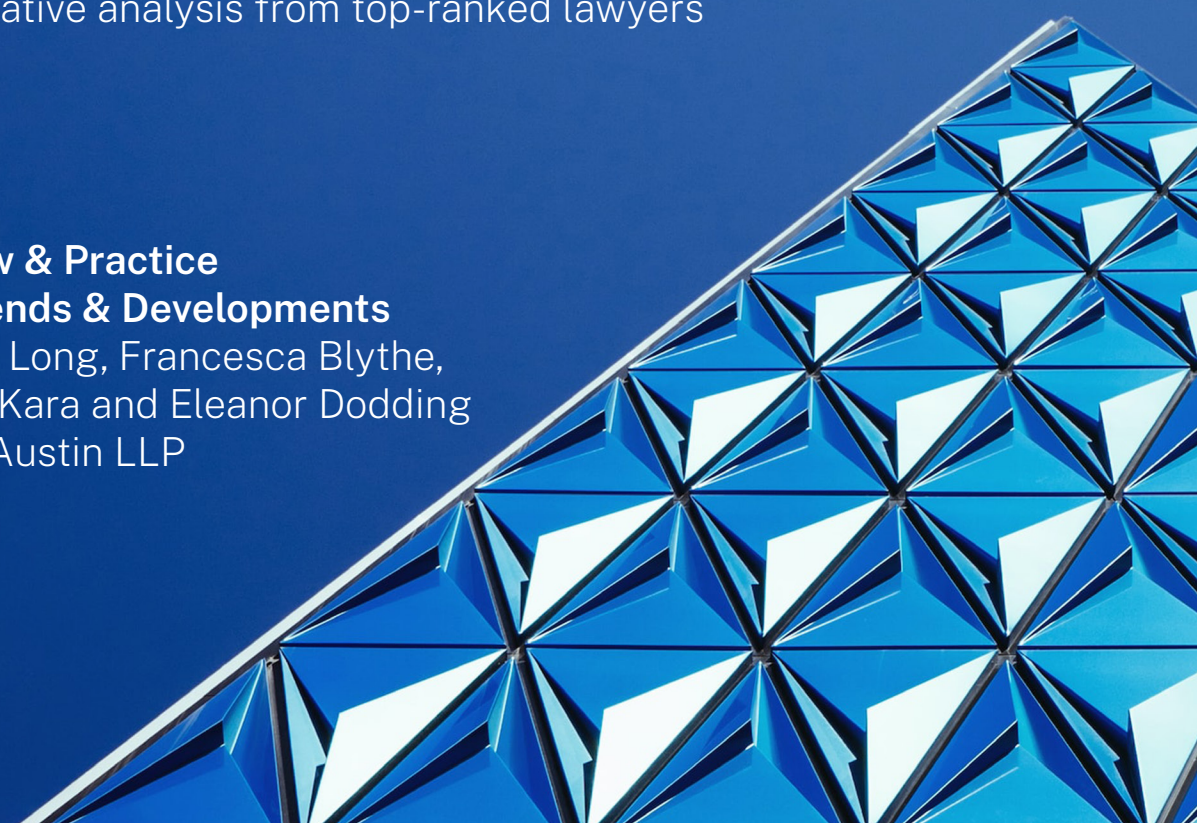
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2024

Definitive global law guides offering comparative analysis from top-ranked lawyers



UK: Law & Practice and Trends & Developments

William Long, Francesca Blythe, Denise Kara and Eleanor Dodding
Sidley Austin LLP

UK

Law and Practice

Contributed by:
William Long, Francesca Blythe, Denise Kara and Eleanor Dodding
Sidley Austin LLP

Contents

Sidley Austin LLP is a premier global law firm with a practice highly attuned to the ever-changing international landscape. The firm advises clients around the globe, with more than 2,300 lawyers in 21 offices worldwide. Sidley Austin maintains a commitment to providing quality legal services and to offering advice on litigation, transactional and regulatory matters spanning virtually every area of law. The firm's lawyers have wide-reaching legal backgrounds and are dedicated to teamwork, collaboration, and superior client service – helping a range of businesses address some of the most challenging matters concerning data protection, privacy, information security and incident response, data commercialisation, internet and computer law, IP, information management and records retention, e-commerce, consumer protection, and cybercrime. The firm advises clients with extensive operations in Europe, as well as in the USA, Asia and elsewhere, on developing and implementing global data protection programmes.

Authors

William Long is a partner at Sidley Austin LLP, where he leads the EU and UK data protection practice and is global co-leader of the firm's highly ranked privacy and cybersecurity practice. William advises international clients on a wide variety of General Data Protection Regulation (GDPR), data protection, privacy, information security, social media, e-commerce and other regulatory matters. He has been a member of the European Advisory Board of the International Association of Privacy Professionals (IAPP) and on the DataGuidance panel of data protection lawyers. William is also on the editorial board of e-Health Law & Policy and assists with dplegal, which is a network for privacy professionals.

Francesca Blythe is a partner at Sidley Austin LLP and advises international clients on a wide range of data protection, privacy, and cybersecurity issues. She has in-depth experience in a number of industries, including asset management and private equity, payments, technology, e-commerce, and manufacturing. Francesca has a particular focus on life sciences, where she advises on a broad range of issues – for example, in relation to real-world evidence and secondary research, clinical studies/investigations, digital health, and use of novel technologies (including AI).

Denise Kara is a senior managing associate at Sidley Austin LLP. She advises international clients on a wide range of data protection, privacy, and cybersecurity matters, including in relation to the General Data Protection Regulation (GDPR), e-privacy laws, the EU's Network & Information Systems (NIS) Directive, and international data transfers (including compliance with Schrems II and the EU–US Data Privacy Framework). Denise assists clients in preparing for, and responding to, sophisticated cybersecurity incidents. Her practice has a particular focus on transactional matters and deal counselling for M&A related to privacy, cybersecurity and data protection compliance, as well as risk mitigation and integration planning strategies.

Eleanor Dodding is a senior managing associate at Sidley Austin LLP. She provides practical and strategic advice to international clients regarding the EU and UK General Data Protection Regulation, e-privacy laws, international data transfers (including with regard to the Schrems II decision) and sector-specific privacy and cybersecurity laws. Eleanor also has experience in assisting clients with preparing for, and responding to, cybersecurity incidents.

Sidley Austin LLP

70 St Mary Axe
London
EC3A 8BE
UK

Tel: +44 (0)20 7360 3600
Fax: +44 (0)20 7626 7937
Email: wlong@sidley.com
Web: www.sidley.com

SIDLEY

1. Basic National Regime

1.1 Laws

The UK has a well-developed – and growing – network of civil and criminal laws relating to cybersecurity, contained in UK legislation, companion rules made under such legislation, decisions of UK courts, and a steady stream of regulatory guidance from UK regulators.

Key cybersecurity requirements imposed on organisations in the UK, or on organisations that are established outside the UK but are processing personal data of individuals located in the UK, are derived from the EU General Data Protection Regulation (EU GDPR). Following the UK's departure from the EU under the terms of the EU (Withdrawal Agreement) Act 2020 on 31 January 2020, the UK government adopted the EU GDPR into English law as the "UK GDPR", which took effect in English law following the end of the Brexit Transition Period on 31 December 2020.

The UK GDPR and the UK Data Protection Act 2018 (DPA), as amended to supplement the UK GDPR in English law, applies to the security of "personal data" under the UK GDPR (eg, any information relating to an identified or identifiable individual who can be identified – directly or indirectly – by reference to an identifier such as a name, an identification number, location data or an online identifier). As such, only those cybersecurity incidents impacting personal data will be regulated by the UK GDPR (see also **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**). The UK GDPR requires organisations to maintain "appropriate" technical and organisational security measures and to comply with certain notification obligations when "personal data breaches" occur. The DPA also allows for criminal prosecutions to be brought for certain cybersecurity-related breaches.

