

# DATA PROCESSING AGREEMENT

pursuant to Article 28 of the UK GDPR

between

**The Controller (the subscribing organisation)**

and

**REVELIO SOFTWARE LTD (trading as Phanera)**

Company number: 17198982

ICO registration reference: ZC140751

(the Processor)

Version 2.0, August 2026

*Supersedes version 1.0 (March 2026). Schedule 3 is the complete list of authorised sub-processors; clauses 13 and 14 cover artificial intelligence features and public portal cookies. The platform loads no analytics tag or hosted font service on any page it serves to the Controller or to the public.*

## Contents

|                   |                                                    |
|-------------------|----------------------------------------------------|
| <b>1</b>          | Introduction and scope                             |
| <b>2</b>          | Definitions                                        |
| <b>3</b>          | Scope and details of processing                    |
| <b>4</b>          | Controller obligations                             |
| <b>5</b>          | Processor obligations                              |
| <b>6</b>          | Sub-processors                                     |
| <b>7</b>          | Security measures                                  |
| <b>8</b>          | Security incidents                                 |
| <b>9</b>          | Data retention and deletion                        |
| <b>10</b>         | Audit and inspection                               |
| <b>11</b>         | Data subject rights                                |
| <b>12</b>         | International data transfers                       |
| <b>13</b>         | Artificial intelligence features                   |
| <b>14</b>         | Public portals, cookies and analytics              |
| <b>15</b>         | Liability                                          |
| <b>16</b>         | Term and termination                               |
| <b>17</b>         | Governing law and jurisdiction                     |
| <b>18</b>         | Contact                                            |
| <b>Schedule 1</b> | Processing details (Article 28(3))                 |
| <b>Schedule 2</b> | Technical and organisational measures (Article 32) |
| <b>Schedule 3</b> | Authorised sub-processors                          |
| <b>Schedule 4</b> | Controller-directed third-party integrations       |
| <b>Schedule 5</b> | International transfers and safeguards             |
| <b>Schedule 6</b> | Execution and record of acceptance                 |

## 1. Introduction and Scope

1.1 This Data Processing Agreement (DPA) is entered into between the organisation subscribing to the Phanera platform (Controller) and REVELIO SOFTWARE LTD, company number 17198982, trading as Phanera (Processor). This DPA forms part of, and is supplemental to, the Terms & Conditions governing the Controller's use of the Phanera platform.

1.2 This DPA sets out the terms on which the Processor will process personal data on behalf of the Controller pursuant to Article 28 of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1.3 In the event of any conflict between this DPA and the Terms & Conditions, the provisions of this DPA shall prevail in respect of data protection matters. Where the Controller's own procurement contract, call-off terms or processing instructions impose stricter data protection obligations on the Processor, those stricter obligations prevail over this DPA to the extent of the inconsistency.

1.4 This DPA shall remain in effect for the duration of the Controller's subscription and for as long as the Processor retains any personal data processed on the Controller's behalf.

1.5 This DPA is accepted electronically by an administrator of the Controller before the platform may be used. The record of that acceptance is described in Schedule 6.

## 2. Definitions

2.1 In this DPA, the following terms have the meanings set out below. Capitalised terms not defined here have the meanings given in the UK GDPR or the Terms & Conditions.

- **Personal Data:** any information relating to an identified or identifiable natural person processed by the Processor on behalf of the Controller through the Phanera platform.
- **Processing:** any operation performed on personal data, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, restriction, erasure, or destruction.
- **Data Subjects:** individuals whose personal data is processed through the platform, including but not limited to requesters, staff members, and third parties involved in information rights requests, complaints, and related correspondence.
- **Sub-processor:** any third party engaged by the Processor to process personal data on the Controller's behalf, as listed in Schedule 3.
- **Controller-directed Integration:** a third-party system that the Controller chooses to connect to the platform using its own credentials or tenancy, as described in Schedule 4. The Processor is not the controller or processor of any processing carried out by such a system on the Controller's own account.
- **AI Features:** the optional platform functions described in clause 13 that submit content to a third-party large language model or embedding model.
- **Security Incident:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

## 3. Scope and Details of Processing

3.1 The details of the processing carried out under this DPA are set out in Schedule 1 (Processing Details). The Processor shall process personal data only to the extent, and in such manner, as is necessary to provide the Phanera platform and related services.

