



Handling Sensitive Information in Legal Practice

Law firms and legal departments routinely manage highly sensitive or confidential material.



In sharing or distributing such documents (via email, internal sharing, external counsel, clients, opposing counsel, or third-party experts), legal teams face several risks and constraints.

Legal teams need a streamlined but robust way to protect, monitor, and control sensitive documents with minimal disruption to workflows.

DocumentGPS is a smart, email-native extension (for Outlook, Gmail, mobile, web) that allows legal teams to tokenize, encrypt, track, and control email attachments, including revocation of access, even after the message is sent.

Because DocumentGPS is built as an email extension (rather than a completely separate portal), legal users can adopt it with minimal disruption to existing workflows, while maintaining compliance.

Document exchange with clients / counterparties / external counsel

Use the Secure Link mechanism to receive sensitive client documents (e.g. tax returns, medical records, business financials) securely, with full audit trail and ability to revoke/limit sharing.

Negotiation & deal documents

In M&A, financing, or real estate deals, share term sheets, internal models, or due diligence materials while preserving control over further dissemination, and monitor who is reading and when.

E-signature and contract execution

Rather than moving to external signing platforms, embed signing directly within the email-attachment context, reducing delays and friction.

Litigation / e-discovery support / chain of custody

Preserve an immutable, time-stamped log of document access and sharing (with possible evidentiary weight), mitigate tampering, and simplify audit. This can be a key differentiator in compliance or disputes.

Third-party expert materials or witness statements

Share sensitive expert reports or case summaries with outside experts or witnesses under strict controls and visibility.

Key Benefits



Reduced Risk of Data Leakage

With screenshot prevention, watermarking, and share blocking, you mitigate unauthorized dissemination.



Stronger Compliance & Audit Posture

The immutable audit trail, encryption, and tokenization help support regulatory, internal audit, and e-discovery obligations.



Error Mitigation

Mistaken sends or disclosures can be mitigated by revoking access, reducing potential exposure or malpractice risk.



Scalable for Teams & Firms

With admin panels, role-based access, team deployment features and co-branding, the solution can scale in a firm environment.



Profitable Differentiator / Client Trust

Market to clients that you protect their sensitive documents end-to-end, strengthening data security reputation.

DocumentGPS offers legal teams a powerful combination of persistent document control, visibility, and security wrapped into the familiar context of email. It addresses major pain points around document leakage, auditability, and security without requiring users to switch away from existing email workflows.