Secondly, the Network and Information Systems Regulations (the "NIS Regulations") apply to two categories of key infrastructure operators – namely, "operators of essential services" (OESs) and "relevant digital service providers" (RDSPs). Like the UK GDPR, the NIS Regulations require organisations that are subject to them to implement certain cybersecurity measures and to provide notices of certain cybersecurity incidents that affect such organisations. In November 2022, the UK government confirmed that legislative changes resulting from a public consultation in January 2022 would be made to boost security standards and to increase reporting of serious cyber-incidents so as to reduce the risk of such attacks causing disruption; however, as of January 2024, there has been no further information as to whether these plans are being advanced. Please see **1.7 Key Developments** for additional information on the development of the NIS Regulations.

Thirdly, the Product Security and Telecommunications Infrastructure Act 2022 (PSTI) requires manufacturers, importers and distributors of UK consumer-connected products to meet certain cybersecurity standards. This includes requirements to follow more stringent security requirements (which will be specifically legislated by the UK Secretary of State), to investigate any compliance failures and take remediation action, as well as notify relevant authorities and other third parties about such compliance failures. Please see **1.7 Key Developments** for additional information on the obligations under the PSTI.

Fourthly, the Computer Misuse Act 1990 (CMA) is the UK's primary legislation with regard to criminalising unauthorised access to comput-

ers and other IT systems. It contains a number of cybersecurity-related offences. A key offence under the CMA (Section 1) is where a defendant obtains "unauthorised access" to a computer – ie, the defendant causes a "computer to perform any function with intent to secure access to any program or data held in any computer" or "to enable such access to be secured" where such access is "unauthorised" and this is known to the defendant at the relevant time.

Fifthly, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), the EU Notification Regulations 611/2013 (the "Notification Regulation"), and the Communications Act 2003 (CA 2003) contain cybersecurity obligations applicable primarily to electronic communications networks and service operations (such as telecommunications systems operators).

There are also sector-specific laws that contain cybersecurity obligations – for example, Financial Conduct Authority (FCA) rules (applicable to organisations that the FCA regulates), the Payment Services Regulations 2017 (PSR) (which transposes the Second Payment Services Directive into English law and applies to payment service providers), and the Official Secrets Act 1989 (OSA) (which is applicable to certain official government information). Similarly, the Investigatory Powers Act 2016 (IPA) and the Regulation of Investigatory Powers Act 2000 (RIPA) regulate electronic surveillance and interception in the UK and contain associated safeguards.

These laws are increasingly being enforced by UK governmental authorities – including the Information Commissioner's Office (ICO) and sector-specific regulators such as the FCA – and private individuals and organisations. Regulators are also increasingly collaborating on cybersecurity enforcement; examples include the ICO teaming up with the Competition and Markets Authority, the Office of Communications (Ofcom) and the FCA to form the Digital Regulation Co-operation Forum (DRCF).

In addition to legislation, English "common law" contains rules that are relevant to cybersecurity: there is a legal and ethical duty of confidence where information is shared in confidence and must not be disclosed without legal authority. The duty applies to information not already in the public domain and is subject to a number of exceptions, including where disclosure:

- has been consented to by the discloser; or
- is required by law.

The FCA rules, the PSR, the OSA, the IPA, the RIPA and other sector-specific or specialised laws or the common law duty of confidence are not further considered in this chapter.

1.2 Regulators

There are different UK regulators for each of the key UK cybersecurity legislations under consideration.

UK GDPR and DPA

In the UK, the ICO is responsible for monitoring the application of the UK GDPR and the DPA and taking enforcement action against organisations for non-compliance with such legislation, including investigating personal data breaches and inadequate security measures. The ICO may initiate an investigation on its own accord or on the basis of a complaint submitted by, for example, a private individual or organisation. The ICO also has the power to conduct both off-site and on-site audits. Please note that prosecutions under the DPA can only be brought by the ICO or

by (or with the consent of) the Director of Public Prosecutions (DPP).

NIS Regulations

With regard to the NIS Regulations, the "competent authority" is determined on an industry-by-industry basis through the Department for Science Innovation and Technology (DSIT), which oversees the implementation of the NIS Regulations across the UK. For OESs in the oil sector, for example, the competent authority in England, Scotland and Wales is the Secretary of State for Business, Energy and Industrial Strategy – whereas in Northern Ireland it is the Department of Finance. The ICO is the competent authority for RDSPs.

Competent authorities may be reactive or proactive in terms of the incidents they choose to investigate and they are supported by the National Cyber Security Centre (NCSC), which offers technical advice (except in healthcare, where this support is offered by NHS Digital). Certain organisations are also subject to regular compliance audits from their relevant competent authority – failing these audits can lead to fines of up to GBP17 million.

PECR and CA 2003

As regards the PECR, the ICO may audit the compliance of service providers pursuant to Regulation 5A of the PECR. Notifiable personal data breaches under Regulation 5A of the PECR must be reported to the ICO. The ICO is, in turn, responsible for investigating the breach and taking any subsequent enforcement action (see also **1.3 Administration and Enforcement Process**). However, with regard to the CA 2003 (which is a companion legislation to the PECR), Ofcom is the primary regulator. Pursuant to Section 105C of the CA 2003, Ofcom may carry out an audit of the security measures taken by a network provider or a service provider under Section 105A. Notifiable security breaches under Section 105 of CA 2003 must be reported to Ofcom, which is in turn responsible for investigating the breach and taking any subsequent enforcement action (see also **1.3 Administration and Enforcement Process**).

CMA

While there is no regulatory authority with oversight of the CMA per se, the provisions of the CMA are enforced by the UK Crown Prosecution Service (CPS), the public authority responsible for prosecuting the majority of criminal cases in the UK. The CPS is notified of CMA investigations and potential offences by the police and other investigative organisations in England and Wales.

1.3 Administration and Enforcement Process

The administration and enforcement process varies on a UK cybersecurity legislation-by-legislation basis. Commentary on the enforcement of certain key UK cybersecurity legislation is provided here.

UK GDPR and DPA

At present, the UK GDPR and the DPA continue to be enforced by the ICO, including with regard to cybersecurity matters – but only to the extent that they impact personal data. The ICO is required to adhere to specific procedures before undertaking enforcement action – for example, before imposing an administrative fine on an organisation for:

- breaching the integrity and confidentiality principle;
- inadequate security measures; or
- failing to report a personal data breach to the ICO or affected data subjects.

Where applicable, the ICO is required under Section 149 of the DPA to first issue the organisation with a written "enforcement notice", which requires the organisation to take steps specified in the notice and/or refrain from taking steps specified in the notice. If the ICO is of the view that the organisation has failed to comply with the enforcement notice, the ICO will then issue a written notice ("penalty notice") imposing a monetary penalty on the organisation of up to the greater of 4% of annual worldwide turnover or GBP17.5 million. When determining the monetary penalty amount, the ICO will consider a number of aggravating or mitigating factors. These factors include the nature, gravity and duration of the infringement – for example, personal data breach or inadequate security measures – and the intentional or negligent character of the infringement.

In determining whether to undertake a criminal prosecution under the DPA, the ICO must reference the Code for Crown Prosecutors and the ICO's own prosecution policy. Although the ICO has a number of enforcement tools available to it (including providing a caution to offending organisations), the ICO's Prosecution Policy Statement requires the ICO to consider aggravating factors in order to bring a prosecution instead of a caution. These include the accused breaching the law for financial gain, abusing a position of trust, or damage or distress being caused to data subjects.

The maximum penalty for criminal offences under the DPA is an unlimited fine. Imprisonment is not available for conviction under any of the DPA offences. Defendants are entitled to normal rights of appeal against a conviction or sentence in the legal system.

PECR, Notification Regulation and CA 2003

The ICO's guidance on notification of PECR security breaches provides that, upon receipt of a notification from a service provider, the ICO will consider the information provided in the notice to assess whether the service provider is complying with its obligations under the PECR. The ICO further states that it will inform the service provider of next steps within two weeks of their notification. Pursuant to Regulation 5C of the PECR, if a service provider fails to comply with the notification requirements of Regulation 5A, the ICO may issue a fixed monetary penalty notice of GBP1,000 against the service provider.

