MASON
HAYES &
CURRAN

Cyber/Data Breach Annual Review 2023

ISSUE 1
MARCH 2024

MHC.ie

Welcome to Mason Hayes & Curran's Cyber/Data Breach Annual Review 2023

Harnessing and understanding data is critical to success in most industries. This is a result of the world becoming increasingly digital. In the present day, the world at large accesses the internet daily for a variety of reasons and as a result, data is now a high value commodity requiring organisations to have robust cybersecurity measures in place.

In an era of rapid technological and legal advancements, ensuring the security of that data is paramount, particularly as cybercrime continues to rise in scale and complexity. Cybercriminals understand the value associated with data and continue to explore new methods to monetise the exploitation of data. In addition to monetary consequences, the loss or unauthorised disclosure of data can have additional serious operational and reputational implications for organisations, not to mention legal consequences such as regulatory enforcement. The last year has demonstrated that businesses must have robust and appropriate security systems in place to adequately protect themselves from falling victim to a cyber incident / data breach.

The potential pitfalls of sub-optimal data security were laid bare in 2023 as a result of several high-profile incidents which attracted significant media and regulatory attention.

The Data Protection Commission investigated a ransomware attack on Centric Health, and the MOVEit data breach impacted an estimated 2,000 organisations. We consider the lessons which can be gleaned from such incidents along with the implications of key European and Irish court decisions from 2023 which may increase the potential for those affected by data breaches to claim damages.

2023 also saw the progress of several significant pieces of legislation which will affect how businesses approach data security on a go forward basis, chief among them the Digital Markets Act and the Digital Operational Resilience Act. We cast an eye to the future and anticipate the implications of changes to the legal landscape for businesses that use data extensively. Enhanced legislative oversight as well as the proliferation of technologies such as generative AI are likely to be key themes in data security going forward.

This annual review aims to consider key developments in the cyber/data security space in 2023 and distil the most important lessons for businesses in the coming year. We hope you enjoy the first edition of this annual review.

Editors

Julie Austin
Partner,
Privacy & Data Security
+353 86 137 2136
jaustin@mhc.ie

Jevan Neilan
Head of San Francisco Office
+1 415 740 0480
jneilan@mhc.ie

Contents

Cyber Attacks/Data Breaches – In The News

Julie Austin
Partner,
Privacy & Data Security
jaustin@mhc.ie

We outline some of the headline-grabbing cybersecurity breaches from 2023.[1]

Centric Health, February 2023

What happened? Centric Health was the victim of a ransomware attack in December 2019, which resulted in patient data being encrypted by hackers, who then asked for payment to decrypt the data. The DPC investigation into the attack found that data of 2,500 patients were permanently affected, as their data was deleted with no backup available. Around 70,000 Centric Health patients were permanently impacted in total. Following an investigation, the DPC handed down a fine of €460,000, as well as issuing a reprimand relating to the infringements. For further information on the breach, see our article on page 6.

PSNI, August 2023

What happened? Details of officers and employees of the PSNI were published online following a freedom of information request, giving the rank and grade data of employees at the PSNI, including surnames, initials and which department they worked in. More than 10,000 PSNI officers and employees were impacted, causing significant concern and impacting public confidence. An independent review of the matter found that there were "missed opportunities" to secure and protect data. The matter has been referred to the Information Commissioner's Office for investigation.

IT Services Firm, October 2023

What happened? More than half a million documents were accessed in a data breach which exposed the driving licences of thousands of road users who had vehicles towed by an Garda Síochána. The breach was caused by a software error at a Limerick-based IT services firm, which was used by a number of tow truck companies engaged by An Garda Síochána. A statutory investigation has been commenced.

Aer Lingus, June 2023

What happened? Aer Lingus confirmed in June that around 5,000 of its employees were impacted by the MOVEit data breach, which resulted in the disclosure of some current and former employee's data, which included names, titles, dates of birth, addresses and (in the majority of cases) PPS/Social Security numbers.

1. *All information shown above obtained from publicly available sources*

MOVEit, May 2023

What happened? MOVEit provides a file transfer tool which allows organisations to send and receive large amounts of often sensitive data. In one of the largest cybersecurity attacks of May 2023 in terms of affected businesses and individuals, an extortion gang raided MOVEit's servers and stole sensitive customer data which was stored in the servers. There have been an estimated 2,700 organisations affected to date, and at least 90 million individuals. Several class action suits have been brought against Progress Software in the US, the owners of the MOVEit software, alleging breach of contract and negligence. The DPC has been notified of a number of Irish breaches related to the attack.

Microsoft Cloud, July 2023

What happened? A total of 60,000 emails were stolen from 10 US State Departments accounts in a major security breach in July. The group behind the cyberattack gained access to the emails via a compromised corporate account of a Microsoft engineer, taking advantage of a coding flaw. Microsoft launched a technical investigation following the breach, and the Cyber Safety Review Board in the US is investigating the incident.

Munster Technological University (MTU), February 2023

Damage: MTU was the victim of a ransomware attack which the university claimed may have been orchestrated by former operatives of the Revil ransomware group. It resulted in a "significant" IT breach and phone outages. The High Court has since granted an injunction preventing the sale or publication of the stolen data on the web. MTU has been in "close and ongoing contact" with the DPC, the National Cyber Security Centre, An Garda Síochána and other relevant stakeholders since the incident, and it remains under investigation.

23andMe, October 2023

What happened? In a filing with the US Securities and Exchange Commission, the company revealed that hackers gained access to the personal data of 0.1% of customers. The stolen data included the person's name, birth year, relationship labels, the percentage of DNA shared with relatives, ancestry reports and self-reported location. 5.5 million people who opted-in to 23andMe's DNA relatives feature were impacted by the breach. In response to the breach, 23andMe required users to reset and change their passwords and turn on multi-factor authentication. Multiple class action suits have been filed against the company in Canada and the US.

The one-stop-shop case digest issued by the European Data Protection Board in January 2024 may also be of interest. This provides an overview of decisions issued by supervisory authorities across the EU on data security and data breaches and is available here. The summary and analysis of these decisions are useful for organisations, both controllers and processors, when assessing whether their security measures are appropriate, both before and following a data breach.

Worried about cybersecurity?
Contact a dedicated member of our Cyber Incident Response team today.

