GDR INSIGHT

HANDBOOK 2020

HANDBOOK
2020

Reproduced with permission from Law Business Research Ltd
This article was first published in November 2019
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: 978-1-83862-235-0

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 inaugural 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 United States that regulates the use of artificial 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 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 October 2019. 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
October 2019

PART 3

Data in practice

RESPONDING TO THE GDPR ENFORCEMENT REGIME

Frances McLeod and Simon Taylor
Forensic Risk Alliance

Overview of the data landscape

In 2017, an IBM study concluded that 90 per cent of global data had been created in the previous two years.[1] By 2020, it is estimated that 1.7 megabytes of data will be created, and then stored, every second for every single person on earth. Personal data of all types originating from human behaviour is being captured, stored and put to commercial use at a staggeringly accelerating pace.

The recent examples of the use of data sets containing tens of millions of personal images, scraped from social media platforms or elsewhere, and then used to train advanced facial recognition software for use in a wide range of public and private surveillance applications, such as for retailers, event organisers, border security, schools and by the Chinese government in their response to the Hong Kong protests, and their mass surveillance and detention of ethnic groups in Xinjiang, are important cases in point. With the advent of always connected devices and the internet of things (IOT), this acceleration will continue to be fuelled. It has, for example, recently emerged from a study by Northeastern University and Imperial College London that smart TVs and streaming 'dongles' were transmitting data such as location and IP address to Netflix, Google, Facebook and third-party advertisers even when the devices were not in use.[2] It is abundantly clear that the possibilities for assembling vast data sets containing personal data and, importantly, combining these data sets in novel and imaginative ways to create immense commercial value, is in all practical senses limitless. However, with these new superpowers sitting in the hands of those who acquire, control, assemble and manipulate personal data come a host of challenges, ranging from cyber attacks and data misuse claims to increased regulatory powers and enforcement penalties.

1 IBM Marketing Cloud study.

2 *The Financial Times*, 18 September 2019.

In addition, there is now the real risk of company executives becoming exposed to criminal charges and intense public scrutiny through numerous public enquiries on data privacy, such as the US Senate hearings for Facebook and the UK Parliamentary Select Committee inquiries into Cambridge Analytica.

Emblematic of this new landscape and approach is the General Data Protection Regulation (GDPR) issued by the European Union, which came into effect in May 2018. (See 'European Union: Privacy' in this book.) The GDPR represented a significant change in the protections afforded to personal data and ramped up the available penalties when those protections are violated. By way of example, pre-GDPR fines in the United Kingdom were capped at £500,000. Criminal sanctions are now available for corporations and for senior executives and managers who can be held criminally responsible for neglect in data misuse. As a result, companies and their executives need to take notice and consider the consequences of not making the protection of personal data a priority.

In this chapter, we consider how companies should respond, given the rapidly changing background described above, when allegations are made of personal data being misused or improperly obtained, or when personal data has been lost as a result of cyber attacks or other compromises. With growing public and political will supporting aggressive regulatory and criminal enforcement, it is important to recognise the value in conducting forensic investigations both to provide affirmative evidence that any breach or misuse is anomalous and non-systemic, and to set foundations stones for remediation plans and compliance programmes.

Fines and penalties under the GDPR

The GDPR has introduced significantly higher fines based on a percentage of an organisation's global revenue. For multinationals, this could mean having to pay billions of pounds. One of the difficulties in determining the level of penalty is that, unlike other regulatory regimes, the starting point is not defined in terms of gain or damages.

There are two tiers of administrative fines that can be levied as penalties for GDPR non-compliance:

- up to €10 million, or 2 per cent of annual global turnover – whichever is greater; or
- up to €20 million, or 4 per cent of annual global turnover – whichever is greater.

The lower-tier fines typically apply to violations of data controllers' and processor's general obligations, while the higher tier generally applies to violations of data subjects' rights. Fines are discretionary rather than mandatory. Under the GDPR, fines must be imposed case by case and should be 'effective, proportionate and dissuasive'.

