International
Comparative
Legal Guides

# Cybersecurity

# 2024

## Sixth Edition

Contributing Editor:
Edward R. McNicholas
Ropes & Gray LLP

glg Global Legal Group

# Expert Analysis Chapters


1 **Generative AI & Cyber Risk in China**
Susan Ning & Han Wu, King & Wood Mallesons

7 **Generative AI & Cyber Risk in India**
Shahana Chatterji, Hemant Krishna, Shashank Mishra & Punya Varma, Shardul Amarchand Mangaldas & Co


# Q&A Chapters


15 **Argentina**
Marval O'Farrell Mairal: Diego Fernández

23 **Australia**
Nyman Gibson Miralis: Dennis Miralis, Jasmina Ceic & Mohamed Naleemudeen

32 **Belgium**
Agio Legal: Steven De Schrijver

43 **Canada**
Baker McKenzie: Theo Ling, Conrad Flaczyk, Ahmed Shafey & John Pirie

54 **China**
King & Wood Mallesons: Susan Ning & Han Wu

67 **Denmark**
Sky Law Advokatfirma: Niels Skyttedal Dahl-Nielsen & Victoria Elmgren

75 **England & Wales**
Ropes & Gray LLP: Rohan Massey, Edward Machin & Robyn B. Bond

86 **Finland**
Borenius Attorneys Ltd: Erkko Korhonen & Floora Kukorelli

92 **Germany**
Eversheds Sutherland: Dr. Alexander Niethammer, Dr. David Rieks, Stefan Saerbeck & Isabella Norbu

101 **Greece**
Nikolinakos & Partners Law Firm: Dr. Nikos Th. Nikolinakos, Dina Th. Kouvelou & Alexis N. Spyropoulos

113 **India**
LexOrbis: Puja Tiwari & Srinjoy Banerjee

122 **Ireland**
McCann FitzGerald LLP: Adam Finlay & Ruth Hughes

130 **Italy**
Paradigma – Law & Strategy: Chiara Bianchi & Giorgia Bevilacqua

140 **Japan**
Mori Hamada & Matsumoto: Hiromi Hayashi, Masaki Yukawa & Daisuke Tsuta

150 **Nigeria**
S.P.A. Ajibade & Co.: John C. Onyido, Sandra Eke, Franklin Okoro & Maryam Abdulsalam

159 **Portugal**
CS'Associados: Jorge Silva Martins, Inês Coré, Joana Avelino Gomes & João Carminho

167 **Singapore**
Drew & Napier LLC: Lim Chong Kin, David N. Alfred & Albert Pichlmaier

178 **Sweden**
TIME DANOWSKY Advokatbyrå AB: Jonas Forzelius, Esa Kymäläinen & Jesper Jakobsson

186 **Taiwan**
Hsu & Associates: Steven Hsu

194 **Thailand**
Silk Legal Co., Ltd.: Dr. Jason Corbett & Don Sornumpol

201 **USA**
Ropes & Gray LLP: Edward R. McNicholas & Kevin J. Angle

# Ireland


Adam Finlay

Ruth Hughes

McCann FitzGerald LLP


## 1 Cybercrime

**1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction: hacking; denial-of-service attacks; phishing; infection of IT systems with malware; distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime; possession or use of hardware, software or other tools used to commit cybercrime; identity theft or identity fraud; electronic theft; unsolicited penetration testing; or any other activity adversely affecting or threatening the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:**

**Hacking**

Yes, under section 2 of the Criminal Justice (Offences Relating to Information Systems) Act 2017 (the "**2017 Act**"), a person who, without lawful authority or reasonable excuse, intentionally accesses an information system by infringing a security measure is guilty of an offence.

**Denial-of-service attacks**

Yes, under section 3 of the 2017 Act, a person who, without lawful authority, intentionally hinders or interrupts the functioning of an information system by:

(a) inputting data on the system;

(b) transmitting, damaging, deleting, altering or suppressing, or causing the deterioration of, data on the system; or

(c) rendering data on the system inaccessible,

is guilty of an offence.