Ransomware Attacks

A look at the Irish Data Protection Commission's €460,000 fine

Jevan Neilan
Partner,
Head of San Francisco Office
jneilan@mhc.ie

As the digital world expands, there has been a corresponding increase in cybersecurity incidents, most notably ransomware attacks.

Significant ransomware attacks which have occurred since the arrival of GDPR include the WannaCry attack on the NHS in 2017, which cost the health service approximately £92 million and resulted in 19,000 cancelled appointments. Worldwide, the WannaCry attack reportedly caused over $4 billion in damages.[1] In another example, on New Year's Eve 2019, London-based foreign currency exchange Travelex was reportedly infiltrated by REvil and paid $2.3 million to secure the return of its data.

In this article, we address a decision issued by the Irish Data Protection Commission (DPC) last year against Centric Health Ltd. (Centric), a healthcare provider, who suffered a ransomware attack in 2019. We look at the DPC's analysis, which addresses several security and organisational shortcomings which it deemed exacerbated the cybersecurity incident, and set out the key learnings from this decision.

1. *AAG IT, 'The Latest 2023 Ransomware Statistics', 17 February 2023, available online here (Updated March 2024)*

Centric's data breach

Centric suffered a ransomware attack that resulted in its staff losing access to the patient administration system, affecting 70,000 patients. Data on the system was backed up nightly and a snapshot of data was taken each day. However, these back-ups were also affected by the malware. Personal data of 2,500 patients was permanently deleted due to back-ups of the system being affected.

The breached data included patients' names, birth dates, PPS numbers , contact details, and some health data, considered special category data or SCD.

Centric paid an unspecified ransom to the attackers in return for a decryptor key. However, the decryptor could not be applied to the affected data as the data had been deleted in the interim.

Ultimately, the DPC found that Centric infringed Articles 5(1)(f), 5(2) and 32 GDPR and imposed a fine of €460,000.

Shortcomings identified by the DPC

1. Risk assessments:

- The DPC found that Centric failed to maintain documented accounts of risk assessments
- The DPC stated it was important to carry out an assessment looking at the:
  (1) Likelihood of unauthorised access, taking into account that SCD was processed, and
  (2) Severity of risks to rights and freedoms of data subjects
- These assessments would have determined the level of appropriate security that should have been implemented
- Centric's last risk analysis took place in May 2018 and deemed its IT infrastructure as high risk

2. Security of processing

- The DPC identified several software patches that had been released by Microsoft in 2018 but which were not applied to Centric's Windows Operating System . The DPC found *"regardless of whether the patches in question would have prevented the installation of Phobos ransomware, the failure to implement any security patches from the implementation of the GDPR onwards is demonstrative of a failing to ensure the security of the Primacare server and Centric's IT systems as a whole".*[2]
- The DPC noted Centric's security failings as follows:
  (1) Failure to implement industry standard measures such as complete patch application
  (2) Failure to implement encryption of data at rest in circumstances where the data at rest in the Patient Administrator System was not encrypted
  (3) Failure to have appropriate levels of server security, and
  (4) Failure to ensure an appropriate level of security of passwords and log in credentials – the forensic report found that the server was fully exposed to the internet with a password that could have been brute forced without much difficulty – which was what happened

3. Organisational measures

- The DPC noted Centric's organisational deficiencies as follows:
  (1) Lack of a business continuity plan demonstrated inadequate organisational measures and a failure to ensure the ongoing accuracy and integrity of personal data held by Centric
  (2) The fact that back-ups were stored on the physical server as opposed to offsite, and
  (3) The lack of records, demonstrating the testing of restores from the backup systems
- These shortcomings, when combined, resulted in the DPC finding that Centric's organisational measures were in violation of the GDPR

4. Accountability

The DPC also found that Centric's failure to retain appropriate documentation, demonstrating whether risks or vulnerabilities had previously been identified, and to demonstrate any planning for mitigation of such risks, amounted to a contravention of the accountability principle, Article 5(2) GDPR.

5. Policies

Centric had numerous policies, including an Information Technology Policy and a Patch Management Policy. However, the DPC decided that these policies were not followed in practice and the steps in the policies were not carried out at the determined intervals set by the policies.

2. *DPC Final Decision, IN-21-2-4, 23 January 2023, para 95, page 21*

Main takeaways from the DPC's decision

Dos	Don'ts
Conduct regular risk assessments and record these to determine and defend your risk classification	Ignore security releases or new industry standards
Regularly conduct testing on your technical and organisational measures to ensure your measures are effective and adequate in light of the risks	Expose your servers to the internet with a password that could be brutally forced without much difficulty
Ensure that your policies and procedures are being implemented. These checks should be documented	Expose your firewall, allowing all inbound and outbound traffic to pass through
Ensure you have a business continuity plan in place	Underestimate the importance of backups and backing up data appropriately

Conclusion

This DPC decision demonstrates the importance of organisations adopting appropriate security measures, such as conducting regular risk assessments and evaluating the adequacy of technical and organisational measures to ensure they are sufficient in light of the identified risks. The decision also makes it explicitly clear that policies and procedures are of little utility if they are not given effect in practice, requiring verifiable oversight as to how staff are actually implementing these documents in practice.

EU Cybersecurity Laws – What's on the Horizon?

Julie Austin
Partner,
Privacy & Data Security
jaustin@mhc.ie

In recent years, there has been a marked increase in the amount of legislation generated at an EU level with a view to improving cybersecurity across Europe. The Network and Information Security Directive (NIS2), the Cyber Resilience Act, the Digital Operational Resilience Act (DORA) and the EU Cybersecurity Act are each aimed at strengthening the EU's cybersecurity framework in light of the heightened threats to cybersecurity in the digital age. In this article, we explore these four key pieces of legislation, and what they might mean for you.

NIS2 Directive

What is it?

In 2018, the Network and Information Security Directive (NIS1) harmonised national cybersecurity capabilities, cross-border collaboration and the supervision of critical sectors across the EU. However, a common criticism levied against NIS1 is that it is inconsistently applied across Member States resulting in divergent security requirements and incident notification requirements. The European Commission conducted a review of NIS1 and developed a proposal for a revised directive, EU Directive 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). NIS2 will repeal and replace NIS1.

The goal of NIS2 is to expand the scope of NIS1, making it "future-proof". It provides legal measures which are geared towards boosting cybersecurity in the EU.

