# DATA PROCESSING ADDENDUM

## 1. BACKGROUND

1.1 This Data Processing Addendum ("**DPA**") applies to the processing of Customer Personal Data (as defined below) by When I Work, Inc ("**WIW**") in connection with the provision of the Service to the Customer (as defined below).

## 2. DEFINITONS

2.1 Unless otherwise set out below, each capitalised term in this DPA shall have the meaning set out in the Agreement, and the following capitalised terms used in this DPA shall be defined as follows:

"**Adequate Jurisdiction**" means the UK, EEA, or a country, territory, specified sector or international organisation which ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data, as set out in:

(a) with respect to personal data relating to data subjects in the EEA, a decision of the European Commission;

(b) with respect to personal data relating to data subjects in the UK, the UK Data Protection Act 2018 or regulations made by the UK Secretary of State under the UK Data Protection Act 2018;

"**Agreement**" means the agreement entered into between the Customer and WIW in respect of the provision of the Service, either on the terms of WIW's Terms of Service at https://wheniwork.com/terms or as otherwise agreed between the parties;

"**Controller-Controller Clauses**" means Module One (controller to controller) of the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914;

"**Controller-Processor Clauses**" means Module Two (controller to processor) of the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914;

"**Customer**" means an organisation that enters into an agreement with WIW in respect of the provision of the Service;

"**Customer Personal Data**" means the personal data described in ANNEX 1;

"**DPA**" has the meaning given to it in the Background;

"**EEA**" means the European Economic Area;

"**GDPR**" means Regulation (EU) 2016/679 (the "EU GDPR") or, where applicable the "**UK GDPR**" as defined in section 3 of the Data Protection Act 2018.

"**Mandatory Clauses**" means Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the UK Information Commissioner and laid before the UK Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 19 of those Mandatory Clauses;

"**Member State**" means a member state of the EEA, being a member state of the European Union, Iceland, Norway, or Liechtenstein;

"**Objection**" has the meaning given in paragraph 7.3;

"**Standard Contractual Clauses**" means the Controller-Controller Clauses and Controller-Processor Clauses;

"**Subprocessor**" means any Processor engaged by WIW who agrees to receive from WIW Customer Personal Data;

"**UK Data Protection Laws**" has the meaning given in paragraph 4.4(a).

2.2 The terms "**personal data**", "**controller**", "**processor**", "**data subject**", "**process**", "**personal data breach**" and "**supervisory authority**" shall have the meanings given to them in the GDPR.

## 3. INTERACTION WITH THE AGREEMENT

3.1 This DPA supplements the Agreement with respect to any processing of Customer Personal Data by WIW.

3.2 Without prejudice to the generality of clause 5 of the Standard Contractual Clauses, in the event of any conflict between the Agreement, this DPA and the Standard Contractual Clauses, the following order of precedence shall apply:

(a) the Standard Contractual Clauses (or, with respect to transfers of Customer Personal Data subject to the UK GDPR, the Standard Contractual Clauses as amended by paragraph 4.4).

(b) the main body of this DPA;

(c) the Agreement.

## 4. STANDARD CONTRACTUAL CLAUSES

4.1 Subject to paragraph 4.4, the Controller-Controller Clauses shall apply to any transfers of Customer Personal Data falling within the scope of the GDPR from the Customer (as data exporter) to WIW (as data importer) where WIW acts as a controller.

4.2 Subject to paragraph 4.4, the Controller-Processor Clauses shall apply to any transfers of Customer Personal Data falling within the scope of the GDPR from the Customer (as data exporter) to WIW (as data importer) where WIW acts as a processor

4.3 For the purposes of the Standard Contractual Clauses:

(a) Annex I.A (*List of parties*) shall be deemed to incorporate the information in ANNEX 1 (with respect to WIW) and the information submitted by the Customer upon signing up to the Service and entering into the Agreement;

(b) Annex I.B (*Description of Transfer*) shall:

(i) for the purposes of the Controller-Controller Clauses, be deemed to incorporate the information in Part 1 of ANNEX 1;

(ii) for the purposes of the Controller-Processor Clauses, be deemed to incorporate the information in Part 2 of ANNEX 1;

(c) Annex I.C (*Competent Supervisory Authority*) shall, subject to paragraph **Error! Reference source not found.**, be deemed to refer to the Data Protection Commissioner (Ireland); and

(d) Annex II (*Technical and Organisational Measures*) shall be deemed to incorporate the information in ANNEX 3.

