

# ProSuitability — Due Diligence & Data Security Summary

Version 1.2 | 09 July 2026

This document summarises how ProSuitability handles data and security for UK FCA-authorised financial advice firms evaluating or using the service. It is intended for compliance files, outsourcing registers, and supplier due diligence. It supplements — and does not replace — the Licence Agreement and Data Processing Agreement (version 2026-07-09).

## Document control

| Field                               | Detail                                                                          |
|-------------------------------------|---------------------------------------------------------------------------------|
| Document title                      | ProSuitability — Due Diligence & Data Security Summary                          |
| Version                             | 1.2                                                                             |
| Publication date                    | 09 July 2026                                                                    |
| Author                              | Bluegrove Financial Solutions Ltd (trading as ProSuitability)                   |
| Review cycle                        | Reviewed when material changes occur; at least annually                         |
| Contractual reference               | Licence Agreement and Data Processing Agreement, version 2026-07-09             |
| General enquiries                   | <a href="mailto:hello@prosuitability.co.uk">hello@prosuitability.co.uk</a>      |
| Privacy / data protection enquiries | <a href="mailto:privacy@prosuitability.co.uk">privacy@prosuitability.co.uk</a>  |
| Website                             | <a href="https://www.prosuitability.co.uk">https://www.prosuitability.co.uk</a> |

## 1. Executive summary

ProSuitability is a cloud-hosted suitability report writing service for UK FCA-authorised financial advice firms. The platform helps advisers and paraplanners produce structured, consistent suitability reports from a managed content library. Client and case data entered by a subscribing firm is processed on the firm's instructions. The firm remains the data controller for client personal data; Bluegrove Financial Solutions Ltd acts as a data processor.

ProSuitability is designed for a regulated environment: access is role-based, significant actions are logged, completed reports are preserved as produced, and hosting is in the United Kingdom. This document describes those measures plainly. It does not constitute a compliance guarantee, regulatory approval, or certification of your firm's advice processes.

## 2. Service overview

ProSuitability provides:

- A web application for creating, editing, and exporting suitability reports;
- A managed content library with firm-level customisation (suppression rules and authored variants);
- Case and client record management linked to report production;
- Role-based user access within each subscribing firm;
- Audit logging of significant workflow and administration actions;
- Word (.docx) export of completed reports.

ProSuitability does not provide:

- Regulated financial advice or a substitute for adviser judgment;
- A compliance surveillance or central monitoring dashboard;
- Supervisor lockdown or mandatory multi-step approval workflows;
- Automated validation against external fact-finds or back-office systems (in the current release);
- A bundled human compliance advisory service.

### 3. Supplier information

| Item              | Detail                                                                                                                         |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Legal entity      | Bluegrove Financial Solutions Ltd                                                                                              |
| Trading name      | ProSuitability                                                                                                                 |
| Company number    | 6363970 (England and Wales)                                                                                                    |
| Registered office | 20a Moreton Avenue, Harpenden, Hertfordshire AL5 2ET                                                                           |
| Regulatory status | Software supplier to FCA-authorised firms; not an FCA-authorised firm                                                          |
| ICO registration  | Registered with the UK Information Commissioner's Office (ICO) as a data processor. Registration details available on request. |
| Governing law     | England and Wales (see Licence Agreement)                                                                                      |

### 4. Regulatory and contractual framework

When a firm subscribes to ProSuitability, it enters into the Licence Agreement and Data Processing Agreement (together, the "Agreement"). Key points for due diligence:

- Your firm is the data controller for client personal data submitted to the service;
- Bluegrove Financial Solutions Ltd is the data processor for that client data;
- We process personal data only on your documented instructions, as set out in the Agreement;

- The Agreement includes processor obligations under UK GDPR (security measures, sub-processor controls, breach notification, assistance with data-subject requests, and deletion/return on termination);
- ProSuitability is a tool to assist report production. Your firm remains solely responsible for the suitability of advice, sign-off before client delivery, and compliance with FCA rules and data protection law.

The current Agreement version is 2026-07-09, published at <https://www.prosuitability.co.uk/legal/licence/> . Firms accept this version at signup; the accepted version is recorded against the firm account.

