Security & GDPR Compliance Plan

This document outlines how the SOF Generator, ET1 Automation, and Schedule of Loss Generator will handle client data securely, maintain GDPR compliance, and prevent any leaks of sensitive information.

Data Minimisation & Purpose Limitation

Only data strictly necessary for generating legal documents will be collected. Data is used solely for drafting Statements of Facts, tribunal forms, and Schedules of Loss. No data is repurposed, shared, or monetised.

Client Consent & Transparency

Clients must provide explicit consent before submitting data. A clear privacy notice explains how their information is used, stored, and retained. Clients can request access, correction, or deletion of their data in line with GDPR rights.

Storage & Encryption

All data is encrypted in transit (TLS 1.2/1.3) and at rest (AES■256). Databases and file storage use disk■level encryption. Sensitive files (payslips, contracts) are additionally encrypted with unique per■file keys.

Access Control & Authentication

Role■based access ensures only authorised lawyers can view client data. Strong authentication (MFA) is enforced for lawyer accounts. Clients only see their own submissions; no cross■access between users.

Data Retention & Deletion

Data is retained only for the duration of the case. Automatic deletion policies purge data after retention periods expire. Secure deletion methods (cryptographic wipe) are applied to ensure no recoverable traces.

Confidentiality & Privilege

All outputs are marked as 'Draft – Lawyer Review Required'. The system does not transmit or expose data to third parties without explicit instruction. Attorney■client privilege is preserved by keeping all processing within secure environments.

Audit Logging & Monitoring

Every access, edit, and export is logged with timestamp, user ID, and action details. Logs are immutable and regularly reviewed to detect anomalies. Monitoring systems flag suspicious behaviour (e.g., bulk exports, repeated failed logins).

Third■Party Processors

If third■party APIs (e.g., OCR, transcription) are used, only GDPR■compliant vendors within approved jurisdictions are selected. Data sent to processors is minimised and anonymised where possible.

Incident Response

A formal breach response plan is in place. If a breach is detected, affected users and regulators are notified within GDPR timelines (72 hours). Post■incident reviews strengthen future safeguards.

User Rights & GDPR Compliance

The system provides mechanisms for data subjects to exercise their GDPR rights: access, rectification, erasure, restriction, portability, and objection. Requests are processed within statutory timeframes.

Summary Commitment

The platform is designed with 'privacy by design and by default'. All security measures aim to protect the confidentiality, integrity, and availability of client data. The highest priority is preventing leaks of sensitive information while maintaining compliance with GDPR and professional standards of legal practice.