CLIFFORD

CHANCE

CYBERSECURITY
WHAT REGULATORS ARE SAYING AROUND THE WORLD

INTRODUCTION

As cyber attacks increase around the globe, regulators are responding with new cyber and data laws. New audit powers and mandatory reporting requirements are putting businesses in the spotlight, and a serious attack could mean significant reputational and financial impact and loss of customers.

Cyber is not just a technology issue. This is now a major legal risk.

In this report, our experts discuss the new regulations taking effect globally, and how these will impact you now and in the future.

We are here to help. Please get in touch with me or my team with any questions.

Jonathan Kewley
Partner, London

CONTENTS

EUROPE
MIDDLE EAST AND AFRICA

EUROPEAN UNION

GDPR, NIS DIRECTIVE AND PSD2

Cybersecurity is a strategic issue for European businesses, which are increasingly gathering and monetising data but are at risk of significant cyber-attacks. Such attacks have led to significant reputational damage, negative media coverage and diminished customer confidence and trust. European legislators are increasingly concerned with protecting the data of individuals and, in response, have introduced pan-European legislation.

THE GENERAL DATA PROTECTION REGULATION (GDPR)

- The GDPR became effective on 25 May 2018. It represents the biggest change in EU data privacy law in a generation. There are very serious sanctions for breach, including fines which can be as high as 4% of global turnover.
- The following are some of the cybersecurity provisions of the GDPR:
    - **Obligations on data processors:** The previous regime did not directly regulate processors. Under the GDPR, data processors are now required to implement appropriate technical and organisational measures, and are subject to breach notification requirements; in addition, contracts between data controllers and processors will be required to contain mandatory provisions relating to data security.
    - **Personal data breach notification:** Data controllers will now be required to report personal data breach to the relevant national data protection authority, generally "without undue delay" and within 72 hours of becoming aware. Data processors will be required to notify data controllers of security breaches affecting personal data.
    - **Information security measures:** Data controllers and processors are required to implement technical and organisational measures to ensure a level of security appropriate to the risk, including, for example: 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 of personal data following an incident; and processes for regularly testing, assessing and evaluating the effectiveness of measures for ensuring the security of data processing.

The GDPR has significantly extended the extraterritorial effect of the EU data protection regime, including the cybersecurity elements. Entities processing

entirely outside the EEA will be within scope if the processing is carried out in order to offer goods and services to, or monitor the behaviour of, individuals within the EEA.

THE DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS (NIS DIRECTIVE)

As an EU Directive, the NIS Directive required member states to adopt and publish local laws necessary to comply with the NIS Directive by 9 May 2018. The purpose of the NIS Directive was to improve the overall level of cybersecurity across the EU. Sanctions for breach are to be determined by each member state; in the UK, for example, the government has indicated that it favours a sanctions regime mirroring that of the GDPR.

Member states will be required to identify operators of essential services (**OESs**), within the following sectors:

- Energy
- Transport
- Banking
- Financial market infrastructure
- Health
- Water
- Digital infrastructure

Operators of essential services will be required to take appropriate and proportionate technical and organisational measures to detect and manage the risks posed to networks and information systems and notify, without undue delay, the competent authority of incidents that have a significant impact on continuity of the core services provided. Additionally, digital service providers (**DSPs**), being broadly online search engines, online marketplaces and cloud computing services, will be required to implement similar technical and organisational measures, to comply with notification obligations. Of course, close attention should be paid to the local law implementation of the NIS Directive, which will provide the detail of the obligations to be complied with.

One thing that is clear is the urgency of the task we all face. High-impact intrusions are becoming more common, the threats are growing more complex and the stakes are higher than ever.

Christopher Wray, Director of the FBI.

Even if entities are not within the scope of the NIS Directive, many counterparties will expect compliance as "best practice".

By way of example, as at the present date, various jurisdictions have taken steps to implement the NIS Directive, including France, Italy, the Netherlands and the United Kingdom (see further below).

