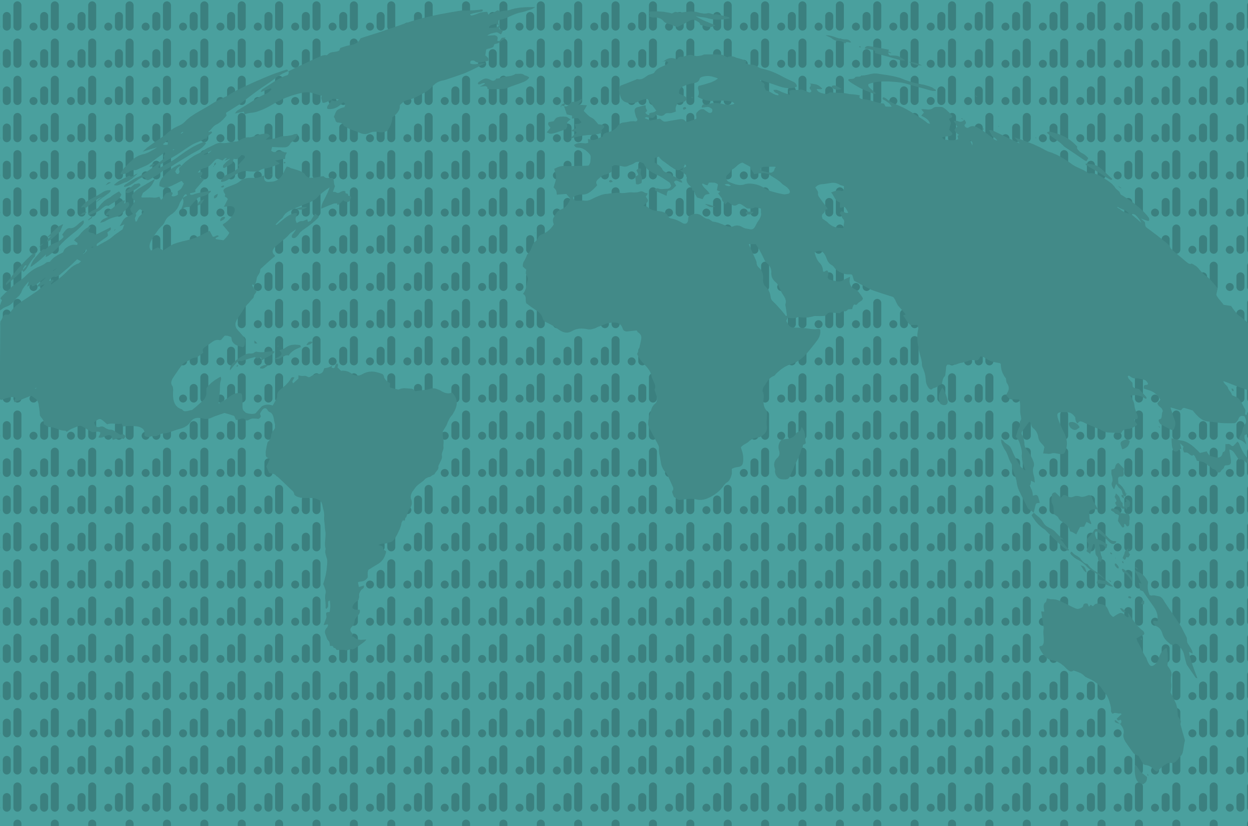
INSIGHT HANDBOOK
2022



GDR Insight Handbook 2022

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

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer–client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at September 2021, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to Law Business Research, at the address above. Enquiries concerning editorial content should be directed to the editor – tom.webb@globaldatareview.com.

ISBN: 978-1-83862-591-7

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

Contents

PART 1: PRIVACY AND CYBERSECURITY LAW

PART 2: DATA IN PRACTICE

Preface

Global Data Review is delighted to publish this third 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 affects 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 US that regulates the use of artificial intelligence, strict data localisation rules emerging in various jurisdictions, and a new data protection framework in China. The handbook provides practical guidance on the implications for companies wishing to buy or sell data sets, and the intersection of privacy, data and antitrust. A chapter is dedicated to assessing how companies should respond to the GDPR enforcement regime.

