AUTOMATING DATA PRIVACY CLAIM HANDLING WITH AI

How legal ops can securely automate high-volume litigation processes

TABLE OF CONTENTS

Introduction	1
Status Quo & Current Challenges	2
Risks	3
Key Difficulties for Legal Departments	4
How Case Management Automation Addresses the Problems	5
Implementing a Case Management Automation Solution: Benefits	6
JUNE: The Case Management Automation Platform for Data Privacy Claims	7
Why Considering JUNE	8
Mini Case Study	9
Conclusion	10
Appendix	11

JUNE

INTRODUCTION

Data privacy lawsuits connected to legal actions taken against companies for failing to protect user data, data breaches, privacy violations, or misuse of personal information often take the form of mass litigation claims, with a significant rise in filings in recent years. Data privacy cases can involve claims for financial loss, emotional distress, and the potential for future harm from data misuse and companies face multi-million-dollar fines and damages for violating privacy laws like the GDPR, DORA or BIPA, as seen in recent cases against Google and Uber for failing to safeguard user data.

There are different types of data privacy lawsuits that legal departments at large corporations that deal with a vast amount of personal customer data can face:

- Data Breach Lawsuits: These lawsuits arise when a company's data is compromised, leading to the exposure of personal information.
- Privacy Violation Lawsuits: These cases involve companies collecting, using, or sharing user data in ways that violate privacy assurances or user consent.
- Class Action Lawsuits (especially in North America): A common legal strategy where a large group of people with similar complaints sue a company, as seen in recent cases involving Google and other platforms.
- Mass Arbitration (also available in Europe): A newer legal technique, similar to a class action lawsuit, that allows many individuals to pursue their claims against a company.

When customer data is stolen, stored improperly, illegally shared with third parties, or gathered without permission, the fallout for businesses goes far beyond financial and reputational damage. Companies are often faced with high costs for responding to claims and dealing with operational hurdles when legal departments are forced to seek help to keep up with all incoming requests.

Increasingly, breaches involving personally identifiable information (PII) have led to multi-plaintiff and class action lawsuits filed by individuals whose data was exposed to unauthorized third parties. Historically, the litigation risk in such cases was relatively contained, as many courts dismissed claims on the basis that plaintiffs lacked standing, arguing that no concrete injury had occurred unless the compromised PII resulted in clear harm such as identity theft or unreimbursed fraudulent charges.

Now, regulations are becoming stricter, more diverse, and incoming claims often involve a lot of documents, manual labor, and the need for external counsel to keep up with deadlines.

STATUS QUO

Data privacy claims

avg. relationship between settlement and operational costs

1:1

of companies already use AI automation in the data privacy cycle

1/3

y-o-y increase in global costs linked to cybercrimes

15%

CURRENT CHALLENGES

Companies that process large volumes of customer data, especially personal data, face mounting complexity. Key challenges include:

• Fragmented data sources: Data arrives via web forms, mobile apps, third-party integrations, legacy systems, emails, and even paper or scanned docs. Formats are inconsistent; some data is incomplete or unstandardized.
• Volume & scale: Thousands or millions of customers create multiple claims, incidents, or privacy requests (access, deletion, correction, etc.). The sheer volume overwhelms manual workflows.
• Regulatory diversity: GDPR is just one example—companies operating internationally must also meet privacy/data protection rules in the U.S. (e.g., CCPA, CPRA), UK, Canada, Asia, etc., each with its own definitions, deadlines, rights, and obligations.
• Coordination demands: Internal units (legal, IT, security, compliance) plus external law firms, third-party processors/responders must all be in sync. Delays, miscommunications, and versioning errors abound.
• Security risks & trust exposure: Personal data misuse, leaks, or mis-handling not only hurt reputation but expose firms to legal, financial, and operational risk.

RISKS

Lawsuits frequently stem from violations of fundamental data rights, such as an individual's right to access, correct, or erase personal information. As public awareness grows and privacy advocacy groups gain traction, more individuals are pursuing legal action against companies that fall short of compliance. For businesses, the consequences extend far beyond the courtroom: protracted proceedings drain resources, escalate costs, and amplify reputational exposure.

