Chambers

GLOBAL PRACTICE GUIDE

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

Cybersecurity

UK
William Long and Vishnu Shankar
Sidley Austin LLP

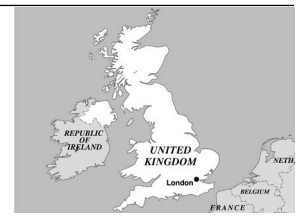
chambers.com

2020

UK

Law and Practice

Contributed by:
William Long and Vishnu Shankar
Sidley Austin LLP see p.13



Contents

1. Basic National Regime

1.1 Laws

The UK has a well-developed – and growing – network of civil and criminal laws relating to cybersecurity. These are contained in EU and UK legislation, companion rules made under such legislation, decisions of EU and UK courts, and a steady stream of regulatory guidance from UK and EU regulators. These laws are increasingly being enforced by UK governmental authorities – including the Information Commissioner's Office (ICO) and sector-specific regulators such as the Financial Conduct Authority (FCA) – and private individuals and organisations. The primary UK cybersecurity legislation comprises the following.

Firstly, the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (DPA). The GDPR and the DPA apply to the security of information that is considered "personal data" under these laws. The 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, Network and Information Systems Regulations (NIS Regulations). The NIS Regulations (which implement the EU Network and Information Systems Directive into UK law) apply to two categories of key infrastructure operators, namely "operators of essential services" (OESs) and "relevant digital service providers" (RDSPs). Like the GDPR, the NIS Regulations requires organisations that are subject to it, to implement certain cybersecurity measures and to provide notices of certain cybersecurity incidents that affect such organisations.

Thirdly, the Computer Misuse Act 1990 (CMA). The CMA is the UK's primary legislation with respect to criminalising unauthorised access to computers 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: 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.

Fourthly, 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). (PECR implements the EU Directive on Privacy and Electronic Communications (Directive 2002/58/EC) (E-Privacy Directive) into UK law.) These laws 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, FCA rules (applicable to organisations that the FCA regulates), Payment Services Regulations 2017 (PSR) (which transposes the Second Payment Services Directive into UK law, and applies to payment service providers), and the Official Secrets Act 1989 (OSA, applicable to certain official government information). Similarly, the Investigatory Powers Act 2016 (IPA) and the Regulation of Investigatory Powers Act 2000 (RIPA regulates electronic surveillance and interception in the UK and contains associated safeguards.

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 (i) has been consented to by the discloser, or (ii) is required by law. The FCA rules, PSR, OSA, IPA, 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.

GDPR and DPA

In the UK, the ICO is responsible for monitoring the application of the 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.

NIS Regulations

With respect to the NIS Regulation, the "competent authority" is determined on an industry-by industry basis. For example, for OESs in the oil sector, the competent authority in England, Scotland and Wales is the Secretary of State for Business, Energy and Industrial Strategy, while in Northern Ireland it is the Department of Finance.

PECR and CA 2003

In regard to PECR, the ICO may audit the compliance of service providers pursuant to Regulation 5A of PECR. Notifiable personal data breaches under Regulation 5A of 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 respect to the CA 2003, which is a companion legislation to PECR, the Office of Communications (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. As noted above, the DPA is enforced by the ICO and prosecutions under the DPA can only be brought by the ICO, or by or with the consent of the Director of Public Prosecutions (DPP).

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 below.

GDPR and DPA

At present, the GDPR and the DPA are being rigorously enforced by the ICO with respect to cybersecurity matters. The ICO is required to adhere to specific procedures before undertaking enforcement action. For example, before imposing an administrative fine on an organisation for (i) breaching the integrity and confidentiality principle, (ii) inadequate security measures, or (iii) 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 EUR20 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. While 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 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 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 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 PECR to issue enforcement notices for breach of the provisions of PECR of up to a maximum of GBP500,000.

Where Ofcom receives a notice under Section 105B of the CA 2003, it may, where it considers it appropriate, notify the European Network and Information Security Agency (ENISA) and regulatory authorities in other member states. 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. Section 1 is hereby considered; as noted previously, an offence under Section 1 is committed if there is "unauthorised" access to a computer system. A Section 1 CMA offence is triable 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.