THE REVISED PAYMENT SERVICES DIRECTIVE (PSD2)

Member states were required to transpose PSD2 into national laws and regulations by 13 January 2018. Member states have discretion regarding sanctions; for example, in the UK, the Financial Conduct Authority has a far-reaching sanctions regime with no upper limit on penalties. PSD2 requires payment service providers to comply with additional cybersecurity obligations, including in relation to:

- **Policies and procedures:** Requirements for payment service providers to have a security policy, security control and mitigation measures, including maintenance of effective incident management procedures and a policy to detect and classify major operational or security incidents relating to payment services.
- **Major incident reporting:** Requirement for payment service providers to notify the national regulator of major operational or security incidents within four hours of detection, with intermediate reports required at least every three days, or whenever there is a new development, and a final report to be submitted once the root cause analysis has been carried out.
- **Customer notification of major incidents:** Requirement for payment service providers to notify customers, directly and without undue delay, if a major operational or security incident might impact the financial interests of customers.
- **Annual risk assessments:** Submission of annual assessments to the national regulator of the operational and security risks relating to the payment services they provide and the adequacy of the mitigation and control mechanisms implemented.
- **Strong customer authentication:** Application of "strong customer authentication" when a payment service user accesses its account online, initiates an electronic payment transaction or carries out any other action through a remote channel that may imply a risk of payment fraud or other abuse.

CZECH REPUBLIC

CYBER SECURITY ACT

As regards the regulation of cybersecurity, the Czech Republic is ahead of many EU member states. The comprehensive regulation of cybersecurity was introduced in 2014 when the Czech Parliament passed Act No. 181/2014 Coll. on Cyber Security (the Cyber Security Act). The Cyber Security Act came into effect on 1 January 2015.

Following the adoption of the NIS Directive, the Cyber Security Act was amended several times to bring the national regulation on cybersecurity in line with the EU law. In particular, Act No. 205/2017 Coll. amending the Cyber Security Act introduced a number of requirements arising from the NIS Directive into the Cyber Security Act.

The Cyber Security Act aims to improve cybersecurity and to ensure active co-operation between the private and public sectors in handling cyber incidents. To achieve this, the Cyber Security Act imposes a number of obligations upon selected entities. These entities include: (i) providers of electronic communication services and operators of electronic communication networks; (ii) authorities and administrators of important networks; (iii) administrators and operators of information systems of critical information infrastructure; (iv) administrators and operators of communication systems of critical information infrastructure; (v) administrators and operators of important information systems; (vi) administrators and operators of information systems of essential services; (vii) operators of essential services and (viii) providers of digital services. Unsurprisingly, public sector entities are subject to more obligations than entities operating in the private sector.

Under the Cyber Security Act, the entities listed under (iii) to (vi) above must adopt security measures to provide for cybersecurity of information and communication systems. Similarly, providers of digital services must implement appropriate security measures with respect to electronic communication networks and information systems which they use to provide their services. Furthermore, the Cyber Security Act requires most of the selected entities to notify the relevant authorities of a cybersecurity incident once it has been detected. However, providers of digital services must only notify incidents that have an essential impact. The operator of the national computer emergency response team, currently the CZ.NIC association, and the National Cyber and Information Security Agency (**NCISA**) are in charge of handling notifications. While the entities listed under (ii) and (viii) above make notifications to the CZ.NIC, the entities listed under (iii) to (vii) above must report incidents to the NCISA. A notification to the CZ.NIC can be made by using a form available on

the webpage https://csirt.cz/cs/hlaseni-incidentu/formular-na-hlaseni/. The NCISA offers three ways in which incidents can be reported, namely (i) by filling in an electronic form available on its webpage https://www.govcert.cz/cs/vladni-cert/hlaseni-incidentu/, whereupon the form needs to be sent via email to the address cert.incident@nukib.cz. (PGP encryption is recommended) or to the NCISA's data box (ID zzfnkp3), (ii) via data interface (for more details see https://github.com/GovCERT-CZ/hlaseniKBI), or (iii) over phone (+420 541 110 777, +420 725 502 878). The details on notifications and classification of cybersecurity incidents are specified in Decree of the National Cyber and Information Security Agency No. 82/2018 on security measures, cybersecurity incidents, reactive measures, details on notifications in the area of cybersecurity and data liquidation.