Recent examples of increased regulator and public scrutiny

In recent months, we have seen the impact of the GDPR and the intent of the regulators in the data protection space, with headline-grabbing fines issued to multinational organisations for GDPR breaches. These fines underline how seriously the regulators are taking these breaches of data protection legislation.

Some of these cases are still subject to appeal and the final penalties may be considerably different. However, whatever the ultimate level of fines that these organisations incur, it is clear there has been a step change in the quantum of penalties. The following examples are some of the first to hit the headlines since the introduction of the GDPR.

United Kingdom: the Information Commissioner's Office (ICO)

The ICO issued Notices of Intent in August 2019 in two cases: *British Airways* and *Marriott International*. See 'England & Wales: Cybersecurity, Post-GDPR' in this book.

Sweden: the Swedish Data Protection Authority

In August 2019, a school in northern Sweden was fined 200,000 Swedish Krona (£16,800) for conducting a pilot programme using facial recognition to keep track of 22 students' attendance. While the school had asked parents and students for consent, the school failed to conduct an impact assessment and the way in which consent was obtained violated the GDPR.

France: Commission nationale de l'informatique et des libertés (CNIL)

Teemo

Teemo, a data ad tech start-up headquartered in Paris, was one of the first to be admonished under GDPR for gathering and processing data without informed consent. In a good faith effort to comply, the company took roughly two months to implement everything the CNIL was asking for and managed to avoid a fine.

Google

Google was issued a €50 million fine in by CNIL for violations of general data protection regulations related to a 'lack of transparency, inadequate information and lack of valid consent regarding ads personalisation'. CNIL also found that Google had failed to provide adequate notice to users about data being used to personalise advertising.

Investigatory response to the altered landscape

So, what happens if a company encounters an allegation that it has misused or unlawfully obtained data or when there is a data breach? What is an appropriate response?

The necessary actions in response to a data breach extend far beyond the immediate technical issues of how the breach occurred or how the data was misused. As with other situations involving allegations of corporate wrongdoing, it is important to establish a clear narrative through a thorough forensic investigation of the events to plan effective remediation measures and inform management responses and dealings with staff, customers, the public, other stakeholders and, of course, the regulator.

In the ICO's guidance, there is a wide range of factors that the regulator will take into account when assessing and mitigating any penalties, and these are a good starting pointing in setting out the investigation plan. These factors include, but are not limited to, the following:

- the nature and seriousness of the breach or potential breach (including, for example, whether any critical national infrastructure or service is involved);
- the gravity and duration of a breach or potential breach;
- where relevant, the categories of personal data affected (including whether any special categories of personal data are involved) and the level of any privacy intrusion;
- the intentional or negligent character of the failure;
- any action taken by the controller or processor to mitigate the damage or distress suffered by data subjects;
- the number of individuals affected, the extent of any exposure to physical, financial or psychological harm, and, where it is an issue, the degree of intrusion into their privacy;
- whether the issue raises new or repeated issues or concerns that technological security measures are not protecting personal data;
- any relevant previous failures by the controller or processor, including whether the organisation or individual involved is representative of a sector or group, raising the possibility of similar issues arising again across that group or sector if not addressed;
- the manner in which the infringement became known to the commissioner, including whether, and if so to what extent, the controller or processor notified the commissioner of the failure and the cost of measures to mitigate any risk, issue or harm;
- the extent to which the controller or processor has complied with previous enforcement notices or penalty notices;
- adherence to approved codes of conduct or certification mechanisms and the degree of cooperation with the commissioner to remedy the failure and mitigate the possible adverse effects of the failure; and
- any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly).

These factors are consistent with the approach and guidance from other regulators (eg, the Competition and Markets Authority, the Financial Reporting Council, UK Bribery Act 2010 and the US Sentencing Guidelines) that aim to help organisations understand what is important to the regulator and also to justify the level of fines for breaches. They also provide insight into elements important to the ICO when assessing a breach and as such provide guidance for areas where effort should be focused. By demonstrating that these factors have been carefully considered and controls have been put in place to attempt to mitigate the associated risks, an organisation can not only demonstrate that it is striving to comply with the spirit of the legislation, but should also provide a basis for reducing penalties.