NIS2 builds on three elements of NIS1:

1. Competent authorities: Improve the level of joint situational awareness and the collective capability to prepare and respond, by:

- Taking measures to increase the level of trust between competent authorities.In Ireland, this is the National Cyber Security Centre (NCSC)
- Sharing more information
- Setting rules and procedures in the event of a large-scale incident or crisis

2. Reduce inconsistencies in resilience: Further aligning:

- The de facto scope
- The security and incident reporting requirements
- The provisions governing national supervision and enforcement

3. Increase the level of cyber-resilience: NIS2 puts in place rules that ensure that public and private entities across the internal market, which fulfil important functions for the economy and society as a whole, such as energy, banking and financial markets, are required to take adequate cybersecurity measures.

Who does it apply to?

NIS2 extends to a larger part of the economy than NIS1. It applies to entities from a number of "critical sectors" including:

- The energy sector
- Financial market infrastructures
- ICT Service Management (managed service providers and managed security service providers)
- Waste management
- Food
- Machinery and equipment
- Digital providers (online marketplaces, online search engines and social networks)

NIS2 defines two categories of public and private entities within scope: "essential" entities and "important" entities, with more onerous obligations for 'essential' entities.

When does it come into effect?

NIS2 was published in the Official Journal on 14 December 2022. As a directive, it must now be transposed into national law by each Member State of the EU. Member States must adopt and publish the measures necessary to comply with NIS2 by 17 October 2024.

The EU Commission will periodically review the functioning of the Directive and report on it to the Council for the first time by 17 October 2027.

What will enforcement look like?

Most entities will fall under the jurisdiction of the Member State in which they have their main establishment. NIS2 provides a wide range of enforcement measures which Member State authorities may take to supervise entities, including regular and targeted audits, on-site and off-site checks, and requests for information. NIS2 also sets up a framework of sanctions across the Union, to include a minimum list of administrative sanctions.

Regarding sanctions, NIS2 distinguishes between essential and important entities. For essential entities, Member States must provide for administrative fines for a breach of NIS2 of up to €10,000,000 or 2% of total worldwide annual turnover for the preceding financial year, whichever is higher. For important entities, NIS2 requires Member States to provide for a maximum fine of at least €7,000,000 or at least 1.4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Cyber Resilience Act

What is it?

The Cyber Resilience Act is a proposal for a Regulation on cybersecurity requirements for products with digital elements. It aims to address the perceived inadequate level of cybersecurity in many products, as well as addressing the inability of consumers and businesses to determine which products are cybersecure.

According to the EU Commission, the Regulation, once implemented, will guarantee harmonised rules for products or software with a digital element. It will also introduce a duty of care obligation for the entire lifecycle of such products, as well as a framework for cybersecurity requirements governing a number of aspects, with a view to providing for obligations to be met at every stage of the value chain.

The main obligations covered by the proposal include cybersecurity by design, vulnerability management and market surveillance.

Who does it apply to?

When in force, the Regulation will apply to "critical" products with digital elements, ie a product with digital elements that presents a cybersecurity risk in accordance with the criteria set out in the proposal. The obligations will differ depending on whether the product is a Class 1 or Class 2 product.

When does it come into effect?

EU Member States and the European Parliament have come to a provisional political agreement on the Regulation. The European Parliament and EU Council must approve the Regulation before it moves to the next stage of the legislative process. Once adopted, it will enter into force 20 days after its publication in the Official Journal.

What will enforcement look like?

The draft proposal provides for a number of administrative fines for various offences. These fines can be up to €15,000,000 for a breach of certain obligations, or 2.5% of an undertaking's total worldwide annual turnover in the preceding year, whichever is higher.

DORA

What is it?

DORA is a package of two pieces of European legislation, a Regulation and a Directive, which aims to strengthen the IT security of financial institutions.

Who does it apply to?

DORA will apply to financial institutions including banks, insurance companies and investment firms but will also have substantial implications for IT service providers who count these institutions as customers.

When does it come into effect?

DORA was adopted in December 2022 and will enter into force in January 2025. 2024 is therefore a critical year for financial institutions to prepare for compliance. Compliance will undoubtedly be aided by the publication of policy documents by EU supervisory entities: the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA).

The first set of final draft technical standards was published on 17 January 2024 and offers clarity on required elements of the risk management framework, the criteria for classifying ICT-incidents and the measures applying to outsourcing, among other things. The second set of draft technical standards was published on 8 December 2023 and remains open for public consultation until 4 March 2024 . A finalised version of the second set of technical standards is scheduled for publication in July 2024.

What will enforcement look like?

DORA imposes a uniform set of rules for ICT risk-management, incident reporting and operational resilience testing for financial institutions as well as for managing the risk posed by third-party ICT-providers. To this end, DORA will impose requirements on the contractual arrangements between financial institutions and ICT providers and will set the parameters of an oversight framework for managing these third-party risks. Several of DORA's key requirements are undergirded by a risk-based approach designed to mitigate the compliance burden on financial institutions. It also contains provisions requiring information and intelligence sharing among financial institutions to mitigate risks on a system-wide level.

For more on DORA please see DORA – Digital Risks in the Financial Sector at page 13.

Cybersecurity Act

What is it?

The Cybersecurity Act is an EU Regulation which came into force in April 2019. It established the EU Agency for cybersecurity (ENISA) and is the basis for an EU-wide framework for the cybersecurity certification of ICT products, processes and services. The European Commission proposed an amendment to the Cybersecurity Act in April 2023 which would enable the adoption of European cybersecurity certification schemes for '*managed security services*' covering areas such as incident response, penetration testing, security audits and consultancy.

Certification is key to ensure a high level of quality and reliability of these highly critical and sensitive cybersecurity services which assist companies and organisations to prevent, detect, respond to or recover from incidents. These certifications could be used to demonstrate compliance with the security obligations under the GDPR.

Who does it apply to?

The proposed new system would apply to those who provide managed security services within the EU. Managed security services are defined as "*carrying out, or providing assistance for, activities relating to... customers' cybersecurity risk management*".

When does it come into effect?

It is not yet clear when the proposed amendment will come into effect but, as of March 2024, the proposed amendment remains the subject of discussion within the European Council. It is expected to progress through the legislative process during the course of the year. Both providers and users of managed security services should be cognisant of the effects of the amendment and may wish to monitor its progress.

What will enforcement look like?

