REPRINT

R&C risk & compliance

EFFECTIVE COORDINATION OF RISK MANAGEMENT AND E-DISCOVERY

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JUL-SEP 2017 ISSUE

www.riskandcompliancemagazine.com

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

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

MINI-ROUNDTABLE

EFFECTIVE COORDINATION OF RISK MANAGEMENT AND E-DISCOVERY

PANEL EXPERTS

Phil Beckett
Managing Director
Alvarez & Marsal Disputes and Investigations, LLP
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.

Rory Conway
Partner
Linklaters LLP
T: +44 (0)20 7456 3382
E: rory.conway@linklaters.com

Rory Conway is a partner in the London dispute resolution group at Linklaters LLP. He has a broad practice, with a focus upon commercial disputes and contentious insolvency matters. He has acted for many financial institutions and corporates, as well as insolvency practitioners from most of the larger accountancy firms.

Jochen Benz
Managing Director
Alvarez & Marsal Disputes and Investigations GmbH
T: +49 89 710 40 60 44
E: jbenz@alvarezandmarsal.com

Jochen Benz, head of Alvarez & Marsal's German economics and forensic practice, is a managing director based in Munich and Frankfurt. Mr Benz is both a competition economist and a forensic expert. He has been selected by Who's Who Legal as being among Germany's leading competition economists and by Global Arbitration Review as being among the world's leading commercial arbitration expert witnesses.

Dr Petra Linsmeier
Partner
Gleiss Lutz
T: +49 89 21667 220
E: petra.linsmeier@gleisslutz.com

Petra Linsmeier regularly advises national and international clients on German and European antitrust law. Her practice focus includes cartel defence and damages cases as well as merger control proceedings. She also regularly advises on compliance issues and internal investigations in Germany, Europe and the rest of the world.

RC: Could you explain, in broad terms, the growing correlation between risk management and e-discovery in today's business world?

Beckett: There has always been a correlation between risk management and the requirement to review documents as they often provide the best source of intelligence and evidence around managing and mitigating risk. The explosion of data in the past few years means e-discovery techniques are coming to the forefront in risk management. Given the ever growing volumes and variety of data, especially that data which exists on the social and most informal channels, such as chat and IM messages, the need to not only grasp data, but positively take advantage of it from a risk management perspective, is critical. Gaining an insight into what is being 'said' across the different forms of communication in a timely and intelligent manner can mean that risks are controlled and mitigated before they have the chance to really damage an organisation.

Benz: With the new regulations around data protection, the need to review data and the associated risk of committing a breach of data privacy law must be balanced. There is, therefore, a strong organisational aspect to it in that robust rules and procedures around managing risks must be established. In particular, e-discovery poses challenges since its scope can extend to numerous legal entities across a variety of jurisdictions. Given the time pressures that usually come with e-discovery during the course of internal investigations, a 'let's cross the bridge when we come to it' approach is inadequate to say the least. This is even more pertinent, since the new EU regulations require privacy by design and data compliance by default.

Conway: Preparedness for a crisis is obviously an essential element of any risk management strategy, and dealing with a crisis in the modern world will inevitably involve e-discovery. So the two are increasingly going hand-in-hand. Organisations need arrangements in place that enable them to capture and review data on a large scale, potentially under time pressure. That means having policies that secure up-front permission from employees to conduct such capture and review. Further, it means having access to data processing centres and document review services, whether directly or through the professional services firms they engage, that enable them to exploit the advances that have occurred in that area in the past few years, be that cloud-based storage or access, machine learning or otherwise. Another aspect that is becoming increasingly important, including in light of the General Data Protection Regulation (GDPR), is the need for organisations to be in a position to identify, and as necessary, delete information that they are holding in respect of an individual or another organisation. Modern

e-discovery tools are increasingly critical to that capability.

Linsmeier: Without e-discovery the facts of a case cannot be fully assessed. Experience has shown that interviewees often need to be reminded of what they said and did in order to establish their full memory. Because of this, e-discovery forms an important part in investigations and as part of a risk mitigating exercise. Obviously, data protection rules need to be taken into account, not only during an e-discovery process but permanently as an essential element of a company's risk management system.

RC: In your opinion, how pressing is the need for organisations to integrate e-discovery considerations into their risk management capabilities?

Beckett: Integrating e-discovery into an organisation's ecosystem is something that should be at the forefront of senior management discussions. Understanding how their business uses data, how their sensitive information is communicated and how and where it is all stored is essential to gaining insights into many of the risks businesses face. In an ideal world, e-discovery processes would be fully integrated into the ecosystem as part of a good information governance programme. This enables all forms of data and communication to be identified, captured, analysed, monitored and securely stored so that it is available when needed and can be used in a pre-emptive sense to monitor and mitigate risks before they get a chance to develop into serious problems for the business.