## 5. Data processed

The categories of data processed depend on how your firm uses the service.

### 5.1 Client and case data (processor data)

- Client identity and contact details (e.g. name, date of birth, address);
- Financial circumstances and objectives entered for suitability reporting;
- Recommendations, case notes, and report content;
- Report sign-off and export records.

Special category data may be included if your firm enters it (for example health-related information relevant to protection recommendations). Your firm is responsible for ensuring a valid lawful basis and appropriate notices are in place before submitting such data.

### 5.2 Firm user and account data

- Firm administrator, adviser, paraplanner, and viewer account details;
- Authentication credentials and security settings (including two-factor authentication where enabled);
- Firm settings, billing contact details, and FCA Firm Reference Number (FRN);
- Usage and audit metadata (see section 10).

### 5.3 Purpose and location of processing

Data is processed to provide, secure, and support the ProSuitability service — including report production, access control, billing, auditability, and service communications. Routine processing takes place in the United Kingdom (London region). We do not routinely transfer client or case data outside the UK.

## 6. Security controls

We implement technical and organisational measures appropriate to a regulated SaaS product handling confidential advice data, in line with Article 32 UK GDPR and the Agreement.

| Control area            | Summary                                                                                                                                                                                                                                                                                      |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access control          | Role-based access within each firm: Firm Admin, Adviser (Content Author), and Viewer roles. Users see only what their role permits. Firms are isolated from one another (tenant separation).                                                                                                 |
| Authentication          | Minimum 12-character passwords; 40-minute inactivity session timeout; two-factor authentication (TOTP) mandatory for Firm Admin accounts and optional for other roles; trusted-device option (30 days) for 2FA bypass; account lockout after five failed login attempts (15-minute lockout). |
| Encryption in transit   | All web traffic over HTTPS/TLS 1.2 or higher. Visitor connections terminate at Cloudflare's edge network; traffic between Cloudflare and our UK application origin uses TLS.                                                                                                                 |
| Network edge protection | Public web traffic to prosuitability.co.uk is proxied through Cloudflare (reverse proxy and unmetered DDoS mitigation on the Free plan). Application and database hosting remain in London; Cloudflare does not store firm client or case database content.                                  |
| Encryption at rest      | Database encrypted at rest on managed PostgreSQL infrastructure.                                                                                                                                                                                                                             |
| Audit logging           | Append-only audit log of significant actions (see section 10).                                                                                                                                                                                                                               |
| Report integrity        | Completed reports and historical cases are preserved as produced. Library and configuration changes apply only to future work, not retroactively to signed-off reports.                                                                                                                      |
| Personnel access        | Platform operator access to production data is limited to what is reasonably necessary for support, security, and operations, under confidentiality obligations.                                                                                                                             |

Certifications: ProSuitability does not currently hold ISO 27001 or SOC 2 certifications. Under clause 15.2 of the Agreement, subscribing firms may request reasonable demonstration of compliance (including relevant policies and control descriptions) once in any 12-month period, subject to confidentiality and reasonable costs.

## 7. Hosting and data residency

| Component                        | Provider / region                                   | Notes                                           |
|----------------------------------|-----------------------------------------------------|-------------------------------------------------|
| Public web edge (DNS, TLS, DDoS) | Cloudflare — global edge network; origin London, UK | Authoritative DNS, reverse proxy, and unmetered |

|                     |                                              |                                                                                      |
|---------------------|----------------------------------------------|--------------------------------------------------------------------------------------|
|                     |                                              | standard DDoS mitigation for proxied hostnames. Does not host application databases. |
| Application hosting | DigitalOcean App Platform — London, UK       | Primary web application runtime.                                                     |
| Primary database    | DigitalOcean Managed PostgreSQL — London, UK | Client, case, report, and configuration data.                                        |
| Object storage      | DigitalOcean Spaces — London, UK             | File storage where applicable.                                                       |
| Primary backups     | DigitalOcean managed backup — UK             | Daily automated backups; point-in-time recovery; 30-day retention.                   |
| Offsite backups     | DigitalOcean Spaces — London, UK             | Weekly encrypted backups; 12-month retention; separate DO project.                   |

Client and case data processed through the live application is hosted in UK data centres. Cloudflare processes HTTP request metadata at the edge (such as IP address and requested URLs) but does not host or store firm client or case database content. We do not use other sub-processors that routinely access client or case content except as necessary to provide hosting and database services.

