Chambers
Global Practice
Guides

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

Cybersecurity 2022

UK: Law & Practice
and
UK: Trends & Developments

William Long and Francesca Blythe
Sidley Austin LLP

practiceguides.chambers.com

UK

Law and Practice

Contributed by:
William Long and Francesca Blythe
Sidley Austin LLP see p.20

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, contained in EU and 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 established outside of the UK but who 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 UK law as the "UK GDPR", which took effect in UK 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 UK 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, 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 UK 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. Please note that the UK government has indicated that it plans to amend the NIS Regulations to widen its scope to include managed service providers (MSPs) which provide specialised online and digital services. MSPs include security services, workplace services and IT outsourcing.

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) 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 Financial Conduct Authority (FCA) – and private individuals and organisations. Regulators are also increasingly collaborating on cybersecurity enforcement with, for example, the ICO teaming up with the Competition and Markets Authority (CMA), the Office of Communications (Ofcom) and the Financial Conduct Authority (FCA) to form the Digital Regulation Cooperation 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 (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.

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.

NIS Regulations

With respect to the NIS Regulation, the "competent authority" is determined on an industry-by industry basis, through the Department for Digital, Culture, Media & Sport (DCMS), which oversees the implementation of the NIS Regulations across the UK. 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. 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) who offer 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

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, 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.

UK GDPR and DPA

At present, the UK GDPR and the DPA are being rigorously enforced by the ICO, including with respect to cybersecurity matters – but only to the extent 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. 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 breach-

ing 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.

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 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 (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 processing personal data of data subjects in the UK to offer goods or services, or to monitor their behaviour. In turn, and as dis-

cussed previously, the ICO regulates the UK 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, 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 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 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. 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 around 400,000 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.

Also in October 2020, the ICO fined Marriott International (Marriott) GBP18.4 million for alleged failures relating to cybersecurity. According to the ICO, Marriott allegedly failed to discover that Starwood Hotels had suffered a serious cyber-attack prior to its acquisition by Marriott.

The UK government is also expected to overhaul its ability to assist and promote cybersecurity through its government cybersecurity strategy for 2022 to 2030. There is to be a focus on government functions, including the establishment of the Government Cyber Coordination 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 prior 12 months include the announcement by the UK government of its National Cyber Strategy 2022, which is built around five key pillars:

- strengthening the UK cyber-ecosystem by investing in cyber skills across the economy;
- tackling cyber-risks so that everyone, but especially businesses, can trust in new technologies and maximise their ability to unlock economic value in digital technology;
- innovating and strengthening frameworks for secure future technologies;
- advancing UK leadership in the cybersecurity world; and
- "detecting, disrupting and deterring UK adversaries" to enhance UK security in and through cyberspace, "making more integrated, creative and routine use of the UK's full spectrum of levels" (including sharing information on malicious cyber actors).

The strategy is complimented by other national strategies on artificial intelligence (AI) and data, which were released in 2021.

Secondly, there have been significant developments regarding "class action" lawsuits for cyberbreaches. In November 2021, the Supreme Court delivered its judgment in the case of Google v Lloyd. The claimant, Mr Lloyd argued that individuals who had their personal data sold to third-party advertisers without their consent, could claim a set amount of minimum damages for the "loss of control" over their personal data. However, the Supreme Court held that a mere "loss of control" over personal data could not lead to a claim for damages. Instead, individuals who had suffered the breach would have to come forward for an individualised assessment of the loss they personally had suffered.

However, the case did not state that class actions could never be successful. The Supreme Court instead stated that class actions could be successful if pursued in two stages: (i) by first having a representative action for declaratory relief on the issue of the cybersecurity breach; and (ii) by having a second opt-in action where individuals could come forward to demonstrate the loss they had faced as a result of the breach. It is at this stage that damages could also be quantified and given. The Supreme Court's judgment has therefore clarified the position of how group actions for cyberbreaches should be pursued in the UK. However, arguably, such actions are now less attractive, as this two-stage process will be more cumbersome to run for litigation funders.

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 UK GDPR and the DPA) and, equally, a robust challenge by organisations that are the subject of any enforcement action. For example, the ICO has stated that one of their key priorities for 2022 is to focus on cyber-attacks and how to counter them – including through taking action against organisations who fail to be aware of cyber-risks, opening themselves up to cyberbreaches.