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 September 2021. Although every effort has been made to ensure that all the matters of concern to readers are covered, data law is a complex and fast-changing field of practice, and therefore specific 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
September 2021

Part 2

Data in practice

Data Governance in Forensic Investigations: Data Collections, Current Challenges and a Proactive Approach to Better Data Management

Frances McLeod, Harsh Sutaria, Simon Taylor and Alejandro Gomez Igbo
Forensic Risk Alliance

Overview

Data that is improperly governed can cause major business problems for organisations. Yet, when managed appropriately, it is an important driver of business strategy and innovation. In this chapter, we will be taking an in-depth look at the role of data governance within forensic investigations, and how taking a proactive and organised approach to managing data is of utmost importance in today's data-driven world.

The first step of the data investigation workflow starts with data collections, which, as we have seen in 2021, has become a challenge in itself. With seemingly limitless new types of business applications, forensic and mobile collections and remote capabilities, the current landscape of data collections is constantly changing.

Data collections

The initial step of any investigation usually involves determining the data scope, which includes reviewing allegations; determining the period of review and jurisdictions; understanding business units, products and, most importantly, 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.

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. It is also key to find the right balance between capturing enough data against costs and efforts being reasonable and proportionate. There are multiple tools that allow users to analyse the data on a server, laptop or other device before migrating the data into a review tool. For instance, some 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.

Finding efficient ways to gather data using such modern tools, to hone down the data to the minimum reasonably needed to fulfil the objectives of the investigation, is extremely valuable. There is now so much data existing, that simply collecting the data is just not enough – this approach leaves the review team with an task of reviewing enormous amounts of data and can lead to huge processing and storage costs and increased data governance risks. Therefore, it is crucial that we understand the demands of the investigation and what would be most useful in a specific case.

Data collections: current landscape

The current landscape of data collections is constantly evolving and presents an ever-changing set of challenges for organisations looking to manage their data effectively. Companies must deal with larger volumes of data; the efficient collection of structured and unstructured data; and the introduction of new data-generating business applications. These data complexities are compounded by a labyrinth of compliance requirements and regulations (often multi-jurisdictional) that dictate how and what information is processed, stored and protected, and the conditions upon which data may be transferred to the place where it is needed. This landscape poses serious risks that, together with the current challenges of remote versus on-site collections, require careful management.

Traditional approaches to eDiscovery collections involve experts arriving on-site to collect data in person from a custodian's computer, mobile device or similar. While preferred for some high-security cases, for most companies, this approach can involve collectors travelling across country or globally to perform data collections, and therefore is not a time- or cost-effective solution. However, with many restrictions now in place for on-site collections, teams have had to find new innovative tools to do the same job.

With the covid-19 pandemic and the need for more cost-effective solutions, remote collections have become the norm. Yet, while they provide a helpful alternative to traditional methods, they do also bring with them their own challenges. It is important to consider that the correct tools are not always available to allow for remote data collections; new technologies may not suit remote collections; and some technologies have their own collection tool and may not be compatible with industry standard tools.

New types of data

Over the past two decades, new types of messaging platforms and apps have emerged as key tools for collaboration and communication in corporate and personal settings. Some of these providers include WhatsApp, Microsoft Teams, Slack and Zoom. The latter three have especially grown in popularity and in users after the onset of covid-19. Although it is easier to track the number of users for these platforms, the nature, volume and content of the messages the users may have sent are significantly harder to track. The volume and processing of this new type of data pose new challenges for data governance and compliance professionals. As their adoption accelerates in the aforementioned settings, more legal questions arise on how to preserve and capture their data.

