GDR INSIGHT

HANDBOOK 2021

HANDBOOK
2021

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2020
For further information please contact Natalie.Clarke@lbresearch.com

Published in the United Kingdom
by Global Data Review
Law Business Research Ltd
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.globaldatareview.com

To subscribe please contact subscriptions@globaldatareview.com

ISBN: 978-1-83862-266-4

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

Privacy

Cybersecurity

Data in practice

PREFACE

Global Data Review is delighted to publish this second edition of the *GDR Insight Handbook*.

The handbook delivers specialist intelligence and research to our readers – general counsel, government agencies and private practitioners – who must navigate the world's increasingly complex framework of legislation that a ects how businesses handle their data.

The book's comprehensive format provides in-depth analysis of the global developments in key areas of data law and their implications for multinational businesses. Experts from across Europe, the Americas and Asia consider the latest trends in privacy and cybersecurity. Attention is also given to new legislation in the United States that regulates the use of arti cial intelligence, and strict data localisation rules emerging in jurisdictions such as China. The handbook provides practical guidance on the implications for companies wishing to buy or sell datasets, and the intersection of privacy, data and antitrust. A chapter is dedicated to the use of arti cial intelligence in cross-border forensic investigations.

In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world and we are grateful for all their cooperation and insight.

The information listed is correct as at November 2020. Although every e ort has been made to ensure that all the matters of concern to readers are covered, data law is a complex and fast-changing eld of practice, and therefore speci c legal advice should always be sought. Subscribers to Global Data Review will receive regular updates on any changes to relevant laws over the coming year.

We would like to thank all those who have worked on the research and production of this publication.

Global Data Review
London
November 2020

PART 3

Data in practice

ARTIFICIAL INTELLIGENCE IN CROSS-BORDER FORENSIC INVESTIGATIONS

Frances McLeod, Britt Endemann, Bennett Arthur and Ailia Alam
Forensic Risk Alliance

Overview

In this chapter, we will be taking an in-depth look at the role of forensics in cross-border investigations, with a focus on the data issues that arise and how technology solutions, including AI and machine learning, can enhance the investigative process, help navigate competing legal regimes, and proactively monitor cybersecurity to reduce risk.

The current forensic investigatory landscape

The nature of economic crimes – and related investigations – are changing. Changes in regulation and advances in technology have caused a global shift in corruption-related schemes, from frequent, lower-value schemes to less frequent, higher-value schemes that deploy more creative approaches to avoid detection or charges.

Cross-border collaboration among authorities and global settlements are becoming increasingly common. When multiple authorities work together to reach a resolution, this reduces further prosecutions and saves time and money for authorities and the companies themselves.

To ensure an investigation complies with all relevant laws, multiple subject-matter experts are often pulled in to address various aspects of the workflow. Forensic accountants can provide crucial support to legal teams. This includes identifying, reviewing and analysing evidence across a range of legal and regulatory matters, including accounting misstatements, quantifying loss, asset misappropriation, bribery and corruption, money laundering, competition infringements, employee misconduct issues, regulatory breaches, market abuse, cybercrimes, commercial disputes and even acute investment or value decline.

Any cross-border element to an investigation brings particular challenges. Economic crime, like fraud and bribery, can create potential liability in multiple jurisdictions – and extraterritorial laws can create liability for offences that took place overseas. Similarly, when conducting an investigation, the investigative team must consider both local and international laws on data collection, migration, security and privacy. It is particularly important

to ensure the highest levels of data security by complying with laws such as the Clarifying Lawful Overseas Use of Data (CLOUD) Act, General Data Protection Regulation (GDPR), blocking statutes and banking secrecy rules.

Outline of an investigation and the case for AI

When an investigation begins, all stakeholders need to ensure each step is legally compliant. Planning is key and will reduce the need for redundant work, like re-collecting data.

