Part 1

Processing Details

Processor	**Nara Solicitors Ltd**, Spaces Canary Wharf, 25 Cabot Square, London E14 4QZ, United Kingdom. Authorised and regulated by the Solicitors Regulation Authority (SRA No. 8006464). Company number 15219728 · ICO registration ZB670355.
Customer name	_____
Customer address	_____ _____
Customer contact	_____
Customer role	Controller (the sponsoring employer)
Effective date	The date the Customer first accepts the Main Agreement or this DPA, whichever is earlier.
Categories of personal data stored or processed through the Services	• Identity & contact: name, address, contact details, date of birth. • Immigration & right-to-work: passport, visa/BRP, Certificate of Sponsorship, RTW/ECS evidence. • Employment: role, SOC code, contract, salary. • Financial: bank/payment details for payroll evidence. • Attendance & absence records. • Any other information the Customer records in accordance with the Main Agreement.
Special categories of personal data	None solicited by the platform. Immigration records can incidentally reveal special-category information; the Customer is responsible for its Article 9 condition (commonly Art. 9(2)(b) — employment law) and must not upload other special-category data in free-text fields without a lawful basis.
Categories of data subjects	The Customer's sponsored workers, prospective workers and, where relevant, their emergency contacts and key personnel.
Frequency of the processing	Continuous, for the duration of the Main Agreement.
Nature of the processing	Storage, organisation, display, reminder generation, export and deletion.
Purpose of the processing	The performance of the Services: hosting and management of UK sponsor-licence compliance records on behalf of the Customer. No automated decision-making with legal effect.

Retention period	The duration of the Main Agreement, plus a 30-day post-termination export window, after which data is deleted per clause 4.8 of Part 2.
Sub-processors	As set out in Schedule 1.

This DPA forms part of the Terms and Conditions and applies from the Customer's acceptance of the Terms. By signing below, the Customer agrees to the data processing terms set out in Part 2 of this Data Processing Agreement and warrants that the information in Part 1 of this Data Processing Agreement is complete and accurate.

Signed for and on behalf of the Customer (entity name):

_____

Name: _____

Position: _____

Date: _____

Part 2

Data Processing Terms

(Version dated 29 July 2026)

This Data Processing Agreement, comprising Part 1 (*Processing Details*) and Part 2 (*Data Processing Terms*) (together, the "DPA") supplements and, from the date on which the Customer accepts the Main Agreement or otherwise agrees to this DPA, forms part of the Sponsor Licence Compliance Guru Terms and Conditions, or such other agreement entered into between the Customer and Nara Solicitors Ltd relevant to the Customer's use of the Services (the "Main Agreement"). It reflects UK GDPR Article 28.

1. DEFINITIONS

1.1 "Personal Data", "Data Subject", "Processing", "Controller", "Processor", "Sub-processor" and "Personal Data Breach" have the meanings given in the UK GDPR and the Data Protection Act 2018. "Customer Data" means the Personal Data the Controller enters or uploads into the platform, as described in Part 1.

1.2 For the purposes of clause 4.7, a Personal Data Breach does not include unsuccessful or trivial incidents that do not compromise the security of Customer Data — for example pings, port scans, or blocked or failed access attempts that are routinely repelled.

2. ROLE OF THE PARTIES

2.1 For Customer Data, the **Customer is the controller** and **Nara Solicitors Ltd is the processor**, processing Customer Data only to provide and support the Sponsor Licence Compliance Guru platform.

2.2 For the Customer's own account, security, audit and billing data, Nara Solicitors Ltd acts as an independent controller under its Privacy & Cookies Policy — that data is outside this DPA. Where the Customer separately engages Nara Solicitors Ltd for legal services, any processing for that matter is carried out by the firm in its capacity as a solicitor under its own client-care terms, not as a processor under this DPA.

3. DETAILS OF DATA PROCESSING

3.1 The subject matter, duration, nature, purpose and frequency of the Processing, the types of personal data and the categories of data subject are set out in Part 1 (Processing Details).

