REPRINT

risk & compliance

ELECTRONIC INFORMATION MANAGEMENT

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
APR-JUN 2017 ISSUE

risk & compliance
APR-JUN 2017
www.riskandcompliancemagazine.com
Inside this issue:
FEATURE
The reputation and compliance dynamic
EXPERT FORUM
Managing FCPA risks in emerging market M&A deals
HOT TOPIC
Developing a strong shareholder engagement plan

www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

A & M
ALVAREZ & MARSAL

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

MINI-ROUNDTABLE

ELECTRONIC INFORMATION MANAGEMENT

PANEL EXPERTS

Phil Beckett
Managing Director
Alvarez & Marsal
T: +44 (0)20 7663 0778
E: pbeckett@alvarezandmarsal.com

Phil Beckett, a managing director with Alvarez & Marsal's Disputes and Investigations practice in London, brings more than 18 years of experience in forensic technology engagements, advising clients on forensic investigations of digital evidence, the interrogation of complex data sets, information governance, cyber risk and the disclosure of electronic documents.

David Dutt
Managing Director
Alvarez & Marsal
T: +44 (0)207 863 4797
E: ddutt@alvarezandmarsal.com

David Dutt is a managing director at Alvarez and Marsal, and leads A&M's business technology practice for Europe. With more than 20 years of experience in business information technology (IT) consultancy, with extensive accomplishments in business technology led transformation assignments across numerous industries in North America, Europe and the UK. Based in London, he has led a wide range of business engagements, specialising in large-scale, ERP-driven transformation, performance improvement, cost reduction and business intelligence.

Peter Jaffe
Senior Associate
Freshfields Bruckhaus Deringer US LLP
T: +1 (202) 777 4551
E: peter.jaffe@freshfields.com

Peter Jaffe is a litigation senior associate the Washington office of Freshfields Bruckhaus Deringer US LLP. He has particular expertise representing financial institutions and multinational corporations in contentious matters. He frequently writes on topics of data, cyber security, and cross-border privilege and discovery issues for the Freshfields digital and risk blogs.

Marcus Turle
Consultant
Herbert Smith Freehills LLP
T: +44 (0)207 466 2886
E: marcus.turle@hsf.com

Marcus Turle leads Herbert Smith Freehill's data protection practice in London. He has been advising on privacy and information law since the late 1990s, when he qualified as a solicitor at the start of the dotcom boom. He has almost two decades experience advising on legal compliance and implementation and he has written numerous articles on data protection and data security. He is general editor of Thomson Reuters' flagship privacy title, Data Protection Laws of the World.

RC: Could you provide an overview of the extent of electronic information that companies have to deal with in today's business world? What specific challenges do they face when it comes to creating, handling, backing-up, storing and disposing of this volume of data?

Beckett: The backbone to all business in the 21st century is instantaneous electronic information: emails, texts, tweets, instant messages, mobile communications, and so on. While traditional data source growth is estimated at 40-60 percent year-on-year in corporates, this is now being compounded with the rise of social network data, and the beginning of the Internet of Things (IOT), with data set to double every 12 months. It is now a challenge for employees to be able to find relevant data, as on average, up to 70 percent of data has no business value, compounded with the lack of data ownership and disparate needs from the business stakeholders. Companies are sitting on unknown levels of risk, due to lack of insight into data stored, and a myriad of different repositories across the enterprise. The lifecycle of information in a business is fundamentally broken – not all data is created equally, yet when it sits on the same storage layer, IT treat it as if it is. Tape backups are used as archives that never get deleted, data is migrated to each new storage system over the years without any consideration to its business value, as IT need the Line of Business (LOB) to make decisions on whether the data has any value. The LOB does not have the time to do this as their focus is on creating net value for the company, not worrying about how much it is costing to store in the back end of the company. Differing stakeholders with differing objectives on the data only compound the issue in the long term. Defensibly disposing of the data means that all the stakeholders need to be aligned, and with the GDPR on the horizon, companies need to be proactive as to what, where and why they are storing data.