Secondly, the DCMS is drafting a whole legislative package to tackle increasing cybersecurity risks which have been exacerbated by the ongoing pandemic. This includes a new law on smart devices, the National Security and Investment Act 2021, the updated NIS Regulations (as explained in **1.1 Laws**) and the Product Security and Telecommunications Infrastructure Bill. The UK government also announced that it will provide detail on actions to improve cybersecurity in its forthcoming Cyber Security Regulation and Incentives Review. The already established UK Cyber Security Council is also to be given higher powers in terms of agreed qualifications and certifications for those working in cybersecurity.

Thirdly, the UK government is making moves to amend 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 cyberhacking 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.

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 Over-Arching Cybersecurity Agency

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 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 to allow for improved cybersecurity across Europe.

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 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, for example, 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 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:

- 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
- 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:

- the FCA (and the Prudential Regulation Authority 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 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 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.

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

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, 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 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 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);
- actively managing software vulnerabilities, including using in-support software and the application of software update policies (patching), and 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.

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. While 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.

PECR and CA 2003

Regulation 5(1A) of 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 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 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 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 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,** as well as **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**, as well as **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**, as well as **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**, as well as **5. Data Breach Reporting and Notification**.

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

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

5. DATA BREACH 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 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:

- confidentiality breach – unauthorised or accidental disclosure of, or access to, personal data;
- integrity breach – 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 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, 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 which 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, 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 UK GDPR if they do not involve personal data.

Comparable with the UK 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 UK GDPR standard of "without undue delay". In such case, the processor would need notify to 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, Breach or Cybersecurity Event**.

5.3 Systems Covered

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

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 UK GDPR and the NIS Regulations. There is also a GDPR-focused Respond to an NHS cyber alert document which explains the intersection between medicine, personal data and cybersecurity.

At an EU level, but highly persuasive from a UK perspective, the Medical Device Coordination Group published updated guidance in June 2020 on cybersecurity for medical devices, which is intended to assist medical device manufacturers meet the cybersecurity requirements in the Medical Devices Regulation and the In Vitro Diagnostic Regulation. According to the updated guidance, manufacturers must consider safety and cybersecurity throughout the lifecycle 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 comments under **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**.

5.6 Security Requirements for IoT

In November 2021, the UK government introduced the Product Security and Telecommunications Infrastructure Bill to regulate IoT. In particular, the new legislation will 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.

The new regime will be overseen by a new (and as yet unnamed) regulator, that will have the power to levy GDPR-style fines. Companies that fail to comply with the bill could be fined GBP10 million or 4% of their annual revenue, as well as up to GBP20,000 a day in the case of an ongoing contravention.

5.7 Requirements for Secure Software Development

Please see comments under **3.3 Legal Requirements** and **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**.

5.8 Reporting Triggers

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

5.9 "Risk of Harm" Thresholds or Standards

Please see comments under **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 respect to any data processing activities that are considered "high risk" under the UK GDPR.

Regarding the UK 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 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 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, Breach or Cybersecurity Event**.

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 Google v Lloyd, British Airways and Marriott/Starwood 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 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 UK GDPR (including through representative actions). The British Airways group litigation and Lloyd v Google 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 fining Marriot 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 for both 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 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.

10. INSURANCE AND OTHER CYBERSECURITY ISSUES

10.1 Further Considerations regarding Cybersecurity Regulation

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 you understand your organisation so that an appropriate level and type of cover is set;
- checking if the cyber insurance policy you are looking at covers claims for compensation by third parties in the event of a cyber-attack, or if personal data is lost as a result of a data breach at an organisation (for example, 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 with the Cyber Security Breaches Survey 2021 revealing that two in five businesses have experienced cyber security breaches in the last 12 months. In particular, the 2022 Cybersecurity Incentives and Regulation Review has highlighted wanting to build a business case for increasing organisational investment in cybersecurity insurance or associated training, providing additional evidence to support external reporting requirements such as a cyber insurance claim and the provision of further data for use with modelling cyber-risk impact as part of insurance claims.

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 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 of Sidley Austin. He is global co-leader of Sidley's highly ranked privacy and cybersecurity practice and leads the EU and UK 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.

