

# Platform Agreement

---

*OPFW Diagnostic Platform · Version 1.0 · Effective 24 April 2026*

## Parties

**One Point Four West Ltd** (Company No. 17094594), registered office at The Commissioners Building, 4 St Thomas Street, Sunderland, SR1 1NW ("**OPFW**", "**we**", "**us**") and

[**Full legal name of the Firm**] (Company No. [\_\_\_\_]), registered office at [\_\_\_\_] (the "**Firm**", "**you**", "**your**").

Each a "**Party**" and together the "**Parties**".

**Effective Date:** the date the Firm accepts this Agreement in accordance with the Acceptance section below.

## Acceptance

This Agreement is entered into by one of the following equally valid routes:

**(a) Click-Through Acceptance (self-serve subscription).** The Firm's authorised representative completes the self-serve subscription flow at onepointfourwest.com and ticks the acceptance checkbox at checkout confirming they have read and agreed to this Agreement (which includes Schedule 1 — Data Processing Agreement, and Schedule 2 — Acceptable Use Policy). OPFW retains an acceptance record (timestamp, acceptor name and email, firm billing email, Stripe customer ID, IP address and User-Agent) as evidence of entry into this Agreement.

**(b) Signed Acceptance (enterprise or bespoke).** The Parties sign the execution block at the foot of the main body of this Agreement.

By following either acceptance path, the person accepting confirms they have authority to bind the Firm to this Agreement. The Effective Date is the date of click-through acceptance or the date of the last signature, as applicable.

## Background

A. OPFW operates a web-based diagnostic platform (the "**Platform**") for conducting structured HR and people assessments, comprising diagnostic tools, scoring frameworks, assessment methodologies, reporting engines and associated software.

B. The Firm wishes to use the Platform to conduct client assessments under its own brand on a white-label basis.

C. This Agreement sets out the terms on which OPFW grants the Firm access to the Platform. The commercial details of the licence (tier, seat limit, fees, term) are set out in the Order Form (Schedule 3). Data protection terms are set out in the Data Processing Agreement (Schedule 1). Acceptable use terms are set out in the Acceptable Use Policy (Schedule 2).

## 1. Definitions

**"Agreement"** means this Platform Agreement, including Schedule 1 (Data Processing Agreement), Schedule 2 (Acceptable Use Policy) and Schedule 3 (Order Form).

**"Applicable Law"** means any law, statute, regulation, order, judgment, directive or binding code of practice applicable to a Party from time to time, including UK Data Protection Laws.

**"AUP"** means the Acceptable Use Policy set out at Schedule 2.

**"Authorised User"** means an individual employed or contracted by the Firm who has been granted a user account on the Platform, up to the Seat Limit. Authorised Users include firm administrators (who manage firm settings, billing and user provisioning) and firm consultants (who run diagnostics).

**"Business Day"** means any day other than a Saturday, Sunday or English public holiday.

**"Client Data"** means client records, diagnostic assessment data, maturity ratings, red and green flag selections, notes, findings and any other data entered into the Platform by Authorised Users.

**"Confidential Information"** means any information, in any form, that is marked or reasonably understood as confidential, including commercial terms, technical information, client lists, and Platform methodologies, but excluding information that falls within the carve-outs in clause 12.

**"Diagnostic Tools"** means the individual assessment instruments available on the Platform, including the HR Function Diagnostic, HR Risk Diagnostic, People Operations Diagnostic, ER Diagnostic, TUPE Diagnostic, Change and OD Diagnostic, Investigations Diagnostic, M&A People Diagnostic, People Strategy Diagnostic, Interim Leadership Diagnostic, Initial Call Diagnostic, HR Systems Transformation Diagnostic, Gap Analysis Roadmap and TOM Design Canvas, together with any further Diagnostic Tools added from time to time (excluding Premium Tools unless separately licensed).

**"DPA"** means the Data Processing Agreement set out at Schedule 1.

**"Fees"** means the licence fees set out in the Order Form.

**"Firm Branding"** means the Firm's logo, company name, consultant biographies, contact details, specialisms and brand colour configuration as uploaded to the Platform.

**"Intellectual Property Rights"** means patents, trade marks, service marks, copyright and related rights, database rights, design rights, rights in confidential information and know-how, and all other intellectual property rights, whether registered or unregistered, and all applications for the same.

**"Order Form"** means the order form at Schedule 3 setting out the licence tier, Seat Limit, Fees, Initial Term and billing cycle.

**"Per-Firm Subdomain"** means the subdomain under `onepointfourwest.com` assigned to the Firm (for example, `yourfirm.onepointfourwest.com`) under which Authorised Users access the Platform.

**"Personal Data"** means as defined in the UK GDPR.

**"Platform"** means the OPFW Diagnostic Platform, including all Diagnostic Tools, shared software modules, APIs, data storage, authentication, reporting infrastructure and the Per-Firm Subdomain.

**"Platform Output"** means reports, exports and other materials generated by the Platform in respect of the Firm's client engagements, carrying the Firm's branding as described in clause 3.