Dutt: Businesses have to deal with multiple sources of data internally and externally. This ranges from third-party electronic data feeds, through to master and transaction data needed to run business transactions, right down to email traffic. Much of this is sensitive, be it HR, financial data, password information, and so on, and the scale of the data is ever increasing. Most businesses do not fully understand the data they have or the security that supports their storage and ultimate use of it. Strategies are rarely employed with full business sponsorship as many do not fully understand or appreciate the value of data in the organisation, outside of the rudimentary reporting usage.

Jaffe: It goes without saying that nearly all information today, from communications to financial transactions to employee and customer information, is electronic. There is an obvious cyber security challenge: to ensure the confidentiality, integrity and availability of that data. Similarly, there is an obvious data privacy challenge, given the complexity of regimes coming into force worldwide. There are also other challenges – particularly legal challenges – that draw less attention. How do you structure the ownership of data that you create or purchase? This requires thought from an intellectual property perspective. Ownership may also have tax implications if the data generates significant revenue, or if it establishes a tax residence in certain jurisdictions. The choice between data creation and acquisition may also affect whether costs can be deducted or must be capitalised.

Turle: It is fair to say that the amount of data handled by business today is unprecedented, and continues to grow exponentially. This is because there has been an historic tendency for companies to keep electronically stored information, such as corporate documents and email, without time limit, so that by default many companies now have huge volumes of data held on a multitude of legacy systems. Companies also now handle ever-increasing amounts of customer data, for example, through the proliferation of IoT technologies and social media. These factors present many challenges, for example, in relation to data security, identification of data when it needs to be retrieved or destroyed, storage costs and, for business critical systems, the need for sufficient resilience and redundancy. Importantly, this is not just an IT issue: there is much legal regulation, such as, the forthcoming General Data Protection Regulation (GDPR) and, in the context of the financial services sector, the FCA's Principles for Businesses and the Systems and Controls set out in the FCA Handbook.

RC: What electronically stored information (ESI) strategies can companies deploy to assist in the smooth implementation and operation of an efficient electronic information management system?

Jaffe: Even in the age of Big Data, the adage 'less is more' has a lot of purchase. From a legal perspective, the best way for companies to manage electronic information is not to collect it in the first place, or to keep it only as long as needed. The risks of Big Data should never cause you to shirk from making a deliberate decision to collect data that is valuable to your business. But collecting and keeping data reflexively or unintentionally is dangerous.

Turle: The key issues here are fitness for purpose of the ESI management system, its scalability and longevity. The requirements for the ESI system will often be dictated by the regulatory framework in which a company operates. If a company is not heavily regulated, it may be that a simple, for example, 10 year retention period can be applied to all corporate data. However, as soon as regulation requires certain types of data be kept, or destroyed, in certain circumstances, or after certain periods of time, then the ESI system needs to be capable of identifying that. This creates difficulties, particularly where data is unstructured or relies on human intervention to categorise it. Scalability and longevity are important because it is common to see systems straining under the volumes of data they contain. The temptation then is often to replace them, but where data is held in multiple systems there will often be problems extracting data when it is needed, for example, for the purposes of litigation or a regulatory investigation.

Dutt: Enterprises need to be clear on the processes and organisation required to support data in the organisation. Too often data is associated with specific business or IT projects but the long-term management is ignored and data, governance and maintenance deteriorate over time. Electronic data management does not need systems as a priority but senior business level support across end-to-end processes. Data management and security solutions clearly have a role, but the basics need to be in place as a priority. Specific technical strategies include 'salting and hashing' for passwords, encryption of sensitive data and enforcement of complex individual passwords to include numeric and alphanumeric characters and minimum string length.