3.2 The Processor shall not process the personal data for any purpose other than as set out in this DPA and the Controller's documented instructions, unless required to do so by applicable law. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.3 The Processor shall not sell, rent, or otherwise make available personal data to any third party for their own commercial purposes.

3.4 The Processor shall not use the Controller's personal data to train, fine-tune or otherwise develop machine learning models, whether its own or a third party's, and shall contract with its sub-processors on that basis (see clause 13).

## 4. Controller Obligations

4.1 The Controller warrants that it has the legal basis to process the personal data and to instruct the Processor to process it on the Controller's behalf.

4.2 The Controller is responsible for ensuring the accuracy and lawfulness of the personal data provided to the Processor.

4.3 The Controller shall issue documented instructions to the Processor regarding the processing of personal data. The Controller acknowledges that the Processor's obligation is to process personal data in accordance with such documented instructions.

4.4 The Controller is responsible for its own configuration choices within the platform, including retention periods (clause 9), whether AI Features are enabled (clause 13), whether CAPTCHA is enabled on public forms, which Controller-directed Integrations are connected (Schedule 4), and the privacy information it publishes to data subjects.

## 5. Processor Obligations

The Processor shall:

- **Documented instructions:** Process personal data only on documented instructions from the Controller, including with regard to transfers of personal data outside the United Kingdom, unless required to do so by applicable law. If the Processor believes an instruction from the Controller infringes the UK GDPR or other applicable data protection law, the Processor shall immediately inform the Controller.
- **Confidentiality:** Ensure that all persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- **Security:** Implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as set out in clause 7 and Schedule 2 (Technical and Organisational Measures).
- **Sub-processing:** Not engage another processor (sub-processor) without prior general written authorisation of the Controller, subject to the provisions of clause 6 and the list at Schedule 3.
- **Assistance with data subject rights:** Taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising data subjects' rights under Chapter III of the UK GDPR.
- **Assistance with obligations:** Assist the Controller in ensuring compliance with Articles 32 to 36 of the UK GDPR, taking into account the nature of processing and the information available to the Processor, including by providing the information in Schedules 1 to 5 for the purpose of the Controller's data protection impact assessments.
- **Deletion or return:** At the choice of the Controller, delete or return all personal data to the Controller after the end of the provision of services, and delete existing copies unless applicable law requires storage of the personal data. The specific provisions for deletion are set out in clause 9.
- **Audit:** Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the UK GDPR, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, subject to clause 10.

## 6. Sub-processors

6.1 The Controller provides general written authorisation to the Processor to engage sub-processors. The sub-processors authorised at the date of this DPA are listed in Schedule 3 (Authorised Sub-processors), which identifies for each sub-processor the service provided, the categories of personal data involved, the processing location and the applicable transfer safeguard.

6.2 Schedule 3 distinguishes between core sub-processors, which are engaged for every Controller, and conditional sub-processors, which are engaged only where the Controller enables the relevant platform feature. A conditional sub-processor processes no personal data of a Controller that has not enabled that feature.

6.3 The Processor shall notify the Controller of any intended changes to sub-processors (additions or replacements) at least 30 days before the change takes effect, by email to the Controller's registered administrator contact, giving the Controller the opportunity to object to such changes.

6.4 If the Controller objects to a new sub-processor on reasonable data protection grounds within 14 days of receiving notice, the Processor shall use reasonable efforts to make available an alternative arrangement. If no alternative is reasonably available, either party may terminate the affected service by giving 30 days' written notice, without penalty to the Controller and with a pro-rata refund of any prepaid fees for the terminated service.

6.5 The Processor shall impose the same data protection obligations as set out in this DPA on any sub-processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures.

6.6 The Processor shall remain fully liable to the Controller for the performance of any sub-processor's obligations.

6.7 The Processor shall maintain Schedule 3 as the current and complete record of its sub-processors and shall reissue this DPA with an incremented version number whenever Schedule 3 changes. The third-party systems listed in Schedule 4 are not sub-processors of the Processor and are not subject to clauses 6.1 to 6.6.