Data-scoping process

Usually, the initial step of any investigation involves determining the data scope, which includes reviewing allegations; determining the period of review and geographies; understanding business units, products and custodians; and mapping the location and type of electronically stored information (eg, communications and financials). As the case progresses and new evidence comes to light, the data scope may change.

The investigation team will then request documents to gain an understanding of how information is circulated through an entity, who is responsible for key tasks, and where and how information is maintained. Document requests are amended based on the interviews and then customised based on the allegations. Initial document requests may include organisational charts and approval matrices, internal control process flows and control narratives, authorised signatories of bank accounts, and relevant corporate policies and procedures.

Document and data collection

Once the data has been mapped, the next step is to coordinate the data collection. This can involve discussions with multiple teams to gain an understanding of the type of data available, where and how the data is stored, and any potential issues regarding collection. One of the goals is to identify and collect data from each source without having to do a re-collection owing to gaps in the dataset. With advances in artificial intelligence tools, often an AI solution can be used to gain quick insights and to sample the data being collected or excluded from collections. There are multiple tools that will allow users to analyse the data on a server, laptop or other device before migrating the data into a review tool. For instance, the tools can be used to identify key terms and concepts within a dataset. If deployed early on in a case, these tools can be used to perform quality control on data excluded from collections to see if any concepts or key phrases are in fact relevant.

From data collection to document review, all relevant data privacy laws must be followed – for example, on data transfer and security. While all investigations will require processing of personal data, multi-jurisdictional investigations will often require more complex security protocols to comply with blocking statutes and country-specific data privacy and national security laws. Due diligence must be performed before the transfer of customer and employee data, including identifying personally identifiable information (PII) requiring redaction. In cross-border investigations in particular, clients may request that data remain on-site due to data security concerns, creating additional challenges for investigators. The transfer of data to non-EU countries needs particular care.

Once the documents have been collected and processed, they can be prepared for both unstructured and structured review. Unstructured review includes reviewing data like emails, chats, text messages, contracts, policies and procedures. It might also include conducting interviews. Structured review focuses on the use of data analytics to substantiate (or disprove) allegations and calculate potential damage. This process is described below.

Data privacy laws: planning and documenting process

As each step progresses, it is important to document the steps taken, from collection to document review to analysis, and to ensure regulators and stakeholders are kept up to date. When sharing findings, while the format of the final report can vary, it is important that – even within the reporting information – sensitive or private information is either anonymised or distributed in a manner that complies with local privacy laws. If technology solutions were used during the investigation, the forensic accounting team must verify that these were used in a manner that complies with local laws. Planning and documentation of the controls is essential.

Finding and deploying AI solutions for added efficiency

AI solutions can be used to complement and add efficiency to all the steps outlined above. When finding and deploying AI solutions within corporate environments, the first step is to ensure that the solutions have been properly vetted and approved by the legal and IT or data science departments. If machine learning is being used, it is important to use the proper dataset, identify potential biases and test the results.

Once the AI has been properly vetted and deployed, it is important that the team is thoroughly trained and understands the intricacies of the tool involved. This step should not prevent the use of AI solutions; in fact, proper vetting and deployment can improve the workflow, including identifying data, verifying compliance with various regulations, and protecting data privacy and PII. Multiple solutions can be used for different aspects of the review or can be overlapped, depending on the case requirements. Common uses include: using data analytics for early case assessment; using machine learning to identify relevant documents; highlighting trends across datasets; flagging items as potentially fraudulent; identifying communication patterns; and isolating individual conversation trends.

Benefits of using AI – enhanced insights, speed, etc

From the outset, AI can be used to identify and exclude irrelevant data or to isolate privileged or confidential material. It can help the investigative team to gain visibility across all data repositories, providing insight into both structured and unstructured data. Corporations, law firms and service providers can improve discovery and achieve compliance with HIPAA, GDPR and other laws by identifying and managing access to personal data. Once the data is in a centralised repository, it can be analysed quickly to reveal patterns, behaviour and other insights on a mass scale.