4. PROCESSOR OBLIGATIONS

Nara Solicitors Ltd shall:

4.1 **Documented instructions.** Process Customer Data only on the Customer's documented instructions (the Main Agreement, this DPA, and use of the platform's features), including as to international transfers, unless required by law — in which case it will inform the Customer first unless the law forbids it. If Nara Solicitors Ltd considers that an instruction infringes data-protection law, it will inform the Customer without undue delay and may, without liability, suspend or decline to carry out that instruction until the Customer confirms or amends it (UK GDPR Art. 28(3)). Without limiting the foregoing, Nara Solicitors Ltd will never:

(a) sell Customer Data or make it available to any third party for consideration;

(b) share Customer Data with any third party for advertising or marketing purposes;

(c) use Customer Data to train machine-learning or AI models;

(d) combine Customer Data with data from other customers or other sources, except as needed to provide the Services; or

(e) retain, use or disclose Customer Data for any purpose other than providing and supporting the platform, or as required by law.

4.2 **Confidentiality.** Ensure personnel authorised to process Customer Data are bound by confidentiality and are subject to the firm's professional confidentiality obligations as solicitors.

4.3 **Security.** Implement appropriate technical and organisational measures (UK GDPR Art. 32) designed to ensure the security of Customer Data, taking into account the nature, scope, context and purposes of the Processing and its risks. Such measures will meet the minimum standards set out in Schedule 2 (Information Security Measures) and may be updated from time to time provided the level of security is not materially reduced.

4.4 **Sub-processors.** The Customer authorises the sub-processors listed in Schedule 1. Nara Solicitors Ltd will impose data-protection obligations equivalent to this DPA on each, remains liable for their performance, will give the Customer prior notice of any intended addition or replacement, and — if the Customer reasonably objects on data-protection grounds within 14 days — will either not appoint that sub-processor or allow the Customer to terminate the Main Agreement without penalty for the affected service.

4.5 **Data-subject rights.** Taking account of the nature of the processing, assist the Customer by appropriate technical and organisational measures to respond to data-subject requests (access, rectification, erasure, restriction, portability, objection). The platform's self-service export and delete features are provided for this purpose and are sufficient to meet this obligation in the ordinary course. A request received directly is forwarded to the Customer within 5 working days and not otherwise responded to, except to confirm it should go to the Customer. Assistance beyond the platform's self-service features may be provided at the Customer's reasonable and documented cost.

4.6 **Assistance.** Assist the Customer in complying with UK GDPR Articles 32–36 (security, breach notification, data-protection impact assessments and prior consultation), taking into account the nature of the processing and the information available to us. Assistance beyond making available the platform's existing security and compliance documentation may be provided at the Customer's reasonable and documented cost.

4.7 **Breach notification.** Notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Data — and where feasible within 48 hours — with the information then available that the Customer reasonably needs to meet its own notification duties. Further information will follow in phases as it becomes available. Such notification is not an acknowledgement of fault or liability.

4.8 **Deletion or return.** On termination, at the Customer's choice, delete or return all Customer Data and delete existing copies (subject to any legal retention requirement and to routine backup cycles, from which data is purged within the documented backup-retention window, currently up to 7 days). A customer-initiated account deletion in the platform deletes Customer Data immediately from the live system. On request, written confirmation is provided that deletion is complete, including when the backup purge window ends. A return is provided in the platform's standard export format at the Customer's reasonable cost. The Customer may request return or export of Customer Data within 30 days of termination (the "Retention Period"); on expiry of the Retention Period, deletion proceeds as above.

4.9 **Audits.** Make available the information necessary to demonstrate compliance with this clause. The Customer agrees to rely first on the Processor's then-current security documentation, policies and any third-party certifications or audit reports, made available on request under confidentiality — and, where such documentation is dated within the previous 12 months and the Processor confirms no material changes to the audited controls, to accept it in lieu of a physical audit of those controls. Where that is not sufficient to address a specific, reasonable concern, the Customer (or an independent auditor it mandates who is not a competitor of the Processor and is bound by confidentiality) may audit on at least 30 days' prior written notice, with scope and timing agreed in writing in advance, no more than once in any 12-month period (or following a Personal Data Breach affecting the Customer's Customer Data), during normal business hours, in a manner that does not materially disrupt the Processor's operations or compromise other customers' security, and at the Customer's own cost. Audit results are the Processor's confidential information, save that the Customer may use them to meet its own regulatory obligations.