**Phishing**

Phishing does not, of itself, constitute an offence under Irish law. However, depending on the circumstances, the practice of phishing (which involves sending fraudulent communications that appear to come from a legitimate source, generally through email or text message, in a bid to induce the recipient to reveal personal data or make payments) may be caught by more general criminal legislation relating to identify theft or fraud (see below).

**Infection of IT systems with malware**

The infection of IT systems with malware may be an offence under section 4 of the 2017 Act, which provides that any person who, without lawful authority, intentionally deletes, damages, alters or suppresses, or renders inaccessible, or causes the deterioration of data on an information system is guilty of an offence.

**Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime**

The distribution, sale or offer for sale of any malware or other tool used to commit cybercrime is an offence under section 6 of the 2017 Act. Any individual who, without lawful authority, intentionally produces, sells, procures for use, imports, distributes, or otherwise makes available, for the purpose of the commission of an offence under the 2017 Act:

(a) any computer programme that is primarily designed or adapted for use in connection with the commission of such an offence; or

(b) any device, computer password, unencryption key or code, or access code, or similar data, by which an information system is capable of being accessed,

is guilty of an offence.

**Possession or use of hardware, software or other tools used to commit cybercrime**

Possession or use of hardware, software or other tools to commit cybercrime is also an offence under section 6 of the 2017 Act, as set out above.

**Identity theft or identity fraud**

There is no specific provision under Irish law that provides that identify theft or identify fraud constitutes an offence. However, such behaviour is potentially caught by section 6 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (the "**2001 Act**"), which prohibits making gain or causing loss by deception. In addition, section 25 of the 2001 Act provides that a person is guilty of forgery if he or she makes a false instrument with the intention that it shall be used to induce another person to accept it as genuine and, by reason of so accepting it, to do some act, or to make some omission, to the prejudice of that person or any other person.

Separately, when a court is determining the sentence to be imposed on a person in relation to a denial-of-service attack or the infection of an IT system with malware (see above), section 8 of the 2017 Act provides that identity theft or fraud is an aggravating factor.

**Electronic theft**

There is no specific provision under Irish law that expressly deals with electronic theft. However, section 9 of 2001 Act provides for the relatively broad offence of "unlawful use of a computer", which occurs where a person dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State, with the intention of making a gain for himself or herself or another, or of causing loss to another.

**Unsolicited penetration testing**

There is no specific provision under Irish law that expressly deals with unsolicited penetration testing. However, if such

penetration testing was executed maliciously by a third party, it may fall under Section 2 of the 2017 Act (see "Hacking" above).

**Any other activity adversely affecting or threatening the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network device or data**

Under section 5 of the 2017 Act, it is an offence to intercept the transmission of data from or within an information system without lawful authority.

Under section 145 of the Data Protection Act 2018 (the "**DPA**"), it is an offence for a person to, without the authority of the controller or processor of any personal data, obtain such personal data and disclose it to another person.

Under section 98 of the Postal and Telecommunications Services Act 1983 (the "**1983 Act**"), subject to limited exceptions, it is an offence for a person to intercept or attempt to intercept telecommunications messages being transmitted by a telecommunications company.

**Penalties**

For offences under the 2017 Act, the penalties range from imprisonment for up to one year and a maximum fine of €5,000 for charges brought "summarily" (i.e., for less serious offences), to imprisonment for up to five years (or 10 years in the case of denial-of-service attacks) and an unlimited fine for more serious offences.

As regards offences under the 2001 Act, the offence of "making a gain or causing a loss by deception" carries a maximum penalty of five years' imprisonment and an unlimited fine. The offences of forgery and "unlawful use of a computer" carry a maximum penalty of 10 years' imprisonment and an unlimited fine.

For an offence under section 145 of the DPA or section 98 of the 1983 Act, the penalties range from imprisonment for up to one year and a maximum fine of €5,000 for charges brought summarily, to imprisonment for up to five years and a maximum fine of €50,000 for more serious offences.