In 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 which must be followed when the CPS makes a decision on cases. While there are no official guidelines for sentencing offences under 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 GDPR and the DPA apply to (i) all organisations established in the four countries of the UK (ie, England, Northern Ireland, Scotland and Wales), and (ii) organisations not established in the UK (or the EEA prior to 31 December 2020) processing personal data of data subjects in the UK to offer goods or services, or to monitor their behaviour. In turn, and as discussed previously, the ICO regulates the GDPR and the DPA across the UK.

While 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. For 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 and 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 which has facilitated the offending may have passed through a server based in a relevant country of the UK.

1.5 Information Sharing Organisations
Please see Section **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 EEA (rather than the USA). Recently, the enforcement of cybersecurity rules in the UK has become very robust, particularly by the ICO. Notably, in July 2019 the ICO issued a notice of intent to fine British Airways around GBP183 million following a cyber-attack. The cyber-attack allegedly resulted in user traffic to the British Airways website and mobile application being diverted to a fraudulent website. This, in turn, allegedly led to customers' personal data – including names, postal addresses, email addresses and payment card details (eg, card numbers, expiry dates and, in some cases, security codes) – being compromised.

Immediately following its announcement regarding British Airways, the ICO also announced its intention to fine Marriott International (Marriott) around GBP99 million for alleged failures relating to cybersecurity. According to the ICO, Marriott failed to conduct appropriate cybersecurity diligence in its acquisition of Starwood Hotels (which failure, in turn, allegedly resulted in Marriott's inability to discover that Starwood Hotels had suffered a serious cyber-attack).

1.7 Key Developments
As noted above, the key cybersecurity legal developments in the UK in the prior 12 months are: firstly, the ICO's intention to fine British Airways and Marriott for alleged cybersecurity failures; secondly, the commencement of a group litigation (similar to US-style class actions) against British Airways with respect to the same cyber-incident; and thirdly, the ICO's first-ever use of the CMA to prosecute offences relating to personal data. The first point was covered in **1.6 System Characteristics**; the second and third points are considered below.

On 4 October 2019, the English High Court granted a group litigation order, approving a group legal action from over 500,000 British Airways customers seeking damages relating to the compromise to their personal data from the cyber-attack. The total amount of claimants is expected to increase, with the High Court extending the deadline for affected data subjects to join the claim to 17 January 2021. This litigation is an important reminder that enforcement action by the ICO is not the only consequence organisations face for allegedly insufficient cybersecurity. In fact, public reports appear to suggest that Brit-

ish Airways could potentially incur damages as high as GBP3 billion.

That the ICO is taking cybersecurity seriously is further demonstrated by the conviction it helped secure in its prosecution of Mustafa Kasim. In this case, the ICO undertook its first prosecution of a data protection-related offence 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". As a result, in November 2018, Mustafa Kasim became the first person to ever be prosecuted under the CMA by the ICO.

Kasim pleaded guilty to a charge of securing unauthorised access to personal data and was sentenced to six months in prison under a Section 1(1) CMA offence. Here, the defendant's used a former co-worker's log-in credentials to steal personal data from his former employer's vehicle repair software. A further hearing in July 2019 found that Kasim had benefitted financially, and he was ordered to pay a GBP25,500 confiscation order and GBP8,000 costs.

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 below.

Firstly, there is likely to be continued robust enforcement of UK cybersecurity laws (in particular, the GDPR and the DPA) and, equally, a robust defence by organisations that are the subject of any enforcement action, including British Airways and Marriott. In fact, under Schedule 16 of the DPA, the period for which the ICO can issue an organisation with a penalty notice (six months following a notice of intent) may be extended upon agreement by the ICO and the alleged offending organisations. The ICO has agreed to an extension with British Airways and Marriott to 31 March 2020. A final decision by the ICO is expected in the next 12 months on both of these enforcement actions, which decision may, in turn, be challenged by British Airways and/or Marriott.

Secondly, developments at the EU level with respect to replacing the E-Privacy Directive and potentially any associated cybersecurity rules are expected. The institutions of the EU have been considering replacing the current E-Privacy Directive with a new E-Privacy Regulation. The draft E-Privacy Regulation, which was originally intended to apply from 25 May 2018, will replace the E-Privacy Directive, (ie, the legislation which is implemented into UK domestic law via PECR). However, protracted negotiations in relation to the draft Regulation mean it is unlikely to enter into force until 2023. The ICO has confirmed that, until the draft Regulation comes into force, PECR will continue to apply.