4.4 With respect to any transfers of Customer Personal Data falling within the scope of the UK GDPR from the Customer (as data exporter) to WIW (as data importer):

(a) the Mandatory Clauses shall form part of this DPA and the Standard Contractual Clauses shall be read and interpreted in light of the provisions of the Mandatory Clauses;

(b) WIW (as data importer) may end this DPA, to the extent the Mandatory Clauses apply, in accordance with Section 19 of the Mandatory Clauses;

(c) neither the Standard Contractual Clauses nor the DPA shall be interpreted in a way that conflicts with rights and obligations provided for in any laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018 (together, the "**UK Data Protection Laws**");

(d) the Standard Contractual Clauses are deemed to be amended to the extent necessary so they operate:

(i) for transfers made by the Customer to WIW, to the extent that UK Data Protection Laws apply to the Customer's processing when making that transfer; and

(ii) to provide appropriate safeguards for the transfers in accordance with Article 46 of the UK GDPR.

## 5. INSTRUCTIONS FOR DATA PROCESSING

5.1 The parties agree that, for the purposes of clause 8.1(a) of the Controller-Processor Clauses, the Agreement and this DPA shall be the Customer's instructions for the processing of Customer Personal Data.

5.2 To the extent that any of the Customer's instructions require processing of Customer Personal Data in a manner that falls outside the scope of the Service WIW may:

(a) make the performance of any such instructions subject to the payment by the Customer of any costs and expenses incurred by WIW or such additional charges as WIW may reasonably determine; or

(b) terminate the Agreement and the Service.

5.3 Notwithstanding clause 8.1 of the Controller-Processor Clauses, WIW may process Customer Personal Data to the extent required by applicable law in the UK, the EEA, or a Member State, in each case to which WIW is subject, in which case WIW shall, to the extent permitted by such applicable law, inform the Customer of that legal requirement before processing that Customer Personal Data.

## 6. CUSTOMER WARRANTIES AND UNDERTAKINGS

6.1 The Customer represents and warrants that:

(a) it has provided all applicable notices to data subjects and, to the extent required, obtained consent from data subjects in each case as required for the lawful processing of Customer Personal Data in accordance with the Agreement and this DPA; and

(b) without prejudice to the generality of clause 8.5 of the Controller-Controller Clauses or clause 8.6 of the Controller-Processor Clauses, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the security measures set out in ANNEX 3 are:

(i) appropriate to ensure the security of the Customer Personal Data, including protection against a personal data breach; and

(ii) otherwise consistent with the Customer's obligations under Article 32 of the GDPR.

## 7. SUBPROCESSORS

7.1 The parties agree that, for the purposes of clause 9 of the Controller-Processor Clauses:

(a) the Customer gives WIW general authorisation to engage Subprocessors from an agreed list; and

(b) ANNEX 2 sets out the list of Subprocessors agreed by the parties.

7.2 WIW shall provide the Customer with seven (7) days' notice of any proposed changes to the Subprocessors it uses to process Customer Personal Data (including any addition or replacement of any Subprocessors), including any information reasonably necessary to enable the Customer to assess the Subprocessor and exercise its right to object.

7.3 If the Customer objects to WIW's use of a new Subprocessor (including when exercising its right to object under clause 9(a) of the Standard Contractual Clauses), it shall provide WIW with:

(a) written notice of the objection within seven (7) days after WIW has provided notice to the Customer as described in paragraph 7.2; and

(b) documentary evidence that reasonably shows that the Subprocessor does not or cannot comply with the requirements in this DPA,

(an "**Objection**").