> **"Integrating e-discovery into an organisation's ecosystem is something that should be at the forefront of senior management discussions."**
>
> *Phil Beckett, Alvarez & Marsal Disputes and Investigations, LLP*

Benz: Considerations with regard to the right organisational place for risk management around e-discovery and for compliance with data protection rules and regulations, is a question for a company's senior management. It needs to be dove-tailed around the various stakeholders across the organisation. In terms of investigations, for the purposes of objectivity, it is important that those responsible for complying with data protection are

not the ones leading investigations. The reason is simple: conducting a forensic investigation is always a balancing act between a person's obligations toward the organisation versus the rights of the concerned employees. So any actual or perceived conflict should be avoided.

Conway: One of the aims of the GDPR is to make data privacy a boardroom issue. Among other things, it will seek to do that by introducing a step change in the sanctions associated with breaches – up to €20m or 4 percent of annual worldwide turnover. This, combined with greater restrictions on the use of personal information, means that privacy issues are likely to become increasingly prevalent. Organisations will need to plan for e-discovery exercises, be they in the context of litigation, a regulatory investigation or otherwise, as a key component of their risk management strategies. By implementing robust information governance processes as part of their BAU approach, organisations can avoid the unnecessary costs and risks associated with a reactive e-discovery process.

Linsmeier: The better prepared a company is for investigations, the better it is. In the aftermath of a dawn raid, it must be quickly established which data was seized and which additional data is available. The clearer the IT structure of a company and the more organised the company's data management system are, the easier the e-discovery process will be. Knowing that in the event of a dawn raid and a following leniency application, time is of the essence to get the best available status as the leniency applicant, being prepared for an e-discovery process can result in substantially lower fines.

> **With the need to implement GDPR, it is even more important for a company to establish clear rules and a clear system of how data is handled within a company."**
>
> *Dr Petra Linsmeier, Gleiss Lutz*

RC: With the General Data Protection Regulation (GDPR) fast-approaching, with data becoming an increasingly valuable asset, what are the key components of a risk management programme that harmonises risk management and e-discovery?

Beckett: Simply increasing data storage relative to business growth is never enough. A defensible

strategy should be in place to control and manage sensitive and confidential information, such as personally identifiable information, which is key to GDPR compliance. The key components involve not only identifying the key data repositories within your organisation, but also understanding business risks and identifying where the two intersect. Once identified, processes need to be defined to ensure that the data is captured through the e-discovery process and then is made available and monitored from a risk management perspective. There is no point implementing these types of processes unless there is a business benefit, so the monitoring and control of data is essential in respect of driving business benefit and avoiding unnecessary pitfalls.

Benz: In particular, the link to e-discovery poses the question: what data is created by employees and where is it stored? This, in turn, leads to questions around what systems and programmes people have access to. This might sound reasonably simple but in fact it can be a significant effort to create such a 'data landscape'. Many programmes in financial services, for example, have a built-in communication platform that IT have no control over. As so many banks have learnt the hard way, this is a significant risk that needs to be managed. Plus, data outside of a company is obviously much harder to retrieve if needs be. So the landscape of potentially relevant documentation responsive to a specific disclosure request or subpoena has just been enormous.

Conway: Appropriate business as usual policies and processes, as well as suitable contingency plans, will remain crucial. So will keeping up with, and taking advantage of, the rapidly increasing array of technological solutions in this area. At the same time, bearing in mind the data privacy requirements, and associated sanctions, arising out of the GDPR, it will be increasingly important that an organisation's approach to risk management balances the need to collect, review and, where appropriate, disclose data as against the need to control the use of personal information.

Linsmeier: Good data management has always been important. With the need to implement GDPR, it is even more important for a company to establish clear rules and a clear system of how data is handled within a company. The GDPR requests companies know exactly which personal data is being handled and by whom. Furthermore, companies must make sure that they can meet the GDPR requirements for accessing personal data when the need for e-discovery suddenly arises. For instance, clear internet and email policies should be established which regulate, or prohibit, employees' use of the company's internet and email accounts for private purposes, and provide legally required information on the handling of emails and internet usage data in case of an internal investigation. Therefore, the more companies do to ensure a proper system is in place,

the better. However, we believe that many companies still need to invest significantly into this area.

RC: To what extent does a company's method for collecting, processing, preserving and deleting data directly impact the e-discovery process?

