

JEEVES INC.

JEEVES APEX DATA PROCESSING ADDENDUM

to the Mutual Confidentiality Agreement (Product Evaluation) and to the Jeeves Apex Master Terms and Conditions

Version 1.0 – October 30, 2026

Key Terms

Customer	[CUSTOMER LEGAL NAME], a [entity type and jurisdiction], [address] (in the Evaluation Phase, the “Counterparty” under the NDA).
Jeeves	Jeeves Inc., a Delaware corporation, 251 Little Falls Drive, Wilmington, Delaware 19808.
Underlying Agreement(s)	[] Mutual Confidentiality Agreement (Product Evaluation) dated [] (the “NDA”), for the Evaluation Phase; and/or [] Order Form No. [] dated [] and the Jeeves Apex and AI Services Master Terms and Conditions (the “Terms”), for the Production Phase. A box is checked as each applies; this DPA continues from one phase to the next.
Jeeves notice contacts	Legal: Brandon S. McGathy, General Counsel & Secretary, legal@tryjeeves.com. Security incidents: the same address, marked “URGENT – SECURITY INCIDENT” in the subject line. Privacy: privacy@tryjeeves.com.
Customer notice contacts	Legal: [name, email]. Security incidents and privacy: [name, email].
Evaluation Period	As stated in the NDA’s Evaluation Details.

1. Scope, Roles and Incorporation

1.1 Purpose; structure. This Data Processing Addendum (this “DPA”) applies to the Processing of Customer Personal Data by Jeeves for Customer. It applies in two phases under the Underlying Agreement(s) identified in the Key Terms: (a) the “Evaluation Phase,” in which Customer evaluates Apex under the NDA and may disclose only Sample Data; and (b) the “Production Phase,” in which Jeeves provides Services under an Order Form and the Terms. This DPA applies from the first disclosure of Customer Personal Data and continues from one phase to the next without re-signature.

1.2 Incorporation; precedence. This DPA forms part of the Underlying Agreement(s). For Customer Personal Data, the order of precedence is: (i) the mandatory terms of any Transfer Clauses; (ii) this DPA; and (iii) the Underlying Agreement. This DPA does not otherwise change the Underlying Agreement, and Section 14 governs liability.

1.3 Evaluation Phase. During the Evaluation Phase Jeeves will Process only Sample Data, as described in Part A of Annex 1, and Customer will not disclose production Customer Personal Data, connect Apex to Customer Systems, or enable any Customer-Facing Agent. This DPA applies in full to Sample Data. If Customer signs an Order Form, Part B of Annex 1 applies to the Production Phase,

and any Sample Data Jeeves then holds becomes Customer Data under the Terms unless Customer asks Jeeves in writing to delete it under Section 12.

1.4 Affiliates. Customer enters into this DPA for itself and for each of its Affiliates that is a controller of Customer Personal Data Processed by Jeeves, and Customer will act as their single point of contact. Jeeves's obligations are owed to Customer, and Customer is responsible for its Affiliates' compliance with this DPA.

1.5 Jeeves as separate controller. Jeeves acts as an independent controller only for the limited purposes in Part C of Annex 1. This DPA does not apply to that Processing, which Jeeves carries out under its privacy notice.

2. Definitions

2.1 Terms from the Underlying Agreement. Capitalized terms not defined in this DPA have the meanings in the Terms (or, in the Evaluation Phase, the NDA). In the Evaluation Phase, "Customer" means the Counterparty named in the NDA, "Order Form" and "Services" mean the Evaluation Access under the NDA, and "Authorized User" means Customer personnel who access the Evaluation Access.

2.2 Definitions. In this DPA:

(a) **"AI Model"** means any machine-learning or other artificial-intelligence model, including large language, embedding and classification models, operated by Jeeves or a third party.

(b) **"Applicable Data Protection Laws"** means all privacy, data-protection, data-security, breach-notification and financial-secrecy laws that apply to the Processing of Customer Personal Data, as amended, including as applicable: the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR") and the UK GDPR; Brazil's Law No. 13,709/2018 ("LGPD"); Mexico's Ley Federal de Protección de Datos Personales en Posesión de los Particulares of 2025 ("LFPDPPP"); Colombia's Law 1581 of 2012 and Decree 1377 of 2013; Chile's Law No. 19,628, as amended by Law No. 21,719; Argentina's Law No. 25,326; Peru's Law No. 29733; Canada's PIPEDA and Quebec's Act respecting the protection of personal information in the private sector; the U.S. Gramm-Leach-Bliley Act and its implementing rules; and the California Consumer Privacy Act, as amended ("CCPA"), and other U.S. state privacy and breach-notification laws.

