willful misconduct, to the extent the law prohibits the limitation.

11.6. Customer will indemnify RWS for the losses, damages, fines and reasonable expenses, including attorneys' fees and amounts paid to Data Subjects, Controllers or End Customers, that demonstrably arise, in proportion to its share in the harmful event: (a) from the absence of a legal basis for, or of adequate information to Data Subjects about, the Personal Data submitted to the Product; (b) from the submission of Restricted Data; (c) from unlawful instructions of Customer or, when it acts as Processor, instructions incompatible with those of its Controller; or (d) from Customer's breach of this DPA. RWS will notify Customer, as soon as it becomes aware, of the third-party claim or of the proceeding initiated by an authority, will allow Customer to conduct the defense, where appropriate, and will cooperate with it, and will not settle or acknowledge liability on Customer's behalf without its prior consent, which will not be withheld without reasonable grounds.

12. Precedence and Term

12.1. This DPA takes effect on the date Customer accepts the Agreement or signs the first Order Form incorporating it, whichever occurs first, and remains in force for as long as RWS processes Customer's Personal Data, even if the Agreement has ended.

12.2. In case of conflict, the order of precedence described in the section "How this DPA works" applies.

13. General Provisions

13.1. Updates. RWS may publish new versions of this DPA to reflect legal or regulatory changes or changes to the Cloud Service. Changes will be communicated to Customer by email 30 days in advance and will take effect at the end of that period, except for changes required by law, which will take effect on the required date. Changes that materially reduce Customer's protections do not apply to Order Forms in force without Customer's written agreement. The version history remains available at rwsintegration.com/pt-br/legal/dpa and at rwsintegration.com/en/legal/dpa.

13.2. Language. This DPA is published in Portuguese and in English. In case of divergence between the versions, the Portuguese version prevails.

13.3. Communications. Communications about this DPA will be sent to the contacts in the Key Terms and in the Order Form. Each party will inform the other, without delay, of any change to those contacts.

13.4. Law and jurisdiction. The Governing Law and the Chosen Courts of the Key Terms apply.

13.5. Severability. If any provision of this DPA is held invalid, the remaining provisions will remain in force and the invalid provision will be replaced by a valid one that achieves an equivalent purpose.

14. Definitions

"Anonymization" means the use of reasonable technical means available at the time of the processing, through which data loses the possibility of association, directly or indirectly, with an individual (art. 5, XI, of the LGPD).

"ANPD" means the Brazilian National Data Protection Authority (Autoridade Nacional de Proteção de Dados).

"Applicable Data Protection Laws" means the LGPD, the ANPD regulations and, where applicable to the processing, the GDPR, the UK GDPR and other data protection laws governing the processing of Personal Data by the Cloud Service.

"Controller" means the person responsible for the decisions concerning the processing of Personal Data (art. 5, VI, of the LGPD), equivalent to "controller" under the GDPR.

"Data Subject" means the natural person to whom the Personal Data refers (art. 5, V, of the LGPD).

"DPA Claim" means any claim of one party against the other arising from this DPA, from the processing governed by it or from a Security Incident, regardless of its basis, whether contractual, non-contractual, indemnity or recourse, including claims brought by Customer on behalf of its Affiliates and of its End Customers.

"End Customers" has the meaning given in the Order Form: the distinct legal entities that maintain a business relationship with Customer and have an active Integration in the Cloud Service.

"Integration" means each flow configured in the Cloud Service to extract, transform and deliver data between systems of Customer and of its End Customers or authorized third parties.

"International Transfer" means the transfer of Personal Data to a foreign country or to an international body of which the country is a member (art. 5, XV, of the LGPD).

"LGPD" means Law No. 13,709/2018, the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais).

"Personal Data" means information related to an identified or identifiable natural person contained in Customer Content and processed by RWS on behalf of Customer (art. 5, I, of the LGPD).

"Processing" means any operation carried out with Personal Data, such as collection, receipt, access, processing, storage, transmission, transfer and deletion (art. 5, X, of the LGPD).

"Processor" means the person that processes Personal Data on behalf of the Controller (art. 5, VII, of the LGPD), equivalent to "processor" under the GDPR.

"Data Protection Officer" means the person appointed by the processing agent to act as a communication channel between the agent, the Data Subjects and the ANPD (art. 5, VIII, of the LGPD).

