

BEHANDELN REGULATORISCHER ANFRAGEN

mit größerer Sicherheit und Effizienz

Die Bereitstellung von Informationen für Bürger, private Gruppen, Regulierungsbehörden und andere ist für eine gut informierte Bürgerschaft und eine funktionierende Demokratie so wichtig, dass dafür Gesetze auf Bundes- und Landesebene erlassen wurden.



Der Umgang mit diesen Anfragen ist jedoch komplizierter als in der Vergangenheit. Informationen werden in vielen Repositories und Content-Systemen gespeichert, was die Suche nach den richtigen Dokumenten erschwert und zeitaufwändig macht. Dokumente sind mehr und mehr digital und erfordern ausgefeiltere Schwärzungstechniken, als nur sensible Informationen auf einer physischen Kopie zu verdecken. Und die Bedrohung durch ausländische Agenten oder Akteure mit böswilligen Absichten, die versuchen, sensible Informationen zu kompromittieren, ist exponentiell gewachsen.

Die Technologie und die damit verbundene Automatisierung sind der Schlüssel, um heutzutage die Anforderungen, die regulatorische Anfragen stellen, zu erfüllen. Dieses Papier befasst sich mit den Faktoren, die eine Überwindung der digitalen Kluft notwendig machen, sowie mit leicht zugänglichen Technologien, die eine effiziente Reaktion auf wachsende Anfragemengen ermöglichen, ohne die Sicherheit des Landes oder ihrer Bürger zu gefährden.

Anpassung an eine immer digitaler werdende Umgebung

Die Bereitstellung staatlicher Informationen an die Bürger erfolgt in der Regel durch:

- **Informationsfreiheitsgesetz (Freedom of Information Act, FOIA).**
FOIA wurde 1966 in Kraft gesetzt, um eine allgemeine Philosophie der vollständigen Offenlegung von Behördendaten umzusetzen. Das Gesetz sieht vor, dass Informationen, die nicht bereits im Federal Register veröffentlicht sind, der Öffentlichkeit zur Einsichtnahme und Vervielfältigung zur Verfügung gestellt werden. Ausnahmen gelten bei Fragen der Vertraulichkeit und des Persönlichkeitsrechts.
- **Gesetze zur Dateneinsicht auf Bundesstaatsebene.**
Während FOIA sich nur auf staatliche Exekutivorgane bezieht, haben die Bundesstaaten ähnliche Gesetze erlassen, die als Sunshine Laws, Public Records Laws und Freedom of Information Laws bekannt sind. Die meisten Gesetze orientieren sich an FOIA, aber sie variieren von Bundesstaat zu Bundesstaat.
- **Elektronisches Auffinden oder eDiscovery.**
E-Mails, Voicemails, Texte, Videos, soziale Medien, von IoT-Geräten erfasste Daten und weitere elektronisch gespeicherte Informationen werden immer wichtiger und sind für Bürger und Gruppen von Interesse, die staatliche Daten anfragen. Das Sammeln dieser Informationen von unterschiedlichen Geräten und Speicherplattformen kann recht mühsam sein, wenn keine geeigneten Systeme vorhanden sind.



Immer häufiger berühren diese Anfragen auf föderaler und bundesstaatlicher Ebene sowie über eDiscovery den digitalen Bereich. Es könnte sich um ein ursprüngliches elektronisches Dokument, elektronisch gespeicherte Informationen oder eine Anfrage handeln, dass die Informationen elektronisch zur Verfügung gestellt werden. Eine Überarbeitung des FOIA im Jahr 2016 schreibt zum Beispiel vor, dass, wenn ein Dokument dreimal oder mehrmals angefordert wurde, eine elektronische Kopie dieses Dokuments veröffentlicht werden muss. Und neue Compliance-Standards von Section 508, die im Januar 2017 erlassen wurden, aktualisieren die Anforderungen zur Erleichterung des Zugangs zu elektronischen Informations- und Kommunikationstechnologien für Menschen mit Behinderungen.