(c) **"Customer Personal Data"** means Customer Data (and, in the Evaluation Phase, Sample Data) that is personal data, personal information, nonpublic personal information or any similar term under Applicable Data Protection Laws, and that Jeeves Processes for Customer. It does not include De-Identified Data, Aggregated Data, Usage Data or Learnings once created under Section 6.

(d) **"Data Subject"** means the individual to whom Customer Personal Data relates, including Customer's personnel, vendors' and payees' contacts and, where a Customer-Facing Agent is enabled, End Customers.

(e) **"Model Subprocessor"** means a Subprocessor that hosts, operates or provides access to an AI Model that Processes Customer Personal Data.

(f) **"Process" or "Processing"** means any operation performed on data, including receipt, storage, use, submission to an AI Model, disclosure, transfer, combination, de-identification and deletion.

(g) **"Sample Data"** means the limited data that Customer discloses during the Evaluation Phase under Section 5.2 and Part A of Annex 1.

(h) **"Security Incident"** means a breach of security of Jeeves's systems or those of its Subprocessors that leads to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to Customer Personal Data. It does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, nor an event caused by Customer, its Authorized Users or Customer Systems, or by credentials Customer has disclosed or failed to protect.

(i) **“Subprocessor”** means a third party, including a Jeeves Affiliate, hosting provider or Model Subprocessor, that Processes Customer Personal Data on Jeeves’s behalf, other than Jeeves’s personnel.

(j) **“Supervisory Authority”** means a governmental, regulatory or supervisory authority with jurisdiction over the Processing of Customer Personal Data, including data-protection authorities and financial regulators.

(k) **“Transfer Clauses”** means the EU SCCs, the UK Addendum, the Brazil SCCs and any other transfer mechanism that applies under Section 11.

2.3 Interpretation. “Including” means “including without limitation.” Terms such as “controller,” “processor,” “business” and “service provider,” and their equivalents under other Applicable Data Protection Laws, have the meanings those laws give them.

3. Roles and Processing Instructions

3.1 Roles. Customer (or the relevant Affiliate) is the controller (responsable, controlador) and “business,” and Jeeves is the processor (encargado, operador) and “service provider,” of Customer Personal Data. Where Customer acts as a processor for its own customers, Jeeves is Customer’s sub-processor on the terms of this DPA.

3.2 Instructions. Jeeves will Process Customer Personal Data only on Customer’s documented instructions, which are the Underlying Agreement and this DPA (including Annex 1), Customer’s configuration and use of Apex (including approval thresholds, permissions, rules and Workflows), and further written instructions from Customer’s contacts in the Key Terms that are consistent with them. Jeeves will inform Customer if it believes an instruction infringes Applicable Data Protection Laws, but is not required to provide legal advice. Jeeves may charge for, and may decline, instructions that go beyond the scope of the Underlying Agreement.

3.3 Purposes. Jeeves will Process Customer Personal Data only to (a) provide, operate, secure, support and improve the Services and Evaluation Access for Customer; (b) create De-Identified Data, Aggregated Data, Usage Data and Learnings as Section 6 provides, which Customer instructs Jeeves to do; (c) for Financial Services, as an independent controller under Part C of Annex 1; and (d) comply with law. Jeeves will not (i) sell or share Customer Personal Data, including for cross-context behavioral advertising; (ii) retain, use or disclose it outside its direct business relationship with Customer or for any purpose other than the business purposes in this Section; or (iii) combine it with personal data from another source, except as Applicable Data Protection Laws permit for the business purposes in this Section. Clauses (ii) and (iii) of this Section do not apply to Processing for Financial Services under Part C of Annex 1, which Jeeves carries out as an independent controller and not on Customer’s instructions; Jeeves will not sell or share Customer Personal Data for it.

3.4 CCPA and GLBA. Jeeves certifies that it understands and will comply with Section 3.3 and the CCPA, will provide the level of privacy protection the CCPA requires, and will notify Customer within five (5) business days if it can no longer meet these obligations. Customer may take reasonable and appropriate steps to ensure that Jeeves uses Customer Personal Data consistently with Customer’s CCPA obligations, and to stop and remediate any unauthorized use. Customer discloses Customer Personal Data to Jeeves only for the limited and specified purposes in Annex 1. Jeeves will use nonpublic personal information subject to the Gramm-Leach-Bliley Act only to provide the Services and will maintain safeguards consistent with Annex 2.

