Information Governance
White Paper: Data Minimization
February 2023

legal-rm.com

Why Data Minimization should be a hot topic for law firms

There was a time when lawyers and law firms were much more comfortable keeping client records and data indefinitely than they were destroying them. But that time has now passed.

iCOMPLi
by LegalRM

Why Data Minimization should be a hot topic for law firms

Chris Giles and Kandace Donovan | 23.02.2023

There was a time when lawyers and law firms were much more comfortable keeping client records and data indefinitely than they were destroying them. But that time has now passed. As **Chris Giles** and **Kandace Donovan** explain in this white paper, in today's legal landscape data minimization has become essential. Firms that don't practice data minimization have greater exposure through security breaches. They also run the risk of some dire cost, performance and reputational consequences.

Did you know that around 2.5 quintillion bytes worth of data are now being generated every day? In 2019, there were 4.4 zettabytes (ZB) of data in the digital universe. By 2020, that figure had increased tenfold to 44 ZB[1] and is forecast to reach 200 ZB by 2025[2]. This is a landscape in which data must be tamed or it threatens to overwhelm us or trip us up. It's one in which data minimization is critical for everyone, not least law firms which otherwise risk falling foul of cybercriminals, inefficiency, clients and regulators. The problem is that all too often firms aren't doing data minimization well – which could be very costly for them in all sorts of ways.

Cybercriminals are coming to get you

A significant danger is the growing incidence of cybercrime targeted at law firms. This has led to a number of high-profile attacks hitting the media with the attendant negative reputational impacts. And it's safe to assume that many more breaches will have occurred that haven't made the press.

Among the nightmare scenarios that couldn't be kept out of the news, a high-profile entertainment law firm in the US suffered a ransomware attack in 2020. To exert pressure, the attackers leaked information about a world-famous client, and asked for a ransom payment of $42 million to prevent the release of further documents about further celebrities. News outlets reported that the criminals eventually received USD$365k.[3]

In the same year a leading UK criminal law firm became the victim of a ransomware attack on its archive servers. Nearly 100,000 individual files were encrypted by the attackers and 60 court bundles exfiltrated and published on an underground market site. The bundles included sensitive personal data including medical files, witness statements, and victim and witness names and addresses.[4] The monetary and reputational cost to the firm isn't known but we do know the UK regulator – the ICO – fined the firm 3.25% of their annual revenue.[5]

Nor are the risks receding. According to ABA's 2021 cybersecurity report, ransomware is: "An increasing threat to attorneys and law firms of all sizes".[6] And unfortunately, the low ebb in international relations between the West and Russia and China only exacerbates the threat, since the Russian and Chinese governments are not currently minded to clamp down on their homegrown cybercriminals. Quite the oppositive.

Microsoft revealed that state-sponsored Chinese hackers have been targeting "US-based universities, defense contractors, law firms and infectious disease researchers".[7] Law firms are on that list because cybercriminals know you hold a wealth of data worth stealing, which is also often ransom-worthy and relatively – in comparison with financial services and big pharma for example – poorly protected.

They also know that the more data held by a firm, the more likely that data will yield rewards for them, so the more effort they will put into breaching your defenses – hence the importance of data minimization. And bear in mind that these cybercriminals are highly organized and determined professionals. It's been estimated that in 2021 cybercrime generated USD$6 trillion. To put that in context, cybercriminals earned more that year than Japan, the world's third largest economy.[8]

Comply or be fined

A second major hazard for those firms not on top of data minimization is incurring a compliance breach – of which there are three types: regulatory compliance, contractual compliance with client Outside Counsel Guidelines (OCGs) and compliance with professional standards.

The challenge with regulatory compliance is that the volume of data privacy regulation is continually growing. The General Data Protection Regulation (GDPR) has been enforceable in the EU and UK since 2018 (the UK version is called the Data Protection Act) but note that GDPR applies anywhere that anyone is handling the data of EU citizens. Organizations found to be in breach of GDPR face a penalty of up to 4% of their global annual revenue or €20m (c.USD$21.5m), whichever is higher.

Subsequent privacy regulation in other jurisdictions is more or less following the GDPR model of having stringent requirements around how Personally Identifiable Information (PII) is obtained and held and for how long it's stored. Hence the relevance to data minimization. Because PII can only be held for a limited period, to maintain compliance firms need to continually purge their PII data or run the risk of large fines and reputational damage.