## 7. Security Measures

7.1 The Processor shall implement and maintain the technical and organisational measures described in Schedule 2 (Technical and Organisational Measures). These measures include, but are not limited to:

- Encryption of all personal data at rest using AES-256 and in transit using TLS 1.2 or higher.
- Multi-tenant data isolation at the database level, with each organisation's data scoped by organisation identifier and cross-tenant access prevented at both application and query layers.
- Storage of sensitive credentials (API keys, client secrets, email pipeline passwords, SSO secrets) in Azure Key Vault with hardware-backed encryption and least-privilege managed identity access.
- Role-based access control with granular permission flags, supporting custom roles per organisation.
- Two-factor authentication (TOTP) and single sign-on (OIDC) support.
- Input validation, HTML sanitisation, CSRF protection, parameterised queries, and file upload validation.
- Comprehensive audit logging of all significant actions with timestamps, user identifiers, and details.
- 24/7 infrastructure monitoring with automated alerting.

7.2 The Processor shall regularly review and, where necessary, update these measures to ensure they remain appropriate to the risks presented by the processing. Any change shall maintain a level of protection no lower than that described in Schedule 2.

## 8. Security Incidents

8.1 The Processor shall notify the Controller without undue delay, and in any event no later than 72 hours after becoming aware of a Security Incident.

8.2 The notification shall include:

- (a) A description of the nature of the Security Incident, including the categories and approximate number of data subjects and personal data records concerned.
- (b) The name and contact details of the point of contact from whom further information may be obtained.
- (c) A description of the likely consequences of the Security Incident.
- (d) A description of the measures taken or proposed to be taken to address the Security Incident, including measures to mitigate its possible adverse effects.

8.3 The Processor shall cooperate with the Controller and take reasonable steps to assist the Controller in meeting its obligations under Articles 33 and 34 of the UK GDPR.

8.4 The Processor shall notify the Controller of any Security Incident affecting a sub-processor listed in Schedule 3 that involves the Controller's personal data, on the same timescale and in the same form, from the point at which the Processor becomes aware of it.

8.5 The Processor shall not make any public statement identifying the Controller in connection with a Security Incident without the Controller's prior written agreement, unless required by law or by a regulator.

## 9. Data Retention and Deletion

9.1 The Phanera platform supports configurable retention periods per request type. Each request type (FOI, SAR, EIR, GDPR, complaints, and any custom types) may be assigned its own retention period by the Controller.

9.2 When a request is closed or moved to trash and the applicable retention period has elapsed, all personal data associated with that request (including messages, attachments, notes, audit log entries, requester information linked solely to that request, and any AI embeddings derived from it) shall be automatically and permanently deleted from the platform.

9.3 The Controller is responsible for configuring appropriate retention periods within the platform. The Processor shall provide the tools necessary for the Controller to do so.

9.4 Upon termination or expiry of the subscription, or at any time on the Controller's own initiative:

- (a) The Controller may export all of its data, including every stored document, at any time and without the Processor's involvement, in a commonly used, machine-readable format.
- (b) The Controller may instruct the Processor to either return all personal data in a commonly used, machine-readable format, or to permanently delete all personal data.
- (c) The Controller may erase its organisation itself from within the platform, without the Processor's involvement. Erasure takes effect seven days after it is requested. Throughout that period the service continues unchanged and any administrator holding the relevant permission may cancel it; no data is destroyed, restricted or made read-only before the period expires.
- (d) On erasure the Processor shall permanently delete all of the Controller's personal data, including all records, all stored documents, the audit trail, and every backup and export archive. Backup archives are destroyed as part of the erasure and are not retained for any rotation, quarantine or recovery period. The Processor thereafter retains no copy of the Controller's personal data, save only for the deletion certificate described at clause 9.5.
- (e) If the Controller neither gives an instruction under (b) nor erases its organisation under (c) within 30 days of termination, the Processor shall permanently delete all personal data within 90 days of termination.

9.5 The Processor shall issue a numbered deletion certificate to each administrator holding the erasure permission. The certificate is issued before the deletion is carried out, and records the reference, who requested the erasure, the time of completion and the number of records destroyed in each table. It is retained outside the erased data and may be reissued against its reference at any time afterwards, when there is no longer an organisation to sign in to.

## 10. Audit and Inspection

10.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out in this DPA and Article 28 of the UK GDPR.

10.2 The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller. The Controller shall give the Processor at least 30 days' written notice of any audit or inspection.

10.3 Audits shall be conducted during normal business hours, shall not unreasonably disrupt the Processor's operations, and shall be subject to reasonable confidentiality obligations.