3.5 Customer responsibilities. Customer is responsible for (a) having a lawful basis, and giving all notices and obtaining all consents required, to disclose Customer Personal Data to Jeeves and to have Jeeves Process it as this DPA describes, including for the de-identification in Section 6 and the Financial Services use in Part C of Annex 1; (b) the accuracy and minimization of Customer Personal Data and the lawfulness of its instructions; (c) not providing Prohibited Data (Terms §7.4); (d) the authority and consents that Terms §18.3 requires to authorize Jeeves’s access to Customer Systems; (e) configuring Apex’s approvals, permissions and retention settings appropriately; (f) for any Customer-Facing Agent, the disclosures, consents and compliance duties in Terms §19; and (g) determining whether the Services meet its own legal obligations.

4. AI-Specific Terms

4.1 Model Subprocessors. Jeeves will disclose Customer Personal Data to a Model Subprocessor only if (a) the AI Model is accessed through an enterprise API or cloud service, not a consumer product, under written terms that prohibit use of inputs or outputs to train or improve any AI Model; (b) the Model Subprocessor retains Customer Personal Data for no more than thirty (30) days (for abuse monitoring only), or not at all where it offers that option; (c) Customer Personal Data is processed only in the regions listed in Annex 3; and (d) the account settings are configured to give effect to this Section.

4.2 No training on identifiable data. Jeeves will not use Customer Personal Data in identifiable form to train or fine-tune any foundation model for the benefit of any third party, and will contract with its Model Subprocessors so that they do not train on it. This Section does not restrict Jeeves's creation and use of De-Identified Data, Aggregated Data, Usage Data and Learnings under Section 6.

4.3 Human oversight; significant decisions. Apex routes actions outside Customer's thresholds to a person and, unless an Order Form enables otherwise, Agents propose but do not post entries or execute payments (Terms §9.2). Jeeves does not use Customer Personal Data to make decisions with legal or similarly significant effects on any individual. If Customer uses an Output in a process that does, Customer is responsible for the notices, human review and other safeguards Applicable Data Protection Laws require, including GDPR Article 22.

4.4 Credentials and actions. Jeeves stores credentials that Customer provides for Customer Systems in an encrypted secrets vault, uses them only to provide the Services, grants access to them only to personnel and Subprocessors that need it, and uses read-only permissions unless Customer expressly enables others (Terms §18.3).

4.5 Transparency. On Customer's request, Jeeves will identify the categories of AI Models and Model Subprocessors it uses and provide the information reasonably needed for Customer's data-protection or AI impact assessments (Section 10.3).

4.6 Prohibited uses. Customer will not use the Services to make decisions about an individual's creditworthiness, employment or eligibility for essential services, or for any other use Jeeves has not agreed in writing, where Applicable Data Protection Laws treat it as high-risk (Terms Schedule 1).

5. Data Minimization; Prohibited Data; Sample Data

5.1 Minimization; Prohibited Data. Customer will send Jeeves only the Customer Personal Data needed for the Services, and will not send Prohibited Data (full card numbers and security codes; government identification numbers, except categories the Order Form expressly permits; special categories of personal data; authentication credentials other than through Jeeves's designated secure mechanism; and personal data Jeeves does not need). If Jeeves receives Prohibited Data, it will not use it except to delete it, will notify Customer within five (5) business days of becoming aware, and will delete it from active systems within thirty (30) days. Receipt alone is not a breach by Jeeves, and Customer is responsible for Prohibited Data it sends.

5.2 Sample Data. In the Evaluation Phase, Customer will disclose only Sample Data that is masked, de-identified or synthetic where practicable, limited to the types and volumes in Part A of Annex 1, and delivered through the secure channel Jeeves designates. Customer will not include names or contact details of individuals, full account or card numbers (masked or truncated numbers are permitted), credentials or government identifiers, or personal data of End Customers.

5.3 No re-identification. Jeeves will not attempt to re-identify any individual from Sample Data or from data Customer has masked or pseudonymized, except as needed to provide the Services and as Customer instructs.

6. De-Identified Data and Anonymization

6.1 Instruction. Customer instructs Jeeves to create De-Identified Data, Aggregated Data, Usage Data and Learnings from Customer Personal Data, Customer Materials and Customer's use of the Services and Evaluation Access, as a Processing operation that is part of the Services.