Thirdly, there may be moves to amend the CMA, which commenced as far back as 1990 and was last amended in 2015, in order to address the Serious Crime Act 2015. The CMA has, arguably, not kept pace with the cybersecurity landscape. For example, in July 2019, a group of British information security companies wrote to the UK Prime Minister asking for reform of the CMA, saying the act "has failed to keep pace with technological and market developments, inadvertently prohibiting a large component of contemporary threat intelligence research". Their requests included the introduction of "statutory defences that apply to accredited professionals who act ethically, in the public interest, to detect and prevent criminal activity". This particular point addresses a concern that the broad drafting of the CMA does not make it entirely clear what is and what is not illegal in the fast-moving world of information security, potentially preventing security professionals from carrying out threat intelligence research and journalists and academics from researching security threats.

Separately, the Criminal Law Reform Now Network has also recently produced a report on Reforming the Computer Misuse Act which highlights similar issues, including 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.

2. Key Laws and Regulators at National and Subnational Levels

2.1 Key Laws

Please see comments at **1.1 Laws**.

2.2 Regulators

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

2.3 Overarching Cybersecurity Agency

The European Union Agency for Cybersecurity (ENISA) supports EEA member states and the UK (during the Brexit transition period) in developing an EEA-wide cybersecurity policy at least with respect to the GDPR and the NIS Regulations. The UK National Cybersecurity Centre (NCSC) is the key UK cybersecurity agency, co-ordinating UK cybersecurity policy and technical standards, particularly with respect to the NIS Regulations and the 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 and relevant authorities in the EEA.

2.4 Data Protection Authorities or Privacy Regulators

Please see comments at **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 respect to the same cybersecurity incident. For example, a major cybersecurity incident affecting an OES that results in the compromise of personal data could implicate the 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, for example, implicate the 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 comments at **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: (i) Principle 3 (Management and Control) of the FCA Handbook *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 (ii) Principle 11 (Relations with Regulators) which requires that "a firm must deal with its regulators in an open and cooperative 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: (i) the FCA (and the Prudential Regulation Authority for dual-regulated firms) should be notified; (ii) if the incident is criminal, Action Fraud (which is the UK's national fraud and cybercrime reporting centre) should be contacted; and (iii) where the incident is also a 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 CiSP platform; please see comments at **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. For example, payment services providers are required to report major operational and security incidents pursuant to the PSR.

2.6 Other Relevant Regulators and Agencies

Please see comments at **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. For example, the ICO recommends that organisations review the UK Cyber Essentials scheme (which is a UK government and industry-backed scheme) that provides 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.

3.2 Consensus or Commonly Applied Framework

Please see comments in **3.1 De Jure or De Facto Standards** and **3.3 Legal Requirements**.

3.3 Legal Requirements

GDPR

The GDPR requires that controllers and processors implement "appropriate" technical and organisational security measures. When adopting such measures, the GDPR requires organisations to take into account the state-of-the-art, costs of implementation and the nature, scope, context, purposes of the processing of personal data and 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).

By way of illustration, the 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 what 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);
- online security – website and mobile application security; and
- device security – considering information security policies for bring-your-own devices, where offered by the organisation.

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.

PECR and CA 2003

Regulation 5(1A) of PECR requires service providers to: (i) restrict access to personal data to only authorised personnel; (ii) protect personal data against "accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure"; and (iii) implement a security policy with respect 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 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 which 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 NCSC – work closely with their counterparts in the EEA, such as other data privacy authorities that comprise the European Data Protection Board (with respect to the ICO) and the ENISA (with respect 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 U.S. Federal Trade Commission, the federal Privacy Commissioner of Canada and New Zealand's Department of Internal Affairs.

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 U.S. Securities and Exchange Commission (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.

4. Key Affirmative Security Requirements

4.1 Personal Data

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

4.2 Material Business Data and Material Non-public Information

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

4.3 Critical Infrastructure, Networks, Systems

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

4.4 Denial of Service Attacks

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

4.5 Other Data or Systems

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

5. Data Breach Reporting and Notification

5.1 Definition of Data Security Incident or Breach

GDPR and DPA

Under the GDPR, "personal data breaches" are potentially reportable data security incidents. A "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 GDPR and DPA – and in turn, applicable notification obligations – only apply where the breach involves personal data. As the Article 29 Working Party (WP29), the predecessor of the European Data Protection Board, notes in its guidance on personal data breaches "all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches".