If regulators confirm violations, organizations may face bans on processing data, strict operational limits, or costly remediation mandates. The damage doesn't stop there: loss of credibility can unsettle key partners, stall contract negotiations, and deter potential clients, particularly in industries where trust and data security are non-negotiable. In today's competitive market, the perception of mishandling personal data can prove just as destructive as the penalties themselves.

When companies handling large customer bases don't fully comply with data privacy norms, the risks are severe. Some of the main ones:

• Litigation: Companies face potential lawsuits from consumers alleging negligence, breach of contract, or other statutory claims following a data breach.
• Regulatory fines and penalties: Under GDPR, companies can be fined up to 4% of global annual turnover or €20 million (whichever is greater).
• Reputational damage: Breaches and penalties erode trust and cause churn.
• Claims costs: Mass claims and class actions are expensive to process and settle. Individuals have the right to sue for both financial and emotional harm caused by a data breach.
• Operational inefficiency: Manual processing increases risks of missed deadlines and errors.
• Cross-border transfer risks: Moving data between jurisdictions raises compliance hurdles.
• Data subject rights: Strict deadlines (often 30 days) require timely responses.
• Legal liability: Which, in worst cases, can lead to business interruption

In recent years, data privacy has become the trigger for a wave of lawsuits. Cases have emerged around everything from the exposure of highly sensitive information such as Social Security numbers, to websites quietly transmitting users' online behavior to third parties, to companies illegally gathering biometric identifiers like fingerprints.

All signs point to this trend accelerating rather than slowing down, especially considering the increasing number of devices and applications that can gather users' data basically 24/7. These lawsuits do more than secure financial redress for affected individuals. They also act as powerful levers for change, compelling organizations to strengthen their security practices and adopt safeguards that reduce the risk of repeat violations.

KEY DIFFICULTIES FOR LEGAL DEPARTMENTS

- Scalability of intake & triage: thousands of claim forms overwhelm manual systems.
- Document overload & disparate formats: difficult to aggregate and compare.
- Data Volume and Dispersal: Legal teams must manage and secure a massive volume of sensitive data stored across numerous, often scattered, data sources, including collaboration platforms and cloud environments.
- Deadline-driven complexity: varying statutory deadlines across jurisdictions.
- Coordination with external law firms: permissioning, data security, version control.
- Risk of inconsistent arguments: inconsistent strategies across cases.
- Compliance & auditability: need to log all actions securely.
- Cost and resources: heavy external counsel fees, long review hours.
- Insight lag: lack of real-time visibility into cases and risks.

Recent Examples: Fines, Litigation and Data Breaches

Company / Country	Key Violation	Penalty / Outcome
TikTok / Ireland	Transferred European user data to China; inadequate transparency	Fine: €530m
Meta (EU)	Stored user passwords in plaintext; poor protection	Fine: €91m
LinkedIn / Ireland	Behavioral ads without valid consent	Fine: €310m
Uber / Netherlands	Stored driver data to U.S. without safeguards in breach of GDPR	Fine: €290m
Avanza Bank / Sweden	Misuse of tracking pixels; data leakage	Fine: €1.33m
Google / USA	Breached users' privacy by ignoring request to turn off tracking	Fine: $360m

HOW CASE MANAGEMENT AUTOMATION ADDRESSES THE PROBLEMS

A Case Management Automation platform supports legal teams by boosting efficiency in claim handling and litigation processes with the help of Artificial Intelligence (AI).
The key elements of a Case Management Automation platform include:

