

Data Handling Agreement

This version of the Data Handling Agreement applies only to those Customers whose Services Agreement commenced before 1 October 2026.

This Data Handling Agreement, and any applicable Schedule(s) and Annexes (together the “**Data Handling Agreement**”), forms part of, and is incorporated by reference into, the Services Agreement (as defined below), and is made between the relevant Yapily entity named on the Order Form and the Customer named on the Order Form (each as defined below) (each a “**Party**” and collectively, the “**Parties**”), and sets out the terms and conditions on which personal data will be handled in connection with the Services. The Data Handling Agreement takes effect on the Effective Date (as defined below). The Yapily group comprises of:

- (A) Yapily Ltd (company number 10842280) with registered office at 86-90 Paul Street, London, England, EC2A 4NE, United Kingdom (“**Yapily Ltd**”);
- (B) Yapily Connect Ltd (“**YC UK**”) (company number 11598433), with registered office at 86-90 Paul Street, London, England, EC2A 4NE, United Kingdom; and
- (C) Yapily Connect UAB (“**YC UAB**”) (company number 305602679) with registered office at Palangos g. 4-101, LT-01402 Vilnius, Lithuania,

each and/or collectively referred to as “**we**” or “**us**” or “**our**” or “**Yapily**”.

The Data Handling Agreement consists of the following components:

- (a) these **General Terms**, which shall apply at all times;
- (b) **Annex A** (Data Sharing Addendum), which applies where the Customer receives any of the following Services by a relevant Yapily entity:
 - i. Yapily Connect Services provided by YC UK and/or YC UAB; and/or
 - ii. the provision of an Agency arrangement by YC UK and/or YC UAB;
- (c) **Annex B** (Data Processing Addendum), which applies where the Customer receives any of the following Services by a relevant Yapily entity:
 - i. Technology Services provided by Yapily Ltd;
 - ii. Support Services provided by Yapily Ltd;
 - iii. Implementation Services provided by Yapily Ltd;
 - iv. Access to the Yapily Data Product Suite [provided by Yapily Ltd]; and/or
 - v. Access to the Yapily Payments Product Suite [provided by Yapily Ltd].

Where the Customer receives different Services by more than one Yapily entity, both the DSA and the DPA may apply, each in respect of the relevant Yapily entity and the relevant activities it carries out.

GENERAL TERMS

1 Definitions and Interpretation

1.1 In this Data Handling Agreement, unless the context otherwise requires:

- (a) **Agreement** means the Order Form(s) and the Services Agreement, made between the relevant Yapily entity and the Customer named on the Order Form, and sets out the terms and conditions under which the Customer shall receive the Services (as defined in the applicable Order Form) from time to time.

- (b) **Customer** means the entity named on the Order Form that is party to the Services Agreement with the relevant Yapily entity and that, in connection with the Services, discloses personal data to, or receives personal data from, that Yapily entity.
- (c) **Data Protection Legislation** means: (a) to the extent the UK GDPR applies, all applicable data protection and privacy legislation in force from time to time in the United Kingdom, including the UK GDPR, the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and (b) to the extent the EU GDPR applies, the General Data Protection Regulation (EU) 2016/679, Directive 2002/58/EC on privacy and electronic communications (as amended, including by Directive 2009/136/EC) and any national legislation implementing it, and all other applicable data protection and privacy legislation of any member state of the EU to which either Party is subject.
- (d) **EEA** means the European Economic Area.
- (e) **EU GDPR** means the General Data Protection Regulation (Regulation (EU) 2016/679), as amended or replaced from time to time.
- (f) **EU** means the European Union.
- (g) **ICO** means Information Commissioner's Office.
- (h) **Order Form** means a Yapily order form agreed between and signed by the Parties setting out the Services and commercial particulars thereof, including the identity of the contracting Yapily entity, the Effective Date, the term, and the fees payable, and incorporating the terms of this Data Handling Agreement and the Services Agreement.
- (i) **Privacy Policy** means the Yapily Privacy Policy available at <https://www.yapily.com/legal/privacy-policy>.
- (j) **Services** means the services to be provided by the relevant Yapily entity to the Customer under the Services Agreement, as identified and described in the applicable Order Form.
- (k) **Services Agreement** means the services agreement entered into between the Customer and the relevant Yapily entity for the provision of the Services, comprising the Order Form and any terms and conditions identified in, or incorporated by reference in, the Order Form.
- (l) **Sub-processors** means the list of active Yapily data subprocessors available at www.yapily.com/legal/subprocessors.
- (m) **UK GDPR** has the meaning given in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

1.2 General

- (a) The terms **controller, processor, data subject, personal data, process or processing, data protection impact assessment, special categories of personal data** and **appropriate technical and organisational measures** have the meanings given to them in the UK GDPR.
- (b) Any terms not defined under this Data Handling Agreement shall have the meaning given under the Services Agreement.