Before serving the enforcement notice, the ICO must serve the service provider with a notice of intent. A service provider may discharge liability for the fixed monetary penalty if such service provider pays GBP800 to the ICO within 21 days of receipt of the notice of intent. A service provider can also appeal the issuance by the ICO of the fixed monetary penalty notice to the First-tier Tribunal (Information Rights). The ICO also has the power under the PECR to issue enforcement notices for breach of the provisions of the PECR of up to a maximum of GBP500,000. However, the UK Data Protection and Digital Information Bill is proposing to increase fines for infringement to align with UK GDPR levels.

Under Section 105E, Ofcom has the power to issue penalties of up to GBP2 million where appropriate and proportionate.

CMA

There are a number of offences under the CMA. As noted previously, an offence under Section 1 is committed if there is "unauthorised" access to a computer system. A Section 1 CMA offence could be tried both summarily in the magistrates' courts and on indictment in the Crown Court.

Offences committed under Section 1 CMA carry up to two years' imprisonment or an unlimited fine (or both) on indictment. On summary conviction, the maximum sentence is 12 months' imprisonment or a fine (or both). In addition, a serious crime prevention order can be made against an individual or an organisation in relation to a breach of the CMA. Defendants are entitled to normal rights of appeal against a conviction or sentence in the legal system.

When determining whether to bring a prosecution under the CMA, the CPS must be satisfied that there is enough evidence to provide a "realistic prospect of conviction" against each defendant and that the public interest factors tending against prosecution outweigh those tending in favour (as set out in the Code for Crown Prosecutors 2018, which sets out the general principles that must be followed when the CPS makes a decision on cases). While there are no official guidelines for sentencing offences under the CMA, judges and magistrates will have to follow the Sentencing Council's general guideline, which applies to all offences without specific sentencing guidelines.

1.4 Multilateral and Subnational Issues

The UK GDPR and the DPA apply to:

- all organisations established in the four countries of the UK (ie, England, Northern Ireland, Scotland and Wales); and
- organisations not established in the UK processing personal data of data subjects in the UK to offer them goods or services or to monitor their behaviour.

In turn, the ICO regulates the UK GDPR and the DPA across the UK.

Although the CMA primarily applies to offences committed within the UK, it allows for prosecutions to be brought in the UK where some or all of the offending acts were committed outside the UK – reflecting the trans-border nature of many cybersecurity-related offences. By way of example, Section 1 of the CMA can apply to offending acts committed outside the UK and can – as a result – be prosecuted in the UK where there is "at least one significant link with the domestic jurisdiction". A significant link can include where:

- the accused is in a relevant country of the UK (England, Wales, Scotland and Northern Ireland) at the time of the offence;
- the target of the CMA offence is in a relevant country of the UK; or
- the technological activity that has facilitated the offending may have passed through a server based in a relevant country of the UK.

1.5 Information Sharing Organisations and Government Cybersecurity Assistance

Please see **7. Cyberthreat Information Sharing Arrangements**.

1.6 System Characteristics

The UK cybersecurity legal system is well developed and is similar to the legal systems across the European Economic Area (EEA), rather than the USA. Since 2018, the enforcement of cybersecurity rules in the UK has increased, particularly by the ICO. Notably, in October 2020 the ICO fined British Airways GBP20 million following a cyber-attack that resulted in user traffic to the British Airways website and mobile application being diverted to a fraudulent website, which allegedly led to the compromise of the personal data of more than 400,000 customers.

Also in October 2020, the ICO fined Marriott International GBP18.4 million for alleged failures relating to cybersecurity in the context of an acquisition.

More recently, in October 2022, the ICO fined a construction company GBP4.4 million for failure to adopt appropriate security measures to prevent a cyber-attack. The cyber-attack was the result of a phishing email received by an Interserve employee, which led to the installation of malware onto another employee's workstation. The ICO considered that the malware was not thoroughly investigated, despite the company's anti-virus software providing an alert and quarantining the malware. As a result, the malware compromised 283 systems and 16 accounts. The malware also encrypted the personal data of 113,000 current and former employees.

2023 saw a number of high-profile cyber-related personal data breaches reported in the public sector, including the UK Electoral Commission in August 2023 and a ransomware attack reported by Greater Manchester police in September 2023. The UK ICO has not yet issued enforcement action (if any) with regard to such incidents.

The UK government is also expected to overhaul its ability to assist and promote cybersecurity through its government cybersecurity strategy for 2022–30. There is to be a focus on government functions, including:

- the establishment of the Government Cyber Co-ordination Centre (GCCC);
- the adoption of the Cyber Assessment Framework (CAF); and
- dedicating more resources into tackling ransomware.

1.7 Key Developments

The key developments in the UK from a cybersecurity perspective in the past couple of years include confirmation from the UK government that it will amend the NIS Regulations as a result of a public consultation by the UK government on proposals for legislation to improve the UK's cyber-resilience. The consultation included proposals for the expansion of the scope of application of the NIS Regulations and new discretionary powers for the UK government to expand the scope and covered entities of the NIS Regulations in order to manage IT risks. Specifically, the planned amendments to the NIS Regulations will include the following.

- Managed service providers (MSPs) will be included in the list of RDSPs.
- A new, two-tier supervisory regime will be introduced, with a proactive supervisory regime applying for the most critical digital service providers and the existing, reactive supervisory regime continuing to apply to the remaining digital service providers. The plans indicate that the ICO would be the competent regulator for the two regulatory regimes.
- The UK government will receive delegated powers to expand the scope of the NIS Regulations without Parliament's consent and may inclusively designate entities as "critical (sector) dependencies" to ensure that entities such as relevant IT supply chain stakeholders that would not be covered by the NIS Regulations are brought into its scope.
- Expanding incident reporting requirements to include "any incident that has a significant impact on the availability, integrity, or confidentiality of networks and information systems, and that could cause, or threaten to cause, substantial disruption to the service".

There is currently no concrete timeline for the planned amendments.

Secondly, the PSTI came into force on 6 December 2022. Under this new act, manufacturers (the person responsible for manufacturing a product, designing a product or otherwise marketing the product under their own name or trade mark) of "UK consumer connectable products" are required to comply with new obligations to manage cybersecurity risk for connected products made available in the UK. Similar obligations will also apply to importers and distributors:

- duty to comply with security requirements as defined by the Secretary of State (see **5.6 Security Requirements to IoT**);
- duty to investigate and take action in relation to compliance failures – this may include preventing the product from being made available in the UK and/or remedying the compliance failure and notifying enforcement authorities, other manufacturers, importers and distributors; and
- duty to maintain records for a minimum of ten years – these records may be requested by the Secretary of State in the course of investigating and enforcing the legislation.

These requirements will apply from 29 April 2024, meaning companies providing in-scope products in the UK as of that date will need to comply with the PSTI. The new regime will be overseen by the Secretary of State, which will have the power to levy GDPR-style fines of GBP10 million or 4% of their annual revenue, as well as up to GBP20,000 a day in the case of an ongoing contravention.

Thirdly, on 12 September 2023, the NCSC and the ICO signed a Memorandum of Understanding (MoU) that sets out the further co-operation of the two bodies going forwards. In particular, the ICO will incentivise engagement with the NCSC, noting that it would look favourably on victims of nationally significant cyber-incidents who report and engage with the NCSC. Of note, the ICO has said that it will consider whether it can provide more specific guidance as to how such engagement might impact its calculation of regulatory fines in such instances.

Fourthly, on 8 July 2022, the ICO and the National Cyber Security Centre (NCSC) sent a joint letter to the Law Society setting out their policy position against paying ransoms in the context of ransomware attacks. The regulators consider that paying hackers ransoms provides no guarantees that the malicious actors will provide the decryption keys and does not ensure the safe return and/or erasure of the exfiltrated data. Additionally, the ICO clarified that it will not take the payment of ransoms into account as a mitigating factor when considering the type or scale of a GDPR enforcement action. The ICO has also published a revised version of its ransomware and data protection compliance guidance on its website.