## 8. Sub-processors

We engage the following sub-processors in connection with the service. Material changes are notified in accordance with the Agreement (including publication of an updated list).

| Sub-processor | Purpose                                                                      | Data accessed                                                                                          | Location                                                                             |
|---------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Cloudflare    | Authoritative DNS, reverse proxy, and DDoS mitigation for public web traffic | HTTP request metadata (IP address, user agent, URLs requested) — not firm client/case database content | Global edge network; origin application in United Kingdom (London)                   |
| DigitalOcean  | Application hosting, managed database, object storage, primary backups       | All firm client/case data stored in the service                                                        | United Kingdom (London)                                                              |
| Stripe        | Subscription billing and payment processing                                  | Firm billing contact, payment metadata — not client/case content                                       | See Stripe's data processing terms; payments processed under Stripe's infrastructure |
| Resend        | Transactional email (account, billing, and                                   | Recipient email addresses and                                                                          | See Resend's data processing terms                                                   |

|            |                                                                                   |                                                                                                                                                                                    |                                                                              |
|------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
|            | service notifications)                                                            | message content for service emails only                                                                                                                                            |                                                                              |
| xAI (Grok) | Optional AI Modules (Ask Support; Paraplanner review / Needs & Demands companion) | Clipped case snapshots, letter excerpts, interaction notes, and fact-find text submitted by authorised users when AI features are enabled — not the full firm client/case database | See xAI's data processing / API terms; international transfers as applicable |

No other sub-processors routinely access client or case data entered into ProSuitability for report production. AI Module processing is limited to inputs authorised users submit when those features are enabled.

## 9. Retention, exit, and data return

Retention balances your firm's need to access records with storage minimisation after a subscription ends.

| Phase                                            | Firm access          | Summary                                                                                                                                                                                                                      |
|--------------------------------------------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Active subscription                              | Full access          | Client, case, and report data retained for the life of the subscription.                                                                                                                                                     |
| Read-only (post-cancellation or payment failure) | View and export only | Historical reports, clients, and cases remain viewable and exportable to Word. New cases, edits, and sign-off are blocked. Billing details may be updated to restore full access. Typically 90 days.                         |
| Cold storage                                     | No firm access       | After the read-only period, data is moved to cold storage and is no longer accessible through the application.                                                                                                               |
| Deletion                                         | N/A                  | Data is deleted in accordance with the Agreement and your firm's instructions, subject to legal retention requirements. Cold-stored data is deleted after approximately two years from cancellation unless otherwise agreed. |

Firms are notified by email in advance of transitions between retention phases. On termination, we will delete or return personal data as set out in the Agreement, except where retention is required by law.

Audit log entries are retained for at least seven years to support accountability and regulatory recordkeeping expectations, even where associated operational data has been deleted. Audit entries record that data existed and what actions were taken.

## **10. Auditability within the product**

ProSuitability maintains an append-only firm audit log. Significant events recorded include (non-exhaustive):

- User login, logout, and failed authentication;
- Two-factor authentication setup and use;
- User account creation, deactivation, and role changes;
- Case creation, editing, sign-off, and supersession;
- Report viewing and Word export;
- Firm settings and suppression rule changes;
- Configuration history changes and restorations;
- Billing and subscription status changes.

Each audit entry includes a UTC timestamp, actor (where applicable), action, target, and relevant metadata. Firm Admins can review their firm's audit log within the application.

Immutability principle: changes to library content, firm settings, or configuration affect future reports only. Previously saved cases and signed-off reports are preserved exactly as produced, with the content versions and settings that applied at that time.

## **11. Availability, support, and incidents**

### **11.1 Service availability**

We use reasonable endeavours to make ProSuitability available 24 hours a day, seven days a week, except for planned maintenance (notified in advance where practicable) and emergency maintenance. The service is provided over the public internet; we are not responsible for networks outside our reasonable control. There is no formal uptime SLA with service credits at the current price point.