Another key benefit of AI technology is that it can automate repetitive tasks. This can be especially beneficial for compliance-related activities, which often involve collecting and aggregating data from multiple sources for screening. With the use of robotic process

automation (RPA), any errors can be eliminated. The process of collecting, storing and analysing data from regulatory agencies and internal datasets can be done with an increasing level of accuracy. As red flags appear, they can trigger a manual review. This means resources can be redirected to higher value tasks.[1]

Visualisation

Using data visualisation tools and dashboards that display key information in a synthesised manner can help the team identify trends or higher priority datasets for review. Investigators can filter by keywords, date, email information and other factors to collect exactly what is required. AI-powered platforms can provide insights on communication, clustering, domain and people analysis that can be used to investigate, analyse and identify relevant datasets. This can radically reduce review time and cost. For instance, mapping communications for key personnel can help determine how communications were taking place, who these personnel were speaking to the most or the least, and even whether there are gaps in the datasets. Additionally, layering smaller datasets with clustering or key phrases is useful in identifying recurrent themes; this information can then be used to develop a review plan.

At the document-review stage, active learning can be used to prioritise and categorise documents. A small team can train the active learning algorithm to identify which documents are most likely relevant or irrelevant.

Other issues: data privacy

Before or during document review, AI solutions can identify PII or sensitive information, either through pattern recognition or through algorithms that are able to identify information, such as organisations and people, within any given dataset. If the data is sensitive, these solutions can redact native files before the data leaves the collection location.

The data analysis stage can be harder if data from different jurisdictions needs to be segregated – or if there are restrictions on what data can leave a client's premises. Being able to cleanse the data and redact sensitive information natively can minimise data privacy concerns. Using an on-site analysis and processing tool can help here.

To successfully pursue and conclude an investigation, it is critical that the strategy and tools are legally compliant.[2] If the investigative team discuss their approach – including any AI tools – with the relevant enforcement or regulatory agency, this will reduce the risk of having to re-collect or process data. Although there are general steps that all investigations will follow, such as collection, processing and review, the workflows will vary depending on the facts. The team will need to understand the various issues in play from data privacy, the type of data and the corporate context; this will allow the team to create a customised approach and use the best solutions.

1 https://bis.lexisnexis.co.uk/blog/categories/data-as-a-service/big-data-shaping-risk-management.

2 https://globalinvestigationsreview.com/insight/asia-pacific-investigations-review-2020/1198063/artificial-intelligence-and-machine-learning.

Comparison with other areas of regulation

With improvements in technology and a better understanding of its capabilities, AI has proven to be a valuable investigation tool across multiple areas of regulation. For example, bribery cases have grown more complex as bad actors develop more sophisticated strategies to hide corrupt behaviour, including by using multiple third-party consultants. A primary consultant may be hired to perform high-risk services and will issue legitimate high-value invoices that raise no red flags when investigated. After a short period, the first consultant may be replaced with another, who is purportedly performing the same work, but in fact issues fraudulent invoices for corrupt purposes.

On investigations into sanctions, money-laundering and corruption involving offshore entities, all funds and relationships with those entities must be properly documented. The lack of ownership registries in offshore jurisdictions makes it difficult to detect illegitimate transactions when ownership details are hidden, especially when sophisticated schemes add additional intermediaries. In these cases, the investigation should focus on detecting the true rationale for the offshore structure and transaction flows.

Under current economic conditions, where corporate profits are falling and governments are providing business assistance, companies are faced with a unique combination of financial incentive and increased opportunity to engage in fraudulent activities. Government regulators are conscious of the growing sophistication of such schemes and are likewise taking more sophisticated steps, including implementing AI tools, to investigate them.

Such uses include real-time thematic reviews to 'increase deterrence and shorten response times when irregularities related to listed corporations are identified.'[3] AI is used in these complicated arrangements to establish links between transactions by matching data from different data sources, including unstructured data, emails, chats and transaction data. Without the use of AI, identifying a single legitimate transaction across such varied data sources would be incredibly time-consuming. The difficulty increases exponentially when high volumes of transactions are intentionally obscured between datasets.