7.4 In the event of an Objection, WIW will use reasonable endeavours to make available to the Customer a change in the Service, or will recommend a commercially reasonable change to the Service to prevent the applicable Subprocessor from processing the Customer Personal Data.

7.5 If WIW is unable to make available such a change in accordance with paragraph 7.4 within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate the Agreement by providing not less than thirty (30) days' written notice to the other party. During such notice period, WIW may suspend the affected portion of the Service.

## 8. SECURITY AND AUDITS

8.1 With respect to any audits conducted under clauses 8.9(c) and (d) of the Controller-Processor Clauses, the parties agree that:

(a) they shall, prior to any audit, agree on the scope of the audit and any reasonable limitations or conditions applicable to such audit in addition to those set out in this paragraph 8.1;

(b) all such audits shall be conducted:

(i) on reasonable written notice to WIW;

(ii) only during WIW's normal business hours; and

(iii) in a manner that does not disrupt WIW's business;

(c) the Customer (or, where applicable, a third-party independent auditor appointed by the Customer) shall:

(i) enter into a confidentiality agreement with WIW prior to conducting the audit in such form as WIW may request; and

(ii) ensure that its personnel comply with WIW's and any Subprocessor's policies and procedures when attending WIW's or Subprocessor's premises, as notified to the Customer by WIW or Subprocessor.

## 9. COSTS

9.1 The Customer shall pay to WIW on demand all costs and expenses incurred by WIW in connection with:

(a) implementing any changes to the Services under paragraph 7.4;

(b) facilitating and contributing to any audits of WIW under or clauses 8.9(c) and (d) of the Controller-Processor Clauses;

(c) facilitating and contributing to any audits of WIW conducted by a supervisory authority;

(d) responding to queries or requests for information from the Customer relating to the processing of Customer Personal Data under clauses 8.9(a), 8.9(c) or 8.9(e) of the Controller-Processor Clauses;

(e) any assistance provided by WIW to the Customer with its fulfilment of its obligations to respond to data subjects' requests for the exercise of their rights under the GDPR; and

(f) any assistance provided by WIW to the Customer with any data protection impact assessments or prior consultation with any supervisory authority of the Customer.

## 10. DURATION AND TERMINATION

10.1 With respect to any Customer Personal Data received by WIW under the Controller-Processor Clauses, WIW shall, within thirty (30) days of the date of termination or expiry of the Agreement:

(a) if requested to do so by the Customer within that period, return a complete copy of all Customer Personal Data by secure file transfer in such a format as notified by the Customer to WIW; and

(b) other than any Customer Personal Data retained by WIW after termination of the Agreement in accordance with clauses 8.5 of the Controller-Processor Clauses and 16(d) of the Standard Contractual Clauses, delete and use all reasonable efforts to procure the deletion of all other copies of Customer Personal Data processed by WIW or any Subprocessors.

## 11. LAW AND JURISDICTION

11.1 Notwithstanding the provisions of the Agreement, this DPA and the Standard Contractual Clauses shall (to the extent permitted under applicable law) be governed by, and construed in accordance with:

(a) where the Customer is established in the UK, the law of England and Wales; and

(b) otherwise, the law of Ireland.

11.2 Notwithstanding the provisions of the Agreement, the parties submit themselves to the jurisdiction of the following courts:

(a) where the Customer is established in the UK, the courts of England and Wales;

(b) otherwise, the courts of Ireland.

## 12. THIRD PARTY RIGHTS

12.1 Other than the right of data subjects or not-for-profit bodies, organisations or associations under the conditions set out in Article 80(1) of the GDPR to bring claims under the Standard Contractual Clauses, a person who is not a party to this DPA may not enforce any of its terms.