800.000

*FOIA-Anfragen im Geschäftsjahr 2016,
eine Rekordzahl*

Darüber hinaus schreiben viele Behörden die Verwendung elektronischer Dokumente vor – insbesondere PDFs – für Rechtsdokumente, einschließlich Beschwerden, Petitionen, Schriftsätze, eidesstattliche Aussagen und Konkurse.

Elektronische Dokumente und Antworten sind zwar zweckmäßiger, aber die Sicherheit dieser Informationen ist eine zusätzliche Herausforderung. Es war schon immer von großer Wichtigkeit, dass Offenlegungen und sensible Informationen nicht in die falschen Hände geraten und Einzelpersonen oder Staatsgeheimnisse gefährden oder zu Gerichtsverfahren oder Compliance-Verstößen führen. Und Bedrohungen gab es immer von Angriffen von außen, von Agitatoren, Whistleblowern und verärgerten Mitarbeitern. Selbst Mitarbeiter, die einfach nur leichtsinnig sind und das falsche Dokument versenden oder sensible Informationen nicht schwärzen, können als Bedrohung betrachtet werden.

Elektronische Dokumente bergen das zusätzliche Risiko, dass Informationen nicht korrekt geschwärzt werden. Eingebettete Daten werden mit dem Dokument weitergegeben und Sachkundige können damit personenbezogene Informationen kompromittieren und Text, der „geschwärzt“ wurde, aufdecken.

Neben den steigenden Sicherheitsefordernissen steigt auch die Zahl der regulatorischen Anfragen, die durch Faktoren wie ein politisch gespaltenes Umfeld, eine besser informierte Bevölkerung und eine noch größere Anzahl von Medien, die investigative Berichterstattung betreiben, angeheizt werden. Die Verarbeitung von immer mehr Anfragen belastet schrumpfende oder stagnierende Budgets, insbesondere bei Behörden, die bereits unterbesetzt sind. Dies kann Verzögerungen nach sich ziehen, die zu Compliance-Verstößen oder sogar zu Rechtsstreitigkeiten führen. Zudem ist die Zeit, die die Mitarbeiter mit der Suche nach relevanten Dokumenten und der Schwärzung sensibler Informationen verbringen, eine verpasste Gelegenheit, da sie sich anderen Aufgaben hätten zuwenden können.

Die Technologie eröffnet eine Möglichkeit, diese Herausforderungen anzugehen, indem sie Schutzschichten hinzufügt und Prozesse automatisiert.

Erhöhte Sicherheit für elektronische Dokumente

Elektronische Dateien werden oft extern in der Cloud oder bei Behörden vor Ort in Content-Management-Systemen gespeichert.

Diese Dienste verfügen zwar über Sicherheitsvorrichtungen wie Firewalls, aber die digitale Natur der Informationen kann sie dennoch anfällig machen. Es ist möglich, dass Dateien geändert, kopiert, auf unsichere Geräte heruntergeladen, an E-Mails und Texte angehängt und anderweitig beschädigt werden oder außerhalb der sicheren Plattform gelangen.

Außerdem müssen bestimmte Schritte unternommen werden, um Informationen vollständig aus elektronischen Dokumenten zu schwärzen, damit nicht nur sensibler Text, sondern auch eingebettete Informationen verdeckt werden. Dies kann in Produkte zur Dokumentenerstellung integriert werden, wie z. B. PhantomPDF von Foxit Software, das sensible Informationen entfernt, bevor das Dokument veröffentlicht wird. Zu diesen Informationen gehören Metadaten, Kommentare, verborgene Daten aus früheren Speicherungen und mehr.