6.2 Standard. Jeeves will apply techniques such as removal of direct identifiers, masking, generalization, aggregation, thresholding and noise, appropriate to the data, so that De-Identified Data (a) does not relate to an identified or identifiable individual, taking into account the means reasonably likely to be used to identify them; (b) cannot reasonably be used to infer information about, or be linked with, a particular individual, household or device; and (c) does not identify Customer. Pseudonymized data remains Customer Personal Data until it meets this Section.

6.3 Commitments. Jeeves will (a) take reasonable measures to ensure De-Identified Data cannot be associated with an individual; (b) maintain and use it only in de-identified form and not attempt to re-identify it; (c) contractually bind any recipient (other than Customer) to the same commitments; and (d) publicly commit to these terms in its privacy notice. Jeeves will not disclose Aggregated Data or benchmarks derived from Customer Personal Data except as Terms §7.3 permits.

6.4 Status. De-Identified Data, Aggregated Data, Usage Data and Learnings are not Customer Personal Data, fall outside this DPA, are owned by Jeeves and may be used as Terms §7.2 (or, in the Evaluation Phase, the NDA) provides, including to train and improve AI Models, Agents and Apex. The deletion obligations in Section 12 do not reach them.

6.5 Restrictions. An Order Form may restrict this Section only if it identifies this Section and is approved under Terms §17.8. Where Applicable Data Protection Laws require a further legal basis for this Processing, Customer is responsible for it under Section 3.5(a).

7. Subprocessors

7.1 General authorization. Customer gives Jeeves general written authorization to engage Subprocessors, including those in Annex 3, and to disclose Customer Personal Data to them and to Jeeves's personnel as needed to provide the Services.

7.2 Changes; objection. Jeeves will give Customer at least thirty (30) days' notice, by email or through a Jeeves portal Customer can subscribe to, before a new or replacement Subprocessor Processes Customer Personal Data, with the information Annex 3 lists. Customer may object in writing within ten (10) business days on reasonable data-protection grounds. The Parties will discuss in good faith. If they cannot resolve the objection, Customer's sole remedy is to terminate the affected Services on written notice and receive a refund of prepaid fees for the unused period of those Services, and no Commitment, early-termination fee or Credit forfeiture applies to the terminated portion.

7.3 Flow-down; liability. Jeeves will bind each Subprocessor in writing to data-protection obligations no less protective than this DPA as applicable to its services (for a Model Subprocessor, enterprise terms that meet Section 4.1 suffice), and remains responsible for each Subprocessor's performance as for its own, subject to Section 14.

8. Security

8.1 Measures. Jeeves will maintain technical and organizational measures appropriate to the risk and the financial and personal nature of Customer Personal Data, including at least those in Annex 2, and will not materially reduce them while it holds Customer Personal Data. This Section supplements Terms §7.5.

8.2 Assurance. Jeeves will maintain [a SOC 2 Type II report covering at least the Security and Confidentiality criteria, or ISO/IEC 27001 certification,] for the systems that Process Customer Personal Data, and will provide them under Section 13.

8.3 Personnel. Jeeves will ensure that personnel and Subprocessor staff who access Customer Personal Data are bound by written confidentiality obligations, are trained on data protection, and access it only as needed to provide the Services. Personnel working in Customer's environments follow the access and change-management rules Customer provides under Terms §3.4.

8.4 Customer's security responsibilities. Customer is responsible for the security of Customer Systems and its own accounts, for the credentials and permissions it grants, and for promptly revoking access that is no longer needed.

9. Security Incidents

9.1 Notice. Jeeves will notify Customer of a Security Incident without undue delay, and in any event within seventy-two (72) hours after becoming aware of it (that is, after it has a reasonable degree of certainty that it has occurred), by email to the Customer notice contacts. This Section supplements Terms §7.7.

9.2 Content. The notice will describe, to the extent known: the nature and timing of the Security Incident; the categories and approximate number of Data Subjects and records affected; the likely consequences; the measures taken or proposed; and a point of contact. Jeeves may provide information in phases as it becomes available and will update Customer as material facts develop.

9.3 Response; notifications. Jeeves will take reasonable steps to contain, investigate and remediate each Security Incident, and will reasonably cooperate with Customer's investigation. Customer decides whether and how to notify any Supervisory Authority, Data Subject or third party, and Jeeves will not make such a notification on Customer's behalf unless law requires it. A notice, or Jeeves's cooperation, is not an admission of fault or liability.