While the text of the amendment has not been finalised, the proposed amendment is intended to mirror the language of, and therefore complement, the NIS2 Directive. Certification of the providers of these services will act as a mark of quality for potential customers with the scheme aiming to ensure that these services are "*provided with the requisite competence, expertise and experience*". The amendment would have particular implications for service providers as it would aim to ensure that the service provider has "*appropriate internal procedures in place to ensure a high level of quality*". While implementing legislation would be required to define the exact standards to be adhered to for certification, the amendment does contemplate a tiered certification system with "*basic*", "*substantial*" and "*high*" levels of assurance proposed.

DORA – Digital Risks in the Financial Sector

Dermot McGirr
Partner,
Privacy & Data Security
dmcgirr@mhc.ie

The financial services sector is a prime target for cyberattacks such as hacking, ransomware and identity theft. This is a result of the financial services sector having integrated complex technology systems and processes into all areas of its business. It is also heavily reliant on third party IT providers to manage data and deliver services. Cyberattacks that access computer systems and harm data are a particular problem for financial firms that hold large amounts of personal data related to bank accounts or insurance arrangements. These attacks can result in reputational and financial damage to both customers and to the firms themselves.

Due to the rapid evolution of technology, EU rules on cybersecurity became fragmented and EU legislation like the GDPR and the Directive on Security of Networks and Information Systems (NIS Directive) plugged the gaps in certain cases, although the disjointed approach created exposure for firms and clients. The Digital Operations Resilience Act (DORA), Regulation (EU) 2022/2554, was published in December 2022. Its key objective is to implement a cohesive regulatory framework in the EU financial services sector to manage digital risks and build resilience against IT-related disruptions, threats and cyberattacks.

DORA will apply to in-scope financial services entities from 17 January 2025.

Scope

DORA will apply to a wide range of financial entities, such as:

- Credit and payment institutions
- Investment firms
- Crypto-asset service providers
- Central securities depositories
- Trading venues
- Trade repositories
- Some insurance and reinsurance undertakings, and
- Service providers operating in the financial services sector

Purpose

DORA sets out new statutory requirements for the security of financial entities' network and information systems, including those related to:

- Risk management
- Incident reporting
- Resilience testing
- Cyber threat information sharing, and
- Contractual arrangements with ICT third-party service providers

Financial entities must, amongst other matters:

- Identify and document ICT supported business functions, roles and responsibilities, information assets, ICT assets and the potential risks that may impact them. In addition, there is a requirement to conduct a business impact analysis of the relevant entity's exposures to severe business disruptions
- Continuously monitor and control the security and functioning of ICT systems and tools and deploy appropriate ICT security tools, policies and procedures
- Implement ICT security policies, procedures and tools to ensure the resilience, continuity and availability of ICT systems
- Implement and test mechanisms to detect anomalous activities, including ICT network performance issues and ICT-related incidents
- Implement post-incident reviews after major ICT-related incidents disrupting core activities in order to analyse the causes and identify improvements
- Maintain a digital operational resilience testing programme

There are extensive reporting requirements, such as reporting the following to competent authorities:

- Major ICT-related incidents. Financial entities must also inform their clients about incidents that have an impact on the financial interests of clients
- An estimate of aggregated annual costs and losses caused by major ICT-related incidents
- Changes implemented following incident reviews

What DORA means for your contracts

DORA sets out detailed provisions regarding the contractual arrangements between financial entities and ICT third-party service providers.

For those entities which have already complied with regulatory guidance on outsourcing, such as that provided by the European Banking Authority (EBA) or the Central Bank of Ireland (CBI), the good news is that DORA closely tracks many of the same contractual requirements.

However, one of the key points to note about DORA is that it does not just apply to outsourcing arrangements, as is the case with existing regulatory guidance on outsourcing. The contractual requirements of DORA apply to the use of "ICT Services". These are defined as *"digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which include the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services"*. DORA may, therefore, cover a significant percentage of the services procured by a financial services entity.

Once the full cohort of ICT service providers has been established, DORA requires financial services entities to assess and divide their ICT providers into two categories - those who provide services that support critical or important functions and those who do not. As would be expected, the contractual requirements applied to critical or important functions are more fulsome than those applied to non-critical suppliers.

A "Critical or Important Function" is defined under DORA as a function:

- The disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or
- The discontinued, defective or failed performance of which would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law

If the financial services entity is already complying with existing regulatory guidance on outsourcing, such as the EBA and CBI outsourcing guidelines, many of the contractual requirements will be familiar. For example:

- Requirements to include specific termination rights
- Requirements dealing with management of exit and transition
- Obligations on the ICT provider to, amongst other matters, comply with appropriate information security standard
- Provisions to ensure access, recovery and return of data in the event of the insolvency, resolution or discontinuation of the operations of the ICT provider, or in the event of the termination of the contract

The DORA requirements, however, are more detailed in places and also raise some novel issues. This issue means that financial services entities who have already complied with regulatory guidance on outsourcing still need to assess their outsourcing agreements against the requirements of DORA.

2023 developments

DORA requires the adoption of specific regulatory technical standards (RTS) and implementing technical standards (ITS) which expand upon the obligations set out in the Regulation itself.

In 2023, we saw the first two batches of draft RTSs under DORA published.

The European Supervisory Authorities (ESAs) published the first batch of draft RTS under DORA in June 2023. One draft RTS specifically relates to the policy set out in the Regulation on contractual arrangements with ICT third party providers, while an ITS was also published on templates for the register of information regarding contractual arrangements with ICT third party service providers.

The ESAs published the second batch of draft RTSs under DORA in December 2023, one of which relates to the RTS and ITS on content, timelines and templates on incident reporting and the RTS on subcontracting of critical or important functions.

The public consultation for this first tranche of RTSs closed on 11 September 2023, with the final amended (as appropriate) standards submitted to the European Commission by 17 January 2024 for adoption. The public consultation for the second tranche of RTS remains open until 4 March 2024, with the final amended (as appropriate) standards submitted to the European Commission by 17 July 2024 for adoption.

Regulatory oversight of critical ICT service providers under DORA

DORA is not just aimed at financial institutions, it also provides for a direct oversight regime which will apply to those ICT providers who are designated as critical. This is a relatively new departure as the previous approach in outsourcing guidelines issued by the various sectoral regulators in the financial services sector was only to seek to indirectly regulate the ICT providers. This indirect approach was achieved by imposing requirements for regulated entities to procure certain rights and obligations through contracts.