» *Dokumentenintelligenz ist eine Technologie, die die **Sicherheit verbessert**, indem sie eine bessere Kontrolle über die Verwendung von Dokumenten bietet.*

Die Dokumentenintelligenz bietet eine bessere Kontrolle über die Verwendung von Dokumenten. Anhand dieser Technologie kann verfolgt werden, wer während des gesamten Lebenszyklus eines Dokuments Zugriff auf was, wo und wann hat. Dies umfasst folgende Informationen:

- Wie viel Zeit ein Prüfer auf jeder Seite verbracht hat
- Welche Seiten von einzelnen Prüfern übersprungen wurden
- Welche Seiten kopiert wurden und von wem
- Welche Daten geschwärzt wurden
- Ob zusätzlicher Schutz hinzugefügt wurde, z. B. Rights Management Services (RMS) oder Digital Rights Management (DRM)
- Ob das Dokument digital signiert wurde
- Ob das Dokument zur gemeinsamen Prüfung versendet wurde

Da die Intelligenz mit dem Dokument mitgesendet wird, können Prüfer mit vollem Zugriff verfolgen, ob die elektronische Datei unbefugten oder böswilligen Zugriffen ausgesetzt ist.

Die ConnectedPDF-Technologie von Foxit Software enthält PhantomPDF und ermöglicht es dem Dokumenteigentümer, ein Dokument fernzusteuern und sogar zurückzurufen. Diese digitalen Dokumente können nur dann geöffnet, gedruckt oder bearbeitet werden, wenn der Eigentümer die Berechtigung dazu erteilt hat. Dies trifft selbst dann zu, wenn das Dokument versendet wurde. Wenn also Informationen absichtlich oder unabsichtlich in die falschen Hände geraten, wird der Besitzer des Dokuments alarmiert. Er kann dann Berechtigungen deaktivieren, wodurch das Dokument effektiv zurückgerufen wird. Die Nachverfolgungsdaten der Technologie werden über die Cloud synchronisiert und anhand einer privaten, lokalen oder öffentlichen Bereitstellung vollständig geschützt.

“ *Elektronische Dokumente bergen das **zusätzliche Risiko**, dass Informationen nicht korrekt geschwärzt werden.* ”

Effizienteres Abrufen von Dokumenten

Da Daten unter staatlicher Obhut sowohl vor Ort als auch extern gespeichert werden, müssen effiziente Systeme und Tools zur Identifizierung des Speicherorts vorhanden sein. Dazu gehören:

- **Moderne eDiscovery-Tools.** Diese Tools verwenden ausgeklügelte Analysen, um elektronisch gespeicherte Informationen zu identifizieren und zu sammeln, damit Benutzer Datensätze in einem Bruchteil der Zeit suchen, sammeln, verarbeiten und überprüfen können. Zu den weiteren Funktionen gehört die Bereitstellung von Workflows, die für die Einhaltung der Transparenzgesetze sorgen und Informationen während der investigativen Phase automatisch organisieren.
- **Case-Management-Systeme.** Diese Systeme bieten eine zentralisierte Verwaltung aller Informationen in einer gemeinsam genutzten Datenbank und machen diese Daten dann für alle autorisierten Mitarbeiter zugänglich. Dies beschleunigt das Anzeigen und Abrufen von Dokumenten und Informationen in Bezug auf eine bestimmte Anfrage oder einen bestimmten Fall. Dies führt zu einer gesteigerten Effizienz des Arbeitsprozesses und einem verbesserten Informationsaustausch zwischen den Mitarbeitern (niemand hat die physische Datei), sodass die Behörden auf regulatorische Anfragen effektiver und effizienter reagieren können.

“ **93%** *eDiscovery begann ernsthaft 1999, als eine Studie der University of California ergab, dass 93 % der in diesem Jahr generierten Informationen in digitaler Form erstellt wurden.* ”

Beschleunigung von Schwärzungen und Produktion

Die Möglichkeit, Dokumente zu prüfen, Informationen schneller zu schwärzen und die Einhaltung von Vorschriften zu beschleunigen, kann Behörden dabei helfen, mit dem wachsenden Volumen an regulatorischen Anfragen Schritt zu halten. Einige der verfügbaren Tools, die hier hilfreich sein können, sind:

- **Gemeinsame Bearbeitung von Dokumenten.** Der traditionelle Single-Flow-Prozess, bei dem Dokumente zwischen den Prüfern hin- und hergeschickt werden, verschwendet Zeit. Dieser Service ermöglicht Multi-Thread-Prüfungen mit Zusammenarbeit in Echtzeit zwischen internen und externen Prüfern, die die Kommentare des anderen sofort sehen können.