> **"Data management and security solutions clearly have a role, but the basics need to be in place as a priority."**
>
> *David Dutt,*
> *Alvarez & Marsal*

Beckett: Companies need to get a handle on their information governance (IG) maturity level. At the moment, we are seeing lots of new tech companies that are creating, collecting or processing a phenomenal amount of data, with the rise of Big Data and Big Analytic platforms. The amounts of data are equally comparable to large, established companies with thousands of employees; the challenge being how to remain small and nimble while operating an effective strategy on their data. As not all data has equal value, the question becomes how to establish an IG framework that adds value to what the company requires, and remains cost effective and not a business bottleneck. Companies need to establish their IG framework, owned by senior stakeholders in the business to make up their data governance council with executive sponsorship. To be able to be effective with data, in light of GDPR requirements, it is necessary to construct data maps to understand where and why data is being used and stored. The company governance team will need to perform analysis of existing data repositories to understand the level of redundant, obsolete or trivial (ROT) data and related risk, and identify potential cost reductions. Current standards that companies can make use of include, for example, ISO 27001 Information Security, SAS 70 Type II and SSAE 16 – the standards that are most closely aligned to their industry.

RC: In your opinion, how concerned should companies be about the unrestrained growth of their electronic information? If this growth goes unchecked, how exposed does it leave companies to increasing costs, as well as legal, regulatory and compliance risks?

Turle: Although electronic data has been around for many years, there are two key differences today. The first is that people's perception of data has changed and they are now more willing to trade their data for services. Secondly, we have the emergence of new technologies that enable organisations to really interrogate and analyse data so as to extract commercial value. This combination is driving major evolution in data monetisation. However, just because the technology exists to enable companies to do weird and wonderful things with data, this does not mean that the law will allow it. There has been a correspondingly pronounced proliferation of laws aimed at restricting data use and protecting individuals – the most obvious example being GDPR.

> "The unrestricted growth of electronic information is a huge problem for a lot of companies; typically it is classed as an IT problem rather than a problem for the business."
>
> *Phil Beckett,*
> *Alvarez & Marsal*

Beckett: The unrestricted growth of electronic information is a huge problem for a lot of companies; typically it is classed as an IT problem rather than a problem for the business. The focus has usually been on the structured data estate – applications and databases. With exponential growth in unstructured data, the 'store everything forever' paradigm now has to change. The answer of 'storage is cheap' as the latest and greatest technologies appear cannot justify the risk held within the data itself. Data growth rates typically are around 40-60 percent per year, with IT required to double its storage every 18 months. On average, the increases in IT budgets are between 1-5 percent per year, with 70-80 percent being spent on only maintaining the current systems. If 80 percent of data is unstructured content in 'dark data' stores such as fileshares, Sharepoint, the cloud, and so on, and 70 percent of this stored data has no business value, questions need to be raised as to why money is being wasted on infrastructure and staff for storing and managing this data – on average, £2 per GB on a company's blended enterprise storage. The data usually contains large amounts of sensitive and personal data, ripe for a data breach and potentially no one would even know what was taken. To sum up, unrestrained data growth means unrestricted costs, and has a direct impact on the ability to comply with upcoming data privacy regulations under GDPR.

Dutt: Increasing amounts of information are being collected for decision-making purposes. Often they do not know what to do with what they have collected, never mind look to pull in more. The term Big Data is an abstract concept and the real focus we see is more basic – how do we want to measure our business? Simply put, they should be concerned. With the rapid growth of data, the next question is to ask, what do we need to do it? Increased spread of information, namely where aspects of the business outsourced or information shared with other offices in different geographies, means there is wider array of vulnerabilities. The maintenance and management of data is an unfortunate consequence. Having a targeted approach to data, rather than a shotgun 'pull in loads of data then decide what we will do with it' is required. Companies continue to be unaware of potential costs, both direct and reputational. In terms of risk and exposure, companies are left very exposed at the moment. There is a clear acknowledgement that longer term needs include increased predictive analytics, machine learning and artificial intelligence supporting processes, but the path to that and the data need is unclear. For now, businesses are doing the basics but it is clear that increased focus will be on the security of data rather than the risk from the sheer volume of data. Companies are being held increasingly accountable for the information they hold.