"Restricted Data" means the data described in Section 2.5.

"Security Incident" means any confirmed adverse event, related to a breach of the properties of confidentiality, integrity or availability, that results in unauthorized access, destruction, loss, alteration, leakage or any form of inadequate or unlawful processing of Personal Data (art. 46 of the LGPD). It does not include unsuccessful attempts, such as scans, blocked login attempts or denial-of-service attacks without access to Personal Data.

"Sensitive Personal Data" means Personal Data concerning racial or ethnic origin, religious belief, political opinion, membership of a trade union or of a religious, philosophical or political organization, health or sex life, or genetic or biometric data (art. 5, II, of the LGPD), and the special categories of art. 9 of the GDPR, where applicable.

"Sub-processor" means the third party engaged by RWS to process Personal Data in the provision of the Cloud Service, including RWS Affiliates.

Annex I: Details of the Processing

A. Parties and roles

Field	Exporter / Customer	Importer / Provider
Identification	As set out in the Order Form	RWS Ltda., CNPJ 46.231.982/0001-23, Av. Santo Amaro, 1047, São Paulo/SP
Contact	Customer Notice Address provided for in the Agreement and the security or privacy contact indicated in the Order Form	dpo@rwsintegration.com (Data Protection Officer) and security@rwsintegration.com (security)
Role	Controller or, when it processes Personal Data on behalf of its End Customers or of another Controller, Processor	Processor (if Customer is Controller) or Sub-processor (if Customer is Processor)

B. Description of the processing

Customer determines, at its sole discretion, which data passes through each Integration. The categories below describe the authorized universe.

Categories of Data Subjects. Depending on the Integrations configured, they may include:

- employees, interns, apprentices, candidates, former employees and dependents of Customer or of its End Customers;
- service providers, self-employed workers and representatives of suppliers and partners;
- customers and consumers of Customer or of its End Customers, where natural persons, and representatives of corporate customers;
- users of integrated applications and portals;
- Users of the Product designated by Customer (for access account purposes, processed by RWS as Controller, Section 1.2).

Categories of Personal Data. Depending on the connected systems, they may include:

Category	Examples
Identification	Name, date of birth, gender, nationality, CPF, RG, CNH, passport, PIS/NIS, CTPS, voter registration, employee number, system identifiers

RWS

Category	Examples
Contact	Email, telephone, home and business address
Professional and HR data	Job title, department, cost center, manager, hiring and termination dates, working hours, time and attendance, vacations, leaves, evaluations, training, employment history
Payroll, compensation and benefits	Salary, pay items, deductions, bank account data for credit, contracted benefits, health and dental plans (enrollment and dependents), transportation and meal vouchers
Financial and transactional	Orders, invoices, tax documents, payments, collections, credit limits, bank account data for payments to suppliers and customers
Commercial and relationship	Customer contacts, leads, opportunities, service history, communication preferences
Device and application usage data	User identifiers, access records, logs of integrated applications, IP address, where present in the payloads
Location	Delivery addresses, service locations, route and geolocation data where present in the integrated systems
Other	Any other categories present in the systems Customer decides to integrate, subject to the Restricted Data

Sensitive Personal Data. It may pass through when necessary for the Integration, in particular in HR, payroll, benefits, occupational health and eSocial flows: union membership, health data (medical certificates, ICD codes, leaves, occupational exams, plan enrollment), biometric time-clock data, racial or ethnic origin in self-declaration fields. Customer is responsible for the legal basis under art. 11 of the LGPD and for restricting the fields to what is necessary. RWS applies to this data the same measures of the Security Policy, without distinction of category.

Data of children and adolescents. It may pass through as dependents in benefits and payroll flows. Customer is responsible for compliance with art. 14 of the LGPD.

Nature and purpose of the processing. Receipt, transformation, routing, delivery and execution logging of data between systems of Customer, of its End Customers and of authorized third parties, in accordance with the configured Integrations, for the exclusive purpose of providing the contracted Cloud Service.

Frequency. Continuous during the term of the Agreement, through events (webhooks), schedules or queries configured by Customer.

Duration and retention. During the term of the Agreement. Data in transit remains in the queues only until delivery and automatic reprocessing in case of failure. Execution logs and

backups: periods defined in the Security Policy. Deletion upon termination as provided in Section 10.

