



Prestigious HOA Portal

PROPERTY MANAGEMENT SERVICES

DATA PROCESSING ADDENDUM

DPA v1.0

GDPR / CCPA / UK-GDPR data-processing terms, sub-processor list, SCCs, and technical + organisational security measures.

This Data Processing Addendum ("DPA") forms part of the Master Subscription Agreement ("MSA") between Prestigious Property Management Services LLC ("Provider", "we", "us") and the Customer identified in the executed Order Form ("Customer", "you") and governs the Processing of Personal Data by Provider on Customer's behalf.

Effective date: On execution of the underlying MSA · Version: 1.0 · February 2026

If there is any conflict between this DPA and the MSA, this DPA controls with respect to data protection.

1 · Definitions

Capitalised terms not defined here have the meaning given in the MSA or in applicable Data Protection Law.

Term	Meaning
Applicable Data Protection Law	All laws applicable to the Processing of Personal Data under the MSA — including EU GDPR (Regulation 2016/679), UK GDPR + Data Protection Act 2018, California Consumer Privacy Act as amended by CPRA (Cal. Civ. Code § 1798.100 et seq.), Colorado Privacy Act, Virginia Consumer Data Protection Act, Connecticut Data Privacy Act, Utah Consumer Privacy Act, and any successor or equivalent statute.
Controller / Business	The party that determines the purposes and means of Processing of Personal Data. Under this DPA, Customer is the Controller / Business.
Processor / Service Provider	The party that Processes Personal Data on behalf of the Controller. Under this DPA, Provider is the Processor / Service Provider.
Personal Data	Any information relating to an identified or identifiable natural person Processed by Provider on Customer's behalf.
Sub-processor	A third party engaged by Provider to Process Personal Data on Customer's behalf.
Data Subject	The identified or identifiable natural person to whom Personal Data relates — typically a resident, owner, board member, vendor, or staff user of the Service.
Security Incident	A confirmed breach of Provider's security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.
Standard Contractual Clauses ("SCCs")	The clauses annexed to Commission Implementing Decision (EU) 2021/914 (module 2 — Controller to Processor).
UK Addendum	The International Data Transfer Addendum to the EU SCCs issued by the UK ICO under s. 119A DPA 2018 (v. B1.0).

Terms not defined take the meaning given in Applicable Data Protection Law.

2 · Scope, Roles and Purpose of Processing

2.1 ROLES

Provider acts as Processor (or Service Provider under CCPA) on behalf of Customer, who is Controller (or Business). Where Provider Processes limited categories of data as an independent Controller (e.g., service billing, security-log analytics, product analytics stripped of identifiers), that Processing is not governed by this DPA and is instead described in Provider's Privacy Notice.

2.2 NATURE AND PURPOSE

Provider Processes Personal Data solely for the purpose of providing the Service to Customer as described in the MSA, including:

- Enabling authentication and role-scoped access
- Storing resident, owner, vendor, and board records
- Processing rent, fees, and vendor payments
- Sending transactional notifications (email + SMS)
- Generating financial, tax, and governance documents
- Providing AI-assisted operational summaries (only over Customer's own workspace data)
- Producing audit logs and enabling regulatory reporting
- Providing customer support at Customer's request

2.3 DURATION

Processing continues for the term of the MSA plus any post-termination wind-down described in § 9 of this DPA.

2.4 CATEGORIES OF DATA SUBJECTS

- Customer's own personnel (property managers, admins, board members, leasing agents)
- Residents / tenants / owners of the communities Customer manages
- Guests / visitors of those residents (guest-pass data only)
- Vendors, contractors, and service providers
- Applicants for lease / residency (via public listings)