Jaffe: No sane manufacturer worries about selling more widgets just because more widgets come with more risk. So if data is your company's widget – or if data is the tool that your company uses to make widgets – why should it be any different? But if the question is about the unrestrained growth of electronic information, then companies should be scared out of their minds. Data does come with risk, and holding data that is not necessary and not profitable, or that does not have the right controls

around it, is a terrible idea. And unfortunately, a lot of companies collect and keep data reflexively, without really thinking about what they are doing – sometimes without even realising that they are doing it.

RC: In light of all the reported data breaches on an almost weekly basis, do you feel that companies are satisfactorily addressing the cyber security requirements? Where should their focus be?

Dutt: Are companies satisfactorily addressing cyber risk regulations? Clearly not; basic security is in place, but it is rudimentary and not linked to the data level. Most security exists at an application layer and relies on compliance checks but this is rudimentary at best. Going forward, businesses need to be more aware of the threat from within, as much as from without. Organisations are starting to invest in increasing their education in better understanding the risks from the threat of data breaches versus the costs on cyber security investment, as well as the more basic human level vulnerabilities. This understanding starts at board level.

Jaffe: The fact that breaches are very common does not mean that the strength of defences is substandard. Even the best company can rarely stop a hacker from exploiting a zero-day vulnerability. Moreover, many reported hacks turn out to be relatively minor in terms of damage. There is no one-size-fits-all answer to the question of focus. The data and systems that pose the highest risk will vary from company to company. So it is difficult to say where companies should focus. But they should start mapping the systems and data that the business holds most dear, or that would pose the greatest risk if compromised.

Beckett: Cyber security is about reducing and better managing risks. From our experience, regionally speaking, UK organisations are 'behind the curve' and are lacking an understanding of what activities are involved in managing cyber security risks, whether externally and internally, including how they respond to a suspected or known breach. Fundamentally speaking, cyber security should help drive a company's risk management process, meaning formal processes and exercises should result in the articulation of what the acceptable level of risk is for their assets, business critical infrastructure and PII. In addition, gadgets cannot do it alone. Cyber security programmes need to be built on policy, and enforced with standard operating procedures by stakeholders and integrated subject matter experts.

Turle: This varies significantly from company to company. Many have put in place appropriate measures to protect their information assets or other infrastructure, particularly in relation to heavily regulated industries, or where specific standards apply, such as the Payment Card Industry Data Security Standard (PCI DSS). Others have done very little. In terms of where the focus should be, the first step in any exercise should be a risk assessment to identify what assets, be it information or critical systems, are exposed to what risk. Only then can a decision be taken as to where the investment needs to be to bring the systems and information security up to scratch.

RC: In your opinion, has there been an historic lack of appetite among companies to invest time and money into robust electronic information management (ESI) policies and procedures? Do companies tend to bring together the right stakeholders when dealing with information governance?

Beckett: ESI management policies and procedures are typically seen as putting the brakes on what companies want to do with the data, whether it is reuse or resell. To add to the mix, there is usually a real lack of ownership for data and no executive sponsor. The answer of what to do with the data has always come down to the lowest cost resolution – 'storage is cheap', therefore keep everything. The current regulation has had minimal impact on bad data practices given the limited fines it can impose, so it has been easier to take a fine if the profitability of the operation covers it. GDPR will now fundamentally change that paradigm. The problem with stakeholders is that typically they are not aligned; there is a complete mismatch and understanding of each group's information governance needs, as there is no central voice. To be effective, and keep costs and risks under control on data, companies are now looking at cross function data governance leadership team with executive level sponsorship as the answer.