Zoom is a pertinent case study for the current data governance climate regarding new types of data. The number of Zoom's active users increased 151 per cent year-over-year in March, breaking its own records. On 31 March 2020, it had 4.84 million daily user volumes within the United States, surpassing Microsoft Teams' 1.56 million users.[1] It is evident from these numbers that Zoom usage has increased exponentially as companies have had to shift to a new way of working. During this rise, thousands of Zoom meeting recordings were exposed online in April 2020.[2] Other than this increased volume of data and data privacy concerns, there is the issue of extracting data of non-recorded Zoom meetings as the information detained is not as expansive as recorded meetings, for example. The information contained on the 'Meetings' tab for non-recorded Zoom meetings includes only the date, time, meeting ID and title of the meeting. This tab also allows the individual user to delete a meeting from their

[1] https://glginsights.com/articles/zoom-microsoft-teams-and-slack-have-exploded-due-to-the-covid-19-pandemic-can-they-hold-onto-this-growth/.

[2] https://thehill.com/policy/cybersecurity/491106-thousands-of-zoom-meeting-recordings-exposed-online-report.

history.[3] Companies therefore need to be more cognisant of the time for which Zoom is being kept as a standard business practice and the way this information is being maintained, saved and collected to ensure they can comply with discovery obligations later. From an eDiscovery perspective, Zoom recordings create an expensive proposition as video and audio files typically are very large file sizes, making hosting this data expensive. This data is further complicated by issues revolving around enabling file or screen sharing during meetings and the logs of what was shared and with whom. Additionally, if a user does not opt for a transcript of the meeting, the video and audio files require significant customisation to be searchable.

The challenges of communication and collaboration platforms are exemplified, respectively, by the widespread use of the aforementioned messaging systems WhatsApp and Slack, as well as Microsoft Teams and Zoom. WhatsApp has introduced disappearing messages in an attempt to protect user privacy, a feature that has also been put in place by Telegram Messenger. However, this feature implies that some data could be missing from investigations when a device is obtained for data extraction, and correspondence or shared files could even be deliberately concealed as a result.

Much like Microsoft Teams and Zoom, Slack is reporting a significant spike in usage recently. With more employees leveraging cloud collaboration platforms during the covid-19 crisis, the need to acquire Slack data for investigative or discovery purposes will undoubtedly increase. Slack data is also hard to review, unstructured and complicated. Each message log contains information on text, attachments, response types, edits and deletions, and more. In addition to messages, Slack's integrations allow it to operate as a centralised hub for many types of information.[4] A Slack integration can create a notification every time a spreadsheet is updated, for example, or allow you to make payroll and finance decisions directly from the platform.

Ultimately, there is need for human-machine collaboration as new types of data emerge – data governance is becoming more difficult due to the nature of the new content, as well as the sheer volume. In collaborative channels such as Zoom and Slack, the data is all cloud-hosted, so with the right software licence, the data can be extracted and collected. Reviewing it, however, becomes much harder because you need to process it in distinct ways with specialist software. This goes hand in hand with compliance risks associated with these messaging apps, as it is rare to have

[3] https://www.jdsupra.com/legalnews/ediscovery-considerations-with-business-18656/.

[4] https://www.logikcull.com/slack/understanding-slack-for-lawyers.

copies of conversations being downloaded to a company server even though business is conducted on these channels (you often need physical access to the device.) Thus, as the data is increasingly unstructured and the volume has skyrocketed across the new platforms, data collection and governance remains a sensitive and complicated, but still essential ordeal in the realm of eDiscovery.

Challenges in data governance

Organisational communication habits have also changed in the past few years, and further accelerated as the covid-19 pandemic gave many companies the final push towards fully remote working. This has led to collaboration and communication platforms being used more frequently than ever before. Data volumes coming from these types of platforms are considerable and create an additional layer of complexity when managing data and performing data collections in response to an investigation.