The NCISA is the central body responsible for cybersecurity, including the protection of classified information in the area of information and communication systems and cryptographic protection. It prepares strategic documents concerning national cybersecurity and submits them to the Czech Government for approval. The Czech Government approved the currently valid National Cyber Security Strategy for 2015-2020 by resolution no. 105 on 16 February 2015, and the Action Plan for the National Cyber Security Strategy for 2015-2020 by resolution no. 382 on 25 May 2015.

The NCISA's competencies also include the right to issue a warning once it becomes aware of a cybersecurity threat. The NCISA may also impose an obligation upon the selected entities to adopt reactive or protection measures, and require the operators of information systems of critical information infrastructure, communication systems of critical communication infrastructure or important information systems to provide traffic data and information concerning the systems to the administrator of such systems. Finally, the NCISA monitors compliance with the Cyber Security Act and may conduct an inspection. In the event of a breach of obligations arising from the Cyber Security Act, it may impose a fine of up to CZK 5 million (approx. EUR 181,360).

In the financial sector, an important piece of legislation concerning cybersecurity is the Act on Payment System, into which the revised Payment Services Directive (**PSD2**)[1] was transposed. The Act on Payment System creates a legal framework for technological novelties in the area of payment services and imposes a number of additional cybersecurity obligations upon payment service providers, such as:

- **Major incident reporting:** Payment service providers must notify the Czech National Bank (**CNB**) of major operational or security incidents without

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

undue delay. Notifications must be made in electronic form using the application called Collection of Information of Regulated Entities (https://oam.cnb.cz/sipresextdad/SIPRESEXT.www_forms.uvod?p_lan=EN). Details on the notifications are laid down in Decree of the CNB No. 141/2018 Coll. on Reporting of Major Security and Operational Incidents by Payment Service Providers.

- **Customer notification of major incidents:** If a major operational or security incident may have an impact on the financial interests of customers, payment service providers must inform them of the incident without undue delay. In addition, they must inform customers of all measures they can take to mitigate the adverse effects of the incident and of the fact that financial interests of customers are no longer impacted by the incident once the risk is mitigated.
- **Annual reporting to the CNB:** Payment service providers must report security and operational risks related to their services and frauds they have encountered on an annual basis, in any case not later than by 30 April of the respective calendar year. Details on the reports are laid down in Decree of the CNB 150/2019 Coll. on Reporting of Security and Operational Risks in the Payment Sector. The report for the CNB must, amongst other things, include an up-to-date list of risks related to the payment services, a description of security measures implemented to mitigate detected security and operational risks, a description of control mechanisms implemented and an assessment of whether the measures implemented and control mechanisms are efficient.
- **Strong customer authentication:** Payment service providers must apply strong customer authentication when a customer accesses its payment account online, initiates an electronic payment transaction, carries out any other action that may imply a risk of payment fraud or other abuses, or requires information on the payment account through a provider of account information services. The strong customer authentication must be achieved by using two or more of the following elements, categorised as: (i) knowledge (i.e. information that is known to the customer only); (ii) possession (i.e. thing that the customer has in his/her possession); and (iii) inherence (i.e. biometric data of the customer). These elements must be independent, so that if one of them is compromised, then the reliability of the others will not be affected.

For breaching obligations under the Act on Payment System, payment service providers may be fined up to CZK 1 million (approx. EUR 36,270).

FRANCE

IMPLEMENTATION OF EU LAW

NIS DIRECTIVE

The French NIS Directive implementing law was published on 27 February 2018 and became applicable on 10 May 2018.

Pursuant to this law, if an OES or a DSP fails to comply with its obligation to notify security breaches to the French National Agency for the Security of Information Systems (l'Agence Nationale de Sécurité des Systèmes d'Information, the **ANSSI**), which have (or, for an OES, which are likely to have) a significant impact on the provision of the services, its managers could be personally subject to penalties of up to EUR 75,000 (in the case of an OES) and EUR 50,000 (in the case of a DSP).

On 9 November 2018, the French Prime Minister (helped by the ANSSI) appointed 122 OESs. This list is strictly confidential and will be updated every year.