Jaffe: To be sure, one challenge has been the attitudes of decision-makers. According to one study, in 2014, only 7 percent of board members viewed cyber security as a high priority, but that is changing rapidly – in just two years, that number has more than quadrupled to 30 percent. Similarly, a common pitfall has been the failure to take an integrated approach. But again, this is changing for the better. We are starting to see more companies assemble broad-based teams to address the challenges of data.

Dutt: Data is not sexy; it is boring and a necessary evil. There is a clear lack of understanding of the value of good data and what that means to the organisation. 'A bird in the hand is worth two in the bush' – investment in things with direct, measurable benefits are more appealing than a protection against potential threats which, if you are doing your job properly, are unlikely to attract much attention. It is not clear why data should be fixed and maintained – so what if a lot of records are incomplete, we can still bill them, right? There are, of course, high profile reputational risks to bad data. For example, British Gas sent swimming vouchers to dead customers, but the effort of investing in data does not always seem worth it – especially at an enterprise level. At a purely functional level you will always see pockets of greater control, for example, in finance, master data is usually maintained with more rigour, but this is not reflected across all data in the enterprise. For a lot of organisations, bringing the right people together to deal with information governance is a poison chalice. Despite data being a critical business asset, there is a reluctance to invest time, money and the right resources in dealing with it.

RC: Do you believe companies are ready for the update in European privacy regulation? How will they address the

new requirements they face under these changes? How much do you expect this to impact global business?

Turle: Many companies are certainly now taking the GDPR seriously, probably because it is clear that it is definitely coming to the UK next year. However, there are very few companies that can be said to be fully ready for GDPR. But the important thing is that companies are taking firm steps to put in place measures to achieve compliance. Many are looking at key areas, such as what they tell individuals when they collect their data, their consent architecture – and whether consent is in fact the right way to legitimise data processing – international data transfers, data security, arrangements with third-party data processors and how to meet the GDPR's new accountability requirements. It is clear that GDPR will have a huge impact on global business and it is a good bet that it will become the common standard for global contracting where personal data is concerned.

Jaffe: Most companies seem to recognise that the GDPR is not to be taken lightly. In a November 2016 survey of privacy professionals, IAPP and TRUSTe found that over 92 percent of companies surveyed had begun preparing for the GDPR by developing at least a preliminary plan. Sixty-seven percent of EU companies and 40 percent of US companies have begun implementing their GDPR plans. Even for companies that already structured their data to comply with EU law, the GDPR may impact operations. The right to be forgotten, reconceptualising consent, and so on, will require companies to change the way they do things. But some companies have never taken European data privacy seriously, in light of the relatively minimal consequences for violations. Those consequences are about to change – and so will these companies.

> **"We are starting to see more companies assemble broad-based teams to address the challenges of data."**
>
> *Peter Jaffe,*
> *Freshfields Bruckhaus Deringer US LLP*

Beckett: In our experience, companies are at the early stages on their journey to compliance. Plenty of advice has been received as to the sort of initiatives that they need to be considering – how to operationalise these initiatives is proving to be the challenge. In some cases, there may be a massive impact on global business – any organisation holding or processing EU individuals' personal data must comply with the regulation. Controllers, which are companies that have a contract with the client, need to ensure that processors, which are companies that are providing analysis of the data for the controller, will comply with the regulation. Fines will be assessed against global turnover rather than the traditional limited fine currently in action. Ultimately, addressing these requirements will require organisational change impacting their people, processes, procedures and technology. Initially though, the key is not to boil the proverbial ocean, but to assess and determine the current IG maturity level to identify and focus on quick win initiatives in line with GDPR.

RC: To what extent do companies need to recalibrate their corporate mindset and measure their effectiveness so they become more inclined to establish definitive information governance policies and procedures to determine what data can be deleted on a routine basis?