Rules can be inputted to identify potential red flags, which could include zero, rounded amounts; duplicative or consecutive invoices; or payments over weekends or holidays. An example of a red flag may be three consecutive payments of US$49,900 being booked into the commission account without being recorded in accounts payable. Other examples could be large increases in sales and administrative costs compared to prior year, or a prepaid expense balance maintained over one year for a vendor. AI tools may be used to mitigate risk and identify bad actors and can even be used to proactively monitor and identify potential fraud, waste and abuse within an agency or firm prior to investigation.

3 https://globalinvestigationsreview.com/benchmarking/the-asia-pacific-investigations-review-2019/1174430/forensic-accounting-in-cross-border-investigations.

Using AI to achieve compliance – and resolve investigations

Many companies already use AI to manage risk and ensure legal compliance – for example, by flagging internal or external suspicious activity. If a company is investigated, part of the remediation can be agreeing to deploy AI tools to identify and assess potential fraudulent activity and circulate reporting. This might discount any penalties and minimise scrutiny of compliance programmes.[4] We look at this below in more detail.

There are multiple benefits of using AI for compliance, such as continuous global monitoring, consistency and quality of items being flagged, cost-savings, prevention, and protection of PII. Collaboration among internal teams will often help identify key issues that should be flagged, develop internal policies and workflows on AI use, and to deploy AI tools. Lawyers, IT professionals, human resources and forensic accountants can all share their expertise to continuously improve the AI solutions and develop policies that help reduce illegal activity.

Proactively monitoring cybersecurity

Real-time monitoring of cybersecurity threads and data manipulation represents one of the most important benefits of AI. The GDPR requires organisations to keep personal data secure, using 'appropriate technical or organisational measures'. This includes assessing risks posed by third-party vendors with access to an organisation's data.

In the past, the assessment of third-party risk would have been the subject of due diligence, including a review of the third party's data security policies. Today, however, cybercriminals increasingly target data vendors specifically to gain access to their contracted parties' networks. To tackle this, an AI technology known as Security Ratings Services can provide real-time monitoring of vendors' and partners' security by using algorithms and predictive analytics to turn 'millions of security data inputs into a prioritised list of security risk factors and issues of concern.'[5]

Resolving investigations

There is an increasing expectation for corporates to proactively identify legal breaches, self-report to relevant authorities and remediate in a timely fashion.[6] Although there is no single, comprehensive tool that can achieve compliance, AI and machine learning can help. As fines increase for non-compliance each year, the use of AI can help reduce false positives, reduce costs and identify human error. It can also simplify compliance programmes, provide more accurate reporting and increase efficiency.[7]

4 https://globalinvestigationsreview.com/insight/asia-pacific-investigations-review-2020/1198063/artificial-intelligence-and-machine-learning.

5 https://securityscorecard.com/blog/cybersecurity-data-breaches-statistics-on-the-rise.

6 https://globalinvestigationsreview.com/insight/asia-pacific-investigations-review-2020/1198063/artificial-intelligence-and-machine-learning.

7 https://a-teaminsight.com/three-ways-artificial-intelligence-improves-compliance/?brand=rti.

As governments and regulators embrace AI and machine learning in their respective processes, they will expect corporates, legal counsel and forensic accountants to deploy AI and machine learning in investigations and compliance programmes. Agreeing to proactively report and monitor for potential legal breaches will be taken into consideration by regulators when determining a penalty and negotiating a settlement agreement, for example, deferred prosecution agreements (DPAs).[8] The two main conditions often tied to a DPA are to continue to cooperate with the investigative entity and to strengthen the internal compliance programme. A key component of that can be deploying AI and machine learning as part of the compliance programme.[9]

Using AI in investigations or for compliance – strategies and pitfalls

While there are several reasons to use AI in a forensic investigation, it is important to consider at the outset the best AI strategies, as well as potential pitfalls.