**"Premium Tool"** means a Diagnostic Tool designated by OPFW at its reasonable discretion as separately licensed or payable.

**"Seat Limit"** means the maximum number of Authorised Users permitted under the Firm's licence, as set out in the Order Form.

**"Term"** means the period defined in clause 9.

**"UK Data Protection Laws"** means the UK GDPR, the Data Protection Act 2018 and any successor or implementing legislation.

**"UK GDPR"** means the retained EU law version of the General Data Protection Regulation as it forms part of the law of England and Wales.

## 2. Licence Grant

**2.1** Subject to the Firm's compliance with this Agreement and payment of the Fees, OPFW grants to the Firm a non-exclusive, non-transferable, non-sublicensable licence to use the Platform during the Term for the purpose of conducting client assessments.

**2.2** The licence includes the right for Authorised Users to access and use all Diagnostic Tools available on the Platform at the date of access, and any new Diagnostic Tools added during the Term, except for Premium Tools which require a separate agreement or upgrade.

**2.3** The Firm may not sublicense, resell, redistribute or provide access to the Platform to any third party outside the Firm without OPFW's prior written consent.

**2.4** The Firm may not use the Platform to benchmark or compare it against any competing product or service.

## 3. White-Label Operation

**3.1** The Platform is operated on a full white-label basis. Firm-facing pages, reports and exports carry Firm Branding. OPFW does not require, and will not add, "powered by OPFW" attribution or equivalent co-branding to Platform Output shown to or shared by the Firm with its own clients.

**3.2** The Firm uploads Firm Branding (logo, name, tagline, accent colour, contact details) through the firm settings interface. Firm Branding appears on:

- the Per-Firm Subdomain header and login page
- the Platform header bar for authenticated users
- Platform Output (PDF reports, DOCX reports, PPTX exports) — including the cover page, footer and contact section
- transactional email sent to firm users and client contacts.

**3.3** The Per-Firm Subdomain is operated by OPFW on the Firm's behalf under OPFW's DNS and hosting arrangements. Nothing in this Agreement transfers ownership of the `onepointfourwest.com` domain (or any part of it) to the Firm. On termination of this Agreement, the Per-Firm Subdomain is retired and redirects cease to be honoured, in line with clause 10.

**3.4** The following elements of the Platform remain OPFW-operated and are not subject to Firm Branding: the OPFW marketing website and signup flow; the Platform codebase, colour design system and component library; legal pages published by OPFW (Terms of Business and Privacy Notice at onepointfourwest.com); the `onepointfourwest.com` apex domain and its favicon.

**3.5** OPFW may update the Platform design, structure and functionality at any time. Where changes materially affect the presentation of Firm Branding, OPFW will give at least 14 days'

prior written notice, and the Firm may within that period request reasonable mitigations or terminate this Agreement on no less than 30 days' written notice.

**3.6** Subject to the Firm's prior written consent (not to be unreasonably withheld), OPFW may list the Firm's name and logo in a customer list and in case studies.

## **4. User Accounts and Access**

**4.1** The Firm may create user accounts for Authorised Users up to the Seat Limit. Each Authorised User must have their own individual account. Account credentials must not be shared.

**4.2** The firm administrator role counts against the Seat Limit. The firm administrator is responsible for inviting, provisioning and de-provisioning Authorised Users within the Seat Limit.

**4.3** The Firm is responsible for all activity that occurs under its Authorised Users' accounts and for maintaining the security of their credentials, including the use of strong passwords and (where available) multi-factor authentication.

**4.4** If the Firm wishes to exceed the Seat Limit, it must agree an upgraded licence tier or additional seats with OPFW before creating further accounts. Provisioning is blocked at the Seat Limit until either a seat is freed or the Firm upgrades tier.

**4.5** OPFW may suspend or terminate any individual user account where there is a reasonable belief that credentials have been compromised, this Agreement has been breached, or the account is being used for purposes outside the scope of this Agreement.

**4.6** OPFW may from time to time and on reasonable notice review Platform records to verify compliance with the Seat Limit.

## **5. Client Data**

**5.1** Client Data entered into the Platform by Authorised Users remains the Firm's data. OPFW does not claim ownership of Client Data.

**5.2** OPFW processes Client Data solely for the purpose of providing the Platform services. The processing of Personal Data is governed by the DPA at Schedule 1, which forms part of this Agreement.

**5.3** The Firm is responsible for ensuring it has an appropriate lawful basis under UK Data Protection Laws for any Personal Data it enters into the Platform and for complying with Applicable Law.

**5.4** Client Data is isolated per firm using row-level security policies. Authorised Users can only access Client Data belonging to their own firm.

**5.5** The Firm will not enter special category data or criminal offence data (as those terms are defined in the UK GDPR) into the Platform without first notifying OPFW in writing and confirming an appropriate lawful basis under Article 9 or 10 UK GDPR.