Transfers to Sub-processors. As set out in Annex III, for the period and for the purposes described there.

C. Competent authority

Brazilian National Data Protection Authority (ANPD), Brazil. For processing subject to the GDPR, the authority of the Member State indicated in the addendum provided for in item 5 of Annex IV.

Annex II: Technical and Organizational Measures

The technical and administrative measures adopted by RWS are those described in the Security Policy, published at rwsintegration.com/pt-br/legal/security (English version at rwsintegration.com/en/legal/security) and incorporated into this DPA by reference. The Security Policy is the single source of those measures and this DPA does not reproduce them. The version in effect on the date of the processing applies, subject to Section 5.2.

Annex III: Sub-processors

The list of authorized Sub-processors, with the purpose, the data processed, the location and the transfer mechanism of each one, is published at rwsintegration.com/pt-br/legal/subprocessors (English version at rwsintegration.com/en/legal/subprocessors) and incorporated into this DPA by reference. That page is the single source of the list and this DPA does not reproduce it. Changes follow Section 3: notice by email 30 days in advance and an objection period of 10 days. Webhooks and other destinations indicated by Customer (Section 2.8) are not Sub-processors.

Annex IV: International Transfer

1. Flow. Customer, in Brazil, delivers Personal Data to RWS, in Brazil, which processes it on AWS infrastructure in the United States. The Customer/RWS relationship does not constitute an International Transfer. The RWS/AWS relationship constitutes an International Transfer, in which RWS is the exporter and AWS is the importer.

2. Mechanism. The RWS/AWS transfer is based on art. 33, II, of the LGPD, through the standard contractual clauses approved by the ANPD in Resolution CD/ANPD No. 19/2024, incorporated without changes to their content into the agreement between RWS and AWS, in the module applicable to transfers between processors under the authorization and

instruction of the Controller. If the ANPD recognizes, through an adequacy decision, the destination country or an equivalent mechanism, RWS may start using it, informing Customer.

3. Authorization and instruction of the Controller. By accepting this DPA, Customer, in its capacity as Controller, authorizes and instructs RWS to carry out the transfer described in item 1 and acts as third-party Controller for the purposes of the standard clauses, where required. When Customer acts as Processor, it represents that it has obtained that authorization from its Controller.

4. Transparency to Data Subjects. The Controller must make available to Data Subjects, in Portuguese, simplified information about the transfer (purpose, destination country, mechanism and Data Subject rights) and provide a copy of the clauses upon the Data Subject's request, in accordance with the ANPD regulations. To support that duty, RWS provides the standard description below, which Customer may reproduce in its privacy policy:

> *We use the integration platform of RWS Ltda. to transmit data between our systems and those of our partners. RWS processes this data, on our behalf, on Amazon Web Services infrastructure located in the United States, on the basis of standard contractual clauses approved by the Brazilian National Data Protection Authority, which ensure a level of protection equivalent to that of the LGPD. You may request a copy of these clauses through our data subject service channel.*

5. GDPR and UK GDPR. If Customer or its End Customers are subject to the GDPR or the UK GDPR and the processing involves Personal Data of Data Subjects in the European Economic Area or in the United Kingdom, the parties will enter into a specific addendum incorporating the standard contractual clauses of the European Commission (Decision 2021/914, Module Two or Three, depending on Customer's role) and the UK International Data Transfer Addendum, with Annexes I and II of this DPA completing the corresponding annexes. That addendum is available upon request to dpo@rwsintegration.com.

6. Additional safeguards. Regardless of the mechanism, RWS: (a) maintains the measures of the Security Policy in all regions; (b) will inform Customer, unless legally prohibited, of requests from foreign authorities for access to Customer's Personal Data and will challenge requests it considers unlawful or excessive; and (c) will not transfer Personal Data to another country without observing Section 4 of the Standard Terms.

Version history

Version	Date	Change
1.0 (current)	June 2026	Original version

Legal documents

Terms of use

Privacy policy

Data Processing Addendum (DPA)

Security Policy

Sub-processors

Last updated: June 2026

This English version is provided for convenience only. The Portuguese version at rwsintegration.com/pt-br/legal/dpa is the official version and prevails in case of any divergence.