WorXflo Data Processing Addendum

Last Updated: 05 February 2026

Controller: Stidston Limited, company number 13242441, whose registered office address is 43 Merchant Gate, Bedford, Bedfordshire, England MK40 1AS, trading as **WorXflo**

Contact: legal@worxflo.com

This Data Processing Addendum (the **Addendum**) forms part of the WorXflo Terms and Condition (and any related documentation), as amended from time to time (the **Master Agreement**), between you (the Customer) and WorXflo.

All capitalised terms not defined in this Addendum have the meaning set out in the Master Agreement.

Background

(A) The Customer and the Supplier entered into the **Master Agreement** that may require the Supplier to process Personal Data on behalf of the Customer.

(B) This Addendum sets out the additional terms, requirements and conditions on which the Supplier will process Personal Data when providing services under the Master Agreement. This Addendum contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) for contracts between controllers and processors.

AGREED TERMS

1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this Addendum.

1.1 Definitions:

Authorised Persons: the persons or categories of persons that the Customer authorises to give the Supplier written personal data processing instructions as identified by the Customer in writing from time to time and from whom the Supplier agrees solely to accept such instructions.

Business Purposes: the services to be provided by the Supplier to the Customer as described in the Master Agreement and any other purpose specifically identified in ANNEX A.

Commissioner: the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing: have the meanings given in the Data Protection Legislation.

Controller: has the meaning given in section 6, DPA 2018.

Data Protection Legislation:

a) To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of Personal Data.

b) To the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Customer or The Supplier is subject, which relates to the protection of Personal Data.

Data Subject: the identified or identifiable living individual to whom the Personal Data relates.

EU GDPR: the General Data Protection Regulation ((EU) 2016/679).

EEA: the European Economic Area.

Personal Data: means any information relating to an identified or identifiable living individual that is processed by the Supplier on behalf of the Customer as a result of, or in connection with, the provision of the services under the Master Agreement; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Processing, processes, processed, process: any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third-parties.

Personal Data Breach: a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

Records: has the meaning given in Clause 12.

Resellers: Independent third-party organisations authorised to resell licences or subscriptions to the Supplier's services. Resellers act as independent controllers, not sub-processors. Any personal data they share with the Supplier for licence provisioning or account setup is processed by the Supplier as a controller, not under this Addendum.

Term: this Addendum's term as defined in Clause 10.

UK GDPR: has the meaning given in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

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

1.3 The Annexes form part of this Addendum and will have effect as if set out in full in the body of this Addendum. Any reference to this Addendum includes the Annexes.

1.4 A reference to writing or written excludes fax but not email.

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Addendum and any provision contained in the Annexes, the provision in the body of this Addendum will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this Addendum and any provision contained in the Annexes, the provision contained in the Annexes will prevail; and

(c) any of the provisions of this Addendum and the provisions of the Master Agreement, the provisions of this Addendum will prevail.

2. Personal data types and processing purposes

2.1 The Customer and the Supplier agree and acknowledge that for the purpose of the Data Protection Legislation:

(a) the Customer is the Controller and the Supplier is the Processor.

(b) the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and

obtaining any required consents, and for the written processing instructions it gives to the Supplier.

(c) ANNEX A describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Supplier may process the Personal Data to fulfil the Business Purposes.

2.2 **Reseller clarification:** Resellers may provide the Supplier with limited customer contact details for licence provisioning. Such data is processed by the Supplier as a controller, not under this Addendum. This Addendum applies only to Customer Personal Data processed inside the SaaS platform on behalf of the Customer.

3. Supplier's obligations

3.1 The Supplier will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions from Authorised Persons. The Supplier will not process the Personal Data for any other purpose or in a way that does not comply with this Addendum or the Data Protection Legislation. The Supplier must promptly notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation.

3.2 The Supplier must comply promptly with any Customer written instructions requiring the Supplier to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 The Supplier will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third-parties unless the Customer or this Addendum specifically authorises the disclosure, or as required by domestic or EU law, court or regulator (including the Commissioner). If a domestic or EU law, court or regulator (including the Commissioner) requires the Supplier to process or disclose the Personal Data to a third-party, the Supplier must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic or EU law prohibits the giving of such notice.

3.4 The Supplier will reasonably assist the Customer, at no additional cost to the Customer, with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of the Supplier's processing and the information available to the Supplier, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with

the Commissioner or other relevant regulator under the Data Protection Legislation.