Beckett: These greatly impact a company's ability and the associated costs for e-discovery and, unless carefully managed, the impact will be negative. Many companies do not know the full extent of what they have and where it is. So, e-discovery becomes a knee-jerk reaction versus a measured and thought-out process. On the other hand, implementing a well-thought out e-discovery process can have very positive impacts, not only from a risk management perspective but also from a legal and compliance perspective – as the company is on the front foot in terms of any document requests or disclosure exercises. Ensuring that data is only preserved for as long as there is a business or legal reason to do so is one key component of this. Too many companies maintain systems to hold data that has no business value. Worse, there are often hidden dangers and

risks lurking within data that has no positive value to the company.

Benz: Again, from an investigative perspective, it can make all the difference whether a company is able to furnish data at short notice and provide assurances regarding its completeness. Investigations that are driven by authorities do expect cooperation and speedy responses to information requests. We have seen many cases in the recent past, often made public in settlement documents and press statements that companies have been heavily fined both for a lack of cooperation, as well as for system and control failures. And there is sometimes a very thin line between the two in that they may have the same root causes. Especially for companies that have rather disparate systems, the implementation of privacy by design and by default will be a challenging and sometimes bumpy road.

Conway: A company's method for collecting, processing and preserving data is an integral part of the e-discovery process. Whereas at one time an e-discovery exercise might have involved taking a copy of everything and then using search terms and human review to sift through it, increasingly the technology facilitates targeted collection. Further, effective information management allows for data, once collected, to be processed more efficiently in the e-discovery process, which can be critical when a crisis arises and time is of the essence. With regard to the deletion of data, large organisations tend to have quite sophisticated data retention and deletion policies, based on a combination of business, regulatory and litigation-risk considerations. Bearing in mind the amount of electronic data generated these days, that is more critical than ever, notwithstanding technological advances in respect of the storage and review of data.

Linsmeier: It is often surprising to see how hard it is to get a full overview of the data available within a company. Nobody seems to know where data is stored and who has access to it. For example, we have seen a case where after a merger the data from the merged company was presumably only stored by the individuals on hard drives. Obviously, this makes it very difficult to get these data and to assess the risks related to the business of the merged company.

RC: What are some of the typical challenges and obstacles that might arise when companies seek to coordinate e-discovery with risk planning?

Beckett: The main challenge, as with any data-related project, is making sure the processes maintain the data's completeness, integrity and accuracy, which must be maintained across a multitude of systems that usually have very frequent changes applied to them. Therefore, companies need to ensure e-discovery is considered within

any change management procedures to ensure that system changes do not increase risk. Furthermore, companies need to ensure that the processes address how users actually use data and computer systems, rather than how IT think they should use them, as the two can often be very different. There are a multitude of other challenges, for example privacy, security, access controls and authority paths. However, another major consideration is ensuring that the e-discovery system delivers results benefiting business needs and that testing is routinely performed to ensure searches are complete and accurate, otherwise the process is self-defeating.

Benz: Another aspect to consider is that there are sometimes opposing, contradictory but at the same time legitimate considerations to risk. The potential financial impact of breaches of data privacy laws has increased significantly. Fines are capped based on total turnover and so the mechanics are pretty similar to cartel fines, for example, albeit lower. So take the example of a leniency application: you are in the rat race with all others and the authorities to find the most relevant documents first but you should also be wary with regard to potential breaches of data privacy law. And you need to make sure that whoever does the processing for you has all the right systems and controls in place too. So we will likely also see a shift to and a rise in data security certifications and data security audits along the supply chain.

Conway: A key challenge is the number of different types of data that an e-discovery exercise may now need to grapple with. Traditional e-discovery tools are well set up to locate information stored on accessible systems in readily searchable format. There are, however, greater challenges associated with the interrogation of unstructured data, as well as with the integration into an e-discovery exercise of hard copy documents. Further, some data that may be crucial to a dispute or investigation may not be immediately accessible by the organisation. For instance, 'bring your own device' policies and the use of personal smartphones to communicate in the workplace

> **"There are sometimes opposing, contradictory but at the same time legitimate considerations to risk."**
>
> *Jochen Benz, Alvarez & Marsal Disputes and Investigations GmbH*

can mean that organisations can only access vitally relevant messages with the cooperation of the individual involved. Further, other potentially relevant information, GPS data, for example, might be stored on such devices. These are data sources and forms that organisations might not have needed to worry about a few years ago. Another common headache is the need to comply with data privacy rules in the context of cross-border regulatory investigations. EU data protection laws only allow personal information to be transferred outside of the EU if certain limited conditions are satisfied. This can give rise to difficult decisions when faced with a document request from, for instance, a US authority. Those decisions are only going to be made harder once the GDPR is in force.