Many of the factors outlined above are proactive in nature, outside of mitigation efforts, but such items do not fully describe an appropriate response to data misuse or breach. A company's response to misuse or breach should include an assessment of the root cause and a plan of remediation to prevent a future breach of a similar nature. These items are discussed in further detail later in this chapter.

Impact of the GDPR on a forensic examination or litigation

Hackers are finding their way in through the tiniest of openings. Two of the biggest recent cyber-attack headlines involved Equifax and Deloitte. At Equifax, hackers obtained the personal information of 143 million people. The Deloitte breach, which was first thought limited to a 'small number of emails', was later found to include all of the firm's administrator accounts as well as its entire internal email system, including attachments with confidential security and design materials, login information and IP addresses. Equifax and Deloitte were able to identify and quantify the data that had been hacked. But what if they could not have quantified what was compromised?

Data breaches also unfortunately lead to internal investigations and often litigation from regulators, shareholders, investors, creditors and other stakeholders. These consequences require a coordinated effort to identify the 'who, what and when' of the breach, including the potential production of data.

Beyond data breaches, in the normal course of business companies are faced with litigation and other disputes that require the production of data. In the ever-increasing global economy, this often involves data housed in multiple jurisdictions and company locations in multiple jurisdictions, potentially involving varying regulatory regimes related to data privacy. This reality and the challenges presented in remaining compliant cannot be ignored because they represent very real risks to companies.

The GDPR, as well as other data privacy regulations, are increasingly presenting additional challenges related to transferring data. Since implementation of the new regulation, European regulators are intensifying GDPR enforcement. This was evident when a number of organisations were targeted in the first six months of 2019. The first enforcement action has been taken by the ICO against AggregateIQ Data Services Ltd, a data controller outside the European Union. As a result, the effort required to get the information needed in a compliant way to respond to investigations and litigation is increasing in complexity and risk.

These warnings, investigations and enforcements demonstrate the potential for enforcement under GDPR against companies inside and outside of the European Union. Companies simply must understand and address the risks presented in the new GDPR world.

Managing conflicts of law in a post-GDPR global investigation

Compainies involved in regulatory investigations or cross-border litigation will find there is no simple solution to protect their organisation from the threat of data privacy violations around the world. There are, however, several measures that an organisation can implement in order to minimise the threat of criminal violations, including:

- Data governance: companies must know what data is within the scope of the investigation, along with where it resides and which data privacy regulations are applicable;
- Collection and preservation planning: once the applicable jurisidictions are identified, companies should implement appropriate risk management tools to ensure compliance with the data regulations that apply to the source of any relevant data;
- Data privacy training: companies should provide updated training programmes for all personnel involved in investigations and data transfers. This should include team members who review data, so that they are aware of high-risk data types and the procedures related to their use.
- Data transfer strategy: it is important to create a specific strategy that accounts for the nature and origin of the data and any data-related constraints. The rationale for the strategy, including what data should be transferred and why, should also be documented.
- Jurisdictional and data privacy issues: this analysis should include the overall logistics of processing, hosting and reviewing the data.

Of the measures outlined above, one of the consistent themes is jurisdiction. Often, the data relevant to an investigation or litigation is not all stored in the same jurisdiction governing the dispute. As a result, the transfer of data should be of concern to avoid infringing on any data privacy laws, including the GDPR. Data privacy considerations in the context of an investigation or litigation should not be minimised; rather, they should be proactively addressed. The consequence of not doing so can be significant, even if unintended.

If there is doubt whether a transfer can be made from a jurisdiction, then data should be maintained and reviewed within the country whenever possible. This is even more important if the data contains restricted content, such as state secret information, as the penalties for exporting restricted data across borders can be harsh, including imprisonment.