Francesca Blythe is a senior managing associate at the firm, and an experienced EU data protection, privacy and cybersecurity lawyer. She 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 with respect to the Schrems II decision) and sector-specific privacy and cybersecurity laws. She also has significant 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 20 7360 3600
Fax: +44 20 7626 7937
Web: www.sidley.com

Trends and Developments

Contributed by:
William Long and Francesca Blythe
Sidley Austin LLP see p.24

Introduction

Cybersecurity has remained a priority issue for both businesses and regulators alike. These regulators include the UK Information Commissioner's Office (ICO), which has continued to take strong enforcement action throughout 2021 and into 2022. This is due in part to the continuation of the COVID-19 pandemic, where increasing reliance on technology and rapid digitisation by businesses has resulted in a surge of phishing, ransomware and distributed denial-of-service (DDoS) attacks. In turn, it is perhaps unsurprising that the UK government is investing more in updating its cybersecurity strategy, with several policy papers and new legislation in the works for 2022.

Continued Growth of Cybersecurity Threats

The threat of ransomware attacks continued to loom in the past 12 months. However, 2021 also saw the growth of additional threats, including nation-state actors launching cyber-attacks for global security information. While the first half of 2021 was marked by cybercriminals targeting large organisations – including infrastructure providers in the USA, who were targeted in May 2021 – the second half of the year saw indiscriminate attacks against all companies, regardless of industry or size. In its fifth annual review, published on 17 November 2021, the UK's National Cyber Security Centre (NCSC) reported that all organisations, including small businesses, were now at risk of such breaches and attacks, with 39% of all UK businesses suffering such an incident in 2020–21; for further details, see NCSC Annual Report 2021.

Ransomware, in particular, has become much more sophisticated in 2021, with a new "triple extortion" technique being used, where malicious actors:

- publicly release confidential company information;
- disrupt company systems – eg, through further loss or encryption of data; and
- blackmail the company.

Technical aspects of a typical attack now also routinely include targeting a company's cloud, managed service providers and/or organisations when they are most vulnerable – such as during holidays or at weekends.

Further, the NCSC, together with its US and Australian counterparts, observed that cybercriminals are becoming far more organised and sophisticated, with the emergence of cybercriminal services for hire being offered online – including ransomware threat actors who offer their victims the services of 24/7 help centres to expedite ransom payment and restoration of encrypted systems or data.

The NCSC also noted that cybercriminals continue to exploit the COVID-19 pandemic as an opportunity to both manipulate people and businesses, as well as to target those in education, health and government authorities – for example, to steal state vaccine and medical research.

Supply-chain attacks continue to be an issue of particular concern following the compromise of several major US companies which have been targeted by malicious state actors. Such actors have infiltrated IT systems and inserted malicious codes into the target's software, sometimes causing global issues across thousands

of organisations in the supply chain. The NCSC has issued practical guidance specific to certain high-profile attacks, including for organisations to:

- update their systems to use the latest version of any software (eg, through patching);
- keep open communication with in-house developers and third-party suppliers to ensure all software is regularly tested and updated; and
- report any incident or compromise to the NCSC.

Cybersecurity Reforms

Given the increasingly sophisticated and prevalent nature of cyber-attacks, many governments have understandably sought to refresh their cybersecurity regimes. The UK government has introduced a whole package of reforms as part of its National Cyber Strategy 2022, which was published on 15 December 2021, and its first Cyber Security Strategy for 2022–2030. The reports recognise that there is currently a "significant gap" in the UK's cyber-resilience and proposes a range of recommendations and measures. These include adopting the NCSC's Cyber Assessment Framework (CAF) to ensure that there is an industry standard of cybersecurity. Further, the UK government will establish a cyber-coordination centre (GCCC) to liaise between government organisations in an effort to share cybersecurity data and intelligence rapidly. In addition, the UK government wants to hone its ability to tackle cyberbreaches – for example, by working in partnership with the Alan Turing Institute to learn how to use artificial intelligence (AI) to detect cyber-attacks more efficiently.

New legislation is also being proposed, especially in those sectors where the UK government perceives there to be the greatest potential impact of cyber-attacks, such as within public authorities and to critical service providers. Thus, in the first instance, updates are expected to the Network and Information Systems (NIS) Regulations. The UK government also hopes to empower intelligence agencies to tackle cybersecurity threats from malicious state actors, including through the Counter State Threats Bill and the plans to amend the Proceeds of Crime Act 2002 (POCA). The aim of the amended POCA is to identify, seize and recover the proceeds of cybercrime.