2.5 CATEGORIES OF PERSONAL DATA

Category	Examples
Identity	Name, date of birth (where required for lease), address
Contact	Email, phone, mailing address
Financial	Bank account (tokenised via Stripe), payment history, ledger balance
Property	Unit number, lease terms, move-in/out dates, pet + vehicle registrations
Communications	SMS threads, email history, in-app messages
Governance	Vote records, ARC applications, violation history
Verification	ID document uploads (transient; not stored beyond verification), W-9 TIN, COI, driving licence for guest passes
Access + audit	Login timestamps, IP addresses, session tokens, audit-log entries
Optional / provided by resident	Emergency contact, insurance policy, photo

Sensitive/Special-category data: Provider does not require and generally does not Process sensitive-category data. Customer represents that it will not upload sensitive personal data (health data, biometric identifiers, sexual-orientation data, racial/ethnic data, religious or political beliefs, precise geolocation, or genetic data) without Provider's prior written agreement. Customer remains solely liable for any such data it chooses to upload.

Children: The Service is not directed at children under 13 (or 16 in the EU). Customer must not knowingly upload data of children below those thresholds without a lawful basis.

3 · Provider's Obligations as Processor

Provider shall:

3.1 PROCESSING ON INSTRUCTIONS

Process Personal Data only on documented instructions from Customer, including with regard to transfers to a third country, unless required to do so by law binding on Provider. Provider will inform Customer of any such legal requirement before Processing (unless prohibited by law).

The MSA + this DPA + Customer's use of the Service configuration + any written direction from Customer constitute Provider's documented instructions. Provider is not obliged to Process Personal Data other than in accordance with those documented instructions.

3.2 PROHIBITION ON SALE / SHARING (CCPA)

Provider shall not:

- Sell or Share Personal Data (as defined by CPRA)
- Retain, use, or disclose Personal Data outside the direct business relationship with Customer
- Retain, use, or disclose Personal Data for any purpose other than the specific purposes disclosed in this DPA and the MSA
- Combine Personal Data received from Customer with Personal Data received from or on behalf of any other person, except as expressly permitted for security-monitoring and fraud-prevention purposes

Provider certifies it understands these restrictions.

3.3 CONFIDENTIALITY

Ensure that persons authorised to Process Personal Data have committed themselves to confidentiality (by contract or statutory duty) and are appropriately trained.

3.4 SECURITY MEASURES

Implement the technical and organisational security measures described in Annex II below, at a minimum. These measures are subject to continuous improvement; Provider will not materially reduce them.

3.5 SUB-PROCESSORS

Engage sub-processors only in accordance with § 4 of this DPA.

3.6 ASSISTANCE WITH DATA SUBJECT RIGHTS

Assist Customer, taking into account the nature of the Processing, by appropriate technical and organisational measures, insofar as possible, in fulfilling Customer's obligation to respond to requests by Data Subjects exercising their rights under Applicable Data Protection Law.

Provider provides self-service tools that Customer can use to fulfil most requests directly:

- Access — `/admin/data-export` returns a JSON dump; `/admin/users/{id}` shows profile
- Rectification — Admin can edit any user record via `/admin/users`
- Erasure — `POST /api/admin/users/{id}/delete` (soft-delete + audit-log preservation)
- Portability — `/admin/data-export` produces a machine-readable dump

For requests Provider must handle itself (e.g., where Customer lacks access), Provider will comply within 30 days of a verified request at no additional charge. High-volume requests (> 20 / month) may be subject to reasonable service fees on notice.

3.7 ASSISTANCE WITH DPIA / CONSULTATION

Provide reasonable assistance to Customer with data protection impact assessments and prior consultations with supervisory authorities that Customer is required to carry out under Articles 35 and 36 GDPR (or equivalents).

3.8 DELETION OR RETURN

At the end of the Provision of Services, at Customer's choice, delete or return all Personal Data (see § 9).

3.9 RECORDS

Maintain records of Processing activities in accordance with Article 30(2) GDPR (or equivalents).

3.10 COMPLIANCE

Make available to Customer, on written request, information reasonably necessary to demonstrate compliance with this DPA (see § 8 Audits).