In the United States there's no federal data privacy law yet – though it's contemplated – but the California Consumer Privacy Act (CCPA) is the first of several state laws already in force or in the pipeline that will mandate how the PII of US citizens is treated.

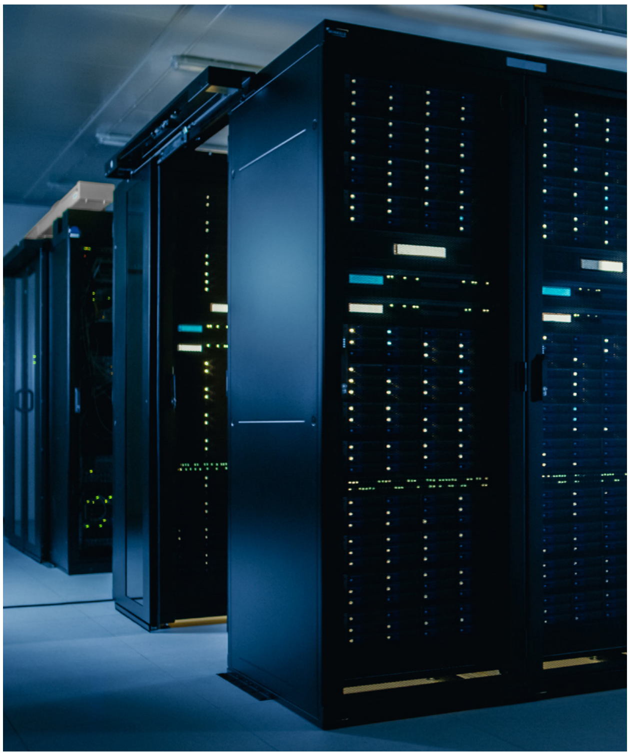
Meanwhile, Brazil has a General Data Protection Law – LGPD – which is close to GDPR; and Canada has the Personal Information Protection and Electronic Documents Act (PIPEDA) which will be strengthened by a new piece of legislation – the Canadian Privacy Bill C-27. This is due to pass into law this year. It includes provisions for mandatory data breach reporting, increased fines for non-compliance and the creation of a new position of Privacy Commissioner of Canada. It imposes yet more data privacy rules and regulations that firms must actively manage if non-compliance is to be avoided. And remember you can not only be fined by the regulator but also sued by a client or data subject if found to be in breach of legislation.

Compliance with the demands of your clients and profession

The next compliance booby-trap for firms is Outside Counsel Guidelines, which are becoming more ubiquitous and more demanding. Whereas they were initially conceived as a mechanism to help ensure the client is getting value for money from the firm, in the light of rising cybercrime OCGs are becoming more prescriptive around how and for how long firms holds client data. In addition, some clients – particularly big corporates – are setting their own "gold standards" for data management that go beyond existing or anticipated legislation, and which will be passed on in OCGs.

It's also the case that when the firm attends pitches and when clients are reviewing the firms they want to retain, clients will want to hear reassurance about how their data, some of which is hyper-sensitive information, is being stored and actively managed in line with best practice, including when it's accessed by collaboration tools and in deal rooms. The ability to point to rigorous information governance systems will strengthen your hand in competitive pitches.

Clients are also increasingly looking for ISO/IEC 27001 certification. To gain this, firms need to demonstrate to a third-party auditor that they've met requirements in relation to physical and electronic information security, including in relation to data retention. The standard's requirements include for an information inventory to be maintained and for information to be classified and labelled according to the information security needs of the firm based on confidentiality, integrity, availability, and relevant interested-party requirements. Controls need to be in place for information access and transfer. Records must be protected from loss, destruction, falsification, unauthorized access, and unauthorized release. Plus, international standards always insist on regulatory compliance, so firms must identify and meet applicable regulations and contractual requirements that protect PII.



Finally, lawyers must also be careful about maintaining compliance with their professional standards in relation to how client data is handled and secured and for how long. But these aren't the only reasons to pay attention to data minimization.

System performance and storage costs

Firms are also well advised to minimize data because of the hidden cost of not doing so. Excess data impairs the efficiency of your systems. Bloated databases take longer to process requests such as searches; and system functions like backups, reorganizations, migrations and disaster recovery protocols take longer.