**Prosecutions**

There have been very few successful prosecutions under any of the legislative provisions mentioned above.

In 2022, there were media reports that an individual prosecuted for intentionally accessing an information system without lawful authority or reasonable excuse by infringing a security measure under sections 2 and 3 of the 2017 Act was the first person to be prosecuted under the 2017 Act. The prosecution arose from an investigation into the hacking of a computer parking system.

**1.2 Do any of the above-mentioned offences have extraterritorial application?**

Yes, offences under the 2017 Act have extra territorial application. Section 10 of the 2017 Act provides that a person may be prosecuted in Ireland under the 2017 Act in relation to an act committed:

(a) by the person in Ireland in relation to an information system outside of Ireland;
(b) by the person outside of Ireland in relation to an information system in Ireland; or
(c) by the person outside of Ireland in relation to an information system outside of Ireland if:
  a. the person is:
    i. an Irish citizen;
    ii. a person ordinarily resident in Ireland;
    iii. a body corporate established under the law of Ireland;
    iv. a company formed and registered under the Companies Act 2014;
    v. an existing company within the meaning of the Companies Act 2014; and
  b. the act is an offence under the law of place where the act was committed.

**1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?**

As in the case of any criminal offence (other than strict liability offences), a person will not be guilty of any of the above offences if they did not have the requisite intent. For offences under the 2017 Act, the requisite intent generally relates to the prohibited act (i.e. intentionally accessing an information system by infringing a security measure; intentionally deleting, damaging, etc. data on an information system, etc.). The absence of intent to make a financial gain would generally not be a defence (since it would not be necessary to prove intention to make such a gain in order to prosecute the offence).

In order to be guilty of an offence under the 2017 Act, a person must engage in the relevant activity without "*lawful authority*". Accordingly, acting with lawful authority is a defence to these offences. Similarly, an offence under section 145 of the DPA will not arise where the relevant person acted with the authority of the controller or processor of the personal data in question.

A company can be charged with an offence under the 2017 Act that was committed by an officer or employee for the benefit of the company, on the basis that the offence was attributable to the failure by a manager or officer of the company to exercise, at the time of the commission of the relevant offence, the requisite degree of supervision or control of the relevant person. Where this happens, a potential defence for that company would be to prove that it took "*all reasonable steps and exercised all due diligence*" to avoid the offence being committed.

## 2 Cybersecurity Laws

**2.1 *Applicable Laws*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, trade secret protection laws, data breach notification laws, confidentiality laws, and information security laws, among others.**

In addition to the 2017 Act and the 2001 Act referenced above, the following laws are relevant to cybersecurity in Ireland:

- **Data Protection**: The General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**") applies in Ireland and is supplemented by the DPA. Under the GDPR, controllers and processors of personal data are required to take appropriate security measures to protect against unauthorised access to, alteration, disclosure or destruction of personal data. Controllers are also obliged, in certain circumstances, to notify the Data Protection Commission (the "**DPC**") and affected data subjects of any personal data breaches.
- **e-Privacy**: The e-Privacy Regulations 2011 (S.I. 336 of 2011), which transpose the e-Privacy Directive 2002/58/EC (as amended by Directives 2006/24/EC and

2009/136/EC) in Ireland (the "**e-Privacy Regulations**") require providers of publicly available telecommunications networks or services to implement appropriate technical and organisational measures to safeguard the security of their services.

- **Network and Information Systems**: The Security of Network and Information Systems Directive 2016/1148/EU (the "**NIS Directive**") was transposed in Ireland by the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 (the "**NIS Regulations**"). The main objective of the NIS Directive, which applies to operators of essential services, is to ensure that there is a common high-level security of network and information systems across EU Member States. The NIS Directive will be replaced by the Directive 2022/2555 (the "**NIS2 Directive**"), which was adopted by the EU in 2022 and is due to be transposed in Ireland by 17 October 2024.
- **Payment Services**: The Payments Services Directive II (Directive 2015/2366/EU or "**PSD2**") was transposed by the European Union (Payment Services) Regulations 2018 (S.I. 6 of 2018) (the "**Payment Services Regulations**"). Under the Payment Services Regulations, payment service providers are required to inform the national competent authority in the case of major operational or security Incidents.