Further, the WP29 categorises personal data breaches in the following three breaches of security: (i) confidentiality breach – unauthorised or accidental disclosure of, or access to, personal data; (ii) integrity breach – unauthorised or accidental alteration of personal data; and (iii) 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 and/or any other relevant EEA data privacy regulator of the breach 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 to address the breach. There are certain narrow exemptions from the obligation to notify data subjects, such as where the compromised personal data was encrypted.

NIS Regulations

Under the NIS Regulations, an OES must notify its relevant competent authority of any incident that has a "significant impact" on the continuity of the essential service the OES provides. An RDSP must provide notification of any incident having a substantial impact on the provision of any digital services that it provides. By comparison to the GDPR, notifiable incidents under the NIS Regulations need not always involve personal data, though they may do. 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 GDPR (if they do not involve personal data).

Comparable with the GDPR, both OESs and RDSPs must notify its 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 3 of PECR defines a personal data breach as 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 in connection with the provision of a public electronic communications service. The security and breach notification requirements under Regulation 5 of PECR apply to personal data.

Under Regulation 5A of PECR, service providers are required to notify the ICO in the event of a personal data breach (as defined under Regulation 3 of 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 105B of CA 2003 apply to public electronic communications networks and systems: network and service providers must notify Ofcom of security breaches which have a significant impact on the operation of a public electronic communications network. By contrast, CA 2003 does not define what is meant by a breach of security. Guidance on Security Requirements, published by Ofcom, provides further clarity on which incidents are likely to be significant and should therefore, be reported.

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 GDPR standard of "without undue delay". In such case, the processor would need notify its controller within such 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 comments under **5.1 Definition of Data Security Incident or Breach**.

5.3 Systems Covered
Please see comments under **5.1 Definition of Data Security Incident or Breach**.

5.4 Security Requirements for Medical Devices
In the UK, NHS Digital (the body responsible for information, data and IT systems in health and social care) 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 which incorporates the notification requirements of the GDPR and the NIS Regulations.

At an EU level, but applicable to the UK, the Medical Device Coordination Group published guidance in 2019 on cybersecurity for medical devices which is intended to assist medical device manufacturers meet the new cybersecurity requirements in the Medical Devices Regulation and the In Vitro Diagnostic Regulation. According to the guidance, safety, security and effectiveness are "critical aspects in the design of security mechanisms" for medical devices.

The guidance in turn states that these concepts should be considered by the device manufacturer at an early stage in the development and manufacturing process and then throughout the life-cycle. A concept of "secure by design" is also introduced in the guidance which closely aligns with the requirement of privacy by design under the GDPR.

5.5 Security Requirements for Industrial Control Systems (and SCADA)
Please see comments under **5.1 Definition of Data Security Incident or Breach**.

5.6 Security Requirements for IoT
In May 2019, the UK Government launched a consultation on regulatory proposals to ensure consumer IoT devices adhere to a basic level of security. The Government published a response to the consultation on 27 January 2020. In particular, the regulations would require that:

- all consumer IoT device passwords be unique and incapable of being reset to any universal factory setting;
- manufacturers of consumer IoT devices provide a public point of contact for reporting vulnerabilities, and that these must be acted on in a timely manner; and

- manufacturers of consumer IoT devices explicitly state the minimum length of time for which the device will receive security updates at the point of sale.

5.7 Reporting Triggers
Please see comments under **5.1 Definition of Data Security Incident or Breach**.

5.8 "Risk of Harm" Thresholds or Standards
Please see comments under **5.1 Definition of Data Security Incident or Breach**.

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 GDPR obligations would need to be complied with. Key GDPR obligations would involve (among other things) providing GDPR-compliant notices to individuals, establishing a legal basis under the under the GDPR for such data processing (such as relying on "legitimate interest", and conducting a data protection impact assessment (DPIA) with respect to any data processing activities that are considered "high risk" under the GDPR.

Regarding the GDPR legal basis, while 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 as between its legitimate interest to implement network monitoring and other cybersecurity defensive measures while 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 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 comments under **6.1 Cybersecurity Defensive Measures**.

7. Cyberthreat Information Sharing Arrangements

7.1 Required or Authorised Sharing of Cybersecurity Information
Please see comments under **5.1 Definition of Data Security Incident or Breach**.