## ANNEX 1

## DETAILS OF PROCESSING

### Part 1 – transfers subject to the Controller-Controller Clauses

1. **Categories of data subjects**

Customer's employees, personnel, authorized users, and any other data subjects whose data the Customer or its authorized users submits, transfers, loads or otherwise provides to When I Work via the Service.

2. **Categories of personal data**

Shifts worked by Customer's personnel, and ancillary data attached to the shift (such as workplace location); time entries (if Customer has Attendance application); and clock-in/clock out (if Customer has Attendance with mobile clock-in functionality is utilized); and Service usage information.

3. **Special categories of personal data**

None. When I Work does not use or store special categories of personal data and does not anticipate the transmission of special categories of data.

4. **Frequency of the transfer**

The transfer is carried out on a continuous basis for the duration of the Agreement.

5. **Subject matter of the processing**

Service maintenance and improvement.

6. **Nature of the processing**

The monitoring and improvement of the Service.

7. **Purpose(s) of the data transfer and further processing**

The analysis of the Customer's and its personnel's use of the Services in connection with identifying errors, generating statistics, and developing new products and features.

8. **Duration**

The personal data will be retained in pseudonymised form for a period of 3 years after termination of the Agreement

9. **Processor (if applicable)**

Transfers to processors are carried out as set out in ANNEX 2.

## Part 2 – transfers subject to the Controller-Processor Clauses

1. **Categories of data subjects**

Customer's employees, personnel, authorized users, and any other data subjects whose data the Customer or its authorized users submits, transfers, loads or otherwise provides to When I Work via the Service.

2. **Categories of personal data**

Name, email address, work site address, job role, work availability, shifts worked and requested, work preferences, the content of any communications between the Customer and its employees, personnel, and authorized users. Provision of mobile telephone number is optional. Geolocation data is required only for the attendance feature of the Service when user level mobile clock-in/clock-out is turned on and the user consents to sharing geolocation data via a mobile device. Geolocation data is not required or collected for the scheduling-only feature of the Service. Mobile Device type and IP addresses are also collected.

3. **Special categories of personal data**

None. When I Work does not use or store special categories of personal data and does not anticipate the transmission of special categories of data.

4. **Frequency of the transfer**

The transfer is carried out on a continuous basis for the duration of the Agreement.

5. **Subject matter of the processing**

The provision of software as a service that enables employee scheduling, time recording, and team messaging.

6. **Nature of the processing**

The collection, storage, and retrieval of data submitted by the Customer in connection with their use of the Service.

7. **Purpose(s) of the data transfer and further processing**

The provision of the Service to the Customer in accordance with the Agreement.

8. **Duration**

The personal data will be retained for the duration of the Agreement, subject to paragraph 10 of the DPA.

9. **Sub-processor (if applicable)**

Transfers to Subprocessors are carried out as set out in ANNEX 2.

## ANNEX 2

## SUBPROCESSORS

| Subprocessor | Subprocessor Function | Technical and organizational measures to assist the Customer |
|---|---|---|
| Amazon Web Services, Inc. (AWS) | Cloud service provider used to host, process, and store data submitted to the Service. | As described at: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf |
| Zendesk, Inc. | Customer service platform, including online helpdesk ticketing service and customer support live chat. | As described at: https://www.zendesk.co.uk/company/privacy-and-data-protection/ |
| Pendo.io, Inc. | Customer messaging and data analytics platform provider | As described at: https://pendo.trust.page/ |
| Stripe, Inc. | On-line payment processing | As described at: https://stripe.com/dpa/legal |
| Google, Inc. | Workplace (*f/k/a* G-suite) Cloud-based collaboration tools and productivity applications, including hosted email and Maps for geolocation data found in the attendance feature of the Service | As described at: https://cloud.google.com/terms/data-processing-terms |
| Twilio Inc. | Optional cloud communication platform to send messages and images from When I Work customers to their users (and, if enabled, between users of the same account) in real time (web and mobile) | As described at: https://www.twilio.com/legal/data-protection-addendum |

## ANNEX 3

## TECHNICAL AND ORGANISATIONAL MEASURES

## Part 1

## Security

### Introduction

WIW employs a combination of policies, procedures, guidelines, and technical and physical controls to protect the personal data it processes from accidental loss and unauthorised access, disclosure, or destruction.