**2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?**

Yes. The NIS Regulations require operators of essential services (i.e. operators in the energy, healthcare, financial services, transport, drinking water supply and digital infrastructure sectors) to have in place a level of security proportionate to the risks posed to the security of the network and information systems it uses to run its operations. This would include network and information systems that its material service providers use to deliver services to such operators of essential services. This security framework must have two elements:

i. management of risks to security; and
ii. prevention and minimisation of the impact of Incidents affecting security, with a view to ensuring continuity.

The implementation of an NIS-compliant security framework requires a balancing of the risks posed to the security of network and information systems as against the state of the art in terms of security.

The Department of Communications, Climate Action and the Environment has published NIS Compliance Guidelines for operators of essential services. The Guidelines set out the following core principles in terms of NIS security requirements for an operator of essential services:

- Identify – develop a risk management framework.
- Protect – develop policies and procedures and appropriate training to staff.
- Detect – ensure consistent monitoring.
- Respond – develop a procedure on responding to potential cyber Incidents.
- Recover – develop a recovery planning framework.

**2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.**

Yes. Organisations are subject to the following obligations under laws applicable in Ireland in relation to the monitoring, detection, prevention and mitigation of Incidents:

- **Data Protection**
  Under Article 32 of the GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, controllers are obliged to ensure risk-based security measures are implemented and maintained against unauthorised access to, alteration, disclosure or destruction of personal data. Potential measures in this regard mentioned in the GDPR include:
  - the pseudonymisation and encryption of personal data;
  - the ability to ensure the confidentiality, integrity, availability and resilience of processing systems;
  - the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical Incident; and
  - the regulator testing of security measures.

  Under Article 35 of the GDPR, a controller is required to carry out a data protection impact assessment prior to carrying out high-risk processing.
  Controllers are also obliged to have regard to the principle of data protection by design and by default when determining how personal data will be processed. This means that controllers are required to implement appropriate technical and organisational measures that are designed to comply with key data protection principles, and to integrate necessary safeguards into these to ensure protection for the data subject's rights and freedoms.
- **e-Privacy**
  Under the e-Privacy Regulations, providers of publicly available telecommunications networks or services are required to take appropriate technical and organisational measures to safeguard the security of their services. These measures include:
  - ensuring that personal data can only be accessed by authorised personnel for legally authorised purposes;
  - protecting personal data against accidental or unlawful destruction, loss, alteration, processing, etc.; and
  - ensuring the implementation of a security policy in relation to the processing of personal data.
- **Network and Information Systems**
  Under the NIS Regulations, operators of essential services and digital service providers are required to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems that they use in the context of offering services. Such measures must ensure a level of security appropriate to the risk posed and take into account a number of elements, including the security of systems and facilities, Incident handling, business continuity management, monitoring, auditing and testing, and applicable compliance with international standards.