Many of the mistakes encountered when adopting AI are due to misunderstanding what AI is and what it can do for your organisation. To begin with, AI cannot 'fix' your data. Companies that have difficulty using their data owing to poor data governance must understand that, like human analysis, AI is subject to the principle of 'garbage in, garbage out'. Effective use of AI is, therefore, contingent on thorough documentation and scoping.

The effectiveness of AI will also be limited by the volume and variety of available data. Algorithms often require large datasets for reliable predictive analytics. And to get most benefit from AI, a broad range of digital information is required.[10] It is not enough that records are digitised: each system must also store data in an intelligent, consistent manner so that it can be reliably correlated.

Organisations must also establish why they wish to use AI. If a technology is adopted only because competitors are using it, difficulties will likely ensue when teams encounter a greater level of complexity than expected or fail to invest the time required to train the algorithms.[11] It is also important that everyone is educated on how the AI technology works and is able to trust the results. For instance, if part of the team invests considerable time and effort to train an algorithm but the process is cut short, support for future projects can be undermined.

One way to counter a lack of trust in AI is to introduce it as a part of a broader strategy. In the context of a corruption investigation, for example, questionable transactions or communications encountered during the course of a traditional review can be flagged for AI analysis. Algorithms can then be set up to search for patterns involving dates, payment amounts and participants in the flagged transactions, with the results brought to the attention of reviewers for traditional analysis.

8 https://globalinvestigationsreview.com/insight/asia-pacific-investigations-review-2020/1198063/artificial-intelligence-and-machine-learning.

9 https://globalinvestigationsreview.com/benchmarking/the-asia-pacific-investigations-review-2019/1174420/deferred-prosecution-agreements-practical-considerations.

10 https://bis.lexisnexis.co.uk/blog/categories/data-as-a-service/artificial-intelligence-project..

11 Ibid. (?) https://bis.lexisnexis.co.uk/blog/categories/data-as-a-service/artificial-intelligence-project

Structuring internal teams to look at data holistically

Given the enormous benefits to be gained from the judicious use of AI, as well as the waste that can result from wrong-footed adoption and deployment, organisations would do well to develop enterprise-wide engagement for the integration of AI and machine learning. Establishing an AI centre of excellence (CoE) can be a first step to increase the pace of adoption of new technologies. An AI CoE can allow a firm to build a centralised approach to implement AI and machine learning, from ensuring proper vetting takes places to assigning responsibilities on how to implement and customise. Additionally, having a CoE will allow organisations to have a centralised repository of all solutions in play and allow for better collaboration.[12]

Closer collaboration between data experts, lawyers, forensic accountants, investigators and compliance professionals is needed to ensure proper and successful integration of AI into investigations and compliance programmes.[13] A CoE creates an internal platform for this to take place.

There are seven core principles[14] that are key for the successful establishment of a CoE:

- Secure executive sponsorship: in addition to having leadership sponsor AI programmes, organisations should establish a board-level advisory council to explore opportunities and risks associated with AI. That council should 'maintain a holistic and forward-looking view of AI, encompassing long-term as well as near-term considerations. Its overarching goal is to ensure that shareholders, customers, employees, and society overall benefit as fully as possible from the company's expanding embrace of AI.'[15]
- Set a clear vision and scope: the vision and scope should prioritise the economic value of AI solutions, identify specific use cases and how it can be used within the organisation. The vision for the CoE should complement business objectives.
- Establish a governance framework for responsible AI: the framework should provide oversight, monitor impact and consider the ethical and compliance issues that could arise from using AI and data analytics to make decisions.
- Drive innovation by engaging the right people across the business.
- Set up clear structures and relationships: clearly communicate the purpose of the CoE and understand the needs of various departments to provide relevant solutions.
- Devolve data architecture design to the CoE: this can include the integration of external data sources.
- Maintain a high profile and communicate success.[16]

12 https://bis.lexisnexis.co.uk/blog/categories/data-as-a-service/artificial-intelligence-centralised-approach.