- (c) A reference to legislation or a legislative provision includes all subordinate legislation made from time to time under that legislation or legislative provision.
- (d) Words in the singular include the plural and vice versa.
- (e) A reference to writing or written includes email.
- (f) Clause headings do not affect interpretation.

1.3 Order of priority

In the case of conflict or ambiguity between the components of the Agreement, the following order of precedence shall apply (in descending order), save that, in respect of indemnities and limitation of liability, the position set out in clause 1.4 (Relationship with the Services Agreement) below shall apply:

- (a) this Data Handling Agreement;
- (b) the Order Form; and
- (c) the Services Agreement.

1.4 Relationship with the Services Agreement; Replacement of Previous Data Protection Terms

- (a) This Data Handling Agreement replaces and supersedes in full any data processing agreement, data protection addendum or equivalent data protection terms previously entered into by the Parties or incorporated by reference into the Order Form or the Services Agreement, all of which shall cease to have effect from the Effective Date.
- (b) Any reference in the Services Agreement or the Order Form to the 'DPA', the 'Data Processing Agreement' or equivalent data protection terms shall be read as a reference to this Data Handling Agreement.
- (c) The indemnity and limitation of liability provisions of the Services Agreement apply to this Data Handling Agreement, and to any breach of it, in the same manner and to the same extent as they applied to the data protection terms that this Data Handling Agreement replaces.

2 Notices

2.1 Any notice given to a Party under or in connection with this Data Handling Agreement shall be in writing and shall be:

- (a) delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or
- (b) sent by email to the email address provided by the Customer and Yapily in the Order Form between the parties.

3 General

3.1 No Partnership or Agency

Nothing in this Data Handling Agreement establishes any partnership, joint venture, or agency relationship between the Parties.

3.2 Roles and Status of the Parties

The description of a Party as a controller, processor or sub-processor in this Data Handling Agreement reflects only the role that Party performs in respect of the specific processing carried out in connection with the relevant Services, as determined by the Data Protection Legislation. It does not alter the Parties' respective roles, rights or responsibilities in respect of any personal data outside the scope of this Data Handling Agreement (as applicable).

Where a Yapily entity acts as a controller in respect of any personal data under this Data Handling Agreement, this does not affect, limit or diminish the Customer's own status as a controller of that personal data in its own right (as may be applicable), or the Customer's rights and responsibilities in respect of that personal data in its own capacity outside the scope of this Data Handling Agreement.

3.3 Variation

Yapily may update this Data Handling Agreement from time to time to reflect changes in applicable law or regulatory guidance, or changes to the Services. Yapily shall notify the Customer of any material changes not less than thirty (30) days in advance of the change taking effect. The Customer's continued use of the Services following the effective date of a variation constitutes acceptance of the updated Data Handling Agreement.

3.4 Severance

If any provision (or part-provision) of this Data Handling Agreement is or becomes invalid, illegal, or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision (or part-provision) shall be deemed deleted. Any modification to or deletion of a provision (or part-provision) under this clause shall not affect the validity and enforceability of the rest of this Data Handling Agreement.

3.5 Waiver

No failure or delay by a Party to exercise any right or remedy provided under this Data Handling Agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy shall prevent or restrict the further exercise of that or any other right or remedy. A waiver of any right or remedy under this Data Handling Agreement is only effective if given in writing.

3.6 Third Party Rights

No person other than the Parties to this Data Handling Agreement shall have any right to enforce any provision of this Data Handling Agreement under the Contracts (Rights of Third Parties) Act 1999. This does not affect any right or remedy of a data subject that exists or is available under the Data Protection Legislation.

3.7 Entire Agreement

The Agreement constitutes the entire agreement between the Parties in relation to its subject matter and supersede all previous agreements, understandings, and arrangements between the Parties, whether written or oral, relating to that subject matter. Each Party acknowledges that, in entering into the Agreement, it does not rely on, and shall have no remedies in respect of, any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in the Agreement. Nothing in this clause shall limit or exclude any liability for fraud or fraudulent misrepresentation.

3.8 Governing Law

This Data Handling Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

3.9 Jurisdiction

Each Party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Data Sharing Agreement or its subject matter or formation.