### Governance and Policies

WIW assigns personnel with responsibility for the determination, review and implementation of security polices and measures.

WIW:

- has documented the security measures it has implemented in a security policy and/or other relevant guidelines and documents;
- reviews its security measures and policies on a regular basis to ensure they continue to be appropriate for the data being protected.

WIW establishes and follows secure configurations for systems and software and ensures that security measures are considered during product development and deployment.

### Breach response

WIW has a breach response plan that has been developed to address data breach events. WIW's disaster recovery and business continuity plans are tested and updated at least once quarterly.

WIW performs a monthly full restore from a recent point-in-time backup into a non-production environment where functional validation is performed.

### Intrusion, anti-virus and anti-malware defences

WIW IT systems used to process personal data have appropriate data security software installed on them, including:

- deployment of firewalls, anti-virus, anti-spyware, anti-malware and intrusion detection systems;
- Annual penetration testing

- Continuous scanning of source code and infrastructure to identify and prioritise defects and vulnerabilities to resolve;
- PHPStan to conduct static scans of every branch ahead of merge into the next release candidate;
- Use of AWS Inspector to monitor and improve the security and compliance of applications deployed on AWS;
- Collection, maintenance, review and audit of event logs using Rollbar and AWS Cloud Trail monitoring;
- Deployment of data loss prevention tools at network and host level;
- Monitoring of all traffic leaving the organisation and unauthorised use of encryption.

**Access controls**

WIW allows Customers to access uploaded by them or stored on their behalf through WIW's REST API and SAML-SSO.

WIW limits access to personal data by implementing appropriate access controls, including:

- limiting internal administrative access privileges and use of administrative accounts following the principle of least privilege, and ensuring that access is appropriate with regard to the authentication method and the user's business function;
- limiting access to production environments through VPN and AWS identity access management;
- use of password management best practices for internal password expiry and rotation;
- requiring personnel to use multi-factor authentication to gain access to IT systems;
- only permitting user access to personal data which the user needs to access for his/her/their job role or the purpose they are given access to WIW's IT systems for (i.e. WIW implements measures to ensure least privilege access to IT systems);
- having in place appropriate procedures for controlling the allocation and revocation of personal data access rights. For example, having in place appropriate procedures for revoking employee access to IT systems when they leave their job or change role;
- encouraging users to use strong passwords, such as passwords with over eight characters, combination of upper and lower case letters, numbers and special characters;

- engineering resources use passwords that are encrypted and scrubbed ahead of movement within systems;
- systems administrators and customer care staff are required to use multi-factor authentication tied to WIW-managed credentials using standard methods such as gpg signed keys, Yubkey physical keys and Google Authentication;
- automatic timeout and locking of terminals used by WIW personnel if left idle;
- access to IT system is blocked after multiple failed attempts to enter correct authentication and/or authorisation details;
- monitoring and logging access to IT systems;
- monitoring and logging amendments to data or files on IT systems.

**Availability and Back-up personal data**

WIW has a documented disaster recovery plan that ensures that key systems and data can be restored in a timely manner in the event of a physical or technical incident. The plan is tested at least quarterly.

WIW performs point-in-time back-end storage snapshots at five-minute intervals. Retention process is managed with alerts for successful backups.

Customer-facing software is hosted in AWS infrastructure with AWS KMS-managed encryption at rest with availability zone failover and cross-region replication within the USA.

**Segmentation of personal data**

WIW:

- separates and limits access between network components and, where appropriate, implements measures to provide for separate processing (storage, amendment, deletion, transmission) of personal data collected and used for different purposes;
- does not use live data for testing its systems;
- data segregation by UUID.