**2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.**

- Under the GDPR, controllers are required to report personal data breaches to the DPC within 72 hours of becoming aware of such a breach occurring, except where the breach is unlikely to result in a risk to the rights and freedoms of the affected data subjects. This notification must include specific details such as type of breach, the number of data subjects concerned, and a proposed remedy. The DPC has published guidelines on data breach notification.
- Under the NIS Regulations, operators of essential services have notification obligations in respect of Incidents that have a "significant impact" on the continuity of an essential service. In deciding whether an Incident has a "significant impact", the operator of the essential service must consider the number of users affected by the disruption, the duration of the Incident and the geographical spread of the area affected. Incidents should be reported within 72 hours of becoming aware of the Incident to the National Cyber Security Centre, which encompasses Ireland's National/Governmental Computer Security Incident Response Team (the "**CSIRT**").
- Under the e-Privacy Regulations, providers of the electronic communications networks and services must notify the Commission for Communications Regulations ("**ComReg**") in the event of such a breach having a significant impact on networks or services.
- Under the Communications Regulation and Digital Hub Development Agency Amendment Act 2023, a provider of public electronic communications networks and services is obliged to notify ComReg of any security Incident that has had or is having a significant impact on the operation of the provider's network or services.
- Under guidance published by the Central Bank of Ireland, regulated firms are required to notify the Central Bank when they become aware of an IT 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.
- Under section 19 of the Criminal Justice Act 2011, it is an offence for a person to fail, without reasonable excuse, to disclose information relating to certain categories of criminal offences to An Garda Síochána (the Irish police force), where the person knows or believes that information might be of material assistance in preventing the commission of such an offence or securing the apprehension, prosecution or conviction of any person for such an offence.

**2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.**

Yes, in certain circumstances. Under Article 34 of the GDPR, controllers are required to notify data subjects of a personal data breach without undue delay where the breach is likely to result in a high risk to the rights and freedoms of the affected data subjects.

Under the ePrivacy Regulations, in the case of a particular risk of a breach to the security of a public communications network, providers of such networks are required to inform their subscribers concerning such risk without delay and, where the risk lies outside the scope of the measures to be taken by the relevant service provider, any possible remedies including an indication of the likely costs involved.

**2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.**

Please see responses to questions 2.4 and 2.5 above.

**2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?**

- If a controller is not compliant with its obligations under the GDPR (including its obligations in relation to the security of personal data and the notification of personal data breaches to the DPC and affected data subjects), it is potentially exposed to significant fines (up to the greater of €20 million or 4% of the annual worldwide turnover of the relevant undertaking), regulatory enforcement actions by the DPC and/or claims for compensation by data subjects.
- If the DPC determines that a breach of the ePrivacy Regulations has occurred, it does not have the power to impose any specific sanction for such a breach. However, it could issue an enforcement notice or information notice and a failure to comply with such notice would constitute a criminal offence. Indictable offences can result in a fine of up to €250,000. If a person is convicted of an offence, the Court may order any material or data that appears to it to be connected with the commission of the offence to be forfeited or destroyed and any relevant data to be erased.
- Under the NIS Regulations, failure by an operator of an essential service or a digital service provider to notify an Incident is an offence and an offender may be liable to a fine of up to €500,000.
- Under the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023, failure by a provider of public electronic communications networks and services to notify ComReg of any Incident of significant impact on networks or services is an offence and an offender is liable on summary conviction to a class A fine.

**2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.**

Most enforcement activities in relation to the above-mentioned requirements have been taken either by the DPC or by the Central Bank of Ireland.

The DPC publishes details of its decisions arising from its enforcement activities, and any subsequent related decisions by courts in respect of appeals against the DPC's decisions, on its website – https://www.dataprotection.ie. Recent decisions by the DPC regarding inquiries it conducted to determine whether organisations had complied with their security and personal data breach reporting obligations include:

- a decision adopted in February 2023 in relation to a ransomware attack on Centric Health, where the DPC decided that Centric Health failed to comply with its security and reporting obligations and imposed a fine of €460,000;
- a decision adopted in February 2023 in relation to security issues regarding Bank of Ireland's banking app, where the DPC decided that Bank of Ireland failed to comply with its security and reporting obligations and imposed a fine of €750,000;
- a decision adopted in December 2022 in relation to a security Incident at Fastway Couriers, where the DPC decided that Fastway Couriers failed to comply with its security and reporting obligations and imposed a fine of €15,000; and
- a decision adopted in March 2022 in relation to security measures of Meta, where the DPC decided that Meta failed to comply with its security obligations and imposed a fine of €17 million.

## 3 Preventing Attacks

**3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems): (i) beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content); (ii) honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data); or (iii) sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)?**

There is no specific prohibition on the use of beacons, honeypots or sinkholes under Irish law. However, any organisation considering implementing any of these measures would need to consider how to do so in compliance with relevant requirements under applicable laws, such as the GDPR and the ePrivacy Regulations.