4 · Sub-processors

4.1 AUTHORISATION

Customer provides general authorisation for Provider to engage the Sub-processors listed in Annex III to Process Personal Data on Customer's behalf. Customer specifically authorises Emergent (hosting), AWS S3 (object storage + backups), Anthropic (Claude Sonnet 4.5 for optional AI features), Stripe (payments), Cloudflare (edge + Turnstile), Resend (transactional email), GoHighLevel (SMS), and DocuSign (signatures).

4.2 FLOW-DOWN OBLIGATIONS

Provider will enter into a written agreement with each Sub-processor imposing data-protection obligations no less protective than those in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures.

4.3 NOTIFICATION OF NEW SUB-PROCESSORS

Provider will notify Customer of any intended additions or replacements of Sub-processors at least 30 days in advance by email to Customer's designated data-protection contact and by updating the list at prestigiouspm.net/legal/subprocessors. Customer may object on reasonable data-protection grounds within 15 days. If objection cannot be resolved through good-faith discussion, Customer may terminate the affected Service without penalty by written notice within 30 days.

4.4 LIABILITY FOR SUB-PROCESSORS

Provider remains fully liable to Customer for the performance of each Sub-processor's data-protection obligations.

5 · International Transfers

5.1 TRANSFERS OUT OF THE EEA / UK / SWITZERLAND

Where Customer's use of the Service results in transfers of Personal Data from the EEA, UK, or Switzerland to countries not deemed adequate by the relevant supervisory authority, the parties agree that:

- EU transfers — the EU Standard Contractual Clauses (Module 2: Controller to Processor), as annexed to Commission Implementing Decision (EU) 2021/914, are incorporated by reference. Customer is the "data exporter"; Provider is the "data importer". Docking clause + Option 1 apply. Governing law + supervisory authority are those of Customer's establishing member state; where Customer has no EEA establishment, Ireland applies.
- UK transfers — the UK Addendum (v. B1.0, template A) is incorporated, with Provider as importer.
- Swiss transfers — the SCCs apply with the following adjustments: references to "GDPR" include the Swiss FADP, the Swiss FDPIC is the supervisory authority, and "member state" includes Switzerland.

5.2 SUB-PROCESSOR TRANSFERS

Where a Sub-processor is located in a non-adequate country, Provider ensures back-to-back SCCs (or an equivalent transfer mechanism) are in place with that Sub-processor.

5.3 SUPPLEMENTARY MEASURES

Provider maintains the technical and organisational measures in Annex II — including encryption in transit and at rest, strict access controls, and pseudonymisation where feasible — as supplementary measures under Schrems II.

5.4 GOVERNMENT ACCESS REQUESTS

Provider will: - Notify Customer of any legally-binding request for disclosure of Personal Data by a law-enforcement or government authority, unless prohibited by law - Use reasonable efforts to challenge overbroad or unlawful requests - Publish annual transparency statistics on prestigiouspm.net/legal/transparency

Customer's rights under Clause 15 of the SCCs are preserved.

6 · Security Incident Notification

6.1 DETECTION

Provider will notify Customer without undue delay — and in any event within 24 hours — after becoming aware of a Security Incident affecting Customer's Personal Data.

6.2 CONTENT

To the extent known at the time of notification, Provider will include:

- The nature of the Personal Data affected
- The categories and approximate number of Data Subjects concerned
- The likely consequences
- The measures taken or proposed to address the incident and mitigate adverse effects
- Contact point for further information

Where all information cannot be provided at once, it will be provided in phases without further undue delay.

6.3 ASSISTANCE

Provider will provide reasonable cooperation and assistance to enable Customer to comply with its own breach-notification obligations to Data Subjects and supervisory authorities.

6.4 COST

Provider bears its own costs of responding to a Security Incident attributable to a failure in its security posture. Costs attributable to Customer's misconfiguration or misuse remain Customer's responsibility.

6.5 RECORD

Provider maintains a Security Incident register available on written request.

7 · Contact Points

Each party designates a data-protection contact:

Provider Data Protection Officer (or equivalent): - Email: dpo@prestigiouspm.net - Postal: 1177 Hypoluxo Road, #113, Lantana, FL 33462

Customer Data-Protection Contact: as identified in the Order Form; Customer must keep this current.