13 https://globalinvestigationsreview.com/insight/asia-pacific-investigations-review-2020/1198063/artificial-intelligence-and-machine-learning.

14 https://bis.lexisnexis.co.uk/blog/categories/data-as-a-service/artificial-intelligence-centralised-approach'

15 Arjun Sethi. 'Why your board needs an AI council.' VentureBeat. April 2019: http://bit.ly/371vNai.

16 https://p.widencdn.net/itbgd9/UK-DaaS-AI-CoE-Checklist-A5

Creating a culture of compliance

Creating a culture of compliance takes time and starts with leadership and proper training for all individuals. Both intentional and unintentional mistakes can be prevented with more vigilance, an educated team and by deploying the right tools. A culture of compliance will organically develop by incentivising good behaviour and acknowledging and correcting mistakes, training individuals to identify anomalies, and leveraging AI technology, such as machine learning. By taking these actions, a climate where ethical behaviour is celebrated and acknowledged will be built. Dealing with investigations and trying to understand the actions that initiated the investigation retroactively is far more difficult than deploying proactive strategies to prevent fraud and corruption. This should incentivise stakeholders to continuously monitor actions, to employ real-time detection and to address dubious actions or red flags as they are identified.

Frances McLeod
Forensic Risk Alliance

Frances McLeod is a founding partner of FRA and head of its US offices. She is a former investment banker and has over 26 years of experience advising diverse clients on sanctions, anti-corruption, fraud, internal controls, asset tracing and money laundering issues.

Frances is ranked among the top 100 Women in Investigations by *Global Investigations Review*, and recognised by *Who's Who Legal* as an industry leader. She is co-head of FRA's data governance technology solutions and forensics practice, and has extensive experience in addressing complex international data transfer issues whether in regulatory investigations or cross-border litigation.

She led the FRA team responding to anti-corruption investigation data requests in all jurisdictions for Alstom in the United States, the United Kingdom, Brazil, Indonesia, Poland and Sweden, among others, which included addressing French data privacy and blocking statute issues. She is leading FRA's GDPR compliance initiative leveraging FRA's decades of experience in addressing data protection issues in cross-border litigation and investigation. An Oxford graduate, Frances was responsible for the design and implementation of claim evaluation and administration systems for the US$1.3 billion Swiss Bank and US$2.5 billion German Slave Labour Holocaust settlements. Frances speaks English, German, French, and Mandarin Chinese.

Bennett Arthur
Forensic Risk Alliance

Bennett Arthur is a global director in FRA's London office. He has over 19 years' experience in the legal field, working at law firms, eDiscovery providers and in-house legal departments. Bennett has advised clients on every stage of the Electronic Discovery Reference Model, including data management, document retention, litigation holds, collections, database design and review management. He has advised clients and counsel regarding data privacy, and Foreign Corrupt Practices Act and Office of Foreign Assets Control investigations, including data identification, analytics and alert generation, and assisted with the coordination and review of risk assessments, audits and testing.

Bennett has managed regulatory and white-collar investigations across global offices including New York, Washington, DC, Paris and London. He was involved in various landmark cases, including the long-running investigation into the manipulation of interbank interest rates such as Euribor/Libor, and assisted with high-profile trials, including the preparation and admission of evidence during trial. Bennett earned his JD from Cardozo School of Law in New York. In addition, he is a Certified Information Privacy Professional/Europe. He is fluent in French, proficient in German and conversational in Japanese.

Britt Endemann
Forensic Risk Alliance

Britt Endemann is FRA's chief technology officer and co-head of its data governance, technology solutions and forensics practice, as well as a partner based in FRA's London and Washington, DC offices. She has extensive experience assisting companies with advanced technology-driven solutions and AI technologies to address corruption risks and financial crimes; respond to regulatory inquiries in multi-jurisdictional matters; navigate Office of Foreign Assets Control compliance reviews; and conduct rigorous internal investigations.