PSD2

PSD2 was implemented into French law by ordinance no. 2017-1252 published on 9 August 2017 (the **Ordinance**) and two decrees, no. 2017-1313 and no. 2017-1314, of 31 August 2017. The Ordinance has been supplemented by four orders (arrêtés) of 31 August 2017. All these legal provisions became applicable between 13 January 2018 and 14 September 2019.

The Ordinance implemented the PSD2 provisions regarding strong authentication, into French law and refers to the relevant EU Regulatory Technical Standards in relation to strong authentication requirements applicable to PSPs. Compliance with PSD2 requirements has required substantial changes and financial investments from all French PSPs. The Banque de France has therefore negotiated a migration plan with the European Banking Authority, pursuant to which full compliance with the PSD2 framework (regarding strong authentication requirements) should be effectively achieved by 2022.

Furthermore, with regard to account security, the Banque de France has been granted important powers to ensure that PSPs comply with their obligations in this area. It can make recommendations to PSPs where it considers that a

[2] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

PSP's measures are insufficient to guarantee effective account security; if the recommendations are not followed by a PSP, then the Banque de France may publish a negative opinion against that PSP in the Official Journal (**Journal Officiel**). It may also carry out investigations and require the PSP to provide any information on account security and the related payment devices.

Finally, in the event of serious operational or security incidents, PSPs must notify the French Prudential and Supervision Authority (l'Autorité de Contrôle Prudentiel et de Résolution, (the "**ACPR"**), in the case of serious operational incidents, and the Banque de France, in the case of serious security incidents. Pursuant to French legislation[3], cyber-attacks qualify as security incidents. Should the incident impact its customers, the PSP must inform them immediately of the incident and indemnify them if necessary.

OTHER RELEVANT LAW AND REGULATION

CIIP LAW

France has focused on making its critical infrastructure more resilient to cyber-attacks. The French military programming law on critical infrastructure information protection (**CIIP Law**) entered into effect on 20 December 2013 with a view to establishing minimum cybersecurity standards for operators of "vital importance". These are defined in the French Defence Code as "public or private operators using or operating plants or structures whose unavailability could strongly threaten the economic or military potential, the security or the resilience of the Nation", or establishments where there is a risk of serious danger for people in the event of destruction of, or damage to, these establishments (e.g. nuclear installations) (the **OVIs**). The application of the CIIP Law is monitored by the ANSSI, which also assists the French government and OVIs with respect to cybersecurity issues. A list of 249 OVIs has been created by the French authorities and is strictly confidential. These OVIs operate in 12 different sectors identified as "critical" – food, health, water, telecoms and broadcasting, space and research, industry, energy, transport, finance, civilian administration, military activities and justice. One of the OVIs' main obligations contained in the CIIP Law consists in putting in place a specific protection plan (dealing with surveillance, alert and material protection issues) that must be approved by the ANSSI.

[3] *Arrêté* dated 3 November 2014, relating to internal control of banking, investment and payments services undertakings, as amended by an *Arrêté* dated 31 August 2017.

On 13 July 2018, the French military programming law for years 2019-2025 has modified and supplemented the CIIP Law, notably with respect to the relationships between the OVIs and the ANSSI (e.g. regarding the assistance that the ANSSI could provide to the OVIs in the event of a threat affecting them).

The CIIP Law also includes four different types of measures:

Measures relating to security rules

The ANSSI has set out technical and organisational rules to protect OVIs' information systems. These rules are very detailed and technical, and relate to the following categories: information systems security policy, security accreditation, security maintenance, security incident detection and handling, alert-processing, administration access control, information systems used for administration, segregation in systems and networks, traffic monitoring and filtering.

In addition, various specific rules have been enacted for each of the 12 critical sectors to take into account the specificities of each sector.

Measures relating to incident notifications

OVIs must notify the ANSSI of security incidents occurring on their critical information systems and include specific information in the notification, such as: a detailed explanation of the security incident; a detailed explanation of its consequences and the corrective measures; and the technical details to enable the ANSSI to determine the level of risk (e.g. whether the incident qualifies as a "major crisis").