Data accessibility is another a challenge to consider, since companies with decentralised operations may lack an efficient way to consolidate their data in a unified system.[5] Not long ago, the process of imaging a computer captured almost all data one needed for a successful data collection. However, the landscape of data collection today has evolved exponentially with more to consider than simply collecting emails and loose files. This can be explained by the fact that previously emails and files were stored locally; however, now they can also be kept in cloud storage and network shares. Some data cannot be accessed remotely due to data structure and storage methods.[6] Securely encrypted devices require decryption keys, which are not always accessible, while data in the form of physical files could be secured in a safe. Moreover, obtaining data could be dependent on the speed of the available internet connection. Notably, numerous tools deployed for data collections in past were designed to support on-site collections; tools supporting remote collections must be developed further and become more widespread.

Organisations put security measures in place to protect their data, including two-factor authentication and blocking access to USB ports. Therefore, remote data collection is often not possible without preliminary discussions with the data custodian on how remote collection can be effectively accommodated.[7] Due to increased levels of security on modern devices, whereby usernames and passwords need to be

[5] https://hbr.org/1990/07/the-centrally-decentralized-is-organization.

[6] https://www.legility.com/insights/safer-ediscovery-data-collection-practice-during-coronavirus.

[7] id.

obtained either from the custodian or from the company's IT team, the custodian may be required to provide support as they are in physical custody of the device. Meanwhile, it is not guaranteed that all data custodians will choose to assist with their data collection, either due to technical skills or due to potential time delays of the process. [8] It would therefore be beneficial for companies to document their attempt to obtain access to custodian devices. This would allow them to present evidence to the appropriate regulators, which, in turn, would demonstrate that all legal measures were exhausted in the case that there was no assistance from a custodian or if their request was denied.[9]

Moreover, it is also important to consider the potential limitations created by companies' security policies that apply to their devices. In the current context, we may find that data is dispersed across different locations and devices as people are increasingly working remotely.[10] Custodians operating outside of their regular workspace may fail to use secure internet connections or may be using their own devices, which could lead to privacy issues when attempting to access such devices for investigations.[11] For instance, if a device is located at a custodian's home, employment laws may become an obstacle, whereas this would pose fewer issues if the devices were located in the company's office.

There has been a considerable uptake in remote data collections in 2021, and while it started as an innovative solution to a worldwide pandemic, the trend is very likely to continue. New approaches must be taken with regard to data collections as the impact of the pandemic on forensic investigations will be long-lasting due to the nature of the work. Companies can save time, money and personnel resources when collecting digital data remotely, while observing any travel restrictions and minimising levels of human interaction.[12] Nevertheless, the sheer volume and various types of data involved play a significant role in the challenges faced. An increasing number of organisations are leveraging the use of cloud and network storage, alongside remote

[8] id.

[9] https://www.nortonrosefulbright.com/en/knowledge/publications/e6fc7d4b/conducting-investigations-remotely-five-key-points-to-navigate-the-new-normal.

[10] https://aceds.org/solving-for-the-top-3-challenges-of-conducting-remote-internal-investigations/.

[11] id.

[12] See footnote 6.

data collection and mobile collections. With these changes, and the increase in new types of messaging platforms to meet the needs of remote corporate life, there is a pressing need for new data governance measures to be taken.

Data privacy considerations

As the landscape of data collections continues to change, it remains essential that all data privacy laws are followed, and organisations are able to manage their compliance and other regulations that dictate how information is stored, protected and transferred. Due diligence is particularly important when it comes to the collection and transfer of employee and customer data, as this data often includes personally identifiable information that requires redaction. While all investigations will require the collection and processing of such personal data, multi-jurisdictional investigations will frequently require enhanced security protocols to remain in compliance with data privacy and security laws specific to certain countries. Furthermore, extra steps must be taken in multi-jurisdictional investigations where data export licences must be acquired from government authorities to simply move the data out of the local jurisdiction. This presents additional time and costs to an already-lengthy process and must be factored into the duration of the investigation.

Investigations involving EU data need particular care, as they may be subject to unique privacy protections. Beyond the need to adhere to country-specific privacy laws, clients may also request that data remain on-site out of concern for data security, creating additional challenges for investigators when collecting and processing data. By complying with the Clarifying Lawful Overseas Use of Data (CLOUD) Act and the General Data Protection Regulation (GDPR), it becomes possible to ensure the highest level of data security throughout the data collection and analysis process.