Fifthly, on 23 January 2024, the UK government published a draft Code of Practice on cybersecurity governance, which has been designed in partnership with the NCSC (among other experts). The Code of Practice is aimed at executive and non-executive directors and other senior leaders and aims to ensure that UK businesses place appropriate focus on cybersecurity issues and that the issues are given equal attention as is given to other threats (eg, financial and legal risks). Key elements of the Code of Practice include ensuring:

- a detailed plan is in place to respond to, and recover from, cyber-incidents (with regular testing);

- ensuring clear governance structures are in place; and
- training employees with the skills and awareness to work alongside new technologies with confidence.

The call for reviews on the Code of Practice closed on 19 March 2024.

1.8 Significant Pending Changes, Hot Topics and Issues

There are three key UK cybersecurity matters on the horizon over the next 12 months, as detailed here.

The first concerns cybersecurity issues associated with developments in AI. By way of example, on 26 November 2023, the US Cybersecurity and Infrastructure Security Agency (CISA) – together with the UK's NCSC – published joint Guidelines for Secure AI System Development (the "AI Guidelines"). The AI Guidelines aim to ensure that developers take a "secure by design" approach, integrating cybersecurity into the development process from the outset and throughout. The AI Guidelines cover secure design, secure development, secure deployment, and secure operation and maintenance. Relatedly, in its annual review published on 14 November 2023, the NCSC noted the significant advances in AI that will enable and enhance existing challenges associated with cybersecurity.

Second, the UK government continues to progress amendments to the CMA, as for many years commentators have stated that the CMA has failed to keep pace with the cybersecurity landscape. The Criminal Law Reform Now Network produced a short comparative report on *Reforming the Computer Misuse Act*, which highlights reforms needed across the landscape of cyber-hacking regulation. This includes issues with the ambiguity around the meaning of "authorisation" and its subsequent impact on cybersecurity professionals, as well as highlighting issues with the current jurisdictional scope of the CMA, given the international nature of many cybersecurity incidents. The UK government held a consultation on CMA reform in 2021 and, in April 2022, future reforms were discussed in Parliament. The UK government then ran a further consultation on 7 February 2023 and published the responses to the consultation on 14 November 2023, whereby it notes that work will continue on engagement with private and public sector organisations to understand further impacts and mitigations in this area before it is considered for legislation.

Third, the UK government published a full draft of the PSTI (Security Requirements for Relevant Connectable Products) Regulations in April 2023, which was signed into law on 14 September 2023, ahead of the coming into force of the regime on 29 April 2024. The regulations cover:

- requirements for default passwords;
- information that must be provided to the public on reporting security issues;
- information about minimum support periods; and
- minimum requirements for statements of compliance, among other things.

Interestingly, the regulations also set out conditions for deemed compliance with security standards, including compliance with relevant parts of ETSI EN 303 645, or in some cases ISO/IEC 29147.

2. Key Laws and Regulators at National and Subnational Levels

2.1 Key Laws

Please see **1.1 Laws**.

2.2 Regulators

Please see **1.2 Regulators** and **1.3 Administration and Enforcement Process**.

2.3 Over-Arching Cybersecurity Agency

The NCSC is the key UK cybersecurity agency, co-ordinating UK cybersecurity policy and technical standards, particularly with regard to the NIS Regulations and the UK GDPR. The NCSC acts as the national computer security incident response team (CSIRT) under the NIS Regulations and supports organisations that suffer cybersecurity incidents. It also acts as a "single point of contact" for competent authorities under the NIS Regulations. Following Brexit, the UK has forfeited its position on the EU Agency for Cybersecurity (ENISA); however, some operational co-operation continues to persist in order to allow for improved cybersecurity across Europe.

2.4 Data Protection Authorities or Privacy Regulators

Please see **1.1 Laws**, **1.2 Regulators** and **1.3 Administration and Enforcement Process**. As a result of overlapping jurisdictions among the various cybersecurity laws, multiple regulators may exercise jurisdiction with regard to the same cybersecurity incident. By way of example, a major cybersecurity incident affecting an OES that results in the compromise of personal data could implicate the UK GDPR and the NIS Regulations and thereby involve notices to both the ICO and the relevant "competent authority" under the NIS Regulations. Similarly, a major cybersecurity incident affecting an FCA-regulated organisation that results in the compromise of personal data could implicate the UK GDPR and the FCA rules and thereby involve notices to both the ICO and the FCA respectively.

2.5 Financial or Other Sectoral Regulators

Please see **1.1 Laws**, **1.2 Regulators** and **1.3 Administration and Enforcement Process**. Also, and by way of illustration, the FCA has demonstrated a strong focus on cybersecurity in the context of the financial services industry. This is particularly relevant in the context of:

- Principle 3 (Management and Control) of the FCA Handbook's *PRIN Principles for Businesses*, which states that "a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems"; and
- Principle 11 (Relations with Regulators), which requires that "a firm must deal with its regulators in an open and co-operative way, and must disclose to the FCA appropriately anything relating to the firm of which that regulator would reasonably expect notice".

In relation to Principle 11, the FCA confirms that organisations must report material cyber-incidents. The FCA considers that an incident may be material if it:

- results in significant loss of data or the availability or control of a firm's IT systems;
- affects a large number of customers; and
- results in unauthorised access to, or malicious software present on, a firm's information and communication systems.

The FCA goes on to require that where such an incident is deemed to be material:

- the FCA (and the Prudential Regulation Authority (PRA) for dual-regulated firms) should be notified;
- if the incident is criminal, Action Fraud (the UK's national fraud and cybercrime reporting centre) should be contacted; and
- where the incident is also a personal data breach, organisations may need to report the incident to the ICO.

The FCA also recommends that firms refer to the NCSC guidance on reporting incidents and reports should be shared on the Cyber Security Information Sharing Partnership (CiSP) platform; please see comments in **7.2 Voluntary Information Sharing Opportunities** for further detail on the CiSP platform. More generally, and as part of the FCA's goal to assist firms in becoming more resilient to cyber-attacks, it recommends that firms of all sizes should develop a "security culture" and be able to identify and prioritise information assets and constantly evolve to meet new threats.

In addition, certain categories of FCA-regulated firms have additional reporting requirements. By way of example, payment services providers are required to report major operational and security incidents pursuant to the PSR.

Further, on 19 December 2023, the FCA (together with the Bank of England and the PRA) published the annual CBEST thematic report in full for the first time. The report contains cyber-resilience good practice and insight, including from the NCSC, for firms to help them maintain their operational resilience. The good practice recommendations are the result of a programme that assesses the cyber-resilience of systemic financial institutions through live testing. The report highlights the importance of building a strong foundation of cyber-hygiene to prevent common cyber-incidents, including training and awareness and robust authentication.

2.6 Other Relevant Regulators and Agencies

Please see **1.1 Laws**, **1.2 Regulators**, **1.3 Administration and Enforcement Process** and **2.4 Data Protection Authorities or Privacy Regulators**.

3. Key Frameworks

3.1 De Jure or De Facto Standards

There are numerous cybersecurity frameworks that are expressly or implicitly recognised by UK cybersecurity regulators. By way of example, the ICO recommends that organisations review the UK Cyber Essentials scheme (a UK government and industry-backed scheme), which provides basic guidance to organisations on how to prevent and limit the impact of cyber-attacks.

Similarly, Ofcom repeatedly references the International Standard for Organization (ISO) standards in its Guidance on Security Requirements. In addition, Ofcom comments that the controls in the UK's Cyber Essentials scheme should be implemented and exceeded; according to Ofcom, obtaining the Cyber Essentials Plus certification is "a powerful way to demonstrate this". Regarding the NIS Regulations, the NCSC has published 14 cybersecurity and resilience principles that provide guidance in the form of the Cyber Assessment Framework (CAF). The CAF is particularly relevant to OESs that are subject to the NIS Regulations.

Lastly, the most used account and payments data security standard, the Payment Card Industry Data Security Standard (PCI DSS), was revised. Version 4.0 was published on 31 March 2022.

3.2 Consensus or Commonly Applied Framework

Please see **3.1 De Jure or De Facto Standards** and **3.3 Legal Requirements and Specific Required Security Practices**.