3.5 The Supplier must notify the Customer promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting the Supplier's performance of the Master Agreement or this Addendum.

4. Supplier's employees

4.1 The Supplier will ensure that all of its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Legislation and how it relates to their handling of the Personal Data and how it applies to their particular duties; and

(c) are aware both of the Supplier's duties and their personal duties and obligations under the Data Protection Legislation and this Addendum.

5. Security

5.1 The Supplier must at all times implement appropriate technical and organisational measures 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 ANNEX B.

5.2 The Supplier must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. Personal data breach

6.1 The Supplier will notify the Customer in writing without undue delay if it becomes aware of:

(a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. The Supplier will restore such Personal Data at its own expense as soon as possible.

(b) any accidental, unauthorised or unlawful processing of the Personal Data; or

(c) any Personal Data Breach.

6.2 Where the Supplier becomes aware of (a), (b) and/or (c) above, it will, without undue delay, also provide the Customer with the following written information:

(a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

(b) the likely consequences; and

(c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

6.3 Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Supplier will reasonably co-operate with the Customer at no additional cost to the Customer, in the Customer's handling of the matter, including but not limited to:

(a) assisting with any investigation;

(b) providing the Customer with physical access to any facilities and operations affected;

(c) facilitating interviews with the Supplier's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.

6.4 The Supplier will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Customer's written consent, except when required to do so by domestic or EU law.

6.5 The Supplier agrees that the Customer has the sole right to determine:

(a) whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.6 The Supplier will cover all reasonable expenses associated with the performance of the obligations under clause 6.1 to clause 6.3 unless the matter arose from the Customer's specific written instructions, negligence, wilful default or breach of this Addendum, in which case the Customer will cover all reasonable expenses.

6.7 The Supplier will also reimburse the Customer for actual reasonable expenses that the Customer incurs when responding to an incident of accidental, unauthorised or unlawful processing and/or a Personal Data Breach to the extent that the Supplier caused such, including all costs of notice and any remedy as set out in Clause 6.5.

7. Transfers of personal data

7.1 The Supplier (and any subcontractor) must not transfer or otherwise process the Personal Data outside the UK or, the EEA without obtaining the Customer's prior written consent.

8. Subcontractors

8.1 The Supplier may engage sub-processors necessary to deliver the Service, subject to:

(a) equivalent contractual obligations

(b) transparency via a published list.

8.2 Those subcontractors approved as at the commencement of this Addendum are as set out in ANNEX A. The Supplier must list all approved subcontractors in Annex A and include any subcontractor's name and location and the contact information for the person responsible for privacy and data protection compliance.

8.3 Resellers Are Not Sub-processors:

Resellers do not act as sub-processors. They act as independent controllers when:

(a) selling licences

(b) managing their own customer relationships

(c) providing customer details to the Supplier for account provisioning

Any data shared by resellers is processed by the Supplier as a controller, not under this Addendum.

9. Complaints, data subject requests and third-party rights

9.1 The Supplier must, at no additional cost to the Customer, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on the Customer by the Commissioner or other relevant regulator under the Data Protection Legislation.

9.2 The Supplier must notify the Customer immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 The Supplier must notify the Customer within 2 Business Days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.4 The Supplier will give the Customer, at no additional cost to the Customer, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 The Supplier must not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the Customer's written instructions, or as required by domestic or EU law.

10. Term and termination

10.1 This Addendum will remain in full force and effect so long as:

(a) the Master Agreement remains in effect; or

(b) the Supplier retains any of the Personal Data related to the Master Agreement in its possession or control (**Term**).

10.2 Any provision of this Addendum that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect the Personal Data will remain in full force and effect.

10.3 The Supplier's failure to comply with the terms of this Addendum is a material breach of the Master Agreement. In such event, the Customer may terminate any part of the Master Agreement involving the processing of the Personal Data effective immediately on written notice to the Supplier without further liability or obligation of the Customer.

10.4 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Agreement obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within 28 days, either party may terminate the Master Agreement on not less than 14 Business Days on written notice to the other party.

11. Data return and destruction

11.1 At the Customer's request, the Supplier will give the Customer, or a third-party nominated in writing by the Customer, a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

11.2 On termination of the Master Agreement for any reason or expiry of its term, the Supplier will securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any of the Personal Data related to this Addendum in its possession or control.