**3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?**

Under the ePrivacy Regulations, the listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users without the consent of the users concerned is prohibited. Neither "interception" nor "surveillance" is defined for these purposes. However, it is likely that monitoring or intercepting the email and internet usage of employees, for example, without consent of the users (i.e. the sender and the recipient) would be contrary to Regulation 5 of the ePrivacy regulations. For the purpose of the ePrivacy Regulations, "consent" is generally construed to mean "consent" as envisaged by the GDPR.

Under section 98 of the 1983 Act, subject to limited exceptions, it is an offence for a person to intercept or attempt to intercept telecommunications messages being transmitted by a telecommunications company without the consent of either the sender or the recipient of the message.

**3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?**

Irish law does not specifically restrict the import or export of technology designed to prevent or mitigate the impact of cyber-attacks. However, the export of dual-use items is regulated by European and Irish law. Dual-use items are products, including software and technology, which can be used for both civil and military purposes. For controlled items, a licence from the Trade Licensing and Control Unit of the Department of Business, Enterprise and Innovation is required prior to exporting such items.

## 4 Specific Sectors

**4.1 Do legal requirements and/or market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.**

Yes, legal requirements vary and market practice in relation to information security also varies across different business sectors.

Some legal requirements (such as those set out in the GDPR) apply to all sectors, while others are sector-specific (e.g. there are additional legal and regulatory requirements in the financial services sector).

Market practice varies from one sector to another partly due to differences in the applicable legal requirements and also partly due to the nature of the data processed in different sectors. For example, market practice in the health sector is reflective of the fact that data processed in this sector is more sensitive than that processed in other sectors.

**4.2 Excluding the requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services, health care, or telecommunications)?**

Yes, there are additional sector-specific requirements in certain sectors. For example:

- there are additional laws and guidelines regarding cybersecurity measures that apply in the financial services sector, which are generally enforced by the Central Bank of Ireland;

- there are additional legal requirements regarding the security of health information that apply in the healthcare sector; and
- as mentioned above, telecommunication service providers are subject to obligations under the ePrivacy Regulations and other laws applicable to them that do not apply more generally.

## 5 Corporate Governance

**5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?**

Directors owe a fiduciary duty of care to their company under both common law and the Companies Act 2014, as well as a general duty to identify, manage and mitigate risk. In relation to cybersecurity, such duties are likely to be interpreted to mean that directors should ensure that their company has appropriate policies and procedures in place to address cybersecurity risks and complies with relevant obligations under applicable law.

**5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?**

There are no such express obligations under Irish company law. However, as a matter of good corporate governance and in order to ensure compliance with other laws applicable to the relevant company (such as data protection law, any sector-specific laws, etc.), it would be prudent for a company to consider implementing some or all of these actions.

**5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?**

There are no specific disclosure requirements under Irish company law. However, disclosure may be required in certain circumstances in accordance with general director fiduciary duties and good corporate governance or, specifically in relation to publicly listed companies, in respect of price-sensitive information.

## 6 Litigation

**6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.**

In the event of an Incident, the potential actions that may be brought would depend on the circumstances, including the relationship between the potential claimant and the organisation who suffered the Incident. Potential causes of action would include:

- breach of contract (if the Incident entailed a breach of a contract between the claimant and the relevant organisation);
- tort of negligence (if the required elements of a claim for negligence, i.e. a duty of care, breach of that duty, causation and damages, were present);
- data protection action (if the Incident entailed a breach of data protection law and the claimant suffered material or non-material damage as a result);
- breach of privacy; and
- breach of confidence (if the required elements of a claim for breach of confidence were present).

**6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.**

The recent cases of *Garry Cunniam v Parcel Connect Ltd t/a Fastway Couriers [2023] IECC 1* and *Kaminski v Ballymaguire Foods Limited [2023] IECC 5* provide useful guidance on the view of the Irish courts in relation data protection claims for non-material damage brought under Article 82 of the GDPR and Section 117 of the DPA.