Her expertise includes analysing complex datasets, dealing with privacy issues, identifying and collecting financial data sources, managing on-site technology solutions for clean rooms, exporting data, overseeing international data transfer, presenting data architecture to authorities; and working to assist clients in the defence sector.

Britt travels the globe advising companies and C-suite management – particularly in the banking, financial services, telecommunications and manufacturing sectors – on issues relating to risk mitigation and developing innovative technology solutions and defensible protocols related to cross-border investigations in Europe, the United States, Asia and the Middle East. Because of her extensive international experience. Britt is uniquely positioned to understand clients' infrastructure, data privacy parameters and business policy burdens.

Ailia Alam
Forensic Risk Alliance

Ailia Alam is a data governance, technology solutions and forensics manager in FRA's Washington, DC office. She specialises in strategic planning for legal technology project management and acts as a liaison to law firms and government agencies to clarify issues, refine ideas and give shape to solutions. Ailia uses analytical and technical skills to identify risk areas and find creative solutions to clients' data governance challenges. She focuses her practice on litigation and investigations, and has particular experience in antitrust issues, contract disputes and Freedom of Information Act requests for commercial and federal clients. She has managed cases from data identification to production, from conducting custodian interviews to assisting with deposition prep. She earned a bachelor's degree in international relations and is fluent in Urdu.

FRA is an international consultancy specialising in regulatory cross-border, multi-jurisdictional investigations, compliance and litigation. We are expert providers of forensic accounting services, eDiscovery and data forensics solutions, with offices in the US, the UK, France, Canada and Switzerland. With nearly 20 years of experience, we are known for delivering bespoke solutions around the world for complex and highly sensitive matters and are experts in analysing large, complex transactional datasets. In an investigation where the data cannot be moved out of the host country we use our Mobile Solution.

We also offer jurisdiction-specific consulting services re data protection, blocking statutes, state secrecy and cyber laws. Our Mobile Solution handles the whole EDRM Cycle – collection, process, filtering, review and production – and can be installed quickly, anywhere in the world. It can be integrated into a client's infrastructure or we can host at a location determined by the client, providing options for accessibility (air-gapped, restricted or remote) rendering access from an external network impossible, ensuring cyber risk is mitigated.

We have state-of-the-art data centres around the world that meet or exceed Tier III standards in the North America and Tier III standards in the UK, Europe and Canada. Our security is of the highest level to protect the assets of our clients and our own organisation. We maintain an advanced, multi-layered security programme, which includes continuous monitoring, annual third-party penetration testing and vulnerability scans as well as maintaining industry security certifications. Unlike traditional accounting firms we do not perform audit or other consulting work, so we typically have no internal conflicts.

Audrey House
16–20 Ely Place
London, EC1N 6SN
United Kingdom
Tel: +44 20 7831 9110

2550 M Street, NW
Washington, DC 20037
United States
Tel: +1 202 627 6580

44, avenue George V
75008 Paris
France
Tel: +33 1 74 88 05 41

www.forensicrisk.com

Frances McLeod
fmcleod@forensicrisk.com

Britt Endemann
bendemann@forensicrisk.com

Bennett Arthur
barthur@forensicrisk.com

Ailia Alam
aalam@forensicrisk.com

The GDR Insight Handbook delivers specialist intelligence and research to our readers – general counsel, government agencies and private practitioners – who must navigate the world's increasingly complex framework of data legislation. In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world.

The book's comprehensive format provides in-depth analysis of the developments in key areas of data law. Experts from across Europe, the Americas and Asia consider the latest trends in privacy and cybersecurity, providing practical guidance on the implications for companies wishing to buy or sell data sets, and the intersection of privacy, data and antitrust.

Visit globaldatareview.com
Follow @GDR_alerts on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-266-4