## **6. Intellectual Property**

**6.1** All Intellectual Property Rights in the Platform, including the Diagnostic Tools, assessment frameworks, scoring methodologies, question libraries, software code, shared modules, PDF generation engine, analysis engine and platform design, are and remain the property of OPFW or its licensors.

**6.2** The licence granted under this Agreement does not transfer ownership of any Intellectual Property Rights to the Firm.

**6.3** Platform Output generated by the Platform may be used by the Firm for its internal business purposes and shared with the Firm's own clients in connection with engagements. The Firm may not resell, republish or make Platform Output available to third parties outside a client engagement without OPFW's prior written consent.

**6.4** The Firm grants OPFW a limited, royalty-free, non-exclusive licence to display Firm Branding within the Platform and on Platform Output solely for the purpose of providing the Platform services under this Agreement.

**6.5** If the Firm provides OPFW with feedback, ideas, suggestions or recommendations relating to the Platform, the Firm grants OPFW a perpetual, irrevocable, royalty-free, worldwide licence to use, reproduce and incorporate such feedback into the Platform without attribution or payment.

**6.6** The Firm must not reverse-engineer, decompile, disassemble or extract the underlying software, frameworks or methodologies of the Platform, save to the extent such restriction is prohibited by Applicable Law.

## **7. Fees and Payment**

**7.1** The Firm will pay the Fees set out in the Order Form. Fees are quoted exclusive of VAT. VAT will be added at the standard rate where applicable.

**7.2** Annual licences are invoiced in advance and payable within 14 days of the invoice date. Monthly licences are collected by direct debit or card payment via Stripe on the same day each month.

**7.3** Where Fees remain unpaid more than 14 days after the due date, OPFW may (a) charge interest under the Late Payment of Commercial Debts (Interest) Act 1998 (currently 8% above the Bank of England base rate), together with fixed compensation amounts and reasonable debt recovery costs; and (b) on no less than 5 Business Days' prior written notice, suspend Platform access. Access will be reinstated promptly on receipt of cleared payment.

**7.4** OPFW may adjust Fees at renewal by giving at least 60 days' written notice before the end of the current Term. Where the Firm does not accept the change, the Firm may decline renewal under clause 9.2 and receive a pro-rata refund of any unused portion of the current Term.

**7.5** All payments are made free and clear of deduction or set-off. The Firm remains liable for reasonable collection costs on unpaid Fees.

## **8. Platform Availability**

**8.1** OPFW will use reasonable endeavours to maintain average monthly Platform availability of at least 99.5%, measured excluding Planned Maintenance and third-party service outages outside OPFW's reasonable control.

**8.2** OPFW will use reasonable efforts to give at least 5 Business Days' advance notice of Planned Maintenance that may cause extended downtime. "Planned Maintenance" means scheduled work on the Platform, typically conducted outside UK business hours.

**8.3** The Platform depends on third-party infrastructure (including Supabase hosted on Amazon Web Services in the United Kingdom and IONOS web hosting in the United Kingdom). OPFW is not liable for outages caused by third-party service failures outside its reasonable control, save where such outages result from OPFW's failure to exercise reasonable care in selecting or managing such providers.

## 9. Term and Renewal

**9.1** This Agreement begins on the Effective Date and continues for the Initial Term set out in the Order Form.

**9.2** At the end of the Initial Term, this Agreement renews automatically for successive periods of the same length (each a "**Renewal Term**") unless either Party gives written notice of non-renewal at least 30 days before the end of the current Term. OPFW will send the Firm a renewal reminder at least 60 days before the end of each Term. For self-serve subscriptions, non-renewal may alternatively be effected by the firm administrator cancelling the subscription through the Stripe Customer Portal.

**9.3** Either Party may terminate this Agreement immediately by written notice if the other Party commits a material breach of this Agreement and fails to remedy it within 14 days of receiving written notice of the breach.

**9.4** Either Party may terminate this Agreement immediately by written notice if the other Party: (a) becomes insolvent, is unable to pay its debts as they fall due, enters into a voluntary arrangement with creditors, or has a receiver, administrator or liquidator appointed; (b) ceases or threatens to cease carrying on business; or (c) undergoes a change of control to a direct competitor of the terminating Party.

## 10. Termination and Off-boarding

**10.1** On termination or expiry of this Agreement:

- OPFW will revoke Platform access for all Authorised Users at the end of the current paid period (for self-serve cancellations) or within 5 Business Days (for termination for breach or insolvency).
- Client Data will be retained for up to 90 days following termination to allow for data export requests. After 90 days, Client Data will be permanently deleted.
- User account data will be deleted within 30 days of account closure.
- Firm Branding will be removed from the Platform within 5 Business Days.
- The Per-Firm Subdomain will be retired and redirects will cease.

**10.2** The Firm may request a bulk export of all Client Data at any time during the 90-day retention period by emailing [dpo@onepointfourwest.com](mailto:dpo@onepointfourwest.com). Exports are provided in JSON format by default; CSV or a zipped bundle of PDF reports may be provided on request at no additional charge.