10. Assistance; Legal Process

10.1 Data Subject requests. Jeeves will forward to Customer within five (5) business days any request from a Data Subject relating to Customer Personal Data, will not respond except to refer the requester to Customer, and will provide reasonable assistance, taking into account the nature of the Processing, to help Customer respond within the time Applicable Data Protection Laws require. Customer is responsible for responding to Data Subjects.

10.2 Legal process. Unless legally prohibited, Jeeves will notify Customer within two (2) business days of any regulatory inquiry, subpoena or other legal demand for Customer Personal Data, will challenge any request it reasonably considers overbroad or unlawful, will disclose only the minimum legally required, and will cooperate with Customer's efforts to obtain protective relief, at Customer's cost.

10.3 Assessments. Jeeves will provide information reasonably requested by Customer for a data-protection, AI or transfer impact assessment or regulatory consultation about the Processing (including under GDPR Article 35 and LGPD Article 38), and will maintain the records of Processing that law requires of processors.

10.4 Cost. Assistance under this Section 10 that goes beyond the reasonable use of the functionality and information Jeeves makes available is subject to a written estimate and Jeeves's then-current rates.

11. International Transfers

11.1 Location; authorization. Jeeves stores and Processes Customer Personal Data in the United States and the other locations in Annex 3, as Terms §7.9 provides. Customer authorizes those transfers and the onward transfers to Subprocessors that Section 7 permits, which will be made in compliance with Applicable Data Protection Laws.

11.2 EU SCCs. To the extent the Processing involves a transfer of Customer Personal Data subject to the GDPR to a country without an adequacy decision (or another mechanism Jeeves elects to rely on), the standard contractual clauses approved by Commission Implementing Decision (EU) 2021/914 (the “EU SCCs”) are incorporated by reference, with Customer as data exporter and Jeeves as data importer, as follows: (a) Module Two applies, and Module Three applies where Customer acts as a processor; (b) Clause 7 applies; in Clause 9(a), Option 2 (general written authorization) applies with a notice period of thirty (30) days under Section 7.2; and the option in Clause 11(a) does not apply; (c) the competent supervisory authority under Clause 13 is as stated in Annex 1; (d) in Clause 17, Option 1 applies with the law of Ireland, and under Clause 18(b) the courts of Ireland have jurisdiction; and (e) Annexes I.A, I.B and I.C are completed by the Key Terms and Annex 1, Annex II by Annex 2, and Annex III by Annex 3. Section 13 governs audits under Clause 8.9, and Section 12 governs deletion under Clauses 8.5 and 16(d).

11.3 UK and Switzerland. For transfers subject to the UK GDPR, the International Data Transfer Addendum (version B1.0) issued by the UK Information Commissioner (the “UK Addendum”) is incorporated by reference, with its Tables 1 to 3 completed by this DPA and its Annexes, and with neither Party able to end it under its Section 19. For transfers subject to Swiss law, the EU SCCs apply with the adaptations Swiss law requires.

11.4 Latin America and other jurisdictions. For Customer Personal Data subject to the LGPD, the Parties will execute, before any transfer and without alteration, the standard contractual clauses approved by Resolution CD/ANPD No. 19/2024 (the “Brazil SCCs”), with the applicable Customer entity as exporter, and the Brazil SCCs prevail in case of conflict. For Customer Personal Data subject to the LFPDPPP or Colombian law, this DPA is the contract governing its remission or transmission (including under Article 25 of Colombia’s Decree 1377 of 2013), and Jeeves will Process it in accordance with Customer’s instructions and privacy notices. The Parties will promptly execute any further model clauses required for transfers from Argentina, Chile, Peru, Canada or any other jurisdiction.

11.5 Government access. Jeeves warrants that, at signature, it has no reason to believe that the laws applicable to it prevent it from fulfilling its obligations under the Transfer Clauses. Section 10.2 applies to government access requests.

11.6 Changes. If a Transfer Clause ceases to be a valid transfer mechanism, the Parties will cooperate to implement an alternative, and either Party may suspend the affected transfers in the meantime.

12. Return and Deletion

12.1 Production Phase. Terms §7.10 governs export and deletion of Customer Data. In summary, Customer may export Customer Data and Outputs during the term and for thirty (30) days afterward, and Jeeves will delete Customer Personal Data in identifiable form from its active systems within thirty (30) days after Customer’s written request, and in any event within ninety (90) days after the export period ends, and from backups in the ordinary backup cycle.