ANNEX A – YAPILY DATA SHARING ADDENDUM

1 Background

- 1.1 This Data Sharing Addendum (“**DSA**”) applies where the Customer receives any of those Services set out in the preamble of the General Terms that apply in relation to this Annex A from any relevant Yapily entity, and sets out the terms on which Yapily and the Customer each acts as independent controllers in respect of personal data shared between them in connection with the provision of the Services under the Services Agreement.
- 1.2 This DSA is an addendum to the Order Form entered into between the Customer and Yapily, and to any renewal or replacement Order Form entered into between the same Parties. On signing the Order Form, the Parties accept the terms and conditions set out in this DSA.
- 1.3 This DSA does not address processing where a Yapily entity acts as processor or sub-processor on behalf of the Customer under the Agreement. Where applicable, such processing is governed by the DPA.
- 1.4 Capitalised terms used but not defined in this DSA have the meanings given to them in the General Terms.

2 Definitions and Interpretation

- 2.1 In this DSA, unless the context otherwise requires:

- (a) **Agreed Purposes** means the purposes described in clause 3.2.
- (b) **Data Plus** means Yapily's transaction categorisation product, comprising (i) the categorisation of, and derivation of insights from, transaction data provided to the relevant PSU as part of the service that PSU has requested; and (ii) the training, maintenance and improvement of the artificial intelligence model underlying the product, using such transaction data (including in anonymised form) for the purpose of providing the categorisation and related insights to the relevant PSU as part of the Open Banking Service that PSU has requested.
- (c) **Open Banking Services** comprise Yapily's regulated Account Information Services (“**AIS**”) and Payment Initiation Services (“**PIS**”), provided via Yapily's proprietary API. These services involve the retrieval and delivery of account information and the initiation of payments on behalf of PSUs, in accordance with applicable payment services regulation.
- (d) **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Shared Personal Data.
- (e) **PSU** means a payment service user whose Personal Data is shared under this DSA.

- (f) **Shared Personal Data** means the Personal Data shared between the parties under clause 5.
- (g) **Supervisory Authority** means the Information Commissioner's Office (ICO) in the UK, the State Data Protection Inspectorate in Lithuania or such other relevant supervisory authority in the territories where the parties to this DSA are established.
- (h) **Value Added Services** or **VAS** comprise additional data-driven services offered by Yapily to the Customer, which may include (without limitation): seamless return-user and checkout experiences; pre-filled onboarding; credit, affordability, and risk scoring; enhanced transaction data and notifications; verified identity and federated login; fraud detection improvements; and other AI and data products.

3 Purpose and Scope

3.1 Relationship of the Parties

- (a) Each Party is an independent controller in respect of its own processing of Shared Personal Data. Nothing in this DSA creates a joint controllership arrangement between them.
- (b) Each Party shall independently determine the purposes and means of its own processing of the Shared Personal Data it receives, subject to the restrictions set out in this DSA.

3.2 Agreed Purposes

- (a) The Customer discloses personal data to Yapily for the following purposes:
 - i. To enable Yapily to meet its legal and regulatory obligations, such as performing KYC or AML checks on PSUs;
 - ii. to enable Yapily to provide Services such as the Open Banking Services to the Customer;
 - iii. the delivery and enhancement of Yapily Services, including Open Banking Services, Value Added Services and Data Plus, subject to 3.2(b)(ii) below.
 - iv. such other purposes as may be agreed in writing between the parties from time to time.
- (b) Yapily may use the Customer's personal data for the following purposes:
 - i. To comply with its own legal and regulatory obligations, such as to perform KYC or AML checks on PSUs.
 - ii. The delivery and enhancement of the Services, including Value Added Services and Data Plus, subject to the PSU having consented to such use when agreeing to receive the Open Banking Services in accordance with relevant requirements under applicable payment services regulations;
 - iii. Providing and improving scoring, risk assessment, verification, or notification outputs delivered to Yapily customers; and

- iv. Any other purposes as may be agreed in writing between the parties from time to time.
- (c) Neither Party shall process Shared Personal Data in a way that is incompatible with the Agreed Purposes set out above.

4 Compliance with national Data Protection Legislation

- 4.1 Each Party must ensure compliance with applicable Data Protection Legislation at all times during the term of this DSA.
- 4.2 Each Party has such valid registrations and has paid such fees as are required by the ICO or its national Supervisory Authority which, by the time that the data sharing is expected to commence, covers the intended data sharing pursuant to this DSA, unless an exemption applies.
- 4.3 Each Party shall ensure that it has legitimate grounds under the Data Protection Legislation for the disclosure and use of the Shared Personal Data for the Agreed Purposes set out above, including but not limited to, providing any required notices and obtaining any required consent.