8 · Audits

8.1 RIGHT OF AUDIT

Customer has a right of audit at Customer's expense once per calendar year (more frequently in the event of a Security Incident or documented material concern). Audits may be:

- Documentation review — SOC 2 report (available from Q4 2026), penetration-test summary, this DPA, security-questionnaire response — default and free
- On-site inspection — only where a documentation review does not satisfy a specific regulatory request and only with ≥ 30 days written notice, during business hours, at reasonable frequency, and subject to Provider's security + confidentiality controls

8.2 SCOPE

Audits are strictly limited to information relevant to compliance with this DPA. Provider need not disclose: - Data of other customers - Internal financial, HR, or commercial information - Trade secrets

8.3 ALTERNATIVE FOR GROUPED CUSTOMERS

For customers auditing on behalf of a larger cohort, Provider may satisfy audit obligations via a pooled audit — a single audit performed by an independent qualified auditor, the results shared with all participating customers.

8.4 FINDINGS

Any material non-conformities identified must be remediated by Provider within a mutually-agreed period, or Customer may terminate the affected Service without penalty.

9 · Return or Deletion on Termination

9.1 GRACE PERIOD

For 30 days after termination of the MSA ("Winding-Down Period"), Provider will retain Customer's Personal Data in read-only mode to enable Customer to export or return the data.

9.2 DELETION

At the end of the Winding-Down Period, Provider will delete all Personal Data from active systems within 30 days. Backup copies will be permanently deleted or rendered inaccessible within 90 days of MSA termination.

9.3 ATTESTATION

On written request, Provider will provide a written attestation confirming deletion, signed by an officer.

9.4 RETAINED DATA

Personal Data need not be deleted where retention is required by law (e.g., financial records retention). Any retained data continues to be Processed only as necessary for the applicable legal obligation and remains protected by the security measures in Annex II.

10 · Liability

Each party's liability under this DPA is subject to the overall limitation of liability provisions in the MSA. Nothing in this DPA excludes or limits liability that cannot be excluded or limited under Applicable Data Protection Law.

11 · Term and Termination

This DPA is effective for the duration of the MSA and any Winding-Down Period. Provisions that by their nature survive (Confidentiality, Deletion, Liability, Records) survive termination.

12 · Order of Precedence

This DPA prevails over any conflicting provision in the MSA or Order Form solely with respect to matters governed by Applicable Data Protection Law. For all other matters, the MSA prevails.

Annex I — Description of Processing

Filled in from § 2 of this DPA. The parties may amend by written agreement.

Element	Value
Categories of Data Subjects	§ 2.4 above
Categories of Personal Data	§ 2.5 above
Sensitive Data	Generally none — see § 2.5
Frequency	Continuous (for the term of the MSA)
Nature of Processing	Storage, retrieval, computation, transmission, deletion, back-up
Purpose	§ 2.2 above
Duration	Term of MSA + Winding-Down Period
Transfers to third countries	Yes, via SCCs — see § 5

Annex II — Technical and Organisational Security Measures

Provider maintains the following controls. This annex is deemed updated when Provider's public trust-centre (prestigiouspm.net/trust) is updated, subject to no material reduction rule in § 3.4.

II.1 PSEUDONYMISATION AND ENCRYPTION

- Data in transit encrypted with TLS 1.2+ and HSTS in production
- Data at rest encrypted with AES-256 in MongoDB (Emergent-managed) and AWS S3
- Backups encrypted at rest + in transit; keys rotated annually
- Passwords stored using bcrypt (cost ≥ 12)
- Payment credentials never touch Provider systems — tokenised via Stripe
- Session tokens signed with HS256 JWT, 24 h TTL, rotated on password change

II.2 ABILITY TO ENSURE ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY, RESILIENCE