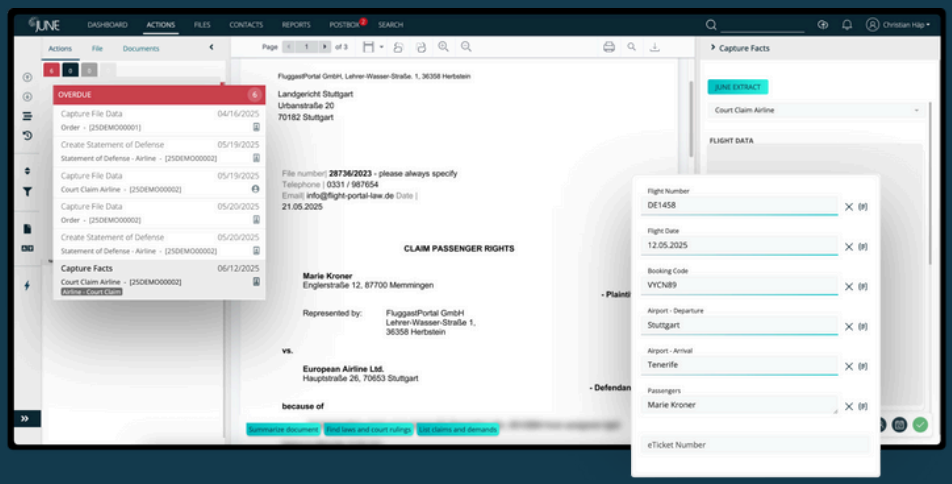
1. Document intake (from different sources and different formats) and centralization
2. Digitization and document classification (so that the system knows what kind of document it is dealing with)
3. Data extraction (all relevant information for document processing, such as parties involved, court, claim, laws, deadlines…)
4. Process automation (utilizing extracted data to properly process claims accurately and in time)
5. Knowledge acceleration (intelligent support with predicative analytics, research, precedents, counterarguments and so on, to support the strategic stance)
6. Document co-creation (to automate outgoing communications and responses)

By receiving assistance and leveraging workflow automation, legal teams that adopted a Case Management Automation solution report lower spending (internal and external legal costs), a much faster response time, higher accuracy, and more opportunities to strategically react to claims and prevent unjustified requests.

Implementing a Case Management Automation Solution: Benefits

- Risk mitigation & compliance assurance with logged workflows and access controls.
- Cost savings from automation, fewer manual hours, and reduced external fees.
- Speed & responsiveness: faster claim handling and regulatory responses.
- Consistency: shared precedents, AI suggestions, coherent strategies.
- Scalability: handle growth without proportional headcount increases.
- Visibility: management gets real-time risk and performance oversight.
- Security: encrypted collaboration spaces demonstrate compliance by design.
- Learning & future preparedness: accumulated knowledge strengthens long-term resilience.

JUNE: THE CASE MANAGEMENT AUTOMATION PLATFORM FOR DATA PRIVACY CLAIMS



JUNE is a Case Management Automation platform that covers all the bases when it comes to high-volume dispute and litigation processes, while also offering additional benefits that lead to an even higher level of accuracy and efficiency.
The platform gathers documents from all sources thanks to native and API integrations with all conventional communications systems and then leverages the latest generative AI technology to classify documents and extract information to trigger rule-based or Agentic workflows.

JUNE also offers an AI-powered virtual co-counsel that supports the team by summarizing documents, researching relevant information, suggesting text snippets for document co-creation, gathering related laws, regulations, similar cases, and more.
But on top of digitization, process automation, and knowledge acceleration, legal teams choose JUNE when it comes to automating data privacy claims because the system also:

- Allows teams to structure work, assign tasks, set alerts for deadlines, and work with individual reminders while maintaining a full overview of actions and activities for each case
- Provides legal teams with KPIs and automated reports to gauge efficiency, identify bottlenecks, predict trends, and make informed strategic decisions
- It is designed to facilitate data centralization and cooperation while guaranteeing security and compliance
- Simplifies processes by using Agentic AI, thus eliminating the need to manually create processes for repetitive tasks that don’t require human supervision

WHY CONSIDERING JUNE

JUNE is not yet another legal platform or a piece of software. JUNE is the central nerve system for successful legal operations at international law firms and in legal departments of global corporations dealing with high-volume privacy claims.

JUNE is the only smart workplace for legal teams that collaborate in real-time to efficiently manage cases from intake to resolution with full transparency and data compliance and within JUNE's Collab Spaces, legal teams can, in fact, cooperate securely on the same case with individual access rights to documents and separated inboxes, deadlines, and workflows.

Within the platform, legal teams centralize documents, data, and knowledge and take full control of processes with a constant 360° overview of everything that happens while working together with an AI-powered legal co-counsel to gain strategic confidence, authority, and visibility.

Secure Legal Collaboration

In JUNE, you work with internal and external partners and legal counsel in separate Collab Spaces where teams manage their own documents, deadlines, and workflows while you retain a full overview of access rights, actions, and activities.