3.3 Legal Requirements and Specific Required Security Practices

UK GDPR

The UK GDPR requires that controllers and processors implement "appropriate" technical and organisational security measures. When adopting such measures, the UK GDPR requires organisations to take into account the state of the art, costs of implementation, and the nature, scope, context and purposes of the processing of personal data, as well as the risks of such processing to the data subject's rights (eg, from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of – or access to – personal data transmitted, stored or otherwise processed by the organisation).

The UK GDPR itself sets out examples of "appropriate" security measures, namely:

- pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of personal data processing.

Importantly, according to the ICO, there is no "one-size-fits-all" approach to "appropriate" security. The level of appropriateness depends on each organisation's processing of personal data – for example, the nature of the organisation's computer systems, the number of personnel with access to the personal data being processed and whether any personal data is held by a vendor acting on the organisation's behalf. The ICO recommends that, before taking a view on what is "appropriate", organisations should assess the level of risk by reviewing the type of personal data held, whether it is sensitive or confidential, and the damage caused to data subjects if compromised (eg, identity fraud).

In addition, when considering which cybersecurity measures to adopt, the ICO recommends that organisations consider:

- system security – security of the organisation's network and information systems (particularly systems that process personal data);
- data security – security of the personal data held in the organisation's systems (eg, ensuring appropriate access controls are in place within the organisation);
- actively managing software vulnerabilities, including using in-support software and the application of software update policies (patching), as well as taking other mitigating steps where patches cannot be applied;
- online security – website and mobile application security; and
- device security – considering information security policies for bring-your-own devices, where offered by the organisation.

While the UK GDPR continues to apply in the UK, the UK is currently in the legislative process for the new UK Data Protection and Digital Information Bill No 2. The proposed Bill looks to reform several aspects of current data protection legislation in the UK, including in relation to information security. Under the current UK GDPR, as noted earlier, organisations are required to

implement "appropriate technical and organisational measures" to ensure a level of security appropriate to the risk of data processing. Under the proposed Bill, organisations would be required to implement "appropriate measures, including technical and organisational measures". This introduces greater flexibility when implementing data security measures, as this approach removes the focus away from "technical and organisational measures" by including it as an example of appropriate measures instead. A final text of the proposed Bill is not yet agreed but it is expected to pass in spring 2024.

NIS Regulations

The NIS Regulations require that OESs and RDSPs adopt "appropriate and proportionate" technical and organisational security measures and "appropriate" measures to prevent and minimise the impact of incidents affecting those systems (taking into account the state of the art) to ensure the continuity of the essential services that the OES provides. Although serious incidents must be reported under the NIS Regulations, the ICO has also explained that software vulnerabilities – ie, weaknesses in a system that can be exploited by an attacker – may also need to be reported, as per the "additional information" required in the ICO's NIS reporting form. As explained in **1.1 Laws**, the UK government is also consulting on updates to the NIS Regulations.

Product Security and Telecommunications Infrastructure Act 2022

As detailed in **1.7 Key Developments** and **1.8 Significant Pending Changes, Hot Topics and Issues** and **5.6 Security Requirementsfor IoT**, the security requirements under the PSTI imposed on manufacturers, importers and distributors of UK consumer-connected products made available in the UK were signed into law in September 2023 and will apply from 29 April 2024 alongside the PSTI.

PECR and CA 2003

Regulation 5(1A) of the PECR requires service providers to:

- restrict access to personal data to only authorised personnel;
- protect personal data against "accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure"; and
- implement a security policy with regard to the processing of personal data.

Service providers are also required to retain a log of the personal data breaches pursuant to Regulation 5A(8) of the PECR.

Guidance on Security Requirements published by Ofcom in relation to the CA 2003 states that "clear lines of accountability (must be established), up to and including board or company director level, and sufficient technical capability to ensure that potential risks are identified and appropriately managed". The guidance further states that "a level of internal security expertise, capacity, and appropriate accountability mechanisms, sufficient to provide proper management of (security risks)" must be maintained. The guidance also references the following:

- the importance of internal risk assessments;
- the need for sufficient oversight of networks and services to enable fast identification of significant security incidents;
- a requirement to put in place security measures that exceed those in the Cyber Essentials scheme; and
- the importance of intelligence-led vulnerability testing to manage cyber-risks.

3.4 Key Multinational Relationships

A number of key UK cybersecurity regulators or organisations – eg, the ICO and the NCSC – work closely with their counterparts in the EEA, such as other data privacy authorities that comprise the European Data Protection Board (with regard to the ICO) and ENISA (with regard to the NCSC). In relation to relationships with other EEA data privacy authorities, the ICO, in particular, has mutual assistance Memoranda of Understanding with the US Federal Trade Commission, the federal Privacy Commissioner of Canada, New Zealand's Office of the Privacy Commissioner (OPC) and Department of Internal Affairs, and the National Privacy Commission of the Philippines.

In addition, sector-specific regulators also work closely with their counterparts within the EEA and elsewhere. By way of illustration, the FCA has a close relationship with the SEC. While the relationship is not cybersecurity-specific, cybersecurity forms part of the regulators' general financial regulatory co-operation. The FCA has also confirmed that it continues to work with governments and other regulators, nationally and internationally, on cybersecurity issues.

Please also see **1.7 Key Requirements** for details of the MoU signed between the NCSC and the ICO.

4. Key Affirmative Security Requirements

4.1 Personal Data

Please see **1.1 Laws**, **1.2 Regulators** and **1.3 Administration and Enforcement Process**, as well as **5. Data Breach Reporting and Notification**.

4.2 Material Business Data and Material Non-public Information

Please see **1.1 Laws**, **1.2 Regulators** and **1.3 Administration and Enforcement Process**, as well as **5. Data Breach Reporting and Notification**.

4.3 Critical Infrastructure, Networks, Systems and Software

Please see **1.1 Laws**, **1.2 Regulators** and **1.3 Administration and Enforcement Process**, as well as **5. Data Breach Reporting and Notification**.

4.4 Denial of Service Attacks

Please see **1.1 Laws**, **1.2 Regulators** and **1.3 Administration and Enforcement Process**, as well as **5. Data Breach Reporting and Notification**.

4.5 Internet of Things (IoT), Software, Supply Chain, Other Data or Systems

Please see **1.1 Laws**, **1.2 Regulators** and **1.3 Administration and Enforcement Process**, as well as **5. Data Breach Reporting and Notification**.

4.6 Ransomware/Extortion

Please see **1.1 Laws**, **1.2 Regulators**, **1.3 Administration and Enforcement Process** and **1.7 Key Developments**, as well as **5. Data Breach Reporting and Notification**.

5. Data Breach or Cybersecurity Event Reporting and Notification

5.1 Definition of Data Security Incident, Breach or Cybersecurity Event

UK GDPR and DPA

Under the UK GDPR, "personal data breaches" are potentially reportable data security incidents.

As explained in **1.3 Administration and Enforcement Process**, "personal data breach" is understood to mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Importantly, organisations' obligations to notify the ICO and affected data subjects do not arise in relation to every cybersecurity incident. Rather, the UK GDPR and DPA – and, in turn, applicable notification obligations – only apply where the breach involves personal data. As the European Data Protection Board (EDPB) notes in its guidance on personal data breaches, "all personal data breaches are security incidents" but "not all security incidents are necessarily personal data breaches".

Further, the EDPB categorises personal data breaches as follows:

- confidentiality breach – where there is an unauthorised or accidental disclosure of, or access to, personal data;
- integrity breach – where there is an unauthorised or accidental alteration of personal data; and
- availability breach – where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

Following the occurrence of a "personal data breach", if the organisation is a controller then it needs to notify the ICO of the breach, unless the breach is "unlikely to result in a risk to the rights and freedoms of individuals"; such notice should be provided "without undue delay" and "where feasible, not later than 72 hours" after the controller became "aware" of the breach, having a "reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised". If the organisation is a processor, then it needs to notify the relevant controller without undue delay after it becomes aware of the breach.