7.2 Voluntary Information Sharing Opportunities
A key information sharing organisation in the UK is the Cyber Security Information Sharing Partnership (CiSP). It is a joint industry and UK government initiative which is 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 respect to British Airways and Marriott/Starwood cybersecurity breaches has already been discussed in **1.6 System Characteristics**.

Another important ongoing UK cybersecurity litigation relates to Morrisons, the UK supermarket chain. In 2018, the English Court of Appeal upheld a ruling that the company was vicariously liable for the deliberate and malicious personal data breach committed by one of its employees. The court found that Morrisons, although not directly liable for the deliberate data breach of its employee, was liable for the employee's breach under the English common law principle of vicarious liability. This is, in turn, significant because it potentially exposes organisations to cybersecurity liability under both statutory and common law regimes.

The English Court of Appeal held that although the (now-repealed) UK Data Protection Act 1998 did not contain any provisions on vicarious liability, this did not prevent Morrisons from being found to be vicariously liable under the English common law torts of breach of confidence and the misuse of private information. Separately, the court rejected Morrisons' argument that as the employee had committed the breach at home there was no link to Morrisons. It held that there was no separation between his work at Morrisons and his disclosure of personal data, but rather that it was a sequence of events which started at the workplace.

The court also rejected Morrisons' arguments that due to the sheer size of the claimant class action – 5,518 employees – a significant burden would be placed on Morrisons were they to be found vicariously liable for their employee's data breach. However, the court took a different view noting that insurance, if obtained by an employer, could prevent serious financial harm to the employers, and that employers who insure against catastrophes can insure against losses caused by dishonest or malicious employees.

Morrisons has now appealed to the UK Supreme Court.

CMA

The ICO's prosecution of Mustafa Kasim under the CMA was discussed in **1.7 Key Developments**. There have been numerous other prosecutions under the CMA, including relating to cyber-extortion, ransomware and misuse of employee online account passwords.

8.2 Significant Audits, Investigations or Penalties

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

8.3 Applicable Legal Standards

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

8.4 Significant Private Litigation

Please see comments under **1.6 System Characteristics**, **1.7 Key Developments** and **8.1 Regulatory Enforcement or Litigation**. In addition, individuals are allowed to bring claims under the GDPR (including through representative actions). The British Airways group litigation has 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 comments under **8.4 Significant Private Litigation**.

9. Due Diligence

9.1 Processes and Issues

The importance of conducting appropriate cybersecurity diligence in connection with corporate transactions is well illustrated by the ICO's intention to fine Marriot around GBP99 million. More generally, M&A acquirers could (post-transaction) be directly liable for the M&A target's GDPR and cybersecurity breaches if the acquirer were to, for example, exercise "decisive control" 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, (among other things) the target and acquirer are at risk for both regulatory fines (of up to 4% of annual worldwide group revenues) for non-compliance and 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 and vulnerability of the target's information technology and software systems, 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.

9.2 Public Disclosure

The matter is not relevant in this jurisdiction.

9.3 Other Significant Issues

All significant issues have already been addressed.

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 2,000 lawyers in 20 offices worldwide. Sidley maintains a commitment to providing quality legal services and to offering advice in 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. Sidley's lawyers help 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, intellectual property, information management and records retention, e-commerce, consumer protection and cybercrimes. 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 of the firm. He is global co-leader of Sidley's privacy and cybersecurity practice and leads the EU data protection practice. He advises international clients on a wide variety of GDPR, data protection, privacy, information security, social media, e-commerce and other regulatory matters. William 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. He is also on the editorial board of e-Health Law & Policy and assists with dplegal, which is a network for privacy professionals.

Vishnu Shankar is a senior associate at the firm, and an experienced EU data protection, privacy, cybersecurity, e-commerce and information technology lawyer. He provides practical and strategic advice to international clients regarding the EU's General Data Protection Regulation, e-privacy laws, the NIS Directive, international data transfers (including the EU-US Privacy Shield) and sector-specific privacy and cybersecurity laws. He also has significant experience in assisting clients with preparing for, and remediating, high-stakes cybersecurity breaches, including responding to regulators. Vishnu also works with clients on data protection legal reforms that are ongoing in Asia, particularly India's efforts to enact a new data protection law.

Sidley Austin LLP

70 St Mary Axe
London
EC3A 8BE

Tel: +44 20 7360 3600
Fax: +44 20 7626 7937
Web: www.sidley.com