The European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA), (together the ESAs), will lead the oversight framework. Following an assessment, the ESAs will designate ICT providers that are "critical" for financial entities, and those ICT providers will be subject to the oversight regime. The assessment for each ICT provider will be based on criteria such as:

- The impact on financial services if the ICT provider were to experience a large-scale operational failure to provide its services
- The systemic character or importance of the financial entities that rely on the ICT provider
- The reliance of financial entities on its ICT services for critical or important functions, and
- The ease of replacing the ICT provider

If an ICT provider is designated as critical then it will have a "Lead Overseer" appointed from one of the regulators referred to above. This regulator will have extensive oversight and audit powers, coupled with the power levy fines if the ICT provider does not comply. The critical ICT provider also has to pay for the Lead Overseers costs incurred in exercising the powers granted to them by DORA.

Financial institutions which use the services of a critical ICT provider may well welcome these aspects of DORA. The direct oversight by European regulators will assist them when they are seeking information, reporting, audit and inspection rights from these providers. This is an issue which has caused problems in the past when financial services businesses were seeking to comply with the associated requirements in sectoral outsourcing guidelines.

The companies which are designated as critical ICT providers may not be as welcoming of these direct oversight provisions. This may be because the powers granted to the Lead Overseer align with the types of things which some providers, usually for good practical reasons, have sought to resist in their contracts with customers, eg detailed rights of audit, inspection, and reporting.

Coupled with this is the threat of very substantial fines and the requirement to pay the costs of the Regulation, these issues mean that the relevant companies should be paying very close attention to this aspect of DORA.

Conclusion

The enforcement of DORA is fast approaching. We recommend that organisations take measures now to ensure they are DORA ready. We are well placed to assist with the implementation of DORA due to our market leading experience in the implementation of the contractual requirements of regulatory guidance on outsourcing.

Contact a member of our Technology or Financial Regulation teams for expert advice and guidance on the implications for your organisation.

What are the Cybersecurity Risks of Generative AI?

Brian McElligott
Partner,
Head of AI
brianmcelligott@mhc.ie

Last year Generative AI dominated headlines, promising to transform the way in which organisations operate by drastically increasing efficiency and reducing labour-intensive tasks. As a result, the overarching narrative was one of adoption or risk becoming obsolete. While there is some truth to these claims, it's also important to bear in mind that as with any new technology, inherent risks equally exist.

What is Generative AI?

Generative AI is a branch of artificial intelligence that focuses on generating new data in the form of text, images, video etc based on existing data. It involves machines and algorithms that continuously improve by learning patterns from the vast amount of data fed into the machine. Put simply, Generative AI involves the following steps:

a) The model or machine is trained using a huge dataset

b) From this large dataset, the model or machine identifies and learns underlying patterns and structures in the dataset, and

c) The generative process enables the creation of new data which mimics these learned patterns and structures.

1. *Forrestor Report, "Maximizing Business Potential With Generative AI: The Path To Transformation", 2023*

Generative AI in cybersecurity

The potential for Generative AI to adversely impact and exacerbate cybersecurity risks is very real. Generative AI has significantly altered the cyber threat landscape as this novel technology is accessible to all and easy to use and understand. It is reported that cybercriminals have already found ways to exfiltrate data from Generative AI tools. These include using platforms based on Generative AI models trained on malware creation data and used for ill intent or to generate malicious code.

In addition, according to research studies, security has been labelled as a top hurdle for companies to overcome when looking to deploy AI. Remarkably, **64%** of companies have indicated that they do not know how to evaluate the security of Generative AI tools.[1]

We focus on five key cybersecurity risks associated with Generative AI, which will need to be carefully considered before seeking to implement this transformative technology:

1) Data breaches

Data breaches pose a significant cybersecurity risk when considering whether to utilise Generative AI. This is because these models store and process a colossal amount of confidential data or sensitive data such as personal data, health records or financial data.

As a result, these models can be exploited by bad actors seeking to gain unauthorised access to private data for their financial gain. For example, by inputting specifically crafted data, an attacker can try to cause the AI model to output information it has been trained on, potentially revealing confidential data.

Internally, a breach may also result from an organisation having inadequate oversight such as insufficient security protocols, inadequate monitoring, weak access controls and/or deficient encryption. Therefore, without appropriate safeguards, GDPR infringements could occur.

2) Malware and ransomware

It is reported that Generative AI can produce new and complex types of malware which are capable of evading conventional detection methods. In the area of ransomware attacks, it is argued that non-cyber criminals who lack IT knowledge may now be able to carry out ransomware attacks by utilising chatbots.[2] In addition, more sophisticated cyber criminals with IT skills necessary for carrying out ransomware attacks may lack expertise in other fields. As a result, it is also argued that this cohort of criminals may also benefit from Generative AI by drafting more persuasive and professional phishing emails.[3]

3) Exposure of software security vulnerabilities

Organisations also run the risk of exposing any existing IT vulnerabilities and creating new ones where their IT systems are outdated, patch releases are not implemented, and/or relevant software updates have not been adopted.

The addition of any new application into a network creates new vulnerabilities that could be exploited to gain access to other areas in an organisation's network.

However, Generative AI poses a unique risk as it can contain complex algorithms that make it difficult for developers to identify security flaws.

According to experts: "AI is not yet sophisticated enough to understand the complex nuances of software development, which makes its code vulnerable ".

4) Data poisoning

Model poisoning is another inherent cyber risk associated with Generative AI. This is a form of attack which targets AI models in their development and testing environments. These attacks involve the introduction of malicious data into training data which then influences the resulting AI model and its outputs. A Generative AI tool which has been the subject of a model poisoning attack may produce significant unexpected deviations in its output. It is also challenging to detect model poisoning, as the poisoned data can appear innocuous. As a result, organisations whose models fall victim to data poisoning, dependent on their security and organisational measures, may find themselves falling foul of the GDPR as well as AI specific legislation.

5) Data leakage

Lastly, where staff are not properly AI trained, the hunt for efficiency can lead to the leakage of sensitive or personal data through Generative AI products. Employees may enter confidential or personal data into a Generative AI product without being aware of the implications, and may even unwittingly disclose personal information through browser extensions and other software.

Additionally, failure to protect personal data from data scraping infringes on GDPR obligations as organisations / digital service providers are obliged to protect users' personal data.