Linsmeier: It is true that due to the new data protection rules, such breaches of the law may eventually result in large fines. On the other hand, leniency applications can save a lot of money. Given this potential conflict, we believe that it is even more advisable to have safeguards in place to be able to react quickly and within the data protection rules in case of a dawn raid.

RC: How do other stakeholders view an organisation's ability to manage data and risk, especially in a contentious circumstance?

Beckett: Stakeholder views will vary depending on the situation. Most will see it falling squarely under senior management and they will also expect this responsibility to be carried out effectively and efficiently. However, in contentious situations, stakeholders tend to take more notice as data risks underpin not only the direct case in hand but can also affect the survival of the organisation, given regulatory and reputation risk. Therefore, documentation of the process and control over how data is managed is key as nobody wants their organisation to be subject to a large regulatory fine, public criticism in a court hearing or a plunging share price due to bad management and PR, because data was not managed in line with the underlying risk.

> **"Some data that may be crucial to a dispute or investigation may not be immediately accessible by the organisation."**
>
> *Rory Conway, Linklaters LLP*

Benz: It is a risky strategy for organisations to have an unclear picture of exactly what they know and what they do not. It has backfired in a number of large-scale investigations and can make the difference between being in the driver's seat and lagging behind. Saying that, the extent to which an organisation is affected is largely dependent upon the industry within which it operates. For example, businesses within the technology, media and telecommunication (TMT) space, whose business model depends on data, are more likely to be vulnerable to issues around data, both from a commercial and a regulatory perspective, than those in manufacturing. We have certainly seen cases where transaction prices have been heavily discounted due to concerns around data. Reputation is also a key consideration. We live in a network economy which allows bad news to carry quickly, and as the issue of data protection is relevant to most people it is likely to carry even quicker which can potentially result in rapid reputational consequences for the organisations concerned.

Conway: Data security is a focus at the moment and it is highly reputationally significant for organisations. Employees, investors and counterparties all want assurances that an organisation takes this issue seriously at a senior management level. It is critical to have in place appropriate safeguards and contingency plans for when things go wrong. In a contentious circumstance, it can be vital that an organisation be seen to get on top of data issues fast.

Linsmeier: Obviously, data protection issues and their management should be a concern for senior management. Senior management can be held liable for any bad handling of the data; it is therefore in their own interest to ensure that a company manages its data properly. Such proper management is even more important in industries where sensitive personal data play a big role, for example, in the health and insurance industry. Also other stakeholders, such as the works council in Germany, will want to have a say in the way data is managed and reviewed in a company.

RC: Going forward, do you expect more companies to incorporate e-discovery into their risk management strategies? Is this issue set to increase in importance over time?

Beckett: With cyber security concerns trending and the GDPR approaching, organisations are under an increasing level of pressure already. However, it is in organisations' long term interest for e-discovery and risk management to not be overlooked. To what extent e-discovery is successfully incorporated into risk management will depend on perceived costs versus benefits. One thing to note is that these issues need not be considered in isolation and e-discovery

can be incorporated into existing demands to help provide a more comprehensive solution. Irrespective of whether there is any 'implementation', companies must consider a comprehensive e-discovery process seriously and plan for how they will approach e-discovery in a measured way. Companies will only benefit from e-discovery in the long run and should definitely consider how best they approach it.

Benz: Often, no news is good news, which means that unless a company is really hit by a case, systems and controls do not change that much. I am not saying that there is no activity but unless it is tangible, companies often go for the simplest and cheapest approach – just rewrite the policies and hope for compliance. This will likely not do the trick.

Conway: Some of the main technological advances in this area have been available for some time, but they now appear to be gaining real traction. In the context of civil litigation, the use of technology assisted review, and predictive coding in particular, has been recognised by the UK courts as an appropriate response to the proliferation of electronic data. Further, many anticipate that a working group, chaired by senior judiciary, currently reviewing the disclosure process under the Civil Procedure Rules, will recommend changes that will further encourage the use of these technologies. In the regulatory sphere, we expect a similar trend in the coming period. We have seen more and more parties, particularly in the banking sector, bring e-discovery capabilities in-house, so as to manage the associated costs and risk. This is a trend which looks set to continue as organisations face increasing pressure effectively to manage their data and to exert greater control over it.

Linsmeier: Experience shows that companies are often willing to invest into preventive measures only if they have experienced the downside of not being prepared. So compliance programmes are often ramped up only after a fine has been handed down, essentially, after it had become official that a company has not handled its risks properly. I have also heard companies saying that the implementation of the GDPR is not one of their top priorities. They do not expect the data protection authorities to become as serious and strong players as the competition authorities, at least not in the beginning. Therefore, in their opinion there still seems to be ample time to implement such rules once the first fines have been imposed. R&C