Measures relating to security inspections

OVIs' information systems can be audited in order to verify both their level of security and their compliance with the CIIP Law. Those controls can be carried out by the ANSSI, State services designated by the French Prime Minister, or a service provider duly qualified as a "Trust Service Provider" by the ANSSI (e.g. cybersecurity audit service providers, incident detection service providers, electronic certification service providers, etc.).

Measures relating to the management of "major crises"

In the case of a "major crisis" (declared by the ANSSI), the ANSSI can impose specific measures on OVIs (e.g. steering and co-ordination of corrective measures, establishment of a business continuation plan, etc.).

GERMANY

IT SECURITY ACT AND CRITIS

In July 2015, thus before the EU Directive on Security of Network and Information Systems ("**NIS Directive**") entered into force, the German legislator had issued the Act to Increase the Security of Information Technology Systems (*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*, "**IT Security Act**") which mainly focused on the protection of installations and facilities of major importance for the functioning of the community and public security (so-called critical infrastructures, "**CRITIS**"). Following the adoption of the NIS Directive, the IT Security Act was amended, in particular, so as to cover also providers of digital services. Currently, a further, comprehensive amendment of the IT Security Act is being discussed in Germany and a second draft bill has been published by the Federal Ministry of the Interior and submitted to the other ministries for consultation in May 2020 ("**Draft Second IT Security Act**"). The second draft reacts to the debate about the first draft bill that had been published March 2019. Currently, the German government is still in discussions about the Draft Second IT Security Act, but it is expected to be passed by Parliament by the end of July 2021. However, the final content of this revised IT Security Act is still a work in progress. It is still unclear when the draft bill will enter into force and in which final form.

The main German authority competent in relation to questions of cybersecurity and the monitoring of the requirements of the IT Security Act is the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, "**BSI**").

Apart from the cybersecurity requirements imposed on CRITIS and providers of digital services and the requirements under the General Data Protection Regulation (see section on the European Union), further statutory obligations apply in relation to cybersecurity that (i) are either sector-specific (e.g. to the financial sector) or (ii) relate to the provision of certain services (e.g. telecommunications services).

IT SECURITY ACT

The IT Security Act amended a number of pre-existing acts. The most relevant provisions were inserted into the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*, "**BSIG**"), which, in particular, imposes a number of obligations on CRITIS and providers of digital services and specifies the competences of the BSI.

CRITIS AND PROVIDERS OF DIGITAL SERVICES

CRITIS in the sense of the BSIG include installations and facilities relating to the following seven sectors which are of major importance for the functioning of the community and public security:

- energy;
- information technology and telecommunication;
- transport and traffic;
- health;
- water;
- nutrition; and
- finance and insurance.

Whether an installation or facility falling within the scope of these sectors in fact qualifies as CRITIS is to be assessed by the operators of the relevant installations or facilities themselves based on the Ordinance on the Determination of Critical Infrastructures under the BSIG (*Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz*). The assessment is mainly to be made based on certain thresholds regarding the contribution to the provision of services or supplies to the public (basic reference value for the different thresholds is the supply to 500,000 persons).

Providers of digital services, in the sense of the BSIG, include providers of online search engines, cloud computing services and online marketplaces.

The current Draft Second IT Security Act provides for a significant extension of the applicability of the BSIG. According to the draft, cybersecurity-related requirements under the BSIG shall also apply to installations and facilities relating, in particular, to the waste sector, the armaments sector and further facilities and installations of particular public interest to be defined in the Ordinance on the Determination of Critical Infrastructures under the BSIG. In addition, the draft provides for specific obligations of manufacturers of IT products, such as components for 5G infrastructures.

OBLIGATIONS OF CRITIS AND DIGITAL SERVICE PROVIDERS

Pursuant to the BSIG, operators of CRITIS and, to some extent, providers of digital services must comply with obligations including (but not limited to):

- designation of a contact point to the BSI which is available at all times;
- implementation of appropriate organisational and technical precautions according to the state of the art to avoid disruption to the availability, integrity, authenticity and confidentiality of information technology systems,

components or processes (compliance with this requirement must be appropriately evidenced at least every two years, e.g. through security audits, tests or certifications);

- notification of the BSI of disruptions to the availability, integrity, authenticity and confidentiality of information technology systems, components or processes that have led or may lead to a failure or significant impairment of the functionality of the relevant installations or facilities.