10.4 The Processor may charge a reasonable fee for time spent supporting audits that exceed one audit per 12-month period, unless the audit is triggered by a Security Incident or regulatory investigation.

10.5 In respect of the sub-processors listed in Schedule 3, the Processor shall on request provide the Controller with the sub-processor's current data processing terms, published certifications and, where available, third-party audit reports, in place of direct inspection of the sub-processor's facilities.

## 11. Data Subject Rights

11.1 The Processor shall promptly assist the Controller in responding to requests from data subjects exercising their rights under Chapter III of the UK GDPR, including rights of access, rectification, erasure, restriction of processing, data portability, and objection.

11.2 The platform provides tools enabling the Controller to manage and respond to data subject rights requests directly. Where additional assistance is required, the Processor shall provide it within a reasonable timeframe.

11.3 If the Processor receives a request from a data subject directly, the Processor shall promptly redirect the data subject to the Controller and notify the Controller of the request.

## 12. International Data Transfers

12.1 All personal data stored by the platform on the Controller's behalf (the database, file attachments, backups and outbound email) is held within the United Kingdom, using Microsoft Azure regions in the United Kingdom and Azure Communication Services with a United Kingdom data location.

12.2 Certain sub-processors listed in Schedule 3 process personal data outside the United Kingdom, either in transit (content delivery and bot protection) or as part of an optional feature enabled by the Controller (AI Features). Schedule 5 identifies each such transfer, the destination, and the safeguard relied upon.

12.3 Where personal data is transferred outside the United Kingdom, the Processor shall ensure that appropriate safeguards are in place in accordance with Chapter V of the UK GDPR, namely an adequacy decision, the International Data Transfer Agreement (IDTA), or the UK Addendum to the EU Standard Contractual Clauses, and shall carry out a transfer risk assessment where required.

12.4 The Processor shall not introduce a new category of international transfer without first notifying the Controller in accordance with clause 6.3.

12.5 A Controller that requires processing wholly within the United Kingdom may disable the AI Features and CAPTCHA described in Schedule 3 as conditional sub-processing. The residual transfers listed in Schedule 5 as in-transit processing cannot be disabled without terminating the service. No transfer arises from analytics or font delivery, because the platform performs neither.

## 13. Artificial Intelligence Features

13.1 The platform offers optional AI Features: semantic indexing of requests, detection of duplicate or related requests, drafting of suggested responses from previously closed requests, and suggestion of redactions in uploaded documents.

13.2 Where the Controller enables AI Features, the text of the request, related correspondence, and text extracted from documents selected for analysis is transmitted to Google's Gemini API for embedding or generation. That text may contain personal data, including special category data where the Controller's records contain it.

13.3 The resulting embeddings are stored within the platform's own database in the United Kingdom and are deleted with the request they belong to under clause 9.2.

13.4 The Processor contracts with the provider of the AI Features on terms that prohibit the use of the Controller's content to train or improve the provider's models, and does not itself use that content for model development.

13.5 AI output is a suggestion only. The Controller remains responsible for reviewing and approving any response, disclosure or redaction before it is issued. No decision producing legal effects concerning a data subject is taken by automated means.

13.6 The Controller may disable AI Features at any time. Where they are disabled, no content is transmitted to the AI sub-processor.

## **14. Public Portals, Cookies and Analytics**

14.1 The platform hosts branded public portals through which members of the public submit requests and view disclosure logs. Portal pages are delivered through the content delivery and bot-protection sub-processors listed in Schedule 3.

14.2 Strictly necessary cookies and equivalent storage are used for session management, authentication and cross-site request forgery protection.

14.3 Where the Controller enables CAPTCHA on public forms, the CAPTCHA provider receives the visitor's IP address, browser and device signals and interaction data, and sets cookies in the visitor's browser. This feature is configured by the Controller using its own provider account keys.

14.4 No page of the platform, whether portal, public or administrative, loads an analytics tag, tag manager, advertising pixel or hosted font service. Fonts and icons are served from the platform's own origin, so a portal page discloses the visitor's IP address to no third party other than the content delivery and bot-protection sub-processors named in Schedule 3. This is enforced in the build: the front-end build fails if a third-party asset host appears in the compiled application, or if the analytics used on the Processor's own marketing website (clause 14.6) is reachable from any other page.