- Multi-tenant isolation: every DB row scoped by `property_id`
- Role-based access control on all endpoints
- Redis-backed cross-pod rate limiting (auth 5-10/min/IP, general 200/min/IP)
- SSRF-guarded outbound calls (private / loopback / cloud-metadata blocked)
- WebSocket + long-poll connections auth'd via JWT
- Sentry error monitoring with PII scrubbing
- Auto-scaling application layer (≥ 2 pods, up to 6 under load)
- MongoDB primary + secondary + arbiter for HA

- Redis with AOF persistence

II.3 ABILITY TO RESTORE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT

- Automated MongoDB snapshots every 6 h (retained 30 d), nightly full (90 d), weekly (12 m)
- Backups replicated cross-region on AWS S3
- Quarterly restore drills verified against a scripted test suite
- RTO: 15 min (app), 2 h (regional DB), 4 h (regional AWS), 24 h (multi-region)
- RPO: 0 (app), 6 h (regional DB)

II.4 PROCESSES FOR REGULAR TESTING, ASSESSING, EVALUATING

- Quarterly disaster-recovery drills
- Continuous dependency scanning (Dependabot / Snyk equivalent)
- Continuous integration tests (pytest backend + frontend E2E)
- Third-party penetration test annually — summary available to customers under NDA
- Static-analysis linters enforced pre-commit
- SOC 2 Type I in progress; Type II targeted Q4 2026

II.5 ACCESS CONTROL

- MFA enforced on all admin consoles (AWS, Emergent, Stripe, GitHub, GHL, DocuSign)
- Role-scoped production access (SRE / on-call / observability tiers)
- All engineering changes go through code review + approval
- Offboarding: access revoked within 4 business hours of separation
- Background checks + annual security training for all production-access personnel

II.6 DATA-MINIMISATION AND PSEUDONYMISATION

- Application collects only data necessary for the stated purpose
- Audit-log PII scrubbing (email/phone/SSN/CC/token/secret/api_key masked in details view)
- Sentry PII scrubbing enabled

II.7 PHYSICAL SECURITY

- Data centres operated by AWS (SOC 2 / ISO 27001 certified) and Emergent (SOC 2 in progress)
- No customer data resides on Provider's local workstations except during authorised support (masked wherever possible)

II.8 VENDOR MANAGEMENT

- Sub-processors listed in Annex III + at prestigiouspm.net/legal/subprocessors

- Each Sub-processor bound by written contract with security + confidentiality obligations
- Vendor concentration limits enforced (no single non-critical vendor exceeds 20% of cost base)

Annex III — Approved Sub-processors

Current as of the DPA Effective Date. Latest list at prestigiouspm.net/legal/subprocessors.

Sub-processor	Purpose	Location	Transfer Mechanism
Emergent	Hosting (Kubernetes) + object storage (S3)	US (AWS)	Intra-EEA where available; SCCs otherwise
AWS S3	Backup storage	US	SCCs
MongoDB Atlas / Emergent-managed	Primary database	US	SCCs
Anthropic	Claude Sonnet 4.5 for optional AI features (only over Customer's own workspace data)	US	SCCs; zero-day retention on API
OpenAI	Whisper transcription (only if voice features enabled)	US	SCCs; 30-day retention
Stripe, Inc.	Payments + Financial Connections	US, Ireland	SCCs
Cloudflare	CDN + WAF + Turnstile bot check	Global	SCCs
Resend	Transactional email	US	SCCs
GoHighLevel	Two-way SMS	US	SCCs
DocuSign	Electronic signature envelopes	US, EU	SCCs
Sentry	Application-error monitoring (with PII scrubbing)	US	SCCs
Google Fonts / Cloudflare Fonts	Web fonts (no personal data)	Global	n/a — no personal data

Provider will maintain this list and provide 30 days advance notice of changes as set out in § 4.3.

Signature

Executed as of the date the MSA was signed. This DPA is incorporated into the MSA by reference.

Provider: ____ Customer: ____ Name/Title: ____ Name/Title: ____ Date: ____ Date: ____