A few points to consider related to data transfer that can assist in mitigating risk of violation include:

- Avoid obtaining consent. Prior to the GDPR coming into effect, in some European jurisdictions, individual consent was obtained. This involved a data subject giving consent to transfer. Under the GDPR this now proves impracticable, as consent must be 'informed' and very clearly and narrowly defined (ie, the data processor and controller must specify very precisely exactly how and for what purpose the data will be used). Given the uncertainties around how exactly data might be used in a changing environment, such as in an investigation, drafting a sustainable 'informed' consent form is almost impossible. Additionally the data subject has the right to withdraw consent at any time, which means there can be no certainty around the validity of any consent obtained.
- Develop a data collection plan that is considered and proportionate. Focus on the richest and potentially most responsive data sources and prioritise these. Data protection authorities take a dim view of broad-brush collection that results in more data being transferred out of a GDPR-compliant environment than is absolutely necessary.

- Take into consideration the need for a review platform that limits access from non-GDPR jurisdictions and that allows for the redaction of PII if data is going to be transferred. Obtain advice on what type of data beyond clear-cut PII may trigger GDPR concerns, for example, data that allows for the identification of individuals, such as titles or job descriptions.
- Consider whether, as a corporate, the development of binding corporate rules (BCRs) is an option. BCRs are a set of rigorous rules based on European data protection standards that require completion of an application and approval of DPAs. Approved BCRs permit the flow of data within the defined corporate group, no matter where the entities are located. The development of BCRs is no trivial feat and requires onerous data mapping exercises as well as the development of the rules themselves and then rigorous enforcement of the rules. It is most likely only worth considering for the largest corporates with integrated systems.
- Prepare standard contractual clauses, also referred to as model contracts, based on clauses issued by the European Commission in order to establish safeguards allowing for the transfer of personal data from the European Union to non-EU countries (such as the United States). These clauses still require the application of GDPR appropriate measures to data before transfer.
- Mutual legal assistance treaty: this is an agreement between countries to share information – specifically recognised in article 48 of the GDPR. Again, this is simply an appropriate mechanism for the transfer of data after it has been appropriately collected, reviewed and deemed producible.
- Privacy shield: this is a framework designed by the US Department of Commerce, the European Commission and the Swiss government to facilitate the personal data transfers from the EU European Union and Switzerland to the United States. The Privacy Shield remains untested in court and is potentially vulnerable to legal challenges.

There are other considerations related to the actual identification and production of data for investigation purposes, such as the use of artificial intelligence (AI) to identify and remove personal information. AI can also be configured to identify personal data as well as national security information. Similarly, sensitive communications can be redacted so that the human reviewer never sets eyes on it, thereby safeguarding highly sensitive and valuable data. For cross-border investigations, such methods could be configured to perform cross-border deduplication or be combined with other technologies.

The use of AI and machine learning by regulators is also on the rise, in particular in the area of enforcement and supervision. In particular, there is an ever-increasing expectation for corporates to proactively identify instances of fraud and breaches of laws and regulations, self-report to the relevant authorities and remediate in a timely fashion.

With governments and regulators embracing AI and machine learning in their respective processes, it is no surprise that they will expect corporates, legal counsels and forensic accountants to deploy AI and machine learning where it is suitable to do so in investigations

and compliance programmes. Such proactive reporting is also considered by regulators in the determination of a penalty and negotiation of a settlement agreement (eg, deferred prosecution agreements (DPAs)).

Misuse of data

Tech entrepreneurs built fortunes on the ability to mine and resell personal data, much of which was obtained on the basis of 'informed' consent at a time when regulation was at best thin on the ground. This era was epitomised by the now infamous words of Facebook's CEO, Mark Zuckerberg, to 'move fast and break things', words which now, in the post-GDPR world, sound particularly hollow. As we discuss below, unless the tech industry wakes up, moves away from broad brush impenetrable consent and understands what compliance really means, it risks being fined into submission by regulators who are now empowered and prepared to act.

While the largest GDPR fines proposed by the ICO to date relate to data breaches from hackers, the higher penalty tier (the greater of €20 million or 4 per cent of global annual turnover) applies to misuse of data. Following the *Cambridge Analytica* scandal, Facebook was fined £500,000 by the ICO. Had the misuse occurred after the enactment of the GDPR, the fine could have been £1.4 billion.