**10.3** Where this Agreement is terminated by OPFW for non-payment, OPFW will continue to make Client Data available for export during the 90-day period on payment of any outstanding Fees accrued to the date of termination.

**10.4** On cancellation by the Firm under the self-serve Stripe Customer Portal, cancellation takes effect at the end of the current paid period; no refund is given for the unused portion. Where OPFW terminates for convenience, or the Firm terminates for OPFW's uncured material breach, OPFW will refund the unused portion of the paid period pro-rata from the termination date.

**10.5** The following clauses survive termination: 5 (Client Data, insofar as relating to retained data obligations), 6 (Intellectual Property), 10 (this clause), 12 (Confidentiality), 13 (Liability and Indemnities), 15 (General), and the DPA at Schedule 1.

## 11. Acceptable Use

**11.1** The Firm and its Authorised Users must comply with the Acceptable Use Policy at Schedule 2 (the "**AUP**"). Without limiting the AUP, the Firm agrees not to:

- use the Platform for any unlawful purpose or in breach of Applicable Law;
- upload or process special category data or criminal offence data without a documented lawful basis under the UK GDPR;
- attempt to access data belonging to other firms;
- reverse-engineer or extract the underlying software, frameworks or methodologies of the Platform;
- introduce malicious code or interfere with Platform operations;
- conduct penetration testing, vulnerability scans or automated security testing without OPFW's prior written consent;
- share account credentials between individuals; or
- use the Platform in a manner that could reasonably be expected to damage the reputation of OPFW.

## 12. Confidentiality

**12.1** Each Party treats Confidential Information received from the other Party as confidential and does not disclose it to third parties without prior written agreement, except as permitted by this clause.

**12.2** Each Party may disclose Confidential Information to (a) its employees, officers, professional advisers, auditors, contractors and affiliates who need to know and are bound by obligations of confidentiality no less onerous than those in this Agreement; and (b) as required by law, regulator or court order, provided (where lawful) the other Party is given reasonable prior notice.

**12.3** The confidentiality obligations in this clause 12 continue for five (5) years following the end of the Agreement, and indefinitely for Confidential Information that constitutes a trade secret.

**12.4** Confidential Information does not include information that is publicly available through no fault of the receiving Party, already known to the receiving Party without a duty of confidence, independently developed without reference to the disclosing Party's Confidential Information, or lawfully received from a third party without a duty of confidence.

**12.5** Each Party acknowledges that damages may not be an adequate remedy for breach of this clause 12 and that the other Party may seek injunctive or other equitable relief without the need to prove actual loss.

## 13. Liability and Indemnities

**13.1** The Platform is provided as a professional tool to support structured assessment. Diagnostic results represent a structured summary of information entered by the user and do not constitute legal, financial or regulatory advice. The Firm is responsible for validating Platform Output before relying on or sharing it with clients or third parties.

**13.2** Subject to clauses 13.3 and 13.5, OPFW's total aggregate liability arising from or in connection with this Agreement (however arising, including in contract, tort, misrepresentation, restitution or otherwise) is limited to the total Fees paid by the Firm in the 12 months preceding the claim (the "**General Cap**").

**13.3** OPFW's aggregate liability for claims arising from (a) a breach of the DPA resulting in unauthorised processing, loss or destruction of Personal Data; or (b) breach of clause 6 (Intellectual Property), is limited to the greater of (i) two (2) times the General Cap, or (ii) £100,000 (the "**Super Cap**"). The Firm acknowledges that OPFW's cyber liability insurance (referred to in clause 13.8) is written on an aggregate basis across all claims in a policy year, and that the Super Cap is a per-Firm contractual cap rather than a guarantee of insurance availability for any particular claim.

**13.4** Neither Party is liable for indirect or consequential loss, loss of profit, loss of anticipated savings, loss of business opportunity, loss of goodwill, or loss or corruption of data (except as expressly required under the DPA or to the extent caused by wilful misconduct).

**13.5** Nothing in this Agreement limits liability for (a) death or personal injury caused by negligence; (b) fraud or fraudulent misrepresentation; or (c) any other liability that cannot lawfully be limited or excluded.

**13.6** OPFW will indemnify the Firm against damages and reasonable costs finally awarded by a court of competent jurisdiction in respect of any third-party claim that the Firm's use of the Platform in accordance with this Agreement infringes that third party's Intellectual Property Rights, subject to the Firm (a) giving OPFW prompt written notice; (b) giving OPFW sole conduct of the defence and settlement; and (c) providing reasonable assistance. OPFW may at its option modify the Platform to avoid infringement, procure the right to continue use, or terminate the affected licence and refund pro-rata prepaid Fees.

**13.7** The Firm will indemnify OPFW against all damages, losses, fines and reasonable costs arising from or in connection with (a) the Firm's breach of clauses 5 (Client Data), 6 (Intellectual Property) or 11 (Acceptable Use); or (b) any claim by a third party arising from Personal Data uploaded to the Platform by the Firm without an appropriate lawful basis.