The Fastway Couriers case involved a cyber-attack (hacking) Incident suffered by the defendant organisation, which resulted in a data breach and the personal information of approximately 450,000 people being leaked, with a number of claims being brought against the defendant by several data subjects. The plaintiff in this case claimed to have suffered what amounted to "non-material" damage, which typically would not be recoverable as a matter of Irish law but which may entitle a plaintiff to compensation specifically where compensation is sought in a claim made under Article 82 GDPR and Section 117 of the DPA. The defendant sought and was granted a stay in these proceedings, since questions regarding the interpretation of Article 82 of the GDPR and the entitlement to compensation for non-material damage that had been referred to the Court of Justice of the European Union (the "**CJEU**") were, at the time, awaiting decisions by the CJEU.

On 4 May 2023 the CJEU published its decision in case *C-300/21 – UI v Österreichische Post AG* and addressed some key questions regarding the interpretation of Article 82. The CJEU held that: (i) mere violation of the GDPR does not confer a right to compensation; (ii) there is no minimum "threshold of seriousness" required in respect of an entitlement to compensation for non-material damage; and (iii) since the GDPR does not prescribe any rules for the assessment of damages, it is a matter for the legal system of each EU Member State to determine the criteria for assessing the extent of the compensation payable for non-material damage, subject to compliance with the principles of equivalence and effectiveness.

Following this, on 11 July 2023, the Irish Circuit Court published its decision in the *Kaminski v Ballymaguire Foods* case, which was the first written judgment in Ireland addressing the question of non-material damage under Article 82 of the GDPR. While this case did not relate to a cybersecurity Incident, it is noteworthy that the Court:

- was of the view that the appropriate level of compensation in many cases for non-material damage will be "modest";
- in the absence of guidelines from the Oireachtas (Irish Parliament), the Superior Courts and/or the Judicial Court, the Court took into account the factors outlined in the Judicial Council Personal Injuries Guidelines 2021 in respect of minor psychiatric damages as instructive guidance; and
- based on the facts of this specific case, awarded the plaintiff €2,000 for the non-material damage suffered.

**6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?**

Yes, further to question 6.1 above, depending on the circumstances, there would be potential liability in negligence.

## 7 Insurance

**7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?**

Yes, cyber insurance is available in Ireland and typically organisations will have some form of cyber insurance in place.

As in the case of all types of insurance, any cyber insurance policy will have certain exclusions and limits regarding what it covers.

**7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?**

No, there are no regulatory limitations to insurance coverage against specific types of loss. However, the common law principle of *ex turpi causa non oritur actio* (i.e. no action can arise from an illegal act) applies in Ireland and it is arguable that this could, in specific circumstances, operate in a way that would prevent an insured party from recovering under an insurance policy. For example, if an insured party incurred an administrative fine imposed by a data protection authority for a breach of the GDPR, then, depending on the circumstances, it may be arguable that the insured party should not be able to recover the amount of the fine under its cyber insurance policy.

**7.3 Are organisations allowed to use insurance to pay ransoms?**

There is no legislation in Ireland that specifically prohibits the payment of a ransom by a victim of a cyber-attack (whether out of the proceeds of an insurance claim or otherwise). However, both the National Cyber Security Centre and the Garda National Cyber Crime Bureau have taken the position that, generally, ransoms should not be paid and there is a risk that paying such a ransom could entail committing an offence under applicable sanctions, terrorism financing or anti-money laundering laws.

In Ireland, where a ransom victim believes that it has been the victim of a criminal offence, it should consider whether that offence ought to be reported to An Garda Síochána under section 19 of the Criminal Justice Act 2011. This provides that it is an offence for a person to fail, without reasonable excuse, to disclose information relating to certain categories of criminal offence to An Garda Síochána, where the person knows or believes that information might be of material assistance in preventing the commission of such an offence or securing the apprehension, prosecution or conviction of any person for such an offence.