According to a recent survey by the Software Engineering Institute, nearly half of respondents had experienced an information security incident involving an insider. Further, insiders were responsible for half of incidents where private information was unintentionally exposed and a third of incidents involved compromised or stolen customer records.[3]

Beyond the prevalence of insider incidents, it is also important to understand the various forms of data misuse that can lead to GDPR violations. In the case of *Cambridge Analytica*, Facebook collected data from users who provided informed consent as well as the members of those users' networks who had not provided consent. The wrongfully collected data was then used to attempt to influence voters in multiple countries around the world.

Less nefarious examples include data misuse by police forces in the UK to 'look up their ex-wife's new boyfriend themselves – even if it is because they are worried about the safety of their children – or find out who owns the car parked across the street'.[4] In another example, in Belgium, a mayor sent a campaign email to citizens whose email addresses were collected for the purposes of a subdivision modification. The Belgian Data Protection Authority fined the mayor €2000 for the misuse of the personal information.

The GDPR's expanded definition of personal data as well as additional protections, notably the right to be forgotten, further increases the risks to organisations. Once a data subject exercises his or her right to be forgotten, the data controller is responsible for deleting the data in their control as well as informing other organisations that had received the data.

3 https://insights.sei.cmu.edu/insider-threat/2017/01/2016-us-state-of-cybercrime-highlights.html.

4 https://www.theregister.co.uk/2017/03/22/coppers_persistently_breaching_data_protecton_laws_with_pnc_and_anpr.

The likelihood of an occurrence of data misuse, and thus aggravated penalties, are set to increase as the ultimate purposes to which data is put becomes far removed from the original basis for its collection. While violations of data privacy laws by misuse can happen deliberately and cynically, they can also happen in other unintended ways, particularly as data is moved, traded and amalgamated at a high speed and with increasing levels of complexity and ingenuity. These factors raise huge challenges for data governance and compliance systems, and also when investigating the root cause of a data misuse allegation.

The importance of a meaningful compliance programme and remediation plan

In the event of an allegation of data misuse or a cyber attack involving data loss, a strong compliance programme and the remediation or mitigation response will be key considerations by regulators in assessing fines and penalties. Companies must pay attention to these critical components of data protection by developing and maintaining robust compliance programmes and having a plan to remediate a potential breach.

Compliance programme considerations

Nefarious data can infiltrate data systems unnoticed in many ways – sometimes intentionally, sometimes innocently. It can come in via employees, including existing employees, new hires, or through a merger or acquisition. Exposure is particularly high in organisations where employees use their own devices (BYOD) – laptops, tablets, mobile phones – and access online services such as personal webmail accounts and cloud storage (iCloud, Dropbox, etc). Employees can generate personal data outside the work environment that, when reintroduced into the workplace, becomes integrated with data stored on the company server. The question for companies is whether they are taking meaningful steps to prevent exposure or simply stating that there is a policy against it.

In an environment of increasingly strict regulation and rigid enforcement, the job of protecting organisations against unwanted data has become tougher and the related financial risk greater. Organisations must be aware of the data they have, the type and the sensitivity of that data, as well as having policies and controls in place to ensure employees and external parties are not bringing in data that could put the organisation at risk.

Before defining priorities for a GDPR compliance programme, it is important for an organisation to clarify what exactly it envisions when referring to 'GDPR compliance'. Data privacy issues are centred on the protection of data, which is, in turn, dependent upon data security systems. To be effective, the programme cannot comply with one regulation alone, but must take into account worldwide practices. Each jurisdiction has its own data regulations and privacy laws. As a result, companies should ensure that requirements of every jurisdiction in which they conducts business are factored into any global data protection programme.

So, what should an organisation's top of mind priorities be when developing an effective data protection compliance programme? First, companies need to know where their data resides. It is imperative to understand the types of data collected by the organisation, how it is collected, for what purpose it is used, and where and how it is stored. For example, using numerous cloud service providers to handle and store ever-increasing volumes of data adds

another layer of complexity to this exercise. In addition, compliance officers must make the IT department and procurement team aware of the repercussions of procuring systems and services that result in data being located in jurisdictions where differing data protection laws can result in additional legal and compliance challenges.