14.5 The Controller is responsible for the privacy notice and any cookie notice published on its portal, and for obtaining consent where required by the Privacy and Electronic Communications Regulations 2003 for anything other than strictly necessary cookies.

14.6 Separately from the platform, the Processor's own marketing website (phanera.co.uk and its news and gallery pages) uses Google Analytics, loaded only after the visitor accepts it and never before. The Processor is the controller of that processing; it is not carried out on the Controller's behalf and is therefore not sub-processing under this DPA. It reaches no portal page, no page of the platform itself, and no personal data processed on the Controller's behalf.

## **15. Liability**

15.1 Each party shall be liable for damage caused by processing that infringes the UK GDPR in accordance with Article 82 of the UK GDPR.

15.2 The Processor shall be liable for damage caused by processing only where it has not complied with obligations of the UK GDPR specifically directed to processors, or where it has acted outside or contrary to the Controller's lawful instructions.

## 16. Term and Termination

16.1 This DPA shall come into effect on the date the Controller first subscribes to the Phanera platform, or on the date the Controller accepts this version, whichever is later, and shall remain in force for the duration of the subscription.

16.2 Where the Processor issues a new version of this DPA, the Controller shall be prompted to review and accept it. Continued use of the platform following acceptance of a new version replaces the previous version prospectively; acceptance records for earlier versions are retained as evidence under Schedule 6.

16.3 Clauses 5 (Processor Obligations: deletion or return), 8 (Security Incidents), 9 (Data Retention and Deletion), 10 (Audit and Inspection), and 15 (Liability) shall survive termination of this DPA.

## 17. Governing Law and Jurisdiction

17.1 This DPA shall be governed by and construed in accordance with the laws of England and Wales.

17.2 Any dispute arising out of or in connection with this DPA shall be subject to the exclusive jurisdiction of the courts of England and Wales.

## 18. Contact

For queries regarding this DPA, to object to a sub-processor under clause 6.4, or to exercise any rights under it, contact the Processor at:

- REVELIO SOFTWARE LTD
- Email: [contact@revelio.co.uk](mailto:contact@revelio.co.uk)
- ICO registration reference: ZC140751

## Schedule 1: Processing Details

*Given pursuant to Article 28(3) of the UK GDPR.*

### Subject matter of processing

The provision of the Phanera information rights management platform, including request intake, tracking, correspondence, disclosure, and compliance reporting.

### Duration of processing

For the duration of the Controller's subscription to the Phanera platform, plus any post-termination retention period as set out in clause 9.

### Nature and purpose of processing

- Account management, authentication and authorisation of the Controller's staff
- Processing, tracking, and managing information rights requests (FOI, SAR, EIR, GDPR, complaints, and custom request types)
- Inbound email ingestion and outbound message delivery
- Verification of requester identity where the Controller requires it for subject access requests
- Third-party consultation and internal review workflows
- Redaction and preparation of disclosure packs
- Optional AI-assisted duplicate detection, response drafting and redaction suggestion (clause 13)
- Generating compliance reports, audit logs, and the ICO Annual Return
- Hosting branded public portals and disclosure logs
- Applying retention policies and automatic deletion of expired requests
- Subscription administration and billing

### Types of personal data

- Requester names, email addresses, postal addresses, and contact details
- Content of information rights requests and associated correspondence
- Attachments and supporting documents submitted by requesters or staff
- Identity verification documents uploaded in support of a subject access request
- Staff names, email addresses, roles, and activity logs
- Authentication credentials (hashed passwords, TOTP secrets, SSO tokens)
- IP addresses, session metadata and DPA acceptance records
- Billing contact details of the Controller's administrator
- Any personal data contained within request responses and disclosed documents

### Categories of data subjects

- Members of the public submitting information rights requests
- Staff members of the Controller who use the platform
- Third parties referenced in or consulted during request processing

### Special categories of data

The Processor does not intentionally process special categories of personal data. However, such data may be present in the content of requests, attachments, identity documents, or disclosed documents uploaded by the Controller or requesters, and may consequently be included in content submitted to AI Features where the Controller has enabled them. The Controller is responsible for ensuring it has a lawful basis for processing any such data.

**Frequency of processing**

Continuous, for the duration of the subscription.