End-to-End Efficiency

JUNE is the ecosystem in which your teams work daily with efficient workflow automation from case intake to resolution. The system gathers incoming documents, classifies them, and truly understands your cases. Unstructured information becomes structured data and insight,s which are used to fill out forms, suggest actions, counterarguments, or text snippets, summarize information, log facts and activities in chronological order, cite references, laws, and judgments, and finally take care of personalized communications at scale.

Full Control and Reusable Legal Intelligence

Within a Casa Management Platform, you are always on top of things. Nothing slips through. Your teams collaborate efficiently and achieve results quickly through systematic procedural precision and rigor.

This allows you to curb risks and financial exposure strategically while overseeing deadlines, workflows and activities, workload, compliance, and results.

When working in JUNE, you can ask direct questions to your AI co-counsel to gather information and insights about case files and documents at any point in time and you can always access case-specific KPIs or aggregate information to assess outcomes and efficiency.

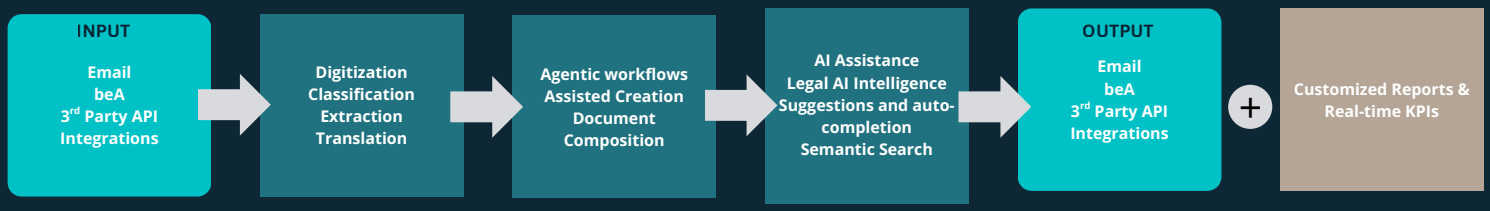
The platform's reporting module is not another colorful dashboard you stare at or screenshot and paste in presentations. JUNE offers a strategic cockpit that allows you to tap into real-time reporting while monitoring all important case KPIs regarding status, success rates, cost-effectiveness, participant structures, procedural features and more to strategically steer decision-making processes and proactively address trends.

The system becomes smarter with each interaction and allows you to expand your internal knowledge base with reusable intelligence contributing to an overall compound effect on future productivity and efficiency rates.

JUNE SUPPORTS LEGAL TEAMS ACROSS THE ENTIRE LIFECYCLE:

- Workflow Automation: Automatic intake, classification, routing, and deadline tracking.
- Secure Collaboration Workspaces: Permissioned access for internal and external teams.
- Agentic AI: Automates repetitive decisions, triggers workflows, and generates model responses.
- AI Legal Assistant: Researches rulings, finds counterarguments, and summarizes documents.
- Real-Time Reporting: Strategic cockpit with KPIs and risk indicators.
- Knowledge Capture: Builds reusable legal intelligence for faster resolution in the future.

JUNE: LEGAL AI & CASE AUTOMATION PLATFORM



MINI CASE STUDY

One of JUNE's customers, a very popular social media network provider, works with different outside counsel on the JUNE platform to manage mass litigation projects.

With JUNE Collab Spaces, each firm operates in a secure, dedicated space with its own workflows and document structures, while Meta maintains a unified, real-time overview. JUNE streamlines collaboration, boosts efficiency, and preserves strict data separation - enabling independent work while keeping all teams aligned.