In addition, controllers are required to notify affected data subjects "without undue delay" if the breach is "likely to result in a high risk to rights and freedoms" of such data subjects. Such data subjects' notices are required to contain specific information, including the consequences of the breach and the steps that the controller has taken (or proposes to take) to address the breach and mitigate its possible adverse effects. There are certain narrow exemptions from the obligation to notify affected data subjects – for example, where the compromised personal data was encrypted and the key has not been compromised.

NIS Regulations

Under the NIS Regulations, different incident reporting obligations apply to OESs and RDSPs respectively. For OESs, cybersecurity event notification is required when any incident has a "significant impact" on the continuity of the essential service that the OES provides – determining this requires a fact-specific analysis of the number of users affected by the disruption of the service, the duration of the incident, and the geographical area affected by the incident, as well as any other relevant guidance issued by their designated "competent authority".

For RDSPs, notification is required where there will be a "substantial impact" on the provision of any relevant service. From 12 January 2022, the ICO (which is the lead regulator for RDSPs) must be notified by an RDSP where there is an incident that has a substantial impact on the provision of any digital services, including online

marketplaces, online search engines and cloud computing services. It should be noted that, by comparison to the UK GDPR, notifiable incidents under the NIS Regulations need not always involve personal data – that is, cybersecurity incidents that do not involve personal data (such as cyber-attacks on industrial control systems) could be notifiable under the NIS Regulations, but would not be notifiable under the UK GDPR if they do not involve personal data.

Comparable with the UK GDPR, both OESs and RDSPs must notify their relevant competent authority and the ICO respectively of an incident "without undue delay" and, in any event, no later than 72 hours after the OES or RDSP (as applicable) becomes aware of the incident.

PECR and CA 2003

Regulation 2(1) of the PECR defines a "personal data breach" as a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of – or access to – personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service. The security and breach notification requirements under Regulation 5 of the PECR apply to personal data.

Under Regulation 5A of the PECR, service providers are required to notify the ICO in the event of a personal data breach (as defined under Regulation 3 of the PECR). Pursuant to Article 2(2) of the Notification Regulation, such notification must be made where feasible, no later than 24 hours after the detection of the personal data breach. A notification to the ICO is not required where an organisation is responsible for delivering part of the service, but does not have a direct contractual relationship with end users. In such cases, the organisation must notify the organisation that does have the contractual relationship with end users and that organisation must then notify the ICO. The service provider is also required to notify, without undue delay, the concerned subscriber or user where the breach is likely to adversely affect their personal data or privacy, unless the service provider can demonstrate to the ICO that the data was made unintelligible (eg, encrypted).

The security breach notification requirements under Section 105K(1)(a) of the CA 2003 apply to public electronic communications networks and systems: network and service providers must notify Ofcom of security breaches that have a significant impact on the operation of a public electronic communications network. Section 105(A) of the CA 2003 broadly defines a "security compromise" as including, among other things, "anything that compromises the availability, performance or functionality of the network or service". In determining whether the effect that a security compromise has – or would have – on the operation of a network or service is "significant", certain matters should be considered, including the length of the period during which the operation of the network or service is or would be affected, the number of affected persons, the geographical size and location affected, and the extent to which activities of persons who use the network or service are or would be affected by the effect on the operation of the network or service.

Other Obligations

To the extent that organisations have contractually agreed with other organisations' or individuals' cybersecurity obligations that are broader or more rigorous than those set out in the specific cybersecurity law, the affected organisation would need to comply with those obligations. For example, many processors in the UK agree

to notify controllers of "personal data breaches" within specific (short) timescales, rather than the more open-ended UK GDPR standard of "without undue delay". In such case, the processor would need notify to its controller within a specific (short) timescale. In addition, depending on the nature of the incident and regardless of the specific cybersecurity law applicable to it, organisations in the UK may wish to notify appropriate UK law enforcement agencies, such as the National Crime Agency and Action Fraud.

5.2 Data Elements Covered

Please see **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**.

5.3 Systems Covered

Please see **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**.

5.4 Security Requirements for Medical Devices

NHS Digital (the body responsible for information, data and IT systems in health and social care in the UK) has published a variety of guidance, including the Data Security and Protection Toolkit, which is an online self-assessment tool that all organisations must use if they have access to NHS patient data and systems. This includes an incident reporting tool that incorporates the notification requirements of the UK GDPR and the NIS Regulations. There is also a GDPR-focused document entitled Respond to an NHS Cyber Alert, which explains the intersection between medicine, personal data and cybersecurity.

At an EU level (albeit highly persuasive from a UK perspective), the Medical Device Co-ordination Group published updated guidance in June 2020 on cybersecurity for medical devices, which is intended to assist medical device manufacturers in meeting the cybersecurity requirements in the EU's Medical Devices Regulation and the In Vitro Diagnostic Regulation. According to the updated guidance, manufacturers must consider safety and cybersecurity throughout the life cycle of a product – that is, they must integrate security "by design". This concept closely aligns with the requirement of privacy by design under the UK GDPR. Manufacturers must also perform increased post-market surveillance and vigilance. Such post-market surveillance should address the following:

- operation of the device in the intended environment;
- sharing and dissemination of cybersecurity information and knowledge of cybersecurity vulnerabilities and threats across multiple sectors;
- vulnerability remediation; and
- incident response.

5.5 Security Requirements for Industrial Control Systems (and SCADA)

Please see **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**.

5.6 Security Requirements for IoT

Schedule 1 of the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023, which will come into force on 29 April 2024, includes the following security requirements:

- all UK consumer connected products passwords must be unique and incapable of being reset to any universal factory setting;
- manufacturers, importers and/or distributors of UK consumer-connected products must provide a public point of contact for reporting vulnerabilities and these must be acted on in a timely manner; and

- manufacturers, importers and/or distributors of UK consumer-connected products explicitly state the minimum length of time for which the device will receive security updates at the point of sale.

5.7 Requirements for Secure Software Development

Please see **3.3 Legal Requirements and Specific Required Security Practices** and **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**.

5.8 Reporting Triggers

Please see **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**.

5.9 "Risk of Harm" Thresholds or Standards

Please see **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**.

6. Ability to Monitor Networks for Cybersecurity

6.1 Cybersecurity Defensive Measures

While effective data security measures usually enhance individuals' privacy protections, excessive or intrusive cybersecurity measures can diminish individuals' privacy and freedoms. Therefore, to the extent that network monitoring or cybersecurity defensive measures involve the processing of personal data, the relevant UK GDPR obligations would need to be complied with. Key UK GDPR obligations would involve (among other things) providing UK GDPR-compliant notices to individuals, establishing a legal basis under the UK GDPR for such data processing – for example, relying on "legitimate interest" and conducting a data protection impact assessment (DPIA) with regard to any data processing activities that are considered "high risk" under the UK GDPR.

As regards the UK GDPR legal basis, even though cybersecurity is acknowledged as a potential "legitimate interest", the organisation would need to conduct a formal "legitimate interest assessment" to assess whether it has appropriately balanced between its legitimate interest in implementing network monitoring and other cybersecurity defensive measures and also protecting the individual's privacy interests.

In addition, certain kinds of employee monitoring measures (including those implemented for network monitoring and other cybersecurity defence reasons) are considered "high risk" under the UK GDPR. As a result, an organisation that intends to implement such measures would be required to conduct a DPIA prior to implementing such measures.

6.2 Intersection of Cybersecurity and Privacy or Data Protection

Please see **6.1 Cybersecurity Defensive Measures**.

7. Cyberthreat Information Sharing Arrangements

7.1 Required or Authorised Sharing of Cybersecurity Information

Please see **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**.

7.2 Voluntary Information Sharing Opportunities

A key information-sharing organisation in the UK is the CiSP. It is a joint industry and UK government initiative managed by the NCSC. The CiSP allows members to voluntarily exchange

cyber-risk information in a secure environment, such that there are reductions to the impact of cyber-risks for UK businesses in general.