5 Shared Personal Data

5.1 Categories of Shared Personal Data

- (a) The following categories of personal Data may be shared by the Customer with Yapily (and by Yapily back to the Customer where applicable as part of Service outputs):
 - i. PSU identity data, including name, email address, phone number, home address, and date of birth;
 - ii. banking and account data, including account identifiers, bank selection, account metadata, and transaction history;
 - iii. payment data, including transaction amounts, dates, merchant references, and payment metadata;
 - iv. device and authentication data, including device tokens, passkey credentials, and session identifiers;
 - v. derived data, including risk scores, affordability assessments, fraud signals, enriched transaction data, and verification status; and
 - vi. such other categories of personal data as may be specified in the Services Agreement or notified to the Customer by Yapily in connection with new or updated Value Added Services.

5.2 Special Categories of Personal Data

- (a) The Parties do not intend to share special categories of personal data under this DSA. However, the Parties acknowledge that special categories of personal data may be

incidentally present within transaction data or other Shared Personal Data (for example, where spending patterns could reveal information about health, religion, or political views).

- (b) Where either Party becomes aware that special categories of personal data are being processed, it shall notify the other Party and the Parties shall cooperate to ensure that appropriate safeguards are in place, including obtaining explicit consent from the relevant PSUs where required.

5.3 Data Minimisation

The Shared Personal Data must not be irrelevant or excessive with regard to the Agreed Purposes. Each Party shall ensure that it only shares or processes personal data that is adequate, relevant, and limited to what is necessary to achieve the Agreed Purposes.

5.4 Transparency

Each Party shall ensure that it provides clear and sufficient information to data subjects, in accordance with the Data Protection Legislation, regarding:

- i. the purposes for which it will process their personal data;
- ii. the legal basis for such processing;
- iii. the categories of recipients to whom personal data may be disclosed; and
- iv. such other information as is required by the Data Protection Legislation.

The Customer shall ensure that PSUs are made aware, at or before the point of data collection, that their personal data will be shared with Yapily and may be used in connection with the Value Added Services, including by providing a link to or reference to the Privacy Policy where appropriate.

5.5 Consent Management

- (a) Where the lawful basis for Yapily's processing is PSU consent, Yapily shall be responsible for obtaining, recording, and managing such consent (including withdrawal of consent) in accordance with the requirements of the Data Protection Legislation.
- (b) Where the lawful basis for the Customer's disclosure of personal data to Yapily is PSU consent, the Customer shall be responsible for obtaining, recording, and managing such consent (including withdrawal of consent) in accordance with the requirements of the Data Protection Legislation, and shall promptly notify Yapily where any such withdrawal affects Yapily's authority to process the relevant Personal Data.
- (c) The Customer shall provide reasonable cooperation to Yapily in facilitating the collection of consent from PSUs, including by integrating consent mechanisms into its user journey where reasonably requested by Yapily.
- (d) Where a PSU withdraws consent via notifying the Customer, Customer shall promptly notify Yapily of the same and Yapily shall cease the relevant processing without undue delay.

6 Data Quality

- 6.1 The Customer shall use reasonable endeavours to ensure that the personal data it shares with Yapily is accurate and up to date at the point of sharing.
- 6.2 Where either Party becomes aware that Shared Personal Data is inaccurate or incomplete, it shall notify the other Party without undue delay.
- 6.3 Yapily shall not be liable for any inaccuracy in Service outputs to the extent that such inaccuracy results from inaccurate or incomplete personal data provided by the Customer or by the PSU.

7 Data Subjects' Rights

- 7.1 Each Party shall be responsible for responding to data subject access requests and other data subject rights requests in respect of the personal data for which it is controller, in accordance with the Data Protection Legislation.
- 7.2 Where a Party receives a request from a PSU or other data subject that relates (in whole or in part) to the other Party's processing, it shall notify the other Party without undue delay and provide reasonable cooperation to enable the other Party to respond within the applicable time limits.
- 7.3 Each Party shall be responsible for maintaining a record of data subject rights requests that relate to the Shared Data. Such records must include copies of the request for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request. This information shall be provided to the other Party when providing a notification in accordance with clause 7.2 above.
- 7.4 Each Party shall maintain appropriate mechanisms to enable PSUs to exercise their rights under the Data Protection Legislation in respect of personal data processed by Yapily, including (where applicable) the right to erasure, the right to data portability, and the right to object to processing.