**Disposal of IT equipment**

WIW:

- has in place processes to securely remove all personal data before disposing of IT systems;
- uses appropriate technology to purge equipment of data and/or destroy hard disks.

**Encryption**

WIW uses encryption technology where appropriate to protect personal data held electronically, including:

- AWS KMS-managed (AES256) encryption at rest;

**Transmission or transport of personal data**

Appropriate controls are implemented by WIW to secure personal data during transmission or transit, including:

- use of VPNs;
- encryption in transit using TLS 1.2 over HTTPS using a strong cipher suite;
- ensuring physical security for personal data when transported on portable electronic devices or in paper form.

**Device hardening**

WIW removes unused software and services from devices used to process personal data.

WIW ensures that default passwords that are provided by hardware and software producers are not used.

**Asset and Software management**

WIW maintains an inventory of IT assets and the data stored on them, together with a list of owners of the relevant IT assets.

WIW:

- documents and implements rules for acceptable use of IT assets.
- requires network level authentication.
- deploys application whitelisting;
- deploys automated patch management tools and software update tools for operating systems and software;
- proactively monitors software vulnerabilities and promptly implements any out of cycle patches;
- permits the use of only the latest versions of fully supported web browsers and email clients.

WIW stores all API keys securely, including as follows:

- WIW stores API keys directly in its environment variables;
- WIW does not store API keys on client side;
- WIW does not publish API key credentials in online code repositories (whether private or not); and
- API keys are provided to customers for access to their data and terminated upon termination of the agreement.

**Physical security**

WIW implements physical security measures to safeguard personal data. This may include:

- Deployment and enforcement of appropriate policies to ensure that:
    - personal data is printed only where this is necessary for a person to perform his/her job role.
    - Sensitive personal data or large amounts of personal data held in hardcopy are kept securely e.g. in locked rooms or filing cabinet. Generally, steps are taken to ensure that access to hardcopy personal data is limited in the same way it would be on an electronic IT system i.e. access is limited to those individuals where it is necessary for them to have access in order for them to perform their job role.
    - Hardcopy documents containing personal data are only taken off site where necessary for a person's job role.
    - When travelling or working away from the office hard copy documents and portable devices containing personal data are kept secure e.g. never left in a car or unsecured in a public place.
    - Paper records which contain confidential information (including personal data and Sensitive personal data) are shredded after use.

**Staff training and awareness**

WIW's agreements with staff and contractors and employee handbooks set out its personnel's responsibilities in relation to information security.

WIW carries out:

- regular staff training on data security and privacy issues relevant to their job role and ensures that new starters receive appropriate training before they start their role (as part of the on boarding procedures);
- appropriate screening and background checks on individuals that have access to sensitive personal data.

WIW ensures that information security responsibilities that are applicable immediately before termination or change of employment and those which apply after termination / change of employment are communicated and implemented.

Staff are subject to disciplinary measures for breaches of WIW's policies and procedures relating to data privacy and security.

**Selection of service providers and commission of services**

WIW assesses service providers' ability to meet their security requirements before engaging them.

WIW has written contracts in place with service providers which require them to implement appropriate security measures to protect the personal data they have access to and limit the use of personal data in accordance with WIW's instructions.

WIW conducts regular audits of vendors that have access to WIW's data either through physical inspection by appropriately qualified security auditors or by reviewing vendors' security accreditation (such as ISO 27001 or SOC II) reports.

WIW's breach response protocol and agreements with vendors provide for the audit of vendors (and subprocessors) following receipt of any notice of a security incident from that vendor.

## Part 2

## Assistance with Data Subject Rights Requests

WIW has implemented appropriate policies and measures to identify and address data subject rights requests, including:

- the data processed on behalf of the Customer is stored separately from data processed by WIW;
- WIW maintains accurate records to enable it to identify quickly all personal data processed on behalf of WIW;
- back-ups of personal data processed by WIW on behalf of the Data Exporter are updated on a regular basis and in any event every 5 minutes to ensure deletion and rectification requests are fully actioned.