Intentional or negligent violations of the obligations under the BSIG may lead to administrative fines against responsible individuals and, under certain circumstances, to corporate administrative fines against legal entities of up to EUR 100,000 per infringement (which can be exceeded if required to siphon off benefits generated from the offence).

Please note that the Draft Second IT Security Act provides for a drastic increase of potential administrative fines imposed in cases of non-compliance with the requirements under the BSIG. The framework relating to fines shall be adjusted to that of the General Data Protection Regulation, i.e., the statutory maximum amount of administrative fines per infringement shall be increased to EUR 20 million or to 4% of the total worldwide annual turnover of the group for the preceding financial year, whichever is higher.

COMPETENCES OF THE BSI

The main German authority competent in relation to questions of cybersecurity is the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, "**BSI**"). Its competences and tasks include, in particular, the following:

- collection and evaluation of information on security risks;
- assessment of the security of information technology systems or components;
- addressing warnings to the public or to affected parties about security gaps, malware or data loss;
- auditing the CRITIS operators' or digital services providers' compliance with their obligations under the BSIG;
- issuance of orders to CRITIS operators and providers of digital services for the elimination of any security deficiencies;
- development of minimum standards for the security of information technology of, primarily, the Federal Government.

Please note that under the Draft Second IT Security Act the competences of the BSI shall be significantly expanded. For example, the BSI shall have the right to issue requests for information subject to a fine to manufacturers of IT

products, or to inform the public on the lack of co-operation of certain companies in the search for security vulnerabilities.

OVERVIEW OF SELECTED SPECIAL STATUTORY REQUIREMENTS FOR CERTAIN SECTORS OR SERVICES

Apart from the requirements imposed on CRITIS and providers of digital services and the requirements under the General Data Protection Regulation (see section on the European Union), there are several further special statutory requirements in relation to cybersecurity applicable to certain sectors or to the provision of certain services, such as, amongst others, the financial sector, the provision of telecommunications services, the operation of energy supply networks or the provision of electronic media services.

SELECTED REQUIREMENTS APPLICABLE TO THE FINANCIAL SECTOR

Cybersecurity requirements in the financial sector include, in particular, the following:

- Under the German Banking Act (*Kreditwesengesetz*, "**KWG**"), financial institutions are required to implement a proper business organisation, which explicitly includes an adequate technical organisation and the determination of an appropriate emergency concept for IT systems. The requirements under the KWG are further specified by the risk management guidelines (*Mindestanforderungen an das Risikomanagement*, "**MaRisk**") published by the German Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht*, "**BaFin**"). Furthermore, in relation to the cybersecurity requirements specified in the KWG and the MaRisk, BaFin published further detailed guidelines (*Bankaufsichtliche Anforderungen an die IT*, "**BAIT**") which set out BaFin's expectations with regard to the secure design of IT systems and the associated processes, as well as the related requirements for IT governance. Pursuant to the BAIT, financial institutions are required, amongst others, to implement the independent function of an information security officer and to keep a central register of their individual data processing applications. Furthermore, the Financial Stability Board published its final report on effective practices for cyber incident response and recovery in October 2020. The report provides a toolkit for institutions and authorities in the financial sector in order to establish and maintain capabilities to respond to cyber incidents, and to recover and restore critical activities, systems and data affected by cyber incidents. Although the report is not legally binding, BaFin has welcomed the toolkit and urges financial institutions to implement the proposed tools.
- Pursuant to the Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz*), payment service providers must, in

particular, (i) implement a proper business organisation, including an appropriate emergency system for IT systems, (ii) establish, maintain and apply appropriate risk mitigation measures and control mechanisms to control operational and security-related risks associated with the provided payment services, which includes cybersecurity-related measures preventing operational disruptions, and (iii) submit to BaFin once a year an up-to-date and comprehensive assessment of the operational and security-related risks associated with the payment services it provides and of the adequacy of the risk mitigation measures and control mechanisms it has put in place to manage these risks. Furthermore, in the event of serious operational or security incidents, payment service providers must notify BaFin and, under certain circumstances, affected payment service users without undue delay. Intentional or negligent violations of this notification duty may lead to administrative fines against responsible individuals and, under certain circumstances, to corporate administrative fines against legal entities of up to EUR 100,000 (which can be exceeded if required to siphon off benefits generated from the offence).