Moreover, the UK government wants to protect more consumers from cyber-attacks and has introduced efforts to do this. One such measure is through regulating the internet of things (IoT) with a new bill entitled the Product Security and Telecommunications Infrastructure Bill (PST). The UK government states that such legislative updates will compliment other policy efforts such as the Plan for Digital Regulation and the National Strategies on AI and data, respectively.

Part of the National Data Strategy is the UK government's recent consultation entitled Data: a new direction, which was published in September 2021. The consultation, responses to which are currently being considered, has significant implications for cybersecurity. In particular, the reforms propose to lower the threshold for data breach reporting, by allowing organisations to avoid reporting a breach at all where an incident is considered to be "not material".

This represents a shift from the previous test for reporting a breach, which was that an organisation had to report to the ICO unless the incident was "unlikely" to result in a risk to people's rights and freedoms. The ICO's reaction to this proposal was mixed. While, on the one hand, they acknowledged that fewer minor data breach reports would free up time and resources to investigate more sophisticated cyberbreaches, they also commented that the UK government proposal lacked detail in terms of what consti-

tuted a "non-material" risk that "need not be reported". Thus, the ICO encouraged the UK government to provide comprehensive guidance on how the new data breach reporting obligations would work in practice. The UK government is expected to take on board the ICO's comments and will introduce legislation on this issue at some point in 2022, though a specific date is yet to be announced. Time will tell if an updated reporting system simplifies cybersecurity compliance for organisations, or if it poses a threat to the data protection rights of individuals.

Data Privacy-Related "Class Actions" in the UK: Google v Lloyd

Another important cybersecurity development is the UK Supreme Court's consideration of data privacy "class action" lawsuits. These large-scale claims have traditionally been a mainstay of US litigation. However, following the filing of several group litigation cases against high-profile organisations between 2018 and 2020, there was a sense amongst legal commentators that such data privacy-related class actions were also becoming more common in the UK.

Google v Lloyd provided, therefore, an important test case for the Supreme Court to consider if an individual could use a representative action to claim a figure of damages on behalf of each individual in a class. The case was about Google illegally tracking individuals and selling their personal data. Mr Lloyd claimed that this data breach amounted to a "loss of control" of personal data, which could be quantified to allow for damages to be claimed across the class. However, the Supreme Court rejected these arguments, seemingly closing the door on any kind of group or representative litigation in relation to cybersecurity breaches.

However, the Supreme Court emphasised that this was not the case, and that class actions could work on a bifurcated basis whereby: (i) there would be a representative action for declaratory relief on the issue of the cybersecurity breach; and (ii) there would then be an opt-in group action for individuals to come forward and claim damages. Therefore, businesses should be wary that there is still the possibility of group actions for cybersecurity breaches, albeit that such actions will be less attractive to litigation funders because of the risks of adverse cost orders, and due to the difficulties in assessing the size of the group in these kinds of opt-in representative actions. Nevertheless, the case does still emphasise the costs that can result when organisations get cybersecurity wrong.

The increase in cyber-attacks, especially relating to sophisticated ransomware, coupled with UK GDPR fines and enforcement actions (detailed in our adjacent **UK Law & Practice** article), the potential for litigation by data subjects, and the fast-developing laws in cybersecurity, illustrates that organisations must maintain a strong cybersecurity regime and be agile to change. Organisations should be ready to assess their compliance and respond, especially in light of the new UK legislative reforms on the horizon in 2022.

This article has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create, and the receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers. The content therein does not reflect the views of the firm.

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 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 of Sidley Austin. He is global co-leader of the firm's highly ranked privacy and cybersecurity practice and leads the EU and UK 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.

Francesca Blythe is a senior managing associate at Sidley Austin, and an experienced EU data protection, privacy and cybersecurity lawyer. She 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 with respect to the Schrems II decision) and sector-specific privacy and cybersecurity laws. She also has significant 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 20 7360 3600
Fax: +44 20 7626 7937
Web: www.sidley.com

Chambers Guides to the Legal Profession

Chambers Directories are research-based, assessing law firms and individuals through thousands of interviews with clients and lawyers. The guides are objective and independent.

practiceguides.chambers.com