**13.8** OPFW maintains the following insurance with reputable insurers, both underwritten by Hiscox Insurance Company Ltd: (a) professional indemnity insurance with a limit of indemnity of £5,000,000 each and every claim or loss, excluding defence costs; and (b) cyber and data insurance with a limit of indemnity of £100,000 in the aggregate, including all costs. OPFW will provide evidence of cover on reasonable request.

## **14. AI-Enhanced Analysis**

**14.1** The Platform includes an optional AI-enhanced analysis feature that sends anonymised diagnostic data to the Anthropic API (Claude) to generate narrative commentary and recommendations.

**14.2** Before data is sent to Anthropic, the organisation name is replaced with a generic placeholder. When the response is received, the placeholder is substituted back to the original organisation name locally in the user's browser. The organisation name is not transmitted to Anthropic.

**14.3** As at the Effective Date, Anthropic does not use API inputs or outputs to train its models, and retains data for up to 7 days for trust and safety purposes only. Extended retention may apply only where a safety classifier flags content. Transfers to the United States are governed by the UK International Data Transfer Addendum to the EU Standard Contractual Clauses (IDTA). OPFW will notify the Firm of material changes to Anthropic's data handling practices as soon as reasonably practicable after becoming aware of them.

**14.4** AI-enhanced analysis is optional. The Platform provides rule-based alternatives that do not involve any third-party AI data processing.

**14.5** AI-generated narrative commentary is provided for convenience and is not warranted for accuracy. The Firm must review and, where appropriate, edit AI outputs before using them with its clients.

## 15. General

**15.1 Entire Agreement.** This Agreement, together with the DPA (Schedule 1), the AUP (Schedule 2) and the Order Form (Schedule 3), constitutes the entire agreement between the Parties and supersedes all prior agreements, representations and understandings. Where OPFW's public Terms of Use (published at [onepointfourwest.com/terms.html](https://onepointfourwest.com/terms.html)) are inconsistent with this Agreement in respect of use by the Firm or its Authorised Users, this Agreement prevails.

**15.2 Governing Law and Jurisdiction.** This Agreement is governed by the laws of England and Wales. The Parties submit to the exclusive jurisdiction of the courts of England and Wales.

**15.3 Assignment.** Neither Party may assign or transfer this Agreement without the prior written consent of the other Party, save that OPFW may assign to an affiliate or to a successor in connection with a reorganisation, merger, sale of assets or similar transaction.

**15.4 Amendments.** Any amendment to this Agreement must be in writing and (for the Signed Variant) signed by both Parties. For click-through firms, amendments are notified under clause 9.2 (Renewal) with the right to decline.

**15.5 Waiver.** A failure to exercise or delay in exercising any right under this Agreement does not constitute a waiver of that right.

**15.6 Severability.** If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions continue in full force and effect.

**15.7 Force Majeure.** Neither Party is liable for failure or delay in performance (other than an obligation to pay money) caused by events outside its reasonable control, including acts of God, war, terrorism, civil unrest, strikes (other than strikes involving its own workforce), pandemic, internet or telecoms failure, or governmental action. The affected Party will notify the other promptly and use reasonable efforts to mitigate.

**15.8 Third Party Rights.** A person who is not a Party has no rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

**15.9 No Partnership.** Nothing in this Agreement creates a partnership, agency, employment or joint venture between the Parties.

**15.10 Notices.** Legal notices under this Agreement (including notices of termination, material breach or claim) are given in writing by email to the Firm's operational notices address recorded in the Order Form or the click-through acceptance record, copied to [hello@onepointfourwest.com](mailto:hello@onepointfourwest.com) for notices to OPFW, and additionally by recorded-delivery post to the registered office for Signed Variant relationships. Operational notices (renewal reminders, breach notifications under the DPA, sub-processor change notices) are given by email to the nominated address and take effect on the next Business Day after sending.

**15.11 Counterparts and Electronic Signature.** Where this Agreement is executed as the Signed Variant, it may be executed in counterparts, each of which when signed is an original and all of which together form one and the same document. Electronic signatures (including via Adobe Acrobat Sign or DocuSign) are valid and binding.

## Execution (Signed Variant)

This section is used only for the Signed Variant. For the Click-Through Variant, acceptance is recorded as described in the Acceptance section above and no signature is required.

**For and on behalf of One Point Four West Ltd**

Signed: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**For and on behalf of the Firm**

Signed: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

## **Schedule 1 — Data Processing Agreement**

**Data Controller:** the Firm (as defined in the Agreement).

**Data Processor:** One Point Four West Ltd.

This Data Processing Agreement ("**DPA**") forms part of and is subject to the Agreement. Terms defined in the Agreement have the same meaning in this DPA. In the event of conflict between this DPA and the main body of the Agreement, this DPA prevails in respect of data protection matters.

Acceptance of this DPA is effected together with the Agreement, by the same Click-Through or Signed Variant route described in the Acceptance section of the Agreement.

### **S1-1. Scope and Purpose of Processing**

**S1-1.1** This DPA sets out the terms on which OPFW processes Personal Data on behalf of the Firm in connection with the Platform services provided under the Agreement.

