

Security & Compliance Overview

Posture, controls and document set for TotalSettle.

Version v3.2 | Last reviewed: 24 July 2026 | Owner: CaseFlow Automation Ltd

Purpose

This document sets out the security and compliance posture of the TotalSettle platform. It is intended for operator IT, security and procurement teams evaluating the service.

Roles

CaseFlow Automation Ltd is the holding company that publishes TotalSettle. When you process claim data through TotalSettle, you remain the Data Controller and CaseFlow Automation Ltd acts as Data Processor under your instructions and a signed DPA.

Regulatory posture

- Registered with the Information Commissioner's Office. ICO ZC013423.
- UK GDPR and Data Protection Act 2018.
- Data hosted in the EEA (AWS eu-central-1, Frankfurt); UK-EEA transfers covered by UK GDPR adequacy regulations.
- Designed to support FCA Consumer Duty evidencing through a complete audit trail.
- No claim of FCA or Ombudsman endorsement.

Security controls

- Encryption of data in transit (TLS 1.2 or higher) and at rest.
- Logical tenant isolation enforced by row-level access controls, server-side, on every request.
- Role-based access control for operator teams. Least-privilege access for staff.
- Settlement portal links are unique per case and verified against the registration and postcode on the case before any details are shown. Links remain live while the case is open and are disabled automatically when the case completes or expires.
- Audit logging on every handler and customer action, with timestamps and user identity.
- Daily encrypted database backups with point-in-time recovery.
- Multi-factor authentication available for operator accounts.

Data retention and minimisation

Automatic data minimisation. Personal data is scrubbed automatically the moment a settlement completes. Cases abandoned for 30 days are anonymised automatically, with an operator warning 7 days beforehand. Only anonymised settlement statistics remain. Every purge is recorded in an audit trail.

Personal data is held only for as long as it is needed to complete the settlement. On completion the platform automatically removes all claimant identifiers from the case, deletes uploaded evidence and redacts email logs. Cases abandoned for 30 days are anonymised automatically and marked expired, with an operator email warning 7 days beforehand. Anonymised settlement statistics are retained so operator reporting keeps working. Purges are recorded in a dedicated audit table and verified by an automated weekly health check. On offboarding, the operator's entire tenant is wiped, subject to legal hold. Settlement links may be sent by email or SMS. SMS delivery is performed by FireText Communications Ltd, a UK sub-processor under a signed data processing agreement with UK-only message routing; the message contains a secure link only, never claim details, and SMS delivery-log personal fields are cleared by the same purge machinery.

AI processing in scope

TotalSettle uses Google Gemini, accessed via the Lovable AI gateway, to extract structured fields from engineer reports and to draft a short plain-English summary for the customer. Before any engineer report text is sent to the AI provider, personal identifiers are replaced with opaque placeholders and restored locally on return. The AI provider does not retain the data and does not use it for training. AI outputs are reviewed by a trained handler before any settlement decision is communicated. AI is not used to make final settlement decisions. Full detail is published at totalsettle.com/ai-data-handling.

Operational practices

- Documented incident response process with notification to controllers within 72 hours of a confirmed personal data breach.
- Change control on infrastructure and application code, with peer review before release.
- Vendor due diligence on all sub-processors. List available on request.
- Regular dependency scanning and security review of the application stack.

Document set

- Security & Compliance Overview (this document).
- AI Safety & Security Policy.
- How We Protect Your Data.
- AI Data Handling (web page at totalsettle.com/ai-data-handling).
- Data & AI Summary.
- Plain English Guide.
- Technical Overview.
- Terms of Use.

CaseFlow Automation Ltd is the holding company that publishes TotalSettle. Registered in England and Wales. ICO registration: ZC013423. Registered office: 7-9 Macon Court, Crewe, CW1 6EA. This document forms part of the TotalSettle policy pack and is provided for information. It does not constitute legal advice. For the signed DPA, sub-processor list, or DPIA, contact info@caseflowautomation.co.uk.