4.10 **Inability to comply.** Notify the Customer promptly if it determines that it can no longer meet its obligations under applicable data-protection law. In that case the Customer may suspend the affected processing and/or exercise its termination rights under the Main Agreement, and Nara Solicitors Ltd will take reasonable and appropriate steps to stop and remediate any unauthorised processing of Customer Data.

4.11 **Public-authority requests.** If Nara Solicitors Ltd receives a legally binding request for Customer Data from a public authority (including a court order or statutory demand), it will notify the Customer before disclosure unless legally prohibited from doing so, disclose only the minimum required to comply, and — where reasonable — challenge a request it considers overbroad or unlawful.

5. CONTROLLER OBLIGATIONS

5.1 The Customer shall:

(a) ensure it has a lawful basis (and, for special-category data, a condition and the worker's explicit consent) to process the Customer Data it uploads;

(b) give only lawful instructions; and

(c) be responsible for the accuracy, quality and legality of the Customer Data and of its collection;

(d) keep its user accounts and credentials secure and use the two-factor authentication the platform provides;

(e) ensure only authorised personnel access the platform on its behalf and remove access promptly when no longer required; and

(f) notify Nara Solicitors Ltd without undue delay if it knows or suspects that an account credential has been compromised.

5.2 **Immigration-law responsibility.** The Customer remains solely responsible for its compliance with UK immigration law, its sponsor-licence duties, Home Office guidance and its employment obligations. The Services support the Customer's record-keeping and monitoring activities but do not constitute legal or immigration advice and do not guarantee compliance, sponsor-licence retention, or any Home Office outcome; automated indications, reminders and scores are aids only and the Customer must not rely on them as a substitute for its own checks or professional advice.

6. INTERNATIONAL TRANSFERS

6.1 Customer Data is hosted in the EU (the Supabase database and document storage are in Ireland, eu-west-1); application hosting and transactional email are processed in the UK (London). Customer Data will not be intentionally transferred or relocated outside the UK or EEA without prior notice to the Customer and an appropriate transfer mechanism in place. Where any sub-processor processes Customer Data outside the UK, Nara Solicitors Ltd will ensure an appropriate transfer mechanism is in place — a UK adequacy decision, or the UK International Data Transfer Agreement / Addendum to the EU Standard Contractual Clauses with a transfer risk assessment. Schedule 1 records the position for each sub-processor.

7. LIABILITY AND INDEMNITY

7.1 Each party is liable for its own breaches of data-protection law and this DPA. The parties' total aggregate liability arising out of or in connection with this DPA is subject to, and counts towards, the limitations and exclusions of liability in the Main Agreement, except where the law does not permit such limitation. This DPA does not create any liability for the Processor beyond that which would exist under the Main Agreement and applicable data-protection law.

7.2 The Customer shall indemnify and hold harmless Nara Solicitors Ltd against any claims, fines, losses and reasonable costs arising from the Customer's own breach of its obligations under clause 5, including its failure to have a lawful basis or (where it uploads special-category data) a valid Article 9 condition, the inaccuracy or unlawful collection of Customer Data, or instructions that infringe data-protection law. This indemnity does not apply to the extent the loss is caused by the Processor's own breach of this DPA or its negligence.

8. GOVERNING LAW

8.1 This DPA is governed by the law of England and Wales, and the courts of England and Wales have exclusive jurisdiction, consistent with the Main Agreement.

9. TERM, DELETION AND SURVIVAL

9.1 This DPA takes effect on the Effective Date and continues for as long as Nara Solicitors Ltd processes Customer Data. Provisions that by their nature should survive termination (including clauses 4.8, 7, 9 and 10) survive.

10. PRECEDENCE AND VARIATION

10.1 This DPA forms part of, and is supplemental to, the Main Agreement. In the event of any conflict between this DPA and the Main Agreement on a data-protection matter, this DPA prevails to the extent of that conflict; on all other matters the Main Agreement prevails.

10.2 Nara Solicitors Ltd may update this DPA on reasonable prior notice where necessary to reflect a change in data-protection law or guidance, a new or replacement transfer mechanism (for example an updated version of the UK IDTA or EU Standard Contractual Clauses), or a change to its sub-processors under clause 4.4, provided no such update materially reduces the protection of Customer Data. Any other variation must be agreed in writing by both parties.