Additionally, the company also uses JUNE to:

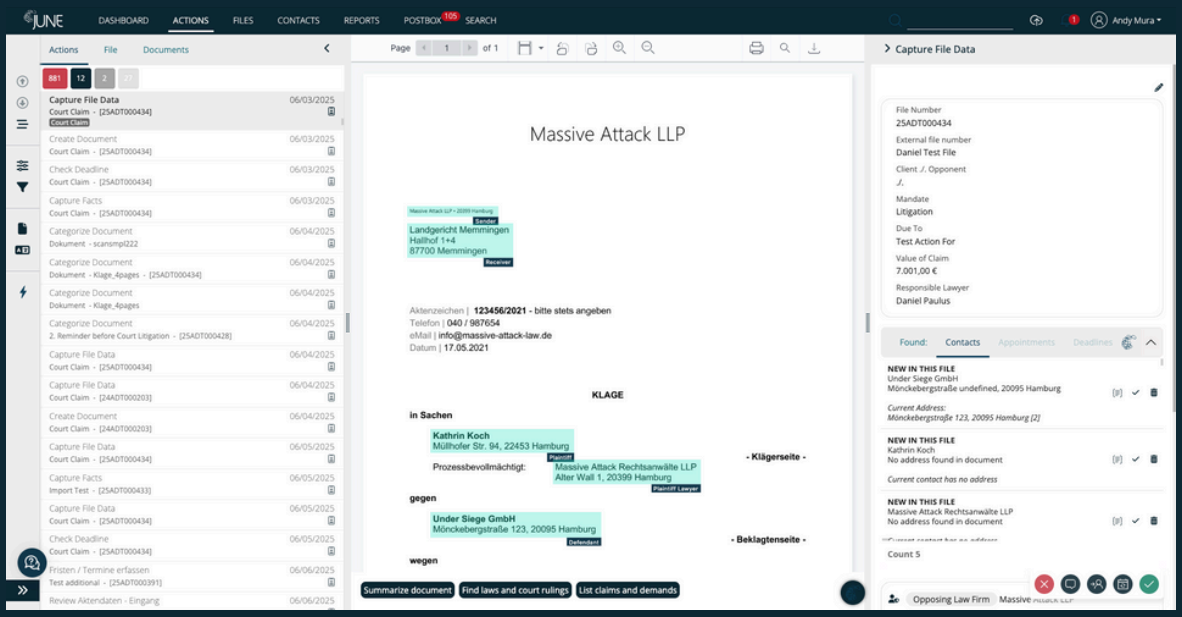
- Extract asserted GDPR claims (information pursuant to Art. 15 GDPR, knowledge, deletion) from out-of-court letters and lawsuits
- Create seamless collaboration between the legal department, internal compliance departments for user data research, and various external lawyers (outside counsel)
- Integrate DSAR (data subject access request) tools used for data research
- Automatically create out-of-court and court responses
- Outcome: Increased efficiency in internal and external processes and full overview and control of legal proceedings conducted by various OCs (individual and collective)

CONCLUSION

Given the accelerating pace of data regulation globally and the growing costs (financial, operational, reputational) of data privacy failures, legal departments cannot rely on manual, patchwork, or siloed workflows. JUNE offers a path not only to compliance, but to superior operational control, defensible legal strategy, and scalable efficiency.

Find out today how Case Management Automation can help your team gain efficiency and reduce costs in data privacy claim hanlding

FREE CONSULTATION



APPENDIX

ROI from day one: How JUNE answers legal challenges in data privacy cases

	Pre-Automation	JUNE
Data management	Unstructured documents from several sources, manual triage and preparation, decentralized data, error-prone manual processes.	Automatically ingest documents/claims from many sources, classify them (type of claim, jurisdiction, urgency), assign internal owners or external counsel, set deadlines, summarize information.
Collaboration	Lots of offloaded cases due to internal constraints, inefficient cooperation on copies of documents in back-and-forth emails and potential compliance issues.	Maximum in-house efficiency and throughput (with reduced need for external counsel), efficient, transparent, and secure cooperation with internal and external teams in dedicated Collab Spaces.
Processing	Inefficient manual repetitive tasks, delays, missed deadlines, errors, high overhead costs, teams hitting a ceiling with high-volume cases.	Context-base reminders, breach notifications, model answers or templates with instant access to similar case rulings, precedents, counterarguments, legal strategies, extraction of relevant clauses, laws, or regulations and more.
Reporting	Lack of detailed KPIs, internal visibility, predictive analytics, cost exposure, success rates, alerts, and insights.	Dashboards for case volumes, workload, status by jurisdiction, cost exposure, success rates, deadlines and obligations, insights into bottlenecks. Smarter functional memory and expanding knowledge base combined with automated reporting.

JUNE


JUNE