2. *International Cybersecurity Law Review, Springer Link, "Ransomware attacks in the context of generative artificial intelligence - an experimental study", Volume 4, 07 August 2023, available here.*

3. *ibid.*

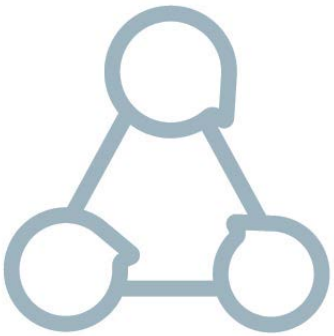
Conclusion

Inherent and significant risks are associated with the use of Generative AI, especially from a cyber perspective. As organisations explore the benefits associated with this transformative technology so do cyber criminals. It is now known that hackers are using Generative AI tools to improve the sophistication of their phishing attacks. This is because this technology enables them to gather personal information at large scale as well as creating more sophisticated spoof websites in a bid to trap individuals into sharing their credentials. As a result, organisations must implement robust security measures to adequately safeguard against these increasingly sophisticated cyberattacks.

Given that the EU AI Act's final text is expected in the coming months, now is the time to ensure organisations' adoption of Generative AI is implemented in compliance with both the GDPR and the AI Act. This is because adopting Generative AI without carefully considering and safeguarding against the inherent security risks exposes organisations to fines under both regimes (once the AI Act comes into effect) as well as reputational damage.

Legal advice should be obtained whereby organisations are unsure as to how they should appropriately safeguard against these security risks when deploying Generative AI.

For more information and expert advice, please contact a member of our Artificial Intelligence team and / or a member of our Cyber Incident Response team.



Comparative Analysis of Cyber Security/Personal Data Breach Reporting Regimes

Julie Austin
Partner,
Privacy & Data Security
jaustin@mhc.ie

Whilst most well known, the GDPR is not the only legal regime which imposes obligations on organisations to report personal data breaches or security incidents leading to personal data breaches.

The table on the following pages identify other legal regimes outside of GDPR which may potentially apply to personal data breaches or other security incidents in force as of January 2024.

There are a number of developments expected in EU cybersecurity law in the coming months and years and so it is important to keep abreast of developments in this space.

Regime	What does it apply to?	Who does it apply to?	Obligation to notify Regulator	Obligation to notify data subjects/users
ePrivacy Directive (ePD)	Personal data breaches	Providers of publicly available electronic communications service (ECS) like: • Internet access services • Number-based interpersonal communication services such as a traditional telecoms services which is registered with ComReg, or • Number-independent interpersonal communication services such as over-the-top communications services like email	ECS's must notify personal data breaches associated with those services to the competent authority in each EU Member State, the DPC in Ireland, where end-users who have been impacted by the breach. Initial notification must be within **24 hours** of detecting the breach and additional information to be provided in more detailed follow up notification within **72 hours**. There is no ECS's mechanism under the ePD and so notification is technically required to the competent authority in every EU Member State where the affected end-users are located. The ePD complements the GDPR. However, where an ECS notifies under ePD, it is not required to notify under GDPR.	ePD also obliges the ECS to notify end users **'without undue delay'** if the breach is likely to adversely affect the personal data or privacy of a subscriber or individual.
Electronic Communications Code (EECC)	Security incidents. These differ from data breaches as they concern the security of the service itself, whereas the ePD concerns the personal data associated with the service.	ECS. Reportable incidents affect any of the following: • Confidentiality, eg attackers access content of communications • Authenticity, eg identity fraud via a man-in-the-middle attack • Integrity, eg routing files altered by malware, and /or • Availability, eg an outage	'Significant' security incidents must be notified to the telecoms regulator in each EU Member State (ComReg in Ireland) in which there were end-users affected **"without undue delay"**. What is considered 'Significant' differs across Member States, generally it involves a combination of: • The number of users affected by the security incident • The duration of the security incident • The geographical spread of the area affected by the security incident • The extent to which the functioning of the network or service is affected • The extent of the impact on economic and societal activities. The timeline for "without undue delay" also differs across Member States, and generally relates to the number of users who are affected.	The EECC also obliges ECS's to inform potentially affected end-users in the case of a particular and significant threat, and to include possible mitigation measures, eg using specific types of software or encryption technologies to protect the security of their communications.
NIS1 Directive[1]	Security incidents.	Operators of essential services (OES) and providers of key digital services (DSPs).	OES and DSPs are required to report cybersecurity incidents that have a significant impact on their operations or the provision of their services to their national competent authorities within **24 hours** of becoming aware of them. The initial report should include a brief overview of the incident including its nature and scope, as well as potential impact. Within **72 hours** of the initial report a more detailed report must be provided including a comprehensive analysis of the incident, root causes, mitigation measures taken, and lessons learned. The national competent authority in Ireland is the computer security incident response team in the Department of Communications.	The competent authority may inform the public about individual incidents, or require the digital services provider to do so, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident.

1. *The NIS1 Directive will be replaced from 18 October 2024 by the updated NIS2 Directive (Directive (EU) 2022/2555). NIS2 provides for an incident notification framework which applies to several types of service providers, including providers of publicly available electronic communication services. Once transposed by Member States, its rules will therefore replace those of the NIS1 Directive as well as the EECC above*

Regime	What does it apply to?	Who does it apply to?	Obligation to notify Regulator	Obligation to notify data subjects/users
Consumer Protection Code, 2012 (the CPC)	Errors. It is important to note that a personal data breach or security incident could be considered an error in certain circumstances	Regulated financial services providers	The CPC, a statutory code, contains a section which deals with errors. It provides that a regulated entity must resolve all errors speedily and no later than **six months** after the error was first discovered, including notifying all affected consumers, both current and former, **in a timely manner**, of any error that has impacted or may impact negatively on the cost of the service, or the value of the product, provided, where possible. A personal data breach of security incident could be considered an error in certain circumstances. Where there is an error which affects consumers and this has not been fully resolved, as outlined above, within **40 business days of the date** the error was first discovered a regulated entity must inform the Central Bank, on paper or on another durable medium, within **five business days** of that deadline.	Yes, for consumers
Cross Industry Guidance for Information Technology and Cybersecurity Risks	Cybersecurity incidents	Regulated financial services providers	This guidance requires that regulated financial services providers notify the Central Bank **when it becomes aware** of a cybersecurity incident that could have a significant and adverse effect on the firm's ability to provide adequate services to its customers, its reputation or financial condition.	Yes, in certain circumstances
Law Enforcement Directive	Personal data breaches, same definition as under GDPR	Competent authorities where the processing of personal data is carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, ie law enforcement purposes. This is not limited to processing by bodies who might be typically considered as 'law enforcement authorities', such as An Garda Síochána, but to any processing for law enforcement purposes, carried out by a public or private body who fits the definition of 'competent authority', such as local authorities when prosecuting litter fines, or Dublin Bus regarding ticket offences.	Similar reporting obligations/requirements as the GDPR.	Similar reporting obligations/ requirements as the GDPR