12.2 Evaluation Phase. Jeeves will delete Sample Data in identifiable form (including embeddings, indexes and logs derived from it) from its active systems within thirty (30) days after Customer’s written request and, unless Customer signs an Order Form, within sixty (60) days after the Evaluation Period ends, and from backups in the ordinary backup cycle.

12.3 Exceptions. Jeeves may retain Customer Personal Data to the extent law requires, in backups under the ordinary cycle (without restoring it except for disaster recovery, and re-deleting it if restored), and as a controller under Part C of Annex 1. Deletion does not extend to De-Identified Data, Aggregated Data, Usage Data, Learnings or Jeeves Technology, or to Outputs already delivered to Customer. Retained Customer Personal Data remains subject to this DPA.

12.4 Confirmation. On Customer's written request after deletion, Jeeves will confirm in writing that it has completed deletion under this Section.

13. Audit and Information

13.1 Information. On Customer's written request (not more than once in any twelve (12) month period, other than after a Security Incident), Jeeves will make available its current assurance report or certificate under Section 8.2, a summary of its latest independent penetration test, and reasonable responses to a security questionnaire, subject to confidentiality.

13.2 Audit. If that information does not reasonably demonstrate Jeeves's compliance with this DPA, or a Supervisory Authority requires it, Customer (or an independent auditor bound by confidentiality that is not a Jeeves competitor) may audit Jeeves's compliance on thirty (30) days' written notice (ten (10) business days after a Security Incident or at a Supervisory Authority's request), during business hours, remotely where practicable, not more than once in any twelve (12) month period except in those cases, and limited to the systems and records relevant to Customer Personal Data. The audit will not extend to other customers' data, to Jeeves Technology source code or to information protected by privilege. Customer bears the costs of the audit, and each Party promptly remediates any material non-compliance found. This Section also governs audits under the EU SCCs.

14. Liability

14.1 Underlying Agreement governs. Each Party's liability arising out of or related to this DPA is subject to the limitations and exclusions in the Underlying Agreement as if set out in it. A breach of this DPA by Jeeves is a breach of Section 7 of the Terms, subject to the Super-Cap in Terms §13.3. In the Evaluation Phase, the limits in Section 8 of the NDA apply.

14.2 Data Subjects; mandatory law. Nothing in this DPA limits either Party's liability to Data Subjects under the Transfer Clauses, or any liability that Applicable Data Protection Laws do not allow to be limited.

14.3 Indemnity. Customer's indemnification obligations under Terms §12.2 apply to claims arising from Customer's breach of Section 3.5 or Section 5.

15. Term; General

15.1 Term. This DPA takes effect on the date it is last signed (the "DPA Effective Date") and continues until Jeeves no longer holds Customer Personal Data. Sections 6, 12, 14 and 15 survive.

15.2 Governing law; venue. This DPA is governed by the laws of the State of New York, without regard to conflict-of-laws principles, except that each Transfer Clause is governed by the law it specifies and Applicable Data Protection Laws apply where mandatory. The state and federal courts located in New York, New York have exclusive jurisdiction over disputes arising out of this DPA, without

prejudice to the forum provisions of any Transfer Clause or either Party’s right to seek injunctive relief in any court of competent jurisdiction.

15.3 Notices. Notices are given as the Underlying Agreement provides, supplemented by the contacts in the Key Terms. Security Incident notices and notices under Sections 5.1, 7.2 and 10 may be given by email.

15.4 Updates. Jeeves may update this DPA on notice if a change in Applicable Data Protection Laws, a Transfer Clause or a regulator’s guidance requires it, or if the change does not reduce the protection of Customer Personal Data. Terms §17.12 applies to other updates.

15.5 Entire agreement; counterparts. This DPA, with the Underlying Agreement, is the Parties’ entire agreement on its subject matter and may be signed in counterparts and electronically.

IN WITNESS WHEREOF, the Parties have executed this DPA by their duly authorized representatives as of the DPA Effective Date.

JEEVES INC.	[CUSTOMER LEGAL NAME]
Signature	Signature
Name: Brandon S. McGathy	Name: _____
Title: General Counsel & Secretary	Title: _____
Date: _____	Date: _____

ANNEX 1 — Description of Processing

This Annex 1 records Customer’s instructions under Section 3.2 and completes Annexes I.A and I.B of the EU SCCs.