**S1-1.2** OPFW processes Personal Data solely for the purpose of:

- authenticating Authorised Users and managing user accounts;
- storing and retrieving Client Data entered by Authorised Users;
- generating diagnostic reports, portfolio views and exports;
- scoping data access to the Firm via row-level security policies; and
- where the Firm opts in, sending anonymised diagnostic data to the Anthropic API for AI-enhanced analysis.

**S1-1.3** OPFW does not process Personal Data for any purpose other than providing the Platform services. OPFW may retain and use aggregated data that does not constitute Personal Data under UK Data Protection Laws (see clause S1-11.3).

### **S1-2. Personal Data Processed**

##### Categories of Data Subjects

- Authorised Users (employees or contractors of the Firm).
- Client contacts (individuals whose contact details are recorded in client records by Authorised Users).

##### Types of Personal Data

- **Authorised User data:** name, email address, firm association, role (admin or consultant), profile biography, specialisms, contact email, contact phone, logo, authentication tokens and session metadata.

- **Client contact data:** client organisation name, sector, contact name, contact email, contact role, contact phone, headcount, structure, HR team size, trade union status, source.
- **Diagnostic assessment data:** maturity ratings, domain scores, red and green flag selections, question answers and notes, session timestamps, completion status, activity log entries.

**S1-2.3** The Platform does not collect Personal Data directly from the individuals being assessed. Assessment data relates to organisational maturity, not individual performance.

**S1-2.4** The Platform does not collect special category data (Article 9 UK GDPR) or criminal offence data (Article 10 UK GDPR). The Firm will not enter such data into free-text fields without first notifying OPFW in writing and confirming an appropriate lawful basis under Article 9 or 10 UK GDPR.

### **S1-3. Duration of Processing**

**S1-3.1** Processing continues for the duration of the Agreement. On termination, OPFW will retain Client Data for up to 90 days to allow data export, then permanently delete it. User account data is deleted within 30 days of account closure.

### **S1-4. Processor Obligations**

**S1-4.1** OPFW will:

- process Personal Data only on the Firm's documented instructions (including those set out in the Agreement and this DPA), unless required to do so by law;
- where required to process by law, inform the Firm of the legal requirement before processing (unless prohibited by law on important grounds of public interest);
- ensure that persons authorised to process the Personal Data are subject to written obligations of confidentiality or statutory obligations of confidentiality;
- implement the technical and organisational measures set out in clause S1-5 to ensure the security of Personal Data;
- comply with the conditions for engaging sub-processors set out in clause S1-6;
- assist the Firm in responding to data subject rights requests, insofar as this is possible using the Platform's functionality, within 5 Business Days of receipt of the Firm's written request;
- assist the Firm in ensuring compliance with Articles 32 to 36 UK GDPR (security, breach notification, DPIAs and prior consultation);
- at the Firm's choice, delete or return all Personal Data on termination and delete existing copies unless retention is required by law; and
- make available to the Firm all information necessary to demonstrate compliance with Article 28 UK GDPR and allow for and contribute to audits conducted by the Firm or its appointed auditor, in accordance with clause S1-10.

### **S1-5. Technical and Organisational Measures**

**S1-5.1** OPFW implements the following technical and organisational measures:

##### Data at rest

- Primary database (Supabase) hosted on AWS United Kingdom (London, eu-west-2), encrypted at rest using AES-256.
- Row-level security (RLS) policies enforce firm-level data isolation at database level.
- Application-level encryption of session data stored in browser localStorage using AES-256-GCM. Keys are derived via PBKDF2 (100,000 iterations, SHA-256) from a server-issued per-session secret. The secret is generated by a Supabase Edge

Function that authenticates the calling user against the Supabase Auth API before issuing. The secret is returned once per session, held only in the browser sessionStorage, rotates every 24 hours and on each new login, and is cleared on sign-out. Keys are never persisted to disk.

#### ##### Data in transit

- HTTPS (TLS 1.2 or higher) for all data transmission between the Platform and the Authorised User's browser.
- API keys for third-party services are stored server-side and never exposed to the browser.

#### ##### Access control

- Authentication managed by Supabase Auth, supporting password and magic-link flows; multi-factor authentication available for administrators.
- Seat limits enforced at authentication time.
- OPFW administrator access to production data is restricted to named personnel and logged.
- Firm tenant access is scoped via row-level security; OPFW staff do not access firm tenant data except where (a) supporting a specific firm-reported issue with that firm's authorisation, or (b) responding to a legal obligation or incident. All such access is logged.

#### ##### AI-enhanced analysis

- Organisation name anonymised before transmission to the Anthropic API.
- Data transmitted via server-side proxy; API key not exposed to the browser.
- Rate limiting applied at 60 requests per hour per IP address.

#### ##### Temporary files

- Generated DOCX and PPTX reports stored in a non-public temporary directory.
- Temporary files automatically deleted after 1 hour.