Plus, the impact of slow systems could be worse than you think. When a system freezes or takes too long to load, the user's train of thought is interrupted and they lose momentum. A University of California study concluded that it takes an average of 23 minutes and 15 seconds to get back to a task after interruption.[9] The impact on productivity is clear, not to mention the impact on lawyer morale and stress levels.

We're also seeing a big rise in matter mobility. Whether clients are moving from firm to firm or lawyers are, the firms that are across their data management and minimization will be penalized much less by matter mobility because you'll simply be able execute it much more quickly and efficiently.

Storage can be pricey

Finally, firms also need to think seriously about the avoidable costs of excess data storage. Until quite recently, data storage was a fixed, but relatively manageable cost. That's changing, partly because the use of cloud collaboration services has rocketed since the start of the pandemic. These tools, such as Microsoft Sharepoint, don't offer archive storage. Everything is just so called "hot" storage – meaning the storage media provide fast, easy access to data.

But it can also mean that the costs of continually increasing electronic data storage volumes are becoming uncomfortable. A December 2022 study showed that 500 UK technology leaders in mid-to-large sized companies were spending up to one-third of their IT budget on ballooning data storage costs. Survey respondents also thought that the rising costs of data would be “unsustainable” by 2025.[10]

Likewise in the US, 68% of IT managers described cost as their main data storage pain point in 2022 because their budgets aren’t keeping up, and the cost of storage is doubling every four years.[11] For law firms who’ve negotiated a per user volume for cloud-based storage in a document management system, rising storage costs may not be immediately troubling, but they will find you. It’s another reason why firms should be managing their data minimization much more actively to control the ever-increasing volume of data.

Law firms are bad at data minimization

So much for the many perils of poor data minimization. But it really matters because there’s evidence that law firms aren’t doing data minimization well. Best practice is a data retention policy, realized via a data retention schedule, that’s enabled by procedures and systems, and backed by controls and oversight. Yet only just over half (53%) of the respondents to the ABA’s 2021 cybersecurity survey said their firm even had a policy to manage data retention.[12] Moreover, even where a policy exists, it’s often not enforced. A poll conducted during a recent LegalRM webinar suggested only 26% of firms with policies were implementing them.

It’s also the case that even when a data retention policy and schedule are being implemented, the agreed schedule often isn’t being applied to the firm’s electronic records. LegalRM recently worked with a mid-sized firm and discovered that more than half of its DMS-based records were overdue for destruction. That’s a considerable amount of excess data exposing the firm to unnecessary costs and risks. Nor did this consider all the other possible data repositories, including File Share, OneDrive, SharePoint, HR database, and the firm’s time and billing or practice and case management systems.

What challenge of data minimization

Why are firms so bad at data minimization? It’s partly because it’s a complex area. Many firms are transitioning from predominantly physical record keeping to on-premises electronic storage and increasingly to cloud-based document management systems. For now, they could have elements of all three. They might be overwhelmed by the sheer number of dispersed physical and electronic data repositories, even as the volume of data held by the firm continues to rise inexorably.

In parallel, data minimization is a discipline that can fall between the cracks that potentially exist between several roles: the Director of Information Governance, the Director of Risk, the Director of Conflicts and Records, the Data Protection Officer, the Chief Information Security Officer, the General Counsel, the Records Manager, and the Chief Information Officer. And in the melee of keeping the firm’s wheels turning, data minimization’s importance gets overlooked.

Nor, in an economic climate dominated by inflation and rising interest rates, does it seem like a propitious time to be spending money on abstractions like risk mitigation and compliance. Yet data minimization processes and systems are not a “nice to have”. They should be recognized as a priority for any law firm, both to avoid the dire consequences of cyberattack and compliance breaches, and to reduce the operational costs of slow systems and rising electronic and physical storage. So how should it be done?

What firms should do now

Firms first need to increase their general level of awareness around data lifecycle management, information governance and the value of data minimization. Each firm is structured differently but broadly there’s a need to engage all the related stakeholders and then develop an understanding of why data minimization matters. Of course, some firms will be ahead of the game with an up-to-date information governance policy and an agreed data retention policy and schedule that is conscientiously implemented.

For everyone else it’s time to look at setting up an internal committee that will likely include the General Counsel, Director of IG or equivalent, CIO, CISO and/or DPO. Their objective is to mobilize a coordinated firmwide data minimization project. The committee should also include representatives from HR and finance.