8 Data Retention and Deletion

- 8.1 Subject to clause 8.2, each Party shall not retain Shared Personal Data for longer than is necessary for the Agreed Purposes, subject to any applicable statutory or regulatory retention obligations.
- 8.2 Notwithstanding clause 8.1 and the expiry or termination of this DSA, the Services Agreement, or any individual Service, Yapily may retain Shared Personal Data for such period as Yapily, acting reasonably, considers necessary for any one or more of the following purposes:
 - (a) performing its obligations under the Services Agreement or any related or successor arrangement between the Parties;

- (b) complying with applicable legal, regulatory, or professional obligations, including (without limitation) record-keeping obligations under payment services regulation, anti-money laundering, tax, accounting, and other financial services or sector-specific requirements;
- (c) establishing, exercising, or defending legal claims, including for the duration of any applicable limitation period and any reasonable period thereafter to allow for late-discovered or threatened claims;
- (d) maintaining audit trails, internal records, and management information required by applicable regulation or by Yapily's internal governance, risk management, or compliance policies;
- (e) responding to requests, investigations, or enquiries from regulators, courts, law enforcement, or other competent authorities;
- (f) protecting against, investigating, and preventing fraud, financial crime, security incidents, and other unlawful activity;
- (g) the delivery and enhancement of the Open Banking Services, the Value Added Services and any outputs generated in connection with the delivery of those services; and
- (h) the delivery and enhancement of the Value Added Services and of Data Plus, in each case only where and to the extent permitted under clause 3.2.

8.3 In respect of any Shared Personal Data retained by Yapily under clause 8.2, Yapily shall act as an independent controller and shall be solely responsible for determining the purposes and means of, and for its compliance with applicable Data Protection Legislation in connection with, such retained data. Yapily shall:

- (a) maintain an appropriate lawful basis under Article 6 of the UK GDPR (and, where applicable, a condition under Article 9) for each retention purpose it relies on;
- (b) ensure that its own privacy information made available to data subjects adequately reflects, in accordance with Articles 13 and 14 of the UK GDPR, the retention purposes and the periods (or criteria) applied; and
- (c) continue to apply appropriate technical and organisational security measures, having regard to the nature of the retained data and the purposes of retention.

8.4 On expiry or termination of this DSA, the Services Agreement, or any individual Service (as applicable), and save to the extent retention is permitted under clause 8.2, Yapily shall, at its election, delete, anonymise, archive, or otherwise restrict access to the relevant Shared Personal Data within a reasonable period.

8.5 Where personal data has been genuinely and irreversibly anonymised such that it no longer constitutes personal data, such anonymised data may be retained and used by Yapily without restriction and for any purpose, including (without limitation) analytics, benchmarking, product development, and the training and improvement of models and services.

- 8.6 The Customer acknowledges and agrees that retention by Yapily in accordance with clause 8.2 is a legitimate and necessary feature of Yapily's business and shall not, of itself, give rise to any claim, liability, or remedy against Yapily under this DSA, provided that Yapily complies with clause 8.3.

9 International Transfers

- 9.1 Where either Party transfers Shared Personal Data outside the United Kingdom or the EEA, it shall ensure that appropriate safeguards are in place in accordance with the Data Protection Legislation, including (where applicable): (a) transfer to a country or territory recognised as providing an adequate level of protection; (b) use of standard contractual clauses adopted or approved by the relevant authority; (c) binding corporate rules; or (d) any other valid transfer mechanism or applicable derogation under the Data Protection Legislation.
- 9.2 Yapily may transfer Shared Personal Data to Sub-processors located outside the United Kingdom or EEA for the purposes of providing the Services, provided that Yapily ensures appropriate safeguards are in place in accordance with clause 9.1.

10 Security

- 10.1 Each Party shall implement and maintain appropriate technical and organisational measures to protect the Shared Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration, or disclosure.
- 10.2 Such measures shall be appropriate to the nature, scope, context, and purposes of the Processing, the state of the art, the costs of implementation, and the risks to data subjects, and shall include (where appropriate):
- (a) pseudonymisation and encryption of personal data;
 - (b) measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems;
 - (c) measures to restore access to personal data in a timely manner following an incident; and
 - (d) regular testing and evaluation of the effectiveness of security measures.

- 10.3 Each Party shall ensure that its personnel who have access to Shared Personal Data are subject to appropriate confidentiality obligations (whether contractual or statutory) and have received appropriate training in data protection.

11 Personal Data Breaches

- 11.1 Each Party shall notify the other Party without undue delay via the details provided under the notice provisions of the Services Agreement upon becoming aware of a Personal Data Breach involving the Shared Personal Data.

- 11.2 Such notification shall include, to the extent available:

- (a) a description of the nature of the breach;
- (b) the categories and approximate number of data subjects affected;
- (c) the likely consequences of the breach; and
- (d) the measures taken or proposed to address the breach and mitigate its effects.

- 11.3 Each Party shall comply with its own obligations to report a Personal Data Breach to the ICO, any relevant Supervisory Authority, and (where applicable) affected Data Subjects in accordance with the Data Protection Legislation.
- 11.4 The Parties shall cooperate in good faith and agree to provide reasonable assistance to investigate, remediate, and mitigate the effects of any Personal Data Breach involving the Shared Personal Data.
- 11.5 Notification of a Personal Data Breach under this clause shall not be construed as an acknowledgement of fault or liability by the notifying Party.