## Schedule 2: Technical and Organisational Measures

*Given pursuant to Articles 28(3)(c) and 32 of the UK GDPR.*

### Infrastructure and hosting

- Hosted on Microsoft Azure in United Kingdom regions
- Application workloads run in isolated container environments on a private virtual network, with the database reachable only from that network
- All data at rest encrypted using AES-256
- All data in transit encrypted using TLS 1.2 or higher
- Encrypted database backups retained per backup rotation schedule
- 24/7 infrastructure monitoring with automated alerting

### Access control

- Multi-tenant architecture with database-level data isolation per organisation
- Cross-tenant access prevented at application and query layers
- Role-based access control with granular permission flags and custom roles per organisation
- Passwords hashed using industry-standard algorithms
- Two-factor authentication (TOTP) supported for all user accounts
- Single sign-on via OpenID Connect (OIDC) with support for Microsoft Entra ID, Google, AWS, and other compliant identity providers
- Bearer token session management with configurable expiry and administrator revocation

### Credential management

- Sensitive credentials stored in Azure Key Vault with hardware-backed encryption
- No secrets stored in source code or production configuration files
- Key Vault access restricted to application managed identity with least-privilege policies
- Secret access fully logged and auditable

### Application security

- Input validation and sanitisation at the API boundary
- HTML sanitisation on all rich-text fields to prevent cross-site scripting (XSS)
- State-based CSRF tokens for sensitive operations
- Parameterised queries via Entity Framework Core to prevent SQL injection
- File uploads validated, size-limited, and stored in isolated per-organisation directories
- Edge DDoS mitigation, TLS termination and web application firewall

### Audit and monitoring

- Comprehensive audit logging of all significant actions with timestamps, user identifiers, and action details
- User activity timelines recording logins, actions, and session history
- Administrative action logs for accountability and compliance
- Email delivery tracking with full inbound and outbound logs
- DPA acceptance records capturing organisation, user, version, timestamp and IP address

### Data retention controls

- Configurable retention periods per request type

- Automatic permanent deletion of all data associated with closed requests once the retention period has elapsed
- Manual deletion capabilities available to authorised administrators
- Backup overwrite cycle not exceeding 30 days

**Organisational measures**

- Confidentiality obligations in the contracts of all personnel with access to personal data
- Access to production systems limited to named personnel on a least-privilege basis
- Written contracts imposing equivalent data protection obligations on every sub-processor listed in Schedule 3
- Documented incident response process meeting the 72-hour notification requirement in clause 8

## Schedule 3: Authorised Sub-processors

The following sub-processors are authorised to process personal data on behalf of the Controller as at the date of this DPA. This Schedule is the complete list for the purposes of clause 6. Systems that the Controller connects using its own credentials or tenancy (its mailbox, document storage, identity provider, reporting tools and webhook endpoints) are not sub-processors of the Processor and are listed separately at Schedule 4.