8. Significant Cybersecurity and Data Breach Regulatory Enforcement and Litigation

8.1 Regulatory Enforcement or Litigation

GDPR and DPA

The key UK regulatory actions and litigation with regard to the British Airways, Marriott/Starwood and Interserve Group Ltd cybersecurity breaches have already been discussed in **1.6 System Characteristics** and **1.7 Key Developments**.

CMA

The ICO is taking cybersecurity increasingly seriously and this is demonstrated by the two convictions it has helped secure in its prosecution of certain individuals. This has been for unauthorised access to personal data in both cases and has led to the imprisonment of the defendants in question. The ICO explained that it is open to undertaking such prosecutions for data protection-related offences, using the CMA "to reflect the nature and extent of the offending and for the sentencing court to have a wider range of penalties available".

8.2 Significant Audits, Investigations or Penalties

Please see **1.6 System Characteristics**, **1.7 Key Developments** and **8.1 Regulatory Enforcement or Litigation**.

8.3 Applicable Legal Standards

Please see **1.1 Laws**, **1.2 Regulators** and **1.3 Administration and Enforcement Process**.

8.4 Significant Private Litigation

Please see **8.1 Regulatory Enforcement or Litigation**. In addition, individuals are allowed to bring claims under the UK GDPR (including through representative actions). The British Airways group litigation and Lloyd v Google have already been noted. Under the CMA, individuals are able to bring a private prosecution without seeking permission from the DPP. The prosecution may be taken over by the CPS if the CPS determines that it is required. Private prosecutions have been bought by individuals (such as in connection with adversarial divorce proceedings). By contrast with the CMA, private prosecutions under the DPA require the consent of the DPP.

8.5 Class Actions

Please see **8.4 Significant Private Litigation**.

9. Cybersecurity Governance, Assessment and Resiliency

9.1 Corporate Governance Requirements

The matter is not relevant in this jurisdiction.

10. Due Diligence

10.1 Processes and Issues

The importance of conducting appropriate cybersecurity diligence in connection with corporate transactions is well illustrated by the ICO fining Marriott GBP18.4 million. More generally, M&A acquirers could (post-transaction) be directly liable for the M&A target's UK GDPR and cybersecurity breaches if the acquirer were to, for example, exercise "decisive influence" over the target. Any regulatory fines could be levied as a percentage of the entire corporate group's (including the acquirer's) annual worldwide gross

revenues. As a result, the target and acquirer are at risk both of regulatory fines (of up to 4% of annual worldwide group revenues) for non-compliance as well as private litigation brought by affected individuals and organisations.

In terms of corporate transaction-related cybersecurity diligence, an M&A acquirer will need to assess what diligence would be appropriate in the circumstances. In many circumstances, a review of the target's cybersecurity policies and procedures (including its written cybersecurity frameworks and certifications, incident response plans, and personal data breach register) would be itself appropriate. In some circumstances, more detailed cybersecurity diligence may be warranted, including forensic review of – and identifying vulnerabilities in – the target's IT and software systems and practices, as well as any products or platforms it offers to its customers.

After identifying any cybersecurity risks associated with the target, an M&A acquirer will then need to negotiate suitable representations and warranties with the target so as to address those risks appropriately. The M&A acquirer may also need to ensure that, post-transaction, the target undertakes measures to remedy any cybersecurity deficiencies that were not remedied previously.

10.2 Public Disclosure

The matter is not relevant in this jurisdiction.

11. Insurance, Artificial Intelligence and Other Cybersecurity Issues

11.1 Further Considerations Regarding Cybersecurity Regulation

The NCSC has issued guidance on cybersecurity insurance, which recommends the following:

- carrying out an audit of the current security measures an organisation has in place;
- getting certified under the Cyber Essentials and Cyber Essentials Plus schemes to get a discount on any insurance;
- ensuring there is a team of lawyers who can deal with contracts, technical experts who can manage IT systems, and HR teams who can oversee cybersecurity processes and procedures;
- ensuring employees understand their organisation so that an appropriate level and type of cover is set;
- checking if the cyber-insurance policy being considered covers claims for compensation by third parties in the event of a cyber-attack or in the event that personal data is lost as a result of a data breach at an organisation (eg, if a customer's personal data is lost); and
- checking the general limits of any policy chosen, including whether support will be provided both during and after a cybersecurity incident.

The UK government has also recognised that affordable and comprehensive cybersecurity insurance is a must. The Cyber Security Breaches Survey 2023 revealed that 32% of UK businesses have experienced a cyber-attack in the past 12 months, but only 21% of UK businesses have an incident response plan.

Trends and Developments

Contributed by:
William Long, Francesca Blythe, Denise Kara and Eleanor Dodding
Sidley Austin LLP

Sidley Austin LLP is a premier global law firm with a practice highly attuned to the ever-changing international landscape. The firm advises clients around the globe, with more than 2,300 lawyers in 21 offices worldwide. Sidley Austin maintains a commitment to providing quality legal services and to offering advice on litigation, transactional and regulatory matters spanning virtually every area of law. The firm's lawyers have wide-reaching legal backgrounds and are dedicated to teamwork, collaboration, and superior client service – helping a range of businesses address some of the most challenging matters concerning data protection, privacy, information security and incident response, data commercialisation, internet and computer law, IP, information management and records retention, e-commerce, consumer protection, and cybercrime. The firm advises clients with extensive operations in Europe, as well as in the USA, Asia and elsewhere, on developing and implementing global data protection programmes.

Authors

William Long is a partner at Sidley Austin LLP, where he leads the EU and UK data protection practice and is global co-leader of the firm's highly ranked privacy and cybersecurity practice. William advises international clients on a wide variety of General Data Protection Regulation (GDPR), data protection, privacy, information security, social media, e-commerce and other regulatory matters. He has been a member of the European Advisory Board of the International Association of Privacy Professionals (IAPP) and on the DataGuidance panel of data protection lawyers. William is also on the editorial board of e-Health Law & Policy and assists with dplegal, which is a network for privacy professionals.

Francesca Blythe is a partner at Sidley Austin LLP and advises international clients on a wide range of data protection, privacy, and cybersecurity issues. She has in-depth experience in a number of industries, including asset management and private equity, payments, technology, e-commerce, and manufacturing. Francesca has a particular focus on life sciences, where she advises on a broad range of issues – for example, in relation to real-world evidence and secondary research, clinical studies/investigations, digital health, and use of novel technologies (including AI).

Contributed by: William Long, Francesca Blythe, Denise Kara and Eleanor Dodding, **Sidley Austin LLP**

Denise Kara is a senior managing associate at Sidley Austin LLP. She advises international clients on a wide range of data protection, privacy, and cybersecurity matters, including in relation to the General Data Protection Regulation (GDPR), e-privacy laws, the EU's Network & Information Systems (NIS) Directive, and international data transfers (including compliance with Schrems II and the EU–US Data Privacy Framework). Denise assists clients in preparing for, and responding to, sophisticated cybersecurity incidents. Her practice has a particular focus on transactional matters and deal counselling for M&A related to privacy, cybersecurity and data protection compliance, as well as risk mitigation and integration planning strategies.

Eleanor Dodding is a senior managing associate at Sidley Austin LLP. She provides practical and strategic advice to international clients regarding the EU and UK General Data Protection Regulation, e-privacy laws, international data transfers (including with regard to the Schrems II decision) and sector-specific privacy and cybersecurity laws. Eleanor also has experience in assisting clients with preparing for, and responding to, cybersecurity incidents.

Sidley Austin LLP

70 St Mary Axe
London
EC3A 8BE
UK

Tel: +44 (0)20 7360 3600
Fax: +44 (0)20 7626 7937
Email: wlong@sidley.com
Web: www.sidley.com

Introduction

Owing to the dynamic nature of the global cybersecurity threat landscape, the importance of secure and resilient cybertechnology remains a high priority for organisations in 2024. In particular, the emergence of state-aligned actors as a new cyberthreat to critical national infrastructure, the continuation of Russia's invasion of Ukraine, and the rapid advancement in the development and deployment of AI technologies further increase existing challenges associated with cybersecurity. Consequently, it is anticipated that much of the UK government's focus in 2024 will be to progress its reform of the UK's cybersecurity legal framework and continue to support the safe and responsible development of AI technologies throughout the UK.