12 Sub-processing and Onward Sharing

- 12.1 Yapily may engage processors to process Shared Personal Data on its behalf for the purposes of providing the Services, provided that Yapily: (a) enters into a written agreement with each processor that complies with the requirements of Article 28 UK GDPR and Article 28 EU GDPR (to the extent applicable); and (b) remains liable to the Customer for the acts and omissions of its processors.
- 12.2 The Customer shall not disclose or onward share any Personal Data received from Yapily (including Service outputs containing Personal Data) to any third party, except: (a) where necessary for the Customer's own legitimate business purposes as an independent Controller; (b) in compliance with the Data Protection Legislation; and (c) subject to the Customer ensuring that the third party recipient is bound by appropriate data protection obligations.

13 Automated Decision-Making

- 13.1 Certain Value Added Services may involve automated profiling or the generation of scores, assessments, or flags relating to PSUs. Where Yapily makes solely automated decisions that produce legal effects or similarly significant effects on PSUs in the course of providing the Services, Yapily shall: (a) ensure that it has a valid lawful basis for such automated decision-making under Article 22 UK/EU GDPR; (b) provide PSUs with meaningful information about the logic involved; and (c) implement appropriate safeguards, including the right to object or obtain human intervention, express a point of view, and contest the decision.
- 13.2 Where the Customer uses Service outputs containing personal data (including risk scores, affordability assessments, or verification data) as the basis for automated decision-making that produces legal effects or similarly significant effects on data subjects, the Customer shall be solely responsible for compliance with Article 22 UK/EU GDPR, including the provision of meaningful information to data subjects and the implementation of the right to object and the right to human review.

14 Compliance and Cooperation

- 14.1 Each Party shall comply with all applicable Data Protection Legislation in its processing of the Shared Personal Data.

14.2 In the event that the data protection requirements of the United Kingdom and the EU conflict, the Parties shall apply the standard that provides the higher level of protection to data subjects.

14.3 Each Party shall provide reasonable cooperation and assistance to the other Party in connection with:

- (a) the conduct of data protection impact assessments where required by the Data Protection Legislation;
- (b) consultations with the ICO or any relevant Supervisory Authority; and
- (c) the handling of complaints from data subjects or regulatory authorities.

15 Warranties

15.1 Each Party warrants that it will:

- (a) process the Shared Personal Data in compliance with all applicable Data Protection Legislation;
- (b) maintain all necessary registrations and fee payments with the ICO and any relevant Supervisory Authority;
- (c) respond to data subject rights requests in accordance with the Data Protection Legislation; and
- (d) maintain appropriate technical and organisational security measures in accordance with clause 10.

- 15.2 The Customer warrants that it is entitled to share the relevant Personal Data with Yapily and that it has provided (or will provide) all necessary transparency information to Data Subjects in accordance with clause 5.4.
- 15.3 Yapily warrants that it will process the Shared Personal Data for the Agreed Purposes and in accordance with this DSA and its Privacy Policy.
- 15.4 Except as expressly stated in this DSA, all warranties, conditions, and terms, whether express or implied by statute, common law, or otherwise, are excluded to the greatest extent permitted by law.

16 Term and Termination

- 16.1 This DSA shall commence on the date on which the Customer first uses any Service under the Services Agreement and shall continue for the duration of the Services Agreement, unless terminated earlier in accordance with this clause 16.1.
- 16.2 This DSA shall automatically terminate upon termination or expiry of the Services Agreement.
- 16.3 On termination of this DSA, the provisions of clause 8 (Data Retention and Deletion) shall apply.
- 16.4 Termination of this DSA shall not affect any rights, obligations, or liabilities that have accrued prior to termination.

17 Dispute Resolution

- 17.1 In the event of a dispute, complaint, or claim brought by a data subject or a Supervisory Authority concerning the processing of Shared Personal Data, the Parties shall inform each other in writing and cooperate in good faith with a view to resolving the matter.
- 17.2 Each Party shall abide by the decision of a competent court or competent supervisory authority in relation to the processing of Shared Personal Data.