There are a number of activities that should be considered to accurately map the data landscape in an organisation, including:

- documenting the number and type of user devices in circulation by collecting all IT asset lists in a central location;
- generating IT-specific questionnaires and interviewing key IT staff about systems, software, mobile apps and collaboration tools used for communication and storing or sharing of data;
- reviewing IT infrastructure diagrams to document the geographic locations of servers; and
- studying IT management documentation regarding policies such as data retention or acceptable uses of technology.

Beyond providing a road map for an effective compliance programme, a comprehensive data map is absolutely crucial to the development of a containment policy. Article 33 requires organisations to provide the supervisory authority with a breach notification within 72 hours of detection. Among the details required in the notification are the categories and number of subjects affected, the number of records affected, the likely consequences of the breach, and steps taken to mitigate the adverse effects. Any organisation that has failed to properly map its data will be ill prepared to fully describe the adverse effects. Launching an adequate containment plan to mitigate those effects may well be impossible.

The second priority when developing an effective compliance programme should be development of technical and organisational measures (TOMs), which are mentioned over 80 times in the GDPR provisions. For example, Article 24 requires data controllers to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the GDPR]'. Likewise, article 28 requires controllers to only use processors 'providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'.

TOMs are essentially the policies, procedures, systems and controls required to comply with GDPR. This emphasises the correlation between driving technical standards of data security in tandem with data privacy and protection compliance objectives. Organisations should focus on their TOMs as a key priority for compliance as these controls are the foundation of a robust data protection programme. Without strong TOMs in place, the company's data protection programme is at risk of remaining a 'paper' programme. TOMs are what make the programme effective.

A third priority relates to the risks associated with third parties. Third-party risk is highly relevant when addressing data protection compliance, the *Cambridge Analytica* scandal being one case in point. Carefully drafted contract terms can help address this risk. These terms are largely technical in nature, such as those relating to access controls, including physical

and network security requirements. The recent Ticketmaster breach, in which 27 million user accounts were compromised, was caused by malicious code on a third-party customer support product.[5] Cyber threat intel firm RiskIQ believes that the same group that hacked Ticketmaster may have changed tactics to target hundreds of additional retailers: 'they seem to have gotten smarter – rather than go after websites, they've figured out that it's easier to compromise third-party suppliers of scripts and add their skimmer.'[6] Performing vendor due diligence, including vulnerability assessments, can bolster an organisation's controls and make it less susceptible to potential breaches caused by their third-party ecosystem.

Finally, as is the case in most areas of compliance, an organisation is most effective when leveraging multidisciplinary skills. Data privacy is not a job for lawyers alone. Whether implementing appropriate technical measures or defining the security standards required of a vendor, professionals experienced in data governance and information technology are a must. Technical know-how and skills are essential to ensuring the effectiveness of any data protection compliance programme.

Developing and executing a remediation plan

During and following an investigation into data misuse or data breach, companies should develop a remediation plan that seeks to address the conditions that allowed the breach or misuse to occur. The remediation plan should, at a minimum, incorporate the investigator's observations and suggested recommendations regarding specific control deficiencies – such as a lack of segregation of duties in an accounting process or a lack of a consistent process related to vendor due diligence. Companies should also take remediation a step further by using this as an opportunity to conduct a broader assessment of their compliance environment to illuminate other aspects of the corporate culture that may have failed in preventing, detecting and deterring the misconduct.

Many companies struggle with remediating deficient controls owing to issues with the remediation plan itself. A well-designed remediation plan should clearly articulate specific actions the company needs to take to address the identified issues. The plan should be pragmatic and risk-based, anticipating the cost benefit of the control and potential resourcing constraints.

Companies should also ensure that the steps in a remediation plan actually mitigate any control deficiencies. Companies far too often create quick fix solutions when developing remediation plans, such as limiting remediation to solving technical deficiencies in isolation, due to a lack of understanding of the root cause of an issue or in an effort to demonstrate that a control has been implemented to address the deficiency. Companies can rush to implement these quick fix solutions for an obvious or superficial issue rather than taking the time to consider whether there were deeper control failures across a broader range of processes and

5 https://www.iq-mag.net/2019/04/ticketmaster-lawsuit-uk-data-breach/#.XYNb0ShKiHs.