Together this committee should start with understanding the various retention and disposition policies that exist within the firm, as well as understanding the rules of retention and disposition and how they vary across different departments and practice areas. For instance, real estate and trademark practices will have ‘wet ink signature’ documents that must be kept in perpetuity. The heads of HR and finance will know how long HR and finance data respectively should be kept in the relevant jurisdictions before destruction. The committee must also fully understand the potential limitations of the systems and processes currently in place.

Find your way with a data map

If the firm doesn't have one already, the committee should direct a data mapping exercise. Bear in mind that the initial picture might be discouraging. It's generally the case that when systems were set up, data governance wasn't front-of-mind. Instead, systems are generally based on the user perspective. People want letters to be called letters, and contracts to be called contracts. So often systems can't distinguish a lease agreement contract from an employment contract that includes time limited PII. That's why firms need to do some data mapping and put the data within systems into a data retention classification structure, being mindful of the governance requirements around retention and disposition. It's also necessary to know the risk profile of data held. Mergers and acquisitions, for instance, might be privy to some extremely market sensitive information that hackers will target.

Thereafter the firm might want to look at building cross-departmental teams of process, system and data owners to understand what's needed and what's possible with existing systems and what can join those two together. For example, data might not be well classified, systems functionality might not allow for you to archive data in a way which meets requirements. At this point firms should be looking at IG governance platform like iCompli that let you go into multiple different data stores and media types to manage and destroy data across systems.

Data minimization for the modern firm

The key in it all is for firms to be proactive in the face of what might seem at times like a blizzard of data. But keep in mind that a data minimization strategy will benefit the whole firm. It should engage the most senior levels, including the CIO, CISO, COO, and General Counsel. These postholders may not be responsible for data strategy but the fallout from a failure to minimize data will still land at their door. Data breaches incur lost productivity and possibly ransom payments, cybercrime expert fees, regulatory and professional fines, and even client and past employee lawsuits. The reputational hit impacts client retention and acquisition and future rates and fees. If your firm is considering the move to a cloud based DMS you will also reduce the duration, fees and ongoing costs of the transition by enacting data minimization. There are many strong reasons to take data minimization seriously, and many ways to regret it if you don't.

To find out more watch our ILTA Masterclass to hear a discussion on the advantages of a data minimization strategy, and in particular why this strategy is of particular importance to a CIO, or the IT budget holder within a firm. To register, click here.

Chris Giles is CEO at LegalRM, which creates market-leading software, services and solutions for records, risk and compliance management and serves some of the world largest law firms as well as blue chip organizations from other industry sectors.

Kandace Donovan is LegalRM's Vice President Operations, North America.

[1] A zettabyte is one trillion gigabytes, see: https://explodingtopics.com/blog/big-data-stats

[2] https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/

[3] https://arcticwolf.com/resources/blog/top-legal-industry-cyber-attacks/

[4] www.dataguidance.com/news/uk-ico-fines-tuckers-solicitors-llp-£98000-data-breach

[5] https://ico.org.uk/action-weve-taken/enforcement/tuckers-solicitors-llp-mpn/

[6] https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/

[7] https://www.cbsnews.com/news/microsoft-chinese-hackers-email-server-bug/

[8] https://news.cybersixgill.com/chinese-russian-cyber-threats/ In 2021, the gross domestic product of Japan was estimated to be around 4.9 trillion U.S. dollars.

[9] https://www.fastcompany.com/944128/worker-interrupted-cost-task-switching

[10] https://techmonitor.ai/technology/data/data-storage-costs-uk-it

[11] https://www.lightedge.com/blog/the-data-explosion-and-hidden-data-storage-costs-in-the-cloud-could-object-storage-be-the-answer/

[12] https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/

About iCompli, from LegalRM

iCompli, from LegalRM, is an intuitive information governance platform for risk-savvy law firms that want to manage the life cycle of their assets from a single, comprehensive application.

For numerous law firms across the world, iCompli simplifies and automates client file transfers, retention, disposition, and overall compliance of both physical and electronic assets from multiple information repositories, seamlessly and securely.

Plus, it delivers the most powerful physical records tracking database available on the market today. Firms have the option of using iCompli's barcode tracking or RFID capabilities for managing physical records in conjunction with the system's information governance features, all within a simple user interface.

To find out more visit www.legal-rm.com.

W legal-rm.com/icompli
legal_rm
in legal-rm