#### ##### Operational controls

- Incident Response Plan maintained and reviewed at least annually.
- Documented change management and code review processes.
- Database backups taken by Supabase in line with its standard service; backup retention and recovery targets available from OPFW on reasonable request.

## **S1-6. Sub-processors**

**S1-6.1** The Firm authorises OPFW to engage the sub-processors set out in Annex A, as updated from time to time. The current list is also published on OPFW's website.

**S1-6.2** OPFW will notify the Firm of any intended changes to sub-processors at least 30 days before the change takes effect. The Firm may object to a new sub-processor on reasonable grounds within 14 days of notification. If the objection cannot be resolved in good faith, the Firm may terminate the Agreement on 30 days' written notice, and OPFW will refund any pro-rata prepaid Fees for the period after termination.

**S1-6.3** OPFW ensures that each sub-processor is bound by written contractual obligations no less onerous than those set out in this DPA.

**S1-6.4** Stripe processes payment and billing data relating to the Firm (not Client Data). This processing is undertaken by Stripe as an independent controller for payment processing purposes and as a processor on behalf of OPFW for billing data. OPFW's processing of Firm billing data is described in OPFW's privacy notice.

## **S1-7. International Transfers**

**S1-7.1** Where Personal Data is transferred outside the UK, the transfer is protected by one or more of the following mechanisms: UK International Data Transfer Addendum to the EU Standard Contractual Clauses (IDTA); Standard Contractual Clauses with the UK Addendum; or the UK Extension to the EU-US Data Privacy Framework ("UK-US Data Bridge") where the relevant sub-processor participates.

**S1-7.2** OPFW has conducted a Transfer Impact Assessment (TIA) for each non-UK sub-processor, available to the Firm on reasonable request.

**S1-7.3** The primary data storage location (Supabase on AWS) is within the United Kingdom (London, eu-west-2). Personal Data does not leave the UK except where the Firm opts in to AI-enhanced analysis (Anthropic, US, under the IDTA) or where Stripe processes payments and billing (Ireland and US).

**S1-7.4** OPFW reviews transfer mechanisms at least annually and retains copies of the relevant transfer agreements.

## **S1-8. Data Breach Notification**

**S1-8.1** OPFW will notify the Firm without undue delay, and in any event within 24 hours, upon becoming aware of a personal data breach affecting Client Data or Authorised User data.

**S1-8.2** The notification will include, to the extent available at the time:

- the nature of the breach, including the categories and approximate number of data subjects and records concerned;
- the likely consequences of the breach;
- the measures taken or proposed to address the breach and mitigate its effects; and
- the contact point for further information.

**S1-8.3** OPFW will cooperate with the Firm in investigating and mitigating the breach and in meeting the Firm's obligations under Articles 33 and 34 UK GDPR.

## **S1-9. Data Subject Rights**

**S1-9.1** OPFW will assist the Firm in responding to requests from data subjects exercising their rights under UK GDPR, including rights of access, rectification, erasure, restriction, portability and objection, within 5 Business Days of receipt of the Firm's written request.

**S1-9.2** If OPFW receives a request directly from a data subject, it will promptly redirect the request to the Firm unless legally required to respond directly.

## **S1-10. Audit Rights**

**S1-10.1** OPFW will make available to the Firm, on reasonable request, all information necessary to demonstrate compliance with this DPA.

**S1-10.2** The Firm or its appointed auditor may conduct an audit of OPFW's data processing activities, provided that: (a) at least 30 days' written notice is given; (b) audits are conducted during normal business hours; (c) audits do not unreasonably disrupt OPFW's operations; (d) the auditor has signed a confidentiality undertaking in a form reasonably acceptable to OPFW; and (e) the Firm bears its own costs of the audit.

**S1-10.3** Audits are limited to once per calendar year unless a personal data breach or regulatory investigation requires additional audit.

**S1-10.4** OPFW may satisfy its audit obligations by providing the Firm with a current independent third-party certification (for example ISO/IEC 27001 or SOC 2 Type II) together with a summary of relevant controls, where such certification is held.

## S1-11. Data Deletion and Return

**S1-11.1** On termination of the Agreement, and subject to the 90-day export period set out in clause 10 of the Agreement, OPFW will permanently delete all Client Data from the Platform and from its sub-processors.

**S1-11.2** OPFW will provide written confirmation of deletion on request.

**S1-11.3** OPFW may retain non-personal, aggregated data that cannot be linked to any identified or identifiable natural person or organisation, for the purpose of improving the Platform, provided this data does not constitute Personal Data under UK Data Protection Laws.

## S1-12. General

**S1-12.1** This DPA is governed by the laws of England and Wales.

**S1-12.2** In the event of any conflict between this DPA and the main body of the Agreement, this DPA prevails in respect of data protection matters.

**S1-12.3** OPFW's data protection contact is Tim Withnall (dpo@onepointfourwest.com). ICO registration number: ZC106734.

## Annex A: Sub-processor List

Current as at the Effective Date. Updates notified to the Firm by email at least 30 days in advance as set out in clause S1-6.2.