11. ANONYMISED DATA AND NOTICES

11.1 Nara Solicitors Ltd may create and use aggregated, anonymised statistics derived from use of the platform (for example feature usage counts) that do not identify, and cannot reasonably be linked to, any Data Subject or any Customer. Such statistics are not Customer Data or Personal Data. Nara Solicitors Ltd will not attempt to re-identify anonymised data and will require the same of any recipient.

11.2 Formal notices under this DPA are given: to the Customer, via the email address registered on its account or the contact stated in Part 1; and to Nara Solicitors Ltd, via privacy@narasolicitors.com (data protection), security@narasolicitors.com (security matters) or dpo@narasolicitors.com (the Data Protection Officer). Notice is effective on the working day after sending, absent a delivery failure.

Schedule 1

Sub-processors

Sub-processor	Description of processing	Location	Transfer safeguard
Supabase	Database and document storage	EU — Ireland (eu-west-1)	EU hosting (UK adequacy applies UK→EU); Art. 28 DPA executed 8 July 2026 incl. EU SCCs + UK Addendum and documented security measures (AES-256 at rest incl. backups, TLS, per-project keys in FIPS 140-2 HSMs)
Vercel	Application hosting / edge delivery	UK — London (eu-west-2, lhr1)	Processed in the UK; Vercel DPA's SCCs + UK Addendum cover any incidental support access from outside the UK
Amazon Web Services (Amazon SES)	Transactional email (confirmation, reminders, notices)	UK — London (eu-west-2)	Processed in the UK; AWS DPA; SCCs + UK Addendum cover any incidental non-UK support access
Functional Software, Inc. (Sentry)	Error monitoring — technical error reports; systems are designed not to include worker records (active only when error monitoring is enabled)	EU / US	Sentry DPA; SCCs + UK Addendum
postcodes.io	UK postcode → address lookup	UK	No personal data sent (postcode only)
Cloudflare, Inc. (Turnstile)	Bot protection (CAPTCHA) on the public signup form	Global edge network	Visitor IP/browser signals only during signup — no Customer Data or worker records sent; Cloudflare DPA; SCCs + UK Addendum

Schedule 2

Information Security Measures

Nara Solicitors Ltd protects Customer Data with the following minimum technical and organisational measures. They may be strengthened or updated over time; they will not be materially reduced (clause 4.3).

Encryption

All network communication is protected by TLS. Data is encrypted at rest (AES-256, including backups) by the hosting sub-processor, with per-project keys protected by hardware security modules. Two-factor authentication secrets are additionally encrypted at application level (AES-256-GCM).

Authentication and access control

Two-factor authentication (TOTP) is mandatory for all customer, worker-portal and administrator accounts — no SMS-based 2FA. Sessions use short-lived, revocable tokens bound to the browser; idle sessions are logged out. Rate limiting and brute-force protections apply to all authentication endpoints. Production access follows least privilege; administrative functions run in a separate, independently authenticated realm.

Tenant isolation

Application-level tenant scoping is enforced on every data access and verified by automated checks in the deployment pipeline, so one customer cannot access another’s data. Documents are held in private storage and served only via short-lived signed links scoped to the owning account.

Monitoring and logging

Security-relevant actions are recorded in an append-only audit log retained for a minimum of 12 months unless a longer period is agreed or required by law. Email delivery, reminder despatch and system health are monitored through operational dashboards.

Vulnerability management and secure development

Dependencies are monitored for published vulnerabilities and patched promptly. Changes pass automated security gates (tenant-scoping lint, database-migration safety) and testing before release. The codebase undergoes independent security code reviews; findings are triaged and remediated on a risk basis.

Backups, continuity and recovery

Customer Data is backed up at least daily; backups are encrypted and stored separately from the live database, and deleted data is purged from backup cycles within the documented window (clause 4.8). The recovery point objective is no more than 24 hours of data. Restoration of service after a data-loss event is targeted within one working day on a reasonable-endeavours basis. Documented disaster-recovery and business-continuity procedures are maintained and reviewed.

Responsible disclosure

Nara Solicitors Ltd welcomes good-faith reports of suspected security vulnerabilities to security@narasolicitors.com and will not pursue researchers acting in good faith and within the law.