6 https://www.riskiq.com/blog/labs/magecart-ticketmaster-breach.

locations that also require remediation. Defining effective remediation steps requires thorough analyses of and reflection on the root cause of an issue and consideration of whether failures were pervasive across multiple processes or business units.

Once defined, the remediation plan needs to be tested. All internal control systems, including remediation plans, need to be monitored. The monitoring specifications should provide a clear plan to test the controls, including the frequency of the testing. Relying on internal audit to perform testing at a later time during a normal course audit is simply not enough, especially for a control that already failed to adequately prevent misconduct.

One of the first information requests typically made when conducting an investigation is for any audit findings and other similar recommendations (eg, stemming from another controls review or risk assessment), as well as the status of remediation of those findings. In many cases, another party, such as internal audit, had already identified a weakness in the same control that failed (or was missing entirely) in the investigated misconduct. However, companies often fail to follow remediation actions through to closure.

It is essential that companies ensure a strong protocol is in place to follow through on the implementation and monitoring of recommended remedial measures (including those resulting from the investigation, internal audit and compliance reviews). Remedial measures, the status of their implementation and the process to test the effectiveness of implementation should be memorialised and tracked and there should be a process in place to test the effectiveness of implementation before considering a remediation 'complete'.

Conclusion

Though the GDPR was enacted in part to simplify data transfers, it is clear that compliance will likely be far more difficult for data controllers and processors, at least in the short term. GDPR has not only increased the maximum penalties for non-compliance, but also expanded the protections afforded to individuals, along with the definitions of personal data and data controllers, all of which make it imperative for organisations of all sizes to reassess their data policies.

With huge financial and reputation risks at stake when things go wrong, forensic standards need to apply not just to the technical aspects of the breach or misuse, but to all aspects of the investigation and remediation plan and the same forensic lens should be applied to any compliance programme assessment. In this respect there are valuable lessons to learn from other areas that, like data privacy today, have seen upheavals in the political and regulatory approach. Financial market abuse through rate rigging and insider information, bribery and corruption and antitrust are just some of the areas forensic investigations skills have underpinned cooperative settlements with regulators, the removal of bad actors from organisations and industries and the development of effective remediation and compliance programmes.

The authors would like to thank Jerry Hansen, Richard Clarke and Bennett Arthur Esq 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 25 years of experience advising diverse clients on sanctions, anti-corruption, fraud, internal controls, asset tracing and money laundering issues.

Frances 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, United Kingdom, Brazil, Indonesia, Poland, Sweden, among others, which included addressing French data privacy and blocking statute issues. She is leading FRA's General Data Protection Regulation compliance initiative leveraging FRA's decades of experience in addressing data protection issues in cross-border litigation and investigation.

Frances has been deeply involved in all of Forensic Risk Alliance's compliance monitorship work, to include US Department of Justice and Securities and Exchange Commission FCPA monitorships, a New York Department of Financial Services bank monitorship, the Ferguson City monitorship, a Public Company Accounting Oversight Board monitorship and a Department of Justice fraud-related monitorship.

Simon Taylor
Forensic Risk Alliance

Simon is in FRA's forensic accounting team with 20 years' experience in white-collar investigations, financial crime and regulatory enquiries. He advises clients on all aspects of corporate governance, internal investigations and complex compliance-related risk assessments.

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 multidisciplinary approach to resolving complex matters. In addition to his investigatory expertise, Simon advises companies on the structure, design and testing of their compliance programs, 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 & Talbot *Confiscation and the Proceeds of Crime,* published by Sweet & Maxwell – in which he writes the 'Investigations' chapter.

Simon is based in FRA's London office. He also provides in-house support to the firm on compliance, forensic accounting and eDiscovery practices.

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 data sets. 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

Simon Taylor
staylor@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 978-1-83862-235-0