ANNEX B – Data Processing Addendum

1. Background

- 1.1. This Data Processing Addendum (“**DPA**”) applies where the Customer receives any of those Services set out in the preamble of the General Terms that apply in relation to this Annex B from a relevant Yapily entity, and sets out the terms on which the Customer, as either, a data controller in its own right or as a data processor for a Customer sub-client, appoints Yapily, as data processor or a sub-processor (as applicable) and the purposes for which Yapily will process personal data when providing the Services under the Services Agreement. This DPA contains the mandatory clauses required by Article 28(3) of the UK GDPR and Article 28(3) of the EU GDPR.
- 1.2. This DPA is an addendum to that Order Form entered into between the Customer and Yapily, and to any renewal or replacement Order Form(s) entered into between the same Parties. On signing the Order Form, the Parties accept the terms and conditions set out in this DPA.
- 1.3. This DPA does not address where a Yapily entity acts as data controller in respect of personal data that it collects for its own legal or contractual requirements falling outside of the scope of the Agreement. Where applicable, this will be covered via a Data Sharing Addendum.
- 1.4. Capitalised terms used but not defined in this DPA have the meanings given to them in the General Terms.

2. INTERPRETATION

- 2.1. Capitalised terms used in this DPA shall have the following meanings:
 - 2.1.1. **IDTA** means the International Data Transfer Agreement or such alternative transfer agreements as may be approved by the UK ICO from time to time.
 - 2.1.2. **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by Yapily or any Sub-processor.
 - 2.1.3. **Standard Contractual Clauses** or **SCCs** means those clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as approved by the European Commission in Implementing Decision (EU) 2021/914 of 4 June 2021, or any set of clauses approved by the European Commission which amends, replaces or supersedes them.
 - 2.1.4. **Sub-processor** means any data processor Yapily (including any affiliate of Yapily) appointed by Yapily to process personal data on behalf of Customer available at www.yapily.com/legal/subprocessors.

3. Processing of Personal Data

- 3.1. The Customer as a controller shall, in its use of the Services, process personal data in accordance with the requirements of Data Protection Legislation, including any applicable requirement to provide notice to data subjects of the use of Yapily as processor (including where the Customer is a processor, by ensuring that the ultimate Customer does so).

- 3.2. The Customer's instructions for the processing of personal data shall comply with Data Protection Legislation. The Customer shall have sole responsibility for the accuracy, quality, and legality of personal data and how the Customer acquired the personal data. The Customer specifically acknowledges and agrees that its use of the Services will not violate the rights of any data subject, including those that have opted-out from sales or other disclosures of personal data.
- 3.3. Unless otherwise required by the Data Protection Legislation, Yapily shall only process the personal data in accordance with the Customer's instructions unless the processing is otherwise required by applicable law to which Yapily is subject, in which case the relevant entity shall to the extent permitted by such law inform Customer of that legal requirement before processing that personal data.
- 3.4. The subject matter of the processing of the Customer's personal data by Yapily is to provide certain Services pursuant to the Agreement. The duration of the processing, the nature and purpose of the processing, the types of personal data and categories of data subjects processed under this DPA are further specified in the Privacy Policy.

4. DURATION

- 4.1. This DPA will remain in full force and effect for so long as:
 - 4.1.1. the Services Agreement is in place; or
 - 4.1.2. Yapily otherwise retains any personal data related to the Agreement in its possession or control.

5. SECURITY

- 5.1. Yapily shall implement appropriate technical and organisational measures to protect against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the personal data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of personal data including, but not limited to, the security measures set out in Schedule 1.

6. PROCESSING OF THE PERSONAL DATA

- 6.1. The subject matter, duration, nature and purpose of processing, the personal data types and data subject categories in respect of which Yapily may process in accordance with this DPA are set out in the Privacy Policy.
- 6.2. Unless otherwise required by the Data Protection Legislation, Yapily shall only process the personal data in accordance with the Customer's instructions unless the processing is otherwise required by applicable law to which Yapily is subject, in which case Yapily shall to the extent permitted by such law inform the Customer of that legal requirement before processing that personal data.

7. SUB-PROCESSING

7.1. Subject to the following, Yapily shall not engage any Sub-processor to process personal data other than with the prior specific or general written authorisation of the Customer. At the Effective Date, the Customer confirms the following:

7.1.1. Where YC UK or YC UAB acts as processor then Yapily Ltd is appointed as Sub-processor.

7.1.2. Yapily has the Customer's written authorisation for Yapily to engage the Sub-processors..

7.1.3. For any Sub-processor outside the scope of 7.1.1 and 7.1.2 above, Yapily shall request the Customer's written authorisation in advance, providing the name, role and country of establishment of the proposed Sub-processor. The Customer shall respond within fifteen (15) business days; if the Customer does not respond within that period, the Sub-processor shall be deemed approved. If Customer raises an objection within the five (5) working-day period, the Parties shall enter into good faith discussions to find a mutually acceptable resolution. If no resolution is achieved within fifteen (15) working days of the original notification, Yapily reserves the right to terminate the Agreement immediately.