With investigations dealing with new types of data, it becomes imperative that regulators are aware of these innovations and that the steps taken in collection and analysis are documented. It is important that sensitive and private information from reporting information is redacted or collected and distributed in compliance with local privacy laws. Furthermore, if technology solutions were used during collection or any other aspect of the investigation, the forensic accounting team must ensure that these technology solutions were used in compliance with all local laws.

Difficulties may arise when there are restrictions on what data can leave specified locations or when data from different jurisdictions need to be separated, but addressing these complications during collection can help minimise data privacy concerns. By using an on-site analysis and processing tool, it becomes possible to cleanse data and redact sensitive information natively.

The ability of a team to utilise tools in a legally compliant manner is vital to the successful pursuit and conclusion of any investigation. By discussing approaches and tools with regulatory agencies, investigators can collect and process data in a legally compliant manner and avoid having to re-collect or re-process data. The issue of data privacy in collections is one that does not only impact investigators, but also affects individuals and organisations. Individuals care more about their privacy now than ever before, and the rise in Data Subject Access Requests (DSARs) highlights the importance of data privacy for organisations. DSARs allow individuals to request access to all the information an organisation holds on them, within 30 days of the request being made. As people become more data aware and conscious of who is using their data, and for what purpose, it is natural that the amount of DSARs increases. The Information Commissioner's Office finds that data protection complaints from the British public nearly doubled from May 2017 to May 2018, going from 21,000 to 41,000 complaints, with nearly 40 per cent of those relating to DSARs.[13]

For organisations, this means there is now the need to be able to pull large amounts of data at a moment's notice in a secure and legally sound fashion. Organisations often have difficulty pulling such data because there is no process in place for such collections and the data is held in multiple jurisdictions. Due to the 30-day turnover period for DSAR requests, it is now important for organisations to be able to find and collect necessary personal data in a quick and accurate manner while keeping the process secure and legally compliant, something many organisations are currently not prepared for. The far-reaching and time-sensitive nature of the data requested often leads to DSAR responses that are imprecise, incomplete and that accidentally release confidential data. Collecting all of the personal data of an individual, and sending them said information within a 30-day time frame, is a process that is fraught with risk at every stage, yet failure to properly comply with DSARs can lead to large fines from relevant regulators and authorities.

A proactive approach to data governance

A lack of efficient data governance and management is a critical problem that many organisations may not even be aware they face. The challenges identified above, which many companies face, have a simple solution: a proactive approach to data governance.

[13] https://trinityflac.files.wordpress.com/2020/09/flac-technology-and-access-to-justice.pdf.

A centralised data governance system tailored to numerous data sources, in which staff understand the different data repositories and the nature of what type of data is stored, is one of the most critical steps to take when implementing a proactive approach to data governance. In a centralised data repository, data insights and analysis are used to identify relevant data sets faster, data is more easily searchable, and risk and fraud can be mitigated at an earlier stage by setting up pertinent rules and processes. Organisations can also invest in tools that perform indexing on their data repository, further improving search ability. Ultimately, a proactive data governance approach will drive business strategy and innovation and assist in investigations. Results from investigations will benefit improved data analysis, early case insights and the opportunity to pinpoint inefficiencies in the process and improve the investigative strategy.[14]

A proactive approach is required for successful data management and starts with ensuring that your business goals align with overall strategy. It is crucial to follow a comprehensive system where data mining, treating (processing) and categorisation are standardised across the board. To create this system, it is crucial to design an optimal workflow, to map out processes, to utilise subject matter experts and to procure appropriate infrastructure support and adequate budget resources. All this must be done while also preserving a strategy for change and stakeholder management. Successful adoption of a robust data management process relies on a risk-averse and proactive team culture that remains flexible to adapt at all levels and true to what makes your firm unique.