| Sub-processor                                                                            | Service provided                                                                                                                                                                                                                                       | Personal data involved                                                                                                                                                                                   | Location and transfer safeguard                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Core sub-processors: engaged for every Controller</b>                                 |                                                                                                                                                                                                                                                        |                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                         |
| <b>Microsoft Ireland Operations Limited (Microsoft Azure)</b>                            | Cloud hosting of the application containers; PostgreSQL database; blob storage of attachments and identity documents; Key Vault; application configuration; platform logging and monitoring; outbound email delivery via Azure Communication Services. | All personal data held in the platform, including request content, attachments, staff and requester records, audit logs and outbound email.                                                              | United Kingdom Azure regions; Azure Communication Services configured with a United Kingdom data location. Microsoft support access from outside the UK is governed by the Microsoft Products and Services Data Protection Addendum, incorporating the EU Standard Contractual Clauses and UK Addendum. |
| <b>Cloudflare, Inc.</b>                                                                  | Authoritative DNS, TLS termination, DDoS mitigation, web application firewall, content delivery, and issuance of custom hostnames for Controller-branded portals.                                                                                      | Visitor and staff IP addresses, request metadata (URL, user agent, timestamps), and page and API content while in transit.                                                                               | Global edge network, with traffic normally served from United Kingdom or European points of presence. Cloudflare's Data Processing Addendum incorporating the EU Standard Contractual Clauses and UK Addendum. No persistent storage of request content.                                                |
| <b>Stripe Payments UK Limited (with Stripe, Inc.)</b>                                    | Subscription billing, checkout, invoicing and payment processing for the Controller's subscription.                                                                                                                                                    | Billing contact name and email address, organisation name, billing address, subscription and invoice records. Card details are captured directly by Stripe; the Processor never receives or stores them. | United Kingdom and EEA, with onward transfer to the United States under Stripe's Data Processing Agreement incorporating the EU Standard Contractual Clauses and UK Addendum. Stripe acts as an independent controller for fraud prevention and for its own regulatory obligations.                     |
| <b>Conditional sub-processors: engaged only where the Controller enables the feature</b> |                                                                                                                                                                                                                                                        |                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                         |
| <b>Google Ireland Limited (Gemini API)</b>                                               | AI Features under clause 13: semantic embedding of requests, duplicate and related request detection, drafting of suggested responses, and redaction suggestions.                                                                                      | Request text, correspondence and text extracted from documents submitted for analysis, which may include special category data present in the Controller's records.                                      | Google data centres, which may be outside the United Kingdom. Google's Cloud Data Processing Addendum incorporating the EU Standard Contractual Clauses and UK Addendum. Content is not used to train Google's models. Not engaged where AI Features are disabled.                                      |
| <b>Google Ireland Limited (reCAPTCHA)</b>                                                | Bot and abuse protection on public request submission forms, where the Controller enables CAPTCHA and supplies its own reCAPTCHA keys.                                                                                                                 | Portal visitor IP address, browser and device signals, and interaction data. Cookies are set in the visitor's browser.                                                                                   | Google data centres, including outside the United Kingdom. Google's Data Processing Terms incorporating the EU Standard Contractual Clauses and UK Addendum. Not engaged where CAPTCHA is disabled.                                                                                                     |

*The Processor shall notify the Controller at least 30 days in advance of any intended addition to or replacement of a sub-processor, in accordance with clause 6.3, and shall reissue this DPA with an incremented version number.*

*The Processor's own marketing website uses consent-gated analytics as described in clause 14.6. That is the Processor's own processing as controller, reaches no page of the platform and no portal, and is recorded here for completeness rather than as sub-processing under Article 28.*

## Schedule 4: Controller-directed Third-party Integrations

The systems below are connected at the Controller's own election, using the Controller's own accounts, tenancies or endpoints. They are not sub-processors engaged by the Processor and are listed here for completeness and for the Controller's data protection impact assessment. Where the Processor holds credentials for such a system, those credentials are protected by the measures in Schedule 2.

| System                                                                           | How it is used                                                                                                                                                              | Data protection position                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Microsoft 365 (Exchange Online, Microsoft Graph, SharePoint and OneDrive)</b> | Connecting the Controller's own mailbox for inbound and outbound request correspondence, and browsing the Controller's own document libraries to attach files to a request. | Connected by the Controller using its own tenancy and OAuth consent. Microsoft acts for the Controller under the Controller's own agreement with Microsoft. Access tokens are held encrypted in Azure Key Vault by the Processor. |
| <b>Google Workspace (Gmail and Google Drive)</b>                                 | Connecting the Controller's own mailbox for request correspondence, and browsing the Controller's own Drive files to attach them to a request.                              | Connected by the Controller using its own Google account and OAuth consent. Google acts for the Controller under the Controller's own agreement with Google.                                                                      |
| <b>SMTP and IMAP servers nominated by the Controller</b>                         | Sending and collecting request correspondence where the Controller uses a mail server other than Microsoft 365 or Google Workspace.                                         | Operated by or for the Controller. Credentials are held encrypted in Azure Key Vault by the Processor.                                                                                                                            |
| <b>OpenID Connect identity providers</b>                                         | Single sign-on for the Controller's staff, using Microsoft Entra ID, Google, AWS or another compliant provider chosen by the Controller.                                    | Selected and configured by the Controller. Client secrets are held encrypted in Azure Key Vault by the Processor.                                                                                                                 |
| <b>Microsoft Power BI and other reporting tools</b>                              | The Controller pulls its own case data from the platform's reporting feed into its own analytics environment.                                                               | The Controller is responsible for the security and lawfulness of processing in its own analytics environment once data leaves the platform.                                                                                       |
| <b>Webhook endpoints configured by the Controller</b>                            | Delivering platform event notifications to a URL of the Controller's choosing.                                                                                              | The destination is chosen by the Controller, which is responsible for the security of that endpoint and for any onward processing.                                                                                                |
| <b>GOV.UK Bank Holidays API</b>                                                  | Retrieving the published list of bank holidays so that statutory working-day deadlines are calculated correctly.                                                            | No personal data is transmitted. Not a processor of personal data.                                                                                                                                                                |