7.2. Once a Sub-processor is authorised, Yapily may engage that Sub-processor as soon as a written agreement is in place that imposes data protection obligations on the Sub-processor no less protective than those set out in this DPA.

7.3. With respect to each Sub-processor, Yapily shall:

7.3.1. include terms in the contract between Yapily and Sub-processor which are no less restrictive than those set out in this DPA; and

7.3.2. remain fully liable to Customer for any failure by each Sub-processor to fulfil its obligations in relation to the processing of any personal data.

8. INTERNATIONAL TRANSFERS

Yapily shall not transfer personal data outside the UK and/or EEA unless it has ensured appropriate safeguards are in place which may include entering into Standard Contractual Clauses, the IDTA or Addendum and where applicable incorporate such terms into the contract between Yapily and Sub-processor to ensure the adequate protection of the transferred personal data, or such other arrangement as Yapily may reasonably determine as providing adequate protection in respect of the processing of personal data in such third country.

9. DATA SUBJECT RIGHTS

Yapily shall, without undue delay, notify the Customer if it receives a request from a data subject under any Data Protection Legislation in respect of their personal data and shall provide reasonable assistance to enable the Customer to fulfil any of its obligations to its data subjects.

10. INCIDENT MANAGEMENT

10.1. Yapily shall promptly notify the Customer via the email addresses provided at clause 14 if there is a suspected or actual data breach in relation to the Customer's personal data.

10.2. Such notification shall, to the extent then known, include:

10.2.1. the nature of the Personal Data Breach, including the categories and approximate number of data subjects and records concerned;

10.2.2. the likely consequences of the breach;

10.2.3. the measures taken or proposed to address the breach and to mitigate its possible adverse effects; and

10.2.4. the name and contact details of the data protection contact point at Yapily.

10.3. Where, and insofar as, it is not possible to provide all such information at once, the information shall be provided to the Customer as it becomes available without further undue delay.

11. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

11.1. Yapily shall, at the Customer's reasonable written request and taking into account the nature of the processing and information available to Yapily, provide reasonable assistance with meeting the Customer's compliance obligations under the Data Protection Legislation, including responding to:

11.1.1. a data protection impact assessments required under Data Protection Legislation; and

11.1.2. a consultation with the UK ICO or the State Data Protection Inspectorate of the Republic of Lithuania.

12. DELETION OR RETURN OF CUSTOMER PERSONAL DATA

12.1. Yapily shall, as soon as reasonably practicable after receipt of a written request from the Customer to do so following termination of the Agreement, either:

12.1.1. return a complete copy of all personal data processed by Yapily to the Customer; or

12.1.2. delete all copies of personal data processed by Yapily unless it is required to retain the same by applicable law or internal policy.

Where Yapily retains any personal data the terms of this DPA shall continue to apply in accordance with clause 3 and Yapily shall not use the personal data for any other purpose that the scope of this DPA.

13. AUDIT RIGHTS

Yapily shall make available to the Customer on reasonable written request all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections conducted by the Customer or a third party auditor mandated and professionally appointed by the Customer provided such audit only includes premises where Yapily processes personal data in which case this shall only take place during business hours, on reasonable prior notice. Any such audits shall be limited to once per calendar year and shall be carried out with professionalism and with as little disruption to Yapily's business as possible.

Schedule 1 - Technical and Organisational Security Measures

Yapily implements the following technical and organisational measures, proportionate to the risk of the processing under the Agreement, to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access:

1. Access control

- Multi-factor authentication (“**MFA**”) on the systems used by Yapily to access the Customer’s personal data, where MFA is supported by the relevant system.
- Access to the Customer’s Salesforce environment is granted only to named individuals approved by the Customer, on a least-privilege basis.
- Unique user IDs for personnel and Sub-processors; no shared credentials.
- Access rights are revoked promptly when personnel or Sub-processors no longer require access.

2. Encryption

- Full-disk encryption on workstations and laptops used to access personal data.
- Encrypted connections (TLS 1.2 or higher) for data in transit.
- Credentials stored in a reputable password manager.

3. Personnel and confidentiality

- Personnel and Sub-processors are bound by written confidentiality undertakings no less protective than those set out in the Agreement and this DPA.
- Workstations are locked when unattended.

4. Data minimisation

- Personal data of the Customer is processed within the Customer’s own environment; Yapily does not maintain independent operational copies of the Customer’s personal data outside that environment.
- Where temporary exports or downloads are required for a specific task, they are deleted as soon as the task is completed.

5. Incident response

- Yapily notifies the Customer of any Personal Data Breach in accordance with the terms of this DPA.

6. Business continuity

- Yapily does not act as the primary data store for the Customer’s personal data; backup, recovery and availability of Salesforce data remain the responsibility of the Customer and the underlying service providers.