Sub-processor	Purpose	Location	Transfer Mechanism
IONOS SE	Web hosting, server-side report generation and temporary report files	United Kingdom	UK-resident data; no international transfer
Supabase Inc. (on AWS)	Database, authentication and file storage for the Platform and GPG Reporter aggregate storage	AWS United Kingdom (London, eu-west-2)	UK-resident data at rest; SCCs with UK Addendum govern US-parent access (support and operations); Supabase DPA in place
Stripe Payments Europe Ltd / Stripe Inc.	Subscription billing, payment processing and Customer Portal (billing data only, not Client Data)	Ireland (EU) and United States	SCCs with UK Addendum; PCI DSS Level 1
Postmark (Wildbit, LLC / ActiveCampaign)	Transactional email delivery (magic links, user invites, billing notifications, incident alerts, service emails)	United States	SCCs with UK Addendum
Google LLC (Google Analytics)	Marketing website analytics (onepointfourwest.com only, IP-anonymised, no Platform telemetry; consent-gated)	United States	SCCs with UK Addendum; UK Extension to the EU-US Data Privacy Framework
Anthropic PBC	AI narrative generation (optional,	United States	UK International Data Transfer Addendum

Sub-processor	Purpose	Location	Transfer Mechanism
	anonymised). No training on inputs/outputs; 7-day trust and safety retention only		(IDTA); TIA on file
Microsoft Corporation (Microsoft 365, OneDrive, Teams)	Internal business systems used by OPFW staff (not used for Platform processing)	United Kingdom primary region; US parent	UK data residency; SCCs with UK Addendum
Otter.ai, Inc.	Optional meeting transcription (opt-in, consultancy engagements only; not used in Platform processing)	United States (AWS US-West)	UK Extension to the EU-US Data Privacy Framework; SCCs with UK Addendum fallback

## Schedule 2 — Acceptable Use Policy

This Acceptable Use Policy ("**AUP**") forms part of and is subject to the Agreement. It applies to all firms and Authorised Users under the Agreement. Capitalised terms have the meanings given in the Agreement.

### S2-1. Scope

This AUP applies to all use of the Platform, including Diagnostic Tools, Platform Output, the admin interface, and any APIs or integrations.

### S2-2. Acceptable Use

The Platform is provided for conducting HR and people diagnostic assessments for the Firm's own clients under the terms of the Agreement. Firms and Authorised Users must:

- use the Platform lawfully and for legitimate business purposes;
- comply with the Agreement, the DPA, and Applicable Law;
- keep credentials secure and not share accounts;
- ensure that data uploaded to the Platform is accurate and lawfully collected;
- review AI-enhanced analysis before relying on or sharing it with clients.

### S2-3. Prohibited Use

Firms and Authorised Users must not:

- use the Platform for any unlawful, fraudulent or deceptive purpose;
- upload or process special category data (Article 9 UK GDPR) or criminal offence data (Article 10 UK GDPR) without a documented lawful basis and prior written notification to OPFW;
- attempt to access Client Data or accounts belonging to another firm;
- reverse-engineer, decompile, disassemble or extract the underlying software, frameworks or methodologies of the Platform, except where permitted by law;
- introduce malicious code (including viruses, trojans, ransomware) or interfere with Platform operations;

- conduct penetration testing, vulnerability scans or automated security testing without OPFW's prior written consent;
- share account credentials between individuals or circumvent Seat Limits;
- use the Platform to benchmark or develop a competing product;
- send spam, phishing or unsolicited marketing through Platform Output;
- impersonate any person or misrepresent the source or nature of any communication;  
or
- use the Platform in a manner that could reasonably be expected to damage the reputation of OPFW.

#### **S2-4. AI Features**

Where AI-enhanced analysis is enabled, the Firm acknowledges that:

- AI outputs are provided for convenience only and are not warranted for accuracy;
- Authorised Users must review and, where appropriate, edit AI outputs before relying on or sharing them;
- the feature is optional and can be disabled at any time.

#### **S2-5. Reporting and Enforcement**

Suspected breaches of this AUP, security incidents or misuse should be reported to OPFW at [hello@onepointfourwest.com](mailto:hello@onepointfourwest.com) without delay.

Where OPFW reasonably believes acceptable use has been breached, OPFW will notify the firm administrator and give 7 days to cure, except where the breach is a credible security threat or involves unlawful activity, in which case OPFW may suspend access immediately and investigate. Serious or repeated breaches may result in termination of the Agreement under clause 9.3 of the Agreement.

#### **S2-6. Changes to This Schedule**

OPFW may update this AUP from time to time. Material changes will be notified to the Firm by email at least 30 days before taking effect. The current version of this AUP forms Schedule 2 of the Platform Agreement in force at the time of notification.

## **Schedule 3 — Order Form**

The Order Form sets out the commercial details of the licence (tier, Seat Limit, Fees, Initial Term and billing cycle). For self-serve subscriptions, the Order Form is completed at checkout and confirmed in the acceptance record; for Signed Variant relationships, the Order Form is issued by OPFW and executed alongside this Agreement.