Define the problem and find the optimal application

Defining the problem is the first task in every problem-solving procedure and this is especially true when optimising your data governance approach. Issue diagnosis will allow you to focus on resolving the root of the problems in your system instead of finding a remedy for its symptoms. This usually is a case of asking the right questions. For example, where does the problem lie when it comes to metadata in your organisation? Do you need to discover a way to store and analyse your ever-increasing volume of metadata or are you lacking governance in how metadata is collected and documented? Could you optimise your metadata collection by improving your definition of metadata or data documentation process?

[14] http://epubs.iltanet.org/i/1188906-ig19/63?_ga=2.218152153.1579376862.1575491724-1329253801.1575491724&utm_content=108604944&utm_medium=social&utm_source=linkedin&hss_channel=lcp-33292289.

Organisational culture – adapt a scientific mindset

Adopting and advancing data management techniques and processes requires an organisation and its people to embrace a more scientific approach. The wider team must become comfortable with the trial-and-error method and be willing to learn from failures, redouble testing to validate the feasibility of the current elements while also introducing new patterns, behaviours or variables to examine the system as a whole. It is crucial to build a continuous feedback loop into your data management process at each stage. Inputs, outputs and outcomes must be examined for anomalies lest corrupt or inaccurate data render data unfit for purpose. Continuous observation of your data allows you to fix issues that may arise, mitigate risk and enhance aspects of your methodology that are working well.

This mental shift in your organisational culture must not only occur in upper management, but in all areas of the firm, including the board and functions such as risk and compliance, HR, and noticeably IT and finance. These functions will play a part in the change or adoption of a data management strategy and will need to be well informed and prepared to add to the conversation. For example, a finance team will have a keen interest in the cost of the solution. The hardware and software costs should be part of the conversation from day one. Consider performance, scalability, and maintenance, among other costs.

Identify the right technologies – hardware and software considerations

Just as every scientist must invest in equipment, your data management team needs to invest in the proper technology and applications to support processes for collection, processing and analysis, which is scalable and adaptable to unstructured and structured data. New hardware tools, particularly graphics processing units, provide powerful parallel processing and enable users to apply multiple processes to a single unit of data simultaneously. Likewise, data management software – of which varying solutions are currently available in the market – underpin the success of data management workflows. Centralising data using these software solutions can provide robust protection against fraud and helps to preserve consistency and integrity in data. However, this is difficult to achieve considering many firms are juggling different data sources, geographic locations and incongruent system integration. To combat this, some tools layered over the organisation's infrastructure pull data from various sources to allow for standardisation, indexing, searching and preservation in the central data repository.

Process optimisation – using AI

When the methodology is mapped out and you have a sense of your firm's preparedness for the changes, it is time to determine the optimal application for your solution in your organisation. This can begin with simplifying the process, making the process 'smarter' and increasing efficiency. This can be achieved using AI. For example, AI has been used in data analysis to examine dozens of data elements to eliminate high numbers of false positives from these rules-based compliance systems. Similarly, internal systems can be improved by learning more about the patterns involved in day-to-day risk mitigation and data management with AI. AI can increase the efficiency and lower the costs of compliance by automating processes that previously required manual work. By automating processes using AI to increase efficiency, the resources spent on key workflows and the overall time spent on deliverables can both reduce.

Human expertise

Human expertise and knowledge are the primary architects of value for every organisation. To truly benefit from a data-driven governance approach and maximise this value, organisations must invest in the expertise of their team. Having multiple data governance experts working across the processes and workflows eliminates errors and allows stakeholders to find, understand and trust the validity of the data.

It is crucial to note that any technology used is only as useful as the people and processes that support it. A good data governance solution will leverage human expertise to provide security, quality control and analysis. This human expertise drives innovation and prepares data for consumption to ultimately optimise a data governance landscape within an organisation.

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 monitor actions continuously, to employ real-time detection and to address dubious actions or red flags as they are identified.