Recent Developments on Data Breach Claims and the Right to Compensation

Deirdre Munnelly
Partner,
Insurance & Risk
dmunnelly@mhc.ie

Colin Monaghan
Partner,
Dispute Resolution
cmonaghan@mhc.ie

The question of what the concept of non-material damage means in data breach claims and when a claimant can recover damages for it has been a hot topic in recent years. Prior decisions from the UK courts indicated that recovery for non-material damage would not be permitted unless a de minimis threshold was met, requiring a minimum level of seriousness of damage to be established. 2023 then saw a number of significant judgments on the issue of non-material damage in GDPR claims which have clarified the position in Ireland and the EU. The CJEU handed down its first judgment on the issue and made it clear that the GDPR and the concept of 'damages' must not be narrowly interpreted, meaning claimants can recover for non-material damage, with no application of a de minimis threshold. Following this, the Irish courts delivered their first judgment on this issue in the case of *Arkadiusz Kaminski v Ballymaguire Foods Limited.* At this stage the Irish courts had the benefit of CJEU guidance and the claimant was successful in recovering damages for embarrassment, sleep loss, and stress which he claimed he suffered because of a data breach.

Just as a degree of certainty seemed to have been reached, the CJEU revisited the issue and delivered two further decisions in December of last year. This saw the expansion of the scope for potential recovery to allow for recovery for 'fear' of future misuse,[1] reputational damage, and loss of confidentiality,[2] while also clarifying that proof of non-material damage is required and confirming that damages in these claims are to be purely compensatory.

We set out these recent developments and a summary of the current, and now-clarified, position in Ireland and the EU regarding non-material damages in GDPR claims.

Prior to 2023, most of the guidance on non-material damage claims came from UK case law. The decision in *Rolfe v Veale Wasbrough Vizards LLP,* which was detailed in our previous article, determined that a minimum threshold of seriousness applied before a claimant could recover for non-material damage. This decision was followed by a decision of the UK Supreme Court in *Lloyd v Google LLC* that determined that damages were not recoverable for a mere loss of control of personal data. These UK decisions generated interest in Ireland and set the scene for some substantial developments in this area.

Decisions stayed pending the first CJEU decision - Irish case, January 2023

The first development in Ireland in 2023 was the case of *Gary Cunniam v Parcel Connect Ltd t/a Fastway Couriers Ireland & Others*,[3] which came before the Irish Circuit Court.

1. *VB v. Natsionalna agentsia za prihodite (C-340/21)*
2. *Krankenversicherung Nordrhein (C-667/21)*
3. *Gary Cunniam v Parcel Connect Ltd t/a Fastway Couriers Ireland & Others [2023] IECC 1*

In this case, the defendant company suffered a third-party hacker attack. The claimant alleged that he had been contacted by unknown third parties, and that he had lost control over his personal data. In addition, the claimant alleged that the damage sustained included interference with his peace and privacy.

After an application by the defendants to stay the proceedings pending CJEU guidance on non-material damage in data breach claims under the GDPR, this claim (along with several similar other claims) was stayed pending the determination of the CJEU in *UI v Osterreichische Post AG*[4]. In granting a stay, the court noted that, even taking the plaintiff's claim at its highest level, damages would likely be small, which suggested that at that stage, the Irish courts agreed with the minimum threshold approach adopted in the UK.

CJEU decision, Post AG, May 2023

The next development came in the form of the CJEU's eagerly awaited judgment in *UI v Osterreichische Post AG.* As summarised, in our previous article, this decision brought some clarity on how non-material damage claims are to be assessed by national courts.

The CJEU determined that:

- A right to compensation for non-material damage does not automatically arise from a mere infringement of the GDPR
- The GDPR does not provide for a de minimis threshold for non-material damage - there is no requirement to meet a threshold which requires a certain degree of seriousness before a claim can succeed, and
- The non-material damage must be causally linked to the alleged data breach

Of particular importance, the CJEU also determined that the assessment of the level of non-material damage is a matter for the national courts of EU Member States to rule upon.

This meant that the Irish position on recovering damages for non-material damage in data breach claims remained uncertain.

First Irish judgment - Kaminski, July 2023

The first Irish judgment[5] on the issue following the *Post AG* decision arrived in July 2023.

In this case, the claimant was employed by a food company at a chilled ready-meal factory. During a training exercise, CCTV clips which purported to highlight unapproved food safety practices were shown to a group of employees. The claimant, who was identifiable in the CCTV footage, alleged that the processing and use of the CCTV footage amounted to unlawful processing of his data and a violation of both the Irish Data Protection Act 2018 and the GDPR.

Regarding the non-material damage suffered, he alleged that it had made him 'more stressed at work', he felt 'humiliated', and he had problems with his sleep for a period of time.

The Irish Circuit Court determined that there are several factors which a court must consider when assessing compensation for non-material damage as follows:

- A mere violation of the GDPR is not sufficient to warrant an award of compensation
- There is no minimum threshold of seriousness required for a claim for non-material damage to exist, but compensation for non-material damage does not cover "mere upset"
- There must be a link between the data infringement and the damage claimed
- Non-material damage must be genuine and not speculative
- Damage must be proved and supporting evidence is strongly desirable
- An apology where appropriate may be considered in mitigation

4. *Case C-300/21 UI v Osterreichische Post AG (the 'Austrian Post Case')*

5. *Arkadiusz Kaminski v Ballymaguire Foods Limited [2023] IECC 5*

- Delay in dealing with a "data breach" by either party is a relevant factor in assessing damages
- A claim for legal costs may be affected by these factors, and
- Even where non-material damage can be proved and is also not trivial, damages in many cases will probably be modest

In determining the appropriate amount of compensation, in the absence of guidance from the Oireachtas, Superior Courts, or the Judicial Council, the court considered the Personal Injuries Guidelines 2021. The court referred to the category of minor psychiatric injuries, though it noted that in some cases non-material damage could be valued below the lowest Guidelines' valuation of €500.