### **11.2 Support**

Reasonable helpdesk support is provided on business days by email ([hello@prosuitability.co.uk](mailto:hello@prosuitability.co.uk)). Support covers use of ProSuitability and does not extend to faults caused by firm equipment, networks, operator error, or third-party services not supplied by us.

### 11.3 Personal data breaches

If we become aware of a personal data breach affecting your firm's personal data, we will notify you without undue delay in accordance with clause 11.4.7 of the Agreement, with information reasonably available to assist your breach assessment and regulatory obligations.

## 12. Business continuity and backups

Operational resilience measures include:

- Daily automated database backups with point-in-time recovery (30-day window);
- Weekly encrypted offsite backups to DigitalOcean Spaces, retained for 12 months in a separate DO project (UK region);
- Encryption of backups at rest;
- Documented restore procedures for disaster scenarios (hosting outage, corruption, account compromise).

Backup and restore capabilities are operational safety measures. Firms should maintain their own copies of exported reports and critical records as part of their file-keeping obligations.

## 13. Firm responsibilities

Successful and compliant use of ProSuitability requires your firm to:

1. Ensure only appropriately authorised staff have user accounts, and review access periodically;
2. Verify report accuracy and suitability before sign-off and client delivery;
3. Maintain valid lawful bases and fair processing notices for client data submitted to the service;
4. Ensure Firm Admin accounts use two-factor authentication;
5. Keep billing and firm contact details current;
6. Export and retain records in line with your FCA and ICO obligations;
7. Notify us promptly if you suspect unauthorised access or a data incident involving the service;
8. Review platform content updates and firm customisations that may affect future reports.

## 14. Limitations and disclaimers

- This summary is for due diligence purposes and may be updated from time to time. The Agreement prevails if there is any inconsistency.
- ProSuitability assists report production; it does not determine suitability of advice.
- We do not guarantee uninterrupted or error-free operation.
- No statement in this document constitutes FCA approval, ISO certification, or a compliance guarantee.

- Your firm remains responsible for its regulated activities and client outcomes.

## Appendix A — Related documents

- Licence Agreement and Data Processing Agreement (version 2026-07-09)
- Due diligence & data security summary — <https://www.prosuitability.co.uk/legal/due-diligence/>
- Privacy notice — <https://www.prosuitability.co.uk/legal/privacy/>
- Cookie policy — <https://www.prosuitability.co.uk/legal/cookies/>
- Security overview — <https://www.prosuitability.co.uk/security/>

## Appendix B — Sub-processor change notification

We may update sub-processors from time to time. Material changes are communicated in accordance with the Agreement — including by publishing an updated sub-processor list and notifying subscribing firms. Firms may object to a new sub-processor on reasonable data-protection grounds as set out in clause 11.4.4 of the Agreement.

The sub-processor table in section 8 of this document reflects the position as at 09 July 2026. Check the security page or contact [privacy@prosuitability.co.uk](mailto:privacy@prosuitability.co.uk) for the current list.

## Document history

| Version     | Date         | Summary of changes                                                                                                                                                                                     |
|-------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.0         | 21 June 2026 | Initial publication.                                                                                                                                                                                   |
| 1.0 (rev 1) | 21 June 2026 | Section 7 and section 12: corrected offsite backup provider from AWS S3 to DigitalOcean Spaces (separate DO project, UK region). No change to backup frequency, retention, or encryption commitments.  |
| 1.1         | 24 June 2026 | Sections 6–8: added Cloudflare as public DNS, reverse proxy, and DDoS mitigation edge; clarified encryption in transit (edge TLS). Cloudflare added to sub-processor table. Licence reference updated. |
| 1.2         | 09 July 2026 | Section 8: added xAI (Grok) as sub-processor for optional AI Modules (Ask Support; Paraplanner review). Licence                                                                                        |

|  |  |                                  |
|--|--|----------------------------------|
|  |  | reference updated to 2026-07-09. |
|--|--|----------------------------------|

*© Bluegrove Financial Solutions Ltd. ProSuitability is a trading name of Bluegrove Financial Solutions Ltd (Company Number 6363970).*