## 8 Investigatory and Police Powers

**8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. anti-terrorism laws) that may be relied upon to investigate an Incident.**

An Garda Síochána has the authority to investigate cybercrime and cybersecurity Incidents under a number of pieces of legislation, which include the 2017 Act, the 2001 Act and the Criminal Justice (Miscellaneous Provisions) Act 1997. A specialised division of the force, the Garda National Cyber Crime Bureau, investigates computer crime and specialises in digital forensics. An Garda Síochána can obtain a warrant that would permit the seizure of anything (e.g. hardware, records, etc.) and/or can obtain a production order requiring the production of material that is believed to be evidence of, or to relate to, the commission of specified categories of offences.

Under the DPA and the GDPR, the DPC has broad powers to investigate potential breaches of data protection law, including breaches of security obligations or obligations regarding handling Incidents.

Other regulatory authorities have investigatory powers that could be used to investigate Incidents that occurred in respect of organisations who are subject to the relevant authority's jurisdiction. For example, the Central Bank of Ireland has investigatory powers that could be used to investigate whether entities it regulates in the financial services sector complied with their obligations under applicable financial services laws and regulations in respect of an Incident.

**8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?**

There is no requirement under Irish law for organisations to implement backdoors in their IT systems. Under the 2017 Act, An Garda Síochána can, when acting under the authority of a warrant issued under the 2017 Act, require any person to provide any password or encryption key necessary to operate a computer or to unencrypt information accessible via that computer.

**Adam Finlay** is a partner in McCann FitzGerald's market-leading Technology & Innovation group. Adam advises on a wide range of data protection, information technology, intellectual property, cybersecurity and outsourcing issues. His clients include international and domestic market leaders, innovative disruptors and regulatory bodies. He acts as a trusted advisor to clients on all aspects of data protection and e-privacy law and compliance strategies, with a particular focus on providing sector-specific and commercial advice.

**McCann FitzGerald LLP**
Riverside One
Sir John Rogerson's Quay
Dublin 2

Tel: +353 1 607 1795
Email: Adam.Finlay@mccannfitzgerald.com
URL: www.mccannfitzgerald.com

**Ruth Hughes** is a senior associate in McCann FitzGerald's market-leading Technology & Innovation group. She has significant experience advising clients in the private and public sectors on a wide range of commercial contract, IT outsourcing, intellectual property, data protection, cybersecurity and freedom of information matters and also provides specialist advice in the areas of advertising and food law.

**McCann FitzGerald LLP**
Riverside One
Sir John Rogerson's Quay
Dublin 2

Tel: +353 1 607 1482
Email: Ruth.Hughes@mccannfitzgerald.com
URL: www.mccannfitzgerald.com

With almost 600 people, including 480 lawyers and professional staff, McCann FitzGerald LLP is one of Ireland's premier law firms.

McCann FitzGerald LLP offers expert, forward-thinking legal counsel to clients in Ireland and internationally. The firm's deep knowledge spans a range of industry sectors, enabling tailored solutions to fit clients' specific needs. Clients are principally in the corporate, financial and business sectors but the firm also advises government entities and state bodies.

McCann FitzGerald LLP is based in Dublin (the firm's principal office), London, New York and Brussels (the firm is the only Irish law firm to have an office at the EU's principal base). The firm is divided broadly into four main groupings of corporate, finance, disputes and real estate and construction. McCann FitzGerald LLP also operates industry sector and specialist practice groups, which comprise professionals from different groupings.

www.mccannfitzgerald.com

McCann FitzGerald

# International Comparative Legal Guides

The **International Comparative Legal Guide** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

**Cybersecurity 2024** features two expert analysis chapters and 21 Q&A jurisdiction chapters covering key issues, including:

- Cybercrime
- Cybersecurity Laws
- Preventing Attacks
- Specific Sectors
- Corporate Governance
- Litigation
- Insurance
- Investigatory and Police Powers

The International Comparative Legal Guides are published by: glg Global Legal Group