Part A — Evaluation Phase (Sample Data)

Parties	Data exporter: Customer. Role: controller (or processor for its own customers). Data importer: Jeeves. Role: processor / service provider. Contacts: as in the Key Terms.
Subject matter and purpose	Customer's evaluation of Apex under the NDA: running Sample Data through Apex demonstrations or a guided sandbox, and scoping discussions.
Nature of Processing	Secure receipt and storage; parsing; AI-assisted matching, classification and summarization using AI Models on the Approved List (inference only); analysis; human review; de-identification under Section 6; deletion.
Categories of Data Subjects	[Customer's employees and vendor or payee contacts whose data appears in the Sample Data, in masked or de-identified form.]
Categories of personal data	[Masked bank-statement lines, ledger and invoice exports with names, contact details and account numbers removed or masked; transaction descriptions, amounts, dates and currencies.] No Prohibited Data. No End Customer data.
Sensitive data	None intended. Section 5.1 applies if received.
Volume and frequency	[One disclosure of up to ____ records, plus up to two supplemental disclosures approved by Jeeves in writing.]
Duration and retention	The Evaluation Period, then deletion under Section 12.2.
Transfer method	Encrypted transfer to a Jeeves-designated workspace. No direct access to, or credentials for, Customer Systems.
Location	United States, in the regions in Annex 3.

Part B – Production Phase

Parties	As in Part A. Where Customer instructs Jeeves on behalf of its Affiliates, each is a data exporter.
Subject matter and purpose	Providing the Services described in the Order Form: operating Apex Workflows and Agents on Customer Data, reconciliation, close and related finance processes, approvals, Forward-Deployed Services, support, and security.
Nature of Processing	Receipt and extraction from Customer Systems; storage; parsing; AI-assisted matching, classification, summarization and drafting using AI Models on the Approved List; approvals and Authorized Actions as Customer configures them; Output generation; logging; de-identification under Section 6; export and deletion.
Categories of Data Subjects	Customer's Authorized Users and other personnel; contacts at Customer's vendors, suppliers and payees; cardholders and account holders in Customer's data; and, only if a Customer-Facing Agent is designated in the Order Form, End Customers. [Complete from the data description in the Order Form.]
Categories of personal data	Identification and contact data; employer and account identifiers; transaction, invoice and payment data (merchant, payee, amount, currency, date, status); bank and ledger data, with account numbers masked where Apex does not need the full number; employee expense and payroll-related data where in scope; correspondence content; and IP address or device data in logs. [Complete from the data description in the Order Form.]
Sensitive data	None intended. Prohibited Data is excluded (Section 5.1).
Frequency	Continuous, as Customer uses the Services.
Duration and retention	The term of the Order Form plus the export and deletion periods in Section 12.1.
Location	United States, unless the Order Form states otherwise (Terms §7.9), and the regions in Annex 3.

Part C – Jeeves as independent controller

Data	Business contact and account data of Customer's Authorized Users; billing and payment records; security and access logs; Usage Data; and, for Financial Services, Customer Data (including in identifiable form) and information Jeeves and its Affiliates hold about Customer from their financial-services relationship (such as payment, card and credit performance data), to the extent the governing agreements and privacy notices permit.
Purposes	Account administration and communication; billing; security, fraud prevention and abuse detection; legal and regulatory compliance; enforcing the Underlying Agreement; analytics and improvement of the Services using Usage Data; and evaluating, underwriting, pricing, offering, monitoring and servicing credit and other financial products and services for Customer and its Affiliates ("Financial Services") under Terms §7.11, which Jeeves does only for Customer and its Affiliates and not for other customers.
Notice	Jeeves's privacy notice. Customer will inform its Authorized Users of it. The privacy notice describes the Financial Services use. Customer may opt out of use for marketing and pre-screening of offers as Terms §7.11 provides.
Legal basis; limits	Jeeves relies on Customer's authorization under Terms §7.11, performance of its contracts with Customer and its legitimate interests, and on any other basis the governing agreements and Applicable Data Protection Laws provide. Jeeves will not use Customer Personal Data for Financial Services to make credit or other decisions about an individual other than one who applies in their own right (such as a guarantor), will not disclose it in identifiable form to any other customer, and will not sell or share it.

Competent supervisory authority (EU SCCs Clause 13)

Authority	Determined under Clause 13(a) of the EU SCCs by the data exporter's establishment or representative: [____]. If the data exporter is established in Ireland, the Data Protection Commission (Ireland).
------------------	--

ANNEX 2 – Technical and Organizational Measures

Jeeves will implement at least the following measures for the systems, AI Models and personnel that Process Customer Personal Data. This Annex 2 completes Annex II of the EU SCCs.