Cybersecurity Threats in 2024: Ever More Complex and Diverse

There is growing appreciation that cyber-attacks are a threat to businesses of all types and sizes, with 32% of businesses confirming a cyber-attack in the latest survey by the UK government, which covered the 12-month period from winter 2022 to winter 2023. The National Cyber Security Centre (NCSC), the UK's technical authority for cybersecurity, also reported its findings in its Annual Review report for 2023 for the period between September 2022 and August 2023 (the "NCSC Report"). The NCSC Report noted that despite geopolitical factors such as in China, Russia, and Iran driving concern around state-sponsored attacks, financial gain remains a key motivator for threat actors.

In this respect, ransomware attacks continue to pose one of the most acute cyberthreats and the nature of such attacks is changing. While the typical approach of stealing and encrypting data continues to be the primary ransomware tactic adopted by cybercriminals, there is an increasing trend towards threat actors adopting data extortion tactics whereby data is stolen but not encrypted. According to the NCSC Report, the NCSC received 297 reports of ransomware activity during this period and urged companies not to pay ransom demands. Instead, businesses are encouraged to report such attacks – especially as evidence suggests that the payment of a ransom does not guarantee decryption of information or the return of exfiltrated data. The UK's Information Commissioner's Office (ICO) has also separately confirmed that ransomware payments would not be taken into account as a mitigating factor when considering enforcement action.

Cyber-enabled fraud continues to be one of the most significant threats faced by UK businesses. Positively, the NCSC noted that there is a greater public awareness of these issues. During the past year, the UK government's Cyber Aware campaign supported individuals and small businesses to significantly improve their personal cyber-resilience. The NCSC's automated "Early Warning" service continued to aid in the prevention of incidents. According to the NCSC Report, by August 2023, the NCSC had sent 24.48 million notifications to 8,704 members of its network via its Early Warning service informing subscribers of potential malicious activity detected on their networks or of exposure to a vulnerability.

Evidencing an increased awareness of cybersecurity issues, the NCSC saw a huge leap in reports of cyber-attacks in 2023. An all-time high of 2,005 reports were received, representing an increase of almost 64% from 2022. Of these reports, four instances were among the most severe incidents managed by the NCSC to date. The NCSC highlighted that 371 incidents involved exfiltration or extortion of data, which is an 18.5% increase from 2022, indicating the increasing use of AI by threat actors to analyse exfiltrated data more efficiently and effectively.

Importantly, on 12 September 2023, the NCSC and the ICO signed a Memorandum of Understanding (MoU) setting out the further co-operation of the two bodies going forward in cybersecurity incident management in the UK. Under the MoU, the ICO will incentivise engagement with the NCSC, noting that it would look favourably on victims of nationally significant cyber-incidents who report and engage with the NCSC. Of note, the ICO has said that it will consider whether it can provide more specific guidance as to how such engagement might impact its calculation of regulatory fines in these instances.

Impact of AI on Cybersecurity

With the rapid increase in the development of AI technologies, the UK government and the NCSC have taken steps to ensure that cybersecurity is at the forefront for the safety, reliability, predictability and ethical use of such technologies in the UK. As part of its National AI Strategy, the UK government aims to leverage the power of AI to increase resilience, productivity, growth and innovation across private and public sectors while ensuring that the UK has an effective framework for regulating and addressing AI risks and harms. Among these are concerns around fairness, bias, discrimination, and the accountability of AI systems. A key focus in the UK's National AI Strategy is ensuring cybersecurity is considered early in the development and deployment of AI systems to prevent such harms from arising, by adopting a "secure by design" approach to mitigating against cybersecurity becoming an afterthought.

In February 2024, the UK government published its much-anticipated consultation response to its March 2023 White Paper on the UK's pro-innovation approach to AI regulation ("the Response"). The Response reasserts that there will be no new AI legislation for the UK. Instead, current regulators will apply their existing powers to matters involving AI that fall within their jurisdictions, with the aim of creating an innovation-friendly regulatory landscape. According to the Response, the UK government is now looking to release a call for views in spring 2024 to obtain further input on its next steps in securing AI models, including a potential cybersecurity Code of Practice for the use of AI.

On 16 January 2024, the UK's national standards body, the British Standards Institution, launched the world's first international standard designed for organisations providing or utilising AI-based products or services – BS ISO/IEC 42001 ("the Standard") – in order to ensure responsible development and use of AI systems. Among other things, the Standard sets requirements for the development and operation of an information security management system to mitigate the risks of breaches and cybercrime.

Further, on 26 November 2023, the NCSC – together with the US Cybersecurity and Infrastructure Security Agency – published Joint Guidelines for Secure AI System Development (the "AI Guidelines"). The AI Guidelines aim to ensure that developers take a "secure by design" approach, integrating cybersecurity into the development process from the outset and throughout the AI life cycle.

Cybersecurity Reform and Guidance

The UK government continues to develop its package of reforms as part of its first Cyber Security Strategy for 2022–30. The new Product Security and Telecommunications Infrastructure Act (PSTI) received royal assent on 6 December 2022 and the UK government agreed the PSTI (Security Requirements for Relevant Connectable Products) Regulations (the "PSTI Regulations") on 14 September 2023, ahead of its coming into force on 29 April 2024. The PSTI applies to "relevant connectable products" – for

example, smartphones, smart TVs, smart speakers, connected baby monitors, and connected alarm systems. Among other requirements, the PSTI Regulations cover:

- requirements for default passwords;
- information that must be provided to the public on reporting security issues;
- information about minimum support periods; and
- minimum requirements for statements of compliance.

Interestingly, the PSTI Regulations also set out conditions for deemed compliance with security standards, including compliance with relevant parts of ETSI EN 303 645 or, in some cases, ISO/IEC 29147. However, while the UK government confirmed in late 2022 its plans to strengthen the Network and Information Systems (NIS) Regulations in order to (among other things) include managed service providers within scope, 2023 did not see any further developments in this regard.

Contrastingly, there has been some movement on the UK Data Protection and Digital Information Bill ("the Bill"), which is now expected to receive royal assent in spring 2024. The Bill aims to reform several aspects of current data protection law in the UK, including in relation to information security. Specifically, it seeks to introduce greater flexibility for organisations when implementing data security measures, shifting the emphasis away from an approach entirely focused on "technical and organisational measures". The Bill is currently awaiting its next review at the committee stage in the House of Lords.

The UK government also continues to progress amendments to the Computer Misuse Act (CMA), which has previously been criticised for failing to keep pace with the evolving cybersecurity landscape. The UK government has put forward a proposal for legislative change, including the introduction of statutory defences for those taking action to protect the UK in cyberspace, a general offence for possessing or using illegally obtained data, and discussion on whether the CMA would benefit from extra-territorial provisions, among other recommendations. Responses to the latest consultation regarding amendments to the CMA were published on 14 November 2023, whereby the UK government noted that it would continue to engage private and public sector organisations in order to understand further impacts and mitigations in this area before the amendments would be enacted.

On 23 January 2024, the UK government published its draft Cyber Governance Code of Practice (the "Code of Practice"), which has been designed in partnership with the NCSC (among other cybersecurity experts). The draft Code of Practice, which is intended for directors and other senior leaders, aims to assist UK businesses in adopting a "top-down" approach to cyber-resilience – in turn, giving cyber-risk the same prominence as financial or legal risk. The draft Code of Practice proposes the following five overarching principles (together with relevant corresponding actions):

- risk management;
- cyberstrategy;
- people;
- incident planning and response; and
- assurance and oversight.

The UK government is exploring how the draft Code of Practice can assist with existing regulatory compliance obligations under the GDPR and NIS Regulations.

Contributed by: William Long, Francesca Blythe, Denise Kara and Eleanor Dodding, **Sidley Austin LLP**

The need for the UK to remain agile and proactive in its approach to cybersecurity governance – in particular, in response to emerging technologies such as generative AI – will undoubtedly be a priority for the UK government in 2024.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com