Having considered the facts of the case, Mr Justice O'Connor accepted that Mr Kaminski's reaction to the incident went beyond mere upset and awarded him €2,000.

It is positive that Judge O'Connor referred to awards for non-material damage as being "modest". It is also likely that going forward, most claims of this nature will be more properly issued in the District Court, which follows the January 2024 commencement of Part 10 of the Courts and Civil Law (Miscellaneous Provisions) Act 2023. Costs in these cases would be assessed on the District Court scale, which is substantially lower than costs awarded in the Circuit Court.

What does the future look like – VB and Krankenversicherung, December 2023

The CJEU once again weighed in on this issue when delivering judgments in *VB*[6] *v Natsionalna agentsia za prihodite*[7] and *Krankenversicherung*[8] in December 2023.

In *VB v Natsionalna agentsia za prihodite,* a Bulgarian public body suffered a cyberattack resulting in a data breach which affected more than 6 million data subjects, several hundred of whom sought compensation. VB, the applicant, sought approximately €510 for non-material damage, which she claimed arose from the *fear* that her personal data might be misused in the future and that she might be at risk of blackmail, assault, or kidnap. One of the questions referred by the Bulgarian court to the CJEU was whether the fear of potential misuse of data arising from a data breach constitutes non-material damage.

In its judgment, the CJEU reiterated how non-material damage claims should be assessed, as previously detailed in *Post AG*. The CJEU once again listed the factors necessary to recover compensation under Article 82:

- Damage
- A breach of the GDPR, and
- A causal link between the damage and the breach, and that national law cannot require non-material damage to reach a certain level of seriousness

The CJEU also determined that *"non-material damage"* can include fear of future misuse of a data subject's personal data, as Article 82 GDPR makes no distinction between present and future misuse of personal data. Having considered Recital 146, the CJEU held that fear of future misuse of one's personal data must be capable of amounting to *"non-material damage"* in order to give a broad interpretation to the meaning of damage. The CJEU also referred to Recital 85, which it considered supports the position that mere *"loss of control"* constitutes damage.

However, the CJEU concluded by emphasising that data subjects must demonstrate that the negative consequences suffered constitute non-material damage. As such, national courts are required to verify that the fear can be regarded as well-founded in the specific circumstances.

6. *VB v. Natsionalna agentsia za prihodite (C-340/21)*
7. *VB v. Natsionalna agentsia za prihodite (C-340/21)*
8. *Krankenversicherung Nordrhein (C-667/21)*
9. *Krankenversicherung Nordrhein (C-667/21)*

In *Krankenversicherung*[9] the issue of non-material damage was again addressed by the CJEU[10]. In this case, a medical service provider (MDK) of a health insurance fund in Germany was found to have processed personal data in violation of the GDPR. MDK drew up reports on the capacity to work of individuals insured by the health insurance fund. Reports were also drawn up relating to MDK's own employees. After learning about the existence of such reports, an incapacitated MDK employee sought compensation under Article 82 of the GDPR.

The CJEU noted that violations of the GDPR in processing the personal data of individuals could lead to physical, material or non-material damage, which could result in data subjects suffering from issues relating to discrimination, identity theft, fraud, reputational damage, loss of confidentiality, or any other significant social harm.

The CJEU also reiterated that Article 82 of the GDPR does not require a certain degree of seriousness for claimants to be able to recover damages i.e., a *de minimis* threshold. The CJEU held that Article 82 requires that the amount recoverable should be determined in such a way as to compensate the claimant in full for the damage actually suffered. This is a helpful takeaway as the CJEU clarified that the right to compensation is purely compensatory and is not punitive in nature. This means that claimants must demonstrate that they actually suffered the alleged damage, whether material or non-material.

Conclusion

Overall, these are positive and welcome developments as the relevant judgments confirm that, despite the possibility of recovery for non-material damage for various types of emotional distress, claimants must now verify that they actually suffered the alleged upset claimed. This means that claimants will now need to produce evidence of some kind to substantiate that they have suffered non-material damage. In addition, the award recoverable by a claimant is unlikely to be significant in value. As clarified in the latest CJEU decision, the right to compensation is purely compensatory. This means that the award will not be punitive and will be calculated by reference to the amount of non-material damage that has actually been suffered.

9. *Krankenversicherung Nordrhein (C-667/21)*
10. *Please note that no official English translation of this judgment is yet available. As such, we've relied on a rough machine translation for the purposes of this blog post*

About us

Our Multidisciplinary Incident Response Team consists of lawyers from our Privacy & Data Security, Public Law and Dispute Resolution Teams.

The team has significant expertise working with clients on all issues around national and cross-border security incidents and personal data breaches at each stage of the journey - from Data Breach Readiness, Incident Response Management, DPC Investigations and Inquiries and Litigation and Dispute Resolution.

Our team has experience across the entire incident response regulatory regime including the GDPR, the NIS Directive, ePrivacy, the Telecoms Framework and the Law Enforcement Directive.

What others say about us

Our Privacy & Data Security Team

"...always go over and above, no matter the issue. They have a wonderful ability to turn advice on complex points around quickly and concisely."

Chambers & Partners, 2023

Our Privacy & Data Security Team

Noted for its "ability to zoom out and focus on the strategic elements of how to approach an issue."

Possesses "unique levels of experience."

Legal 500 2023

Key contacts

Philip Nolan
Partner, Head of Privacy & Data Protection
+353 86 812 4140
pnolan@mhc.ie

Catherine Allen
Partner, Public, Regulatory & Investigations
+353 86 382 1009
callen@mhc.ie

Julie Austin
Partner, Privacy & Data Security
+353 86 137 2136
jaustin@mhc.ie

Declan Black
Partner, Dispute Resolution
+353 86 811 4853
dblack@mhc.ie

Deirdre Munnelly
Partner, Insurance
+353 86 828 9546
dmunnelly@mhc.ie

Colin Monaghan
Partner, Dispute Resolution
+353 87 798 3777
cmonaghan@mhc.ie

Jevan Neilan
Head of San Francisco Office
+1 415 740 0480
jneilan@mhc.ie