11.3 If any law, regulation, or government or regulatory body requires the Supplier to retain any documents, materials or Personal Data that the Supplier would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents, materials or Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

11.4 The Supplier will certify in writing to the Customer that it has deleted or destroyed the Personal Data within 5 days after it completes the deletion or destruction.

12. Records

12.1 The Supplier will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved subcontractors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in Clause 5.1 (**Records**).

12.2 The Supplier will ensure that the Records are sufficient to enable the Customer to verify the Supplier's compliance with its obligations under this Addendum and the Data Protection Legislation and the Supplier will provide the Customer with copies of the Records upon request.

12.3 The Customer and the Supplier must review the information listed in the Annexes to this Addendum at least once a year to confirm its current accuracy and update it when required to reflect current practices.

13. Audit

13.1 The Supplier will permit the Customer and its third-party representatives to audit the Supplier's compliance with its Agreement obligations, on at least 14 days' notice, during the Term. The Supplier will give the Customer and its third-party representatives all necessary assistance to conduct such audits at no additional cost to the Customer. The assistance may include, but is not limited to:

(a) physical access to, remote electronic access to, and copies of the Records and any other information held at the Supplier's premises or on systems storing the Personal Data;

(b) access to and meetings with any of the Supplier's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

(c) inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to process the Personal Data.

13.2 The notice requirements in Clause 13.1 will not apply if the Customer reasonably believes that a Personal Data Breach has occurred or is occurring, or the Supplier is in material breach of any of its obligations under this Addendum or any of the Data Protection Legislation.

13.3 If a Personal Data Breach occurs or is occurring, or the Supplier becomes aware of a breach of any of its obligations under this Addendum or any of the Data Protection Legislation, the Supplier will:

(a) conduct its own audit to determine the cause;

(b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

(c) provide the Customer with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit within 30 days.

14. Warranties

14.1 The Supplier warrants and represents that:

(a) its employees, subcontractors, agents and any other person or persons accessing the Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;

(b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

(c) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Master Agreement's contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to

prevent the accidental, unauthorised or unlawful processing of Personal Data and the loss or damage to, the Personal Data, and ensure a level of security appropriate to:

(i) the harm that might result from such accidental, unauthorised or unlawful processing and loss or damage;

(ii) the nature of the Personal Data protected; and

(iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in Clause 5.1.

14.2 The Customer warrants and represents that the Supplier's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

15. Indemnification

15.1 The Supplier agrees to indemnify, keep indemnified and defend at its own expense the Customer against all costs, claims, damages or expenses incurred by the Customer or for which the Customer may become liable due to any failure by the Supplier or its employees, subcontractors or agents to comply with any of its obligations under this Addendum and/or the Data Protection Legislation.

16. Notice

16.1 Any notice given to a party under or in connection with this Addendum shall be in writing and shall be delivered by hand or by pre-paid first-class post or other next Business Day delivery service at its registered office (if a company) or its principal place of business (in any other case.

16.2 Any notice shall be deemed to have been received:

(a) if delivered by hand, at the time the notice is left at the proper address; or

(b) if sent by pre-paid first-class post or other next Business Day delivery service, at 9:00am on the second Business Day after posting.

16.3 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

ANNEX A Personal Data processing purposes and details

Subject Matter:
Processing of Customer Personal Data inside the SaaS platform.

Duration:
For the term of the Master Agreement.

Nature and Purpose:

- Account provisioning
- Authentication
- Support
- Storage and processing of Customer Data
- Usage analytics (aggregated/anonymised where possible)

Categories of Data:

- User identity data
- Contact details
- Login credentials
- Usage logs
- Customer-uploaded content

Data Subjects:

- Customer employees
- Customer contractors
- Customer end-users (if applicable)

Sub-processors:
[List or link]

Resellers:
Resellers are **independent controllers** and not sub-processors.

ANNEX B Security measures

The Supplier maintains industry-standard technical and organisational measures, including:

- Encryption in transit and at rest
- Role-based access controls
- Multi-factor authentication for administrative access
- Network and application monitoring
- Regular vulnerability scanning and penetration testing
- Secure software development lifecycle
- Backup and disaster recovery processes
- Logging and audit trails
- Incident response procedures