Dutt: Before they understand what can be deleted they need to be clear on what they need. There are too many gaps and inconsistencies between how business drivers are defined and rippled down through consistent metrics within the organisation. Too often we see silos of reporting, where reports are generated for no clear business reasons. For this to change there needs to be clear senior leadership and engagement to help transform the organisation into an 'information centric' business where data is used to proactively drive decision making. It is closely linked to advanced analytics and performance management as these are key areas that can help drive and shape the electronic data agenda.

> **"The potentially very high penalties under the GDPR make it imperative that companies establish robust and effective information governance and data retention policies from May 2018."**
>
> *Marcus Turle,*
> *Herbert Smith Freehills LLP*

Jaffe: Provided that adequate safeguards are put in place, it is fine to make a deliberate decision to hold profitable data, but it is stupid to hold data that you do not need. Measuring the value of data is the fundamental first step in this calculus.

Beckett: The need and use of information during its lifecycle falls under the contrasting requirements of various business stakeholders: legal, records management, compliance, privacy IT, and Line of Business. While the stakeholders will need to coordinate and comply with disparate needs, rules and regulations, the ultimate ownership of data is defaulted to IT, which is unable to decide on its business value and therefore its retention, as this requires an insight into the operational business context. Typically, this results in a 'keep everything forever' mindset. By establishing a data governance council consisting of the key stakeholders with executive sponsorship, it ensures that an information governance programme has the authority required to implement the necessary change – both from an organisational and IT perspective.

Turle: Data protection law throughout the EU requires that data should not be retained for longer than necessary, so this is akin to a positive obligation to delete personal data. The potentially very high penalties under the GDPR – up to 4 percent of global annual turnover – make it imperative that companies establish robust and effective information governance and data retention policies from May 2018. For non-personal data, the risks from over-retention tend to be more practical than legal. For example, the more data a company retains, the greater the compliance burden when dealing with a subject access request. Similarly, in any litigation, it increases the volume of information, and the expense involved when complying with disclosure obligations. Retaining data also increases cyber risk and necessarily incurs cost associated with physical and virtual storage.

RC: What advice can you offer to companies on updating and improving their data management strategies to protect against internal and external risks and threats?

Jaffe: This is mostly a question for IT professionals rather than lawyers. For lawyers, the job is more to make sure there is a legal and policy framework so that IT professionals can be effective. That means ensuring that the company designates a CISO with independent authority, that the board addresses cyber security and related risks and authorises adequate resources to combat those risks, and that there is a compliance structure that enforces the technical and human elements of cyber security. Moreover, and this is critical, it means ensuring that IT professionals are involved in due diligence on all significant counterparties, and that your contracts with those counterparties provide legal protections, such as cyber security representations and warranties and audit rights.

Beckett: We recommend that companies should position themselves objectively on the IG maturity model, to assist in identifying gaps that need to be filled. It is important that companies break down the problem into bite-sized, manageable chunks. Data mapping activities could quite easily tie up considerable resource for months if run across the complete business, so be very focused on the needs and go from there. It is important to be able to understand the hidden risks and costs contained within their data. Proactively identifying the sources of sensitive, personal, business and confidential data lying dormant in dark data repositories, can all be acted upon for securing, archiving or deleting where appropriate. Steps should be in place to establish data ownership and accountability structures within the company. This is extremely important, as most data breaches are typically due to internal weaknesses, giving employees access to information that they should not have or do not need, with an appropriate mechanism to audit or track should a breach occur.

Turle: The GDPR is quite prescriptive about what companies are required to do to keep data secure. Companies must implement "appropriate technical and organisational measures" to ensure a level of security appropriate to the risk, taking account of cost, the state of the art, and the nature, scope, context and purposes for which the data is processed. The GDPR expressly refers to the pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

Dutt: Companies need to better understand what the threats are, work with internal audit and risk teams to devise holistic risk strategies and clearly understand and categorise the risks within and without. They need to communicate this to senior leaders and get them to buy-in, and convince them how this links into the need for a robust data strategy, including data governance, security, compliance and authorisations, among others. They must be able to show why this is important at a tangible, practical level.