## Schedule 5: International Transfers and Safeguards

This Schedule supports the Controller's transfer risk assessment under Chapter V of the UK GDPR. It lists every transfer of personal data outside the United Kingdom arising from the Processor's own sub-processing. Transfers arising from a Controller-directed Integration under Schedule 4 are a matter for the Controller's own agreement with that provider.

| Recipient                  | Data transferred                                                                                             | Destination                                                             | Safeguard and necessity                                                                                                                                                                         |
|----------------------------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Microsoft (Azure)</b>   | Support access to platform data in exceptional circumstances. Stored data does not leave the United Kingdom. | United Kingdom, with possible support access from EEA and United States | Microsoft Products and Services Data Protection Addendum, incorporating the EU Standard Contractual Clauses and the UK Addendum. Necessary for the provision of the hosting service.            |
| <b>Cloudflare</b>          | IP addresses, request metadata and page content in transit.                                                  | Global edge network; normally United Kingdom or EEA points of presence  | Cloudflare Data Processing Addendum with the EU Standard Contractual Clauses and UK Addendum. Necessary to deliver and protect the service; cannot be disabled without terminating the service. |
| <b>Stripe</b>              | Billing contact details and subscription records.                                                            | United Kingdom and EEA, with onward transfer to the United States       | Stripe Data Processing Agreement with the EU Standard Contractual Clauses and UK Addendum. Necessary to take payment for the subscription.                                                      |
| <b>Google (Gemini API)</b> | Request text, correspondence and extracted document text submitted to AI Features.                           | Google data centres, which may be outside the United Kingdom            | Google Cloud Data Processing Addendum with the EU Standard Contractual Clauses and UK Addendum. Optional: avoided entirely by disabling AI Features.                                            |
| <b>Google (reCAPTCHA)</b>  | Portal visitor IP address, device signals and interaction data.                                              | Google data centres, which may be outside the United Kingdom            | Google Data Processing Terms with the EU Standard Contractual Clauses and UK Addendum. Optional: avoided entirely by disabling CAPTCHA.                                                         |

*A Controller that requires processing wholly within the United Kingdom can achieve it by disabling AI Features and CAPTCHA. The residual transfers are then limited to data in transit through the content delivery and security layer, and to billing data.*

## Schedule 6: Execution and Record of Acceptance

### Incorporation

This DPA is incorporated into and forms part of the Terms & Conditions governing the Controller's use of the Phanera platform.

### Electronic acceptance

An administrator of the Controller accepts this DPA within the platform before the service may be used. On acceptance the Processor records the Controller organisation, the accepting user, the version accepted, the date and time of acceptance, and the IP address from which acceptance was given. That record is retained for the duration of the subscription and is available to the Controller on request as evidence of the Article 28 contract.

Where the Processor issues a new version, administrators of the Controller are prompted to review and accept it; records of earlier acceptances are retained.

### Version history

| Version | Date        | Change                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.0     | March 2026  | First issue.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 2.0     | August 2026 | Schedule 3 reissued as the complete list of authorised sub-processors, identifying each service, the personal data involved and the transfer safeguard. Schedule 4 added for Controller-directed integrations, Schedule 5 for international transfers and Schedule 6 for execution. New clauses 13 (artificial intelligence features) and 14 (public portals, cookies and analytics). Analytics and hosted fonts removed from every page of the platform and confined to the Processor's own marketing website behind consent. Clauses 1, 3, 4, 5, 6, 8, 10, 12 and 16 extended accordingly. |

### Signature (optional)

Electronic acceptance within the platform is sufficient to bind both parties. Where the Controller's procurement process requires a signed counterpart, this page may be executed in addition to, and without displacing, the electronic acceptance record.

| For the Controller | For the Processor |
|--------------------|-------------------|
| Name:              | Name:             |
| Position:          | Position:         |
| Signature:         | Signature:        |
| Date:              | Date:             |