Conclusion

While organisations have responded to external influences such as covid and GDPR, and have adapted data collections accordingly, there are additional steps that can be taken. A holistic and flexible approach to data governance is vital. New data types will continue to evolve, and it is better for organisations to get a grasp of how that data works and how it is stored, as this will likely be needed going forwards. While remote collections do offer certain benefits, such as saving time and money, reducing the workload of employees, and avoiding any potential risks during the covid-19 pandemic, they still come at a cost that can be reduced if a proactive approach to data management is taken. Proactive data management should be implemented in organisational culture. Any company can be subject to an investigation or DSAR, and as more individuals are being empowered to take control of their personal data, it is vital that companies organise the data that they hold on individuals.

The authors would like to acknowledge Sadiya Ossoble (associate), Valeria Filippova (associate), Ilke Arkan (analyst), and Benjamin Bizot (analyst) for their contributions to this chapter.

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. 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. An Oxford graduate, Frances speaks English, German, French, and Mandarin Chinese.

HARSH SUTARIA

Forensic Risk Alliance

Harsh Sutaria is FRA's chief innovation officer. Harsh drives the firm's innovation initiative, working with emerging technologies, engaging the start-up community, and driving the transformation of next generation technologies into practical solutions. He implements foundational platforms and programmes, orchestrating all of our businesses to innovate on a global scale. Harsh focuses to wholly understand technologies and to identify strategies that embrace market opportunities created by the constantly evolving technological, regulatory, and business landscapes. Harsh is an expert in disruptive & business model innovation, ecosystem strategy and development, and emerging technologies. He is the firm's leader on the critical components of innovation, including strategy, new-product development, business-model creation, open innovation, culture change, and research and development. He has extensive experience delivering measurable value for companies in product development, go-to market, and customer experience strategy.

Harsh is fluent in Hindi and Gujarati and holds a Bachelor's in Management Information Systems.

SIMON TAYLOR

Forensic Risk Alliance

Simon Taylor, CIPP/E, CIPM is a partner and certified data privacy expert in FRA's forensic accounting team with 20 years' experience in investigations, financial crime and regulatory enquiries. He advises clients on the design, implementation and testing of compliance programmes across a range of industries and sectors, corporate governance and data privacy issues. Simon's areas of expertise include money laundering, bribery, corruption, sanctions abuse, tax evasion and corporate fraud. He works with both external and in-house counsel to corporations and financial institutions, bringing a multi-disciplinary approach to resolving complex matters. In addition to his investigatory expertise, Simon advises companies on the structure, design and testing of their compliance programmes, helping them rise to best-in-class standards across key jurisdictions. His international experience extends to numerous geographies – including the UK, US, Switzerland, France, the Nordic region, Eastern Europe, Russia, India and China – and a variety of sectors. Simon is a dual qualified lawyer (solicitor and barrister) and an editor of the leading academic textbook on the UK Proceeds of Crime Act 2002 – *Mitchell, Taylor and Talbot on Confiscation and the Proceeds of Crime* published by Sweet & Maxwell – in which he writes the 'Investigations' chapter.

ALEJANDRO GOMEZ IGBO

Forensic Risk Alliance

Alejandro Gomez-Igbo is a director in FRA's data governance, technology solutions and forensics team, based in London. Alejandro's unique experience traverses both structured and unstructured data, providing holistic strategic perspective on the collection, analysis and reporting of large quantities of multiple types of data, while leveraging the latest advanced technology offerings.

Alejandro specialises in complex data issues, primarily involving interviewing and advising clients to understand IT business processes and identifying responsive data for disclosure exercises. He has been a key player in high-profile cases and has supported and managed cases of varying sizes involving the biggest UK and US regulatory bodies.

Alejandro completed university with a BSc Honours degree in Business Management and Information Systems, and is fluent in Spanish and Italian.

FRA

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 of interest.

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

www.forensicrisk.com

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

Frances McLeod
fmcleod@forensicrisk.com

Harsh Sutaria
hsutaria@forensicrisk.com

Simon Taylor
staylor@forensicrisk.com

Alejandro Gomez Igbo
agomezigbo@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

ISBN 978-1-83862-591-7