Governance	A written information-security program approved by management with a named security lead; risk assessments at least annually; security and privacy policies reviewed annually; background screening of personnel where lawful; written confidentiality undertakings; annual security and privacy training.
Assurance	[SOC 2 Type II (Security and Confidentiality) or ISO/IEC 27001 covering in-scope systems;] independent penetration testing at least annually, with critical and high findings remediated.
Encryption	TLS 1.2 or higher for data in transit; AES-256 (or equivalent) at rest, including backups; keys held in a managed KMS or HSM with restricted access and rotation.
Tenant separation	Logical separation of each customer's data and indexes, with controls designed to prevent cross-tenant retrieval; dedicated environments only where an Order Form states so (Terms §18.6).
Access control	Single sign-on with multi-factor authentication for access to production systems; named individual accounts; least-privilege, role-based access; access reviews at least quarterly; revocation within 24 hours of a role change or departure.
Credentials and secrets	Customer System credentials held in an encrypted secrets vault, accessed by services rather than people, with read-only scopes by default and logged access.
Logging and monitoring	Logging of access to and export of production Customer Personal Data, protected against tampering and retained at least twelve (12) months, with alerting on anomalous access.
Vulnerability management	Patching of critical vulnerabilities within seven (7) days and high vulnerabilities within thirty (30) days; code and dependency scanning; secure development lifecycle and change management.
Endpoints	Company-managed devices with full-disk encryption, endpoint detection and response and automatic screen lock; no Customer Personal Data on personal devices or removable media.
AI-specific controls	Model Subprocessor accounts configured for no training and the retention in Section 4.1; customer content treated as untrusted input and kept separate from system instructions; mandatory approval steps and confidence thresholds as Terms §9.2 provides; output checks for leakage of personal data and secrets; documented model and pipeline configuration.
Forward-deployed personnel	Access to Customer environments only through Customer-provisioned accounts and as authorized under Terms §3.4; no copying of Customer Personal Data out of Customer's environment except through Apex's configured functions.
Incident response	A documented incident-response plan, tested at least annually, with escalation able to meet Section 9.
Backups and continuity	Encrypted backups purged on a rolling cycle; business-continuity and disaster-recovery plans.
Deletion	Secure deletion consistent with NIST SP 800-88 or cryptographic erasure; deletion records kept to support confirmation under Section 12.4.

Physical security	Hosting only in data centers operated by providers holding SOC 2 Type II or ISO/IEC 27001 attestations.
Subprocessor management	Security and privacy due diligence before engagement, written terms under Section 7.3, and periodic review.

ANNEX 3 — Approved Subprocessors and AI Models

This Annex 3 completes Annex III of the EU SCCs. The “Approved List” below may be updated under Section 7.2, and Jeeves will provide the information in column headings for each addition.

Subprocessor	Function	Customer Personal Data Processed	Location	Retention and training terms
[Cloud hosting provider]	Hosting and storage	All	[United States — region]	Customer data deleted under Section 12
[Model provider(s) — name, model, access route]	AI inference	Inputs needed for the Workflow	[Region]	No training; retention [zero / up to 30 days]
[Vector database / search provider]	Retrieval and indexing	Embeddings and indexes	[Region]	Deleted under Section 12
[Observability and logging provider]	Monitoring, tracing	Logs and metadata; no content unless stated	[Region]	[Retention]
[Jeeves Affiliate(s)]	Support and engineering	As needed to provide the Services	[Countries]	Customer data deleted under Section 12

ANNEX 4 — Jurisdiction-Specific Terms

EEA, UK and Switzerland. This DPA is intended to satisfy GDPR and UK GDPR Article 28(3). The Transfer Clauses in Section 11 apply as stated.

United States. This DPA is intended to satisfy the service-provider and processor contract requirements of the CCPA and of other U.S. state privacy laws, and the service-provider requirements of the Gramm-Leach-Bliley Act. Jeeves does not sell or share Customer Personal Data.

Brazil. Customer is the controller and Jeeves the operator under the LGPD. Jeeves will give Customer the information it needs to notify the ANPD and Data Subjects of a Security Incident, and Customer is responsible for those notifications.

Mexico and Colombia. Jeeves acts as encargado, in accordance with Customer's instructions, privacy notices and processing policies, and will not Process Customer Personal Data for its own purposes except as Section 6 and Part C of Annex 1 provide.

Canada and other jurisdictions. Jeeves will Process Customer Personal Data as a service provider on Customer's behalf, and the Parties will execute any additional terms Applicable Data Protection Laws require under Section 11.4.