PhantomPDF mit der ConnectedPDF-Technologie von Foxit Software ist ein solches Produkt, das sicherstellt, dass ein Kommentar eines internen oder externen Prüfers automatisch mit allen anderen autorisierten Prüfern synchronisiert wird, sodass niemand die falsche Version liest. Die Zusammenarbeit in Echtzeit ermöglicht Prüfern mit größerer Autorität, eine vorgeschlagene Schwärzung sofort zu genehmigen oder abzulehnen, um Zeitverluste zu minimieren. Mit der Dokumentfreigabefunktion können Benutzer schnell, einfach und sicher Informationen über einen Datelink, soziale Medien oder privat mit einer ausgewählten Gruppe von Empfängern teilen.

- **Automatisierte Massenschwätzungen.** Serverbasierte Produkte, z. B. Rendition Server von Foxit Software, sind mit Datencenter-Infrastrukturen integrierbar und verwenden Muster und Schlüsselwörter, um Schwätzungen bei großen Dokumentmengen zu beschleunigen. Rendition Server ist ein lokaler Webdienst, der die Konvertierung von Office-Dateien, E-Mails, gescannten Dokumenten, PDFs und PostScriptDateien in einfach durchsuchbare PDF- oder PDF/ADokumente ermöglicht. Foxit PhantomPDF ermöglicht die automatische Suche und Schwätzungen bei einzelnen Dateien.
- **Automatisierte Lösungen für Konformität mit Section 508.** Neue Regeln des United States Access Board besagen, dass offizielle Dokumente, die online veröffentlicht werden, 508-konform sein müssen. Dokumentenmanagement, Katalogisierung, Archive, Überweisungsdaten und E-Mails müssen für langfristige Zugriffe aufbewahrt werden. Durch die Automatisierung der Compliance mit dieser Richtlinie sparen Sie Zeit für die manuelle OCR und das Tagging. Foxit-Serverlösungen und PhantomPDF automatisieren diese Verarbeitung. Andere Funktionen bieten Massenkonzertierungen von E-Mails und Anhängen, überprüfen vorhandene Dokumente auf die Einhaltung von Section 508 und ermöglichen eine einfache Nachbearbeitung von PDFs, die es Benutzern mit Behinderungen ermöglichen, diese Dokumente mit oder ohne unterstützende Software und Geräte zu lesen.

Zusammenfassend ist festzuhalten, dass Volumen und Umfang der regulatorischen Anforderungen weiter zunehmen dürften. Hinzu kommt, dass die heutigen Informationen aus zahlreicheren Quellen stammen und mehr davon nun vollständig digitalisiert sind. Um diese Herausforderungen zu meistern, bedarf es technologischer Lösungen, einschließlich der Dokumentenintelligenz und der Zusammenarbeit, eDiscoveryTools und Case-Management-Systemen. Diese können sicherstellen, dass regulatorische Anfragen effizienter bearbeitet werden, ohne die Sicherheit sensibler Informationen zu gefährden.

Über Foxit Software

Foxit Software ist ein führender Anbieter von schnellen, günstigen und sicheren PDF-Lösungen. Mehr als 560.000.000 Benutzer bei 100.000 Kunden in 200 Ländern verlassen sich auf Foxit-Produkte, die speziell entwickelt wurden für:

- **Connected PDF.** Führende Technologie, die Dokumentenintelligenz, Sicherheit und Zusammenarbeit für PDF-Dateien bietet.
- **Enterprise Automation.** Server-Software für PDF-Dokumentenmanagement und Datenerfassung in großem Maßstab.
- **Entwicklerlösungen.** APIs, Entwickler-Kits und mehr, die es ermöglichen, leistungsstarke PDF-Technologie in Anwendungen zu integrieren.

Um mehr zu erfahren, besuchen Sie foxitsoftware.com

¹ *Internet der Dinge*

² *Internationale Organisation für Normung*