RC: How do you expect the way companies manage their electronic information to evolve in the months and years to come? Will this issue continue to grow in importance? What does the future hold?

Turle: Management of electronic information will almost certain grow in importance, particularly given the forthcoming GDPR which will bring in more stringent requirements and a higher level of accountability, along with much higher penalties for non-compliance. It is very likely that the GDPR will come to be seen as the global standard for the contracting of personal data.

Dutt: External risks will increase but much of the data agenda will be driven by advanced analytics, machine learning and predictive analytics to support critical business processes and drive business growth while enabling cost savings. Until data has a direct link with the bottom and top lines, very little will change and to do that senior leaders need to see more than buzz words, they need tangible evidence why they need to invest in data – not just reputational, high profile risk cases reported in the press. Arguably, the importance of electronic information will not grow; rather it will be better appreciated.

Jaffe: Though I am no prognosticator, a couple of trends interest me. First, if the current backlash against globalisation continues, it may both simplify and complicate international data flows. It may simplify data flows because there will be fewer of them. But it may also complicate things because jurisdictions will be less receptive to the arguments of companies that need to move data between jurisdictions to conduct international business. Second, we may see companies rethink the roles and responsibilities of various c-suite individuals. The tension between CIOs, CISOs, DPOs and sometimes CTOs has been around for a while. But as companies increasingly think about monetisation challenges, and not just security and privacy, the picture gets cloudier. Finally, I suspect that data strategies will complicate M&A. It is often said that companies need to conduct extensive diligence on a target's systems; the subtler point is what comes after an acquisition. If companies want to manage data effectively, they will need to integrate the systems of targets much more quickly than in the past. From a data and IT perspective, it is increasingly difficult to manage a Frankenstein company with a bunch of cobbled-together, incompatible systems. Unfortunately, many corporate behemoths today are exactly that.

Beckett: The evolution of technology has revolutionised how organisations perform, resulting in the exponential growth of data, the majority of which is without context or value. The growing awareness of the risks associated with this data and its potential for public damage is driving the revolution on regulations – for example, the GDPR putting the individual's data rights above the needs of an organisation. Therefore, a robust IG strategy is required to marry the data requirements and business processes with the ever changing regulatory, technological and cyber landscape.

With escalating IT costs, Big Data and Big Analytics platforms becoming more prevalent, increased fines from the data privacy regulations such as GDPR, and the potential for executive incarceration – keeping everything forever and taking no preventative action is no longer an option. Improving IG within the corporation is going to be – if it is not already – a high priority for executives and the board. If the GDPR becomes the standard of accountability for use of personal data, companies will have to have much tighter controls and management over their electronic information thus driving better information governance and security. R&C

A & M ALVAREZ & MARSAL

EDITORIAL PARTNER

Alvarez & Marsal

www.alvarezandmarsal.com

Companies, investors and government entities around the world turn to **Alvarez & Marsal** (A&M) when conventional approaches are not enough to activate change and achieve results. Privately-held since 1983, A&M is a leading global professional services firm that delivers performance improvement, turnaround management and business advisory services to organisations seeking to transform operations, catapult growth and accelerate results through decisive action. Our senior professionals are experienced operators, world-class consultants and industry veterans who draw upon the firm's restructuring heritage to help leaders turn change into a strategic business asset, manage risk and unlock value at every stage. When action matters, find us at www.alvarezandmarsal.com

KEY CONTACTS

Phil Beckett
Managing Director
London, UK
T: +44 (0)20 7663 0778
E: pbeckett@alvarezandmarsal.com

Julian Jones
Managing Director
London, UK
T: +44 (0)20 7072 3237
E: jjones@alvarezandmarsal.com

James Donnelly
Senior Director
London, UK
T: +44 (0)20 7072 3226
E: jdonnelly@alvarezandmarsal.com

R&C risk & compliance

APR-JUN 2017

www.riskandcompliancemagazine.com