SELECTED REQUIREMENTS FOR THE PROVISION OF TELECOMMUNICATIONS SERVICES

Cybersecurity requirements for the provision of telecommunications services include, in particular, the following:

- Under the German Telecommunications Act (*Telekommunikationsgesetz*, **TKG**), providers of telecommunications services are required to take technical precautions and measures according to the state of the art to protect the secrecy of telecommunications and personal data. In the event of a data breach, providers of publicly available telecommunications services are obliged to notify the Federal Network Agency (*Bundesnetzagentur*, **BNetzA**) and the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*) without undue delay as well as, under certain circumstances, the persons affected by the data breach.
- Furthermore, under the TKG, there are obligations imposedupon operators of public telecommunications networks and providers of publicly available telecommunications services the following obligations:
    - obligation to take adequate technical and other measures for protection against interference with, and unauthorised access to, the networks and services;
    - obligation to implement a security officer and prepare a security plan setting out, amongst others, the technical or other measures needed to fulfil the security requirements;

- obligation to notify both the BNetzA and the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) without undue delay of interference with telecommunications networks and services such as which lead or could lead to significant security breaches.

- Until late 2019, the German government took a manufacturer-neutral approach with regard to suppliers of 5G components. However, in December 2019, several members of the federal parliament publicly called for a complete ban of certain (Chinese) component suppliers from the deployment of the 5G network. After months of (public and non-public) discussions, the German government seems to have found a compromise between the two opposing positions in September 2020. This compromise which now has to be implemented in the Draft IT Security Act 2.0 includes a two-step approach in order to determine whether 5G components may be used in the telecommunication sector:
  - Firstly, security-relevant network and system components that fulfil critical functions (*kritisiche Komponenten,* "**critical components**") using 5G components have to be determined and certified by the BSI in accordance with the EU Cyber Security Act before they may be used in telecommunications networks and services. Critical components may include components of both core and peripheral telecommunications networks. This certification is of a technical nature.
  - Secondly, the component suppliers need to declare their trustworthiness vis-à-vis the telecommunication operators which shall exclude any influence by foreign states. This declaration of trustworthiness shall be checked for credibility by the ministries involved with the help of intelligence information. Only if each ministry involved agrees, components from the respective supplier may be used.
    - The BNetzA published a security catalogue providing guidance on, amongst others, the fulfilment of the aforementioned cybersecurity-related requirements under the Telecommunications Act. Intentional or negligent violations of these requirements may lead to, in particular, administrative fines against responsible individuals and, under certain circumstances, to corporate administrative fines against legal entities of up to EUR 100,000 (which can be exceeded if required to siphon off benefits generated from the offence). In August 2020, the BNetzA published a revised security catalogue which amends and updates the current security catalogue in order to take into account new developments with regard to cyber security in the telecommunications sector. It is expected to come into force

in January 2021 and in particular, addresses the ongoing debate on the deployment of 5G infrastructure. Taking this into account as well as other developments in the telecommunications sector, the revised security catalogue, *inter alia*, requires the telecommunications operators to: Require produce suppliers to declare their trustworthiness in order to be eligible as a supplier for critical components. The security catalogue therefore provides for a list of non-exhaustive requirements which have to be included in the declaration of trustworthiness;

- Identify and subsequently certify their core components in accordance with the EU Cyber Security Act and other legislation;
- Ensure the integrity of their products during the entire life cycle;
- Introduce a safety monitoring system in order to continuously avoid, detect, isolate or eliminate disturbances or errors in telecommunications systems;
- Provide for sufficient redundancies to avoid incidents as far as possible or to at least minimize downtimes;
- Diversify their supply chain in order to avoid monoculture. Therefore, components or systems from at least two different manufacturers must be used for the core network, the transport network and for access networks.

SELECTED REQUIREMENTS FOR THE OPERATION OF ENERGY SUPPLY NETWORKS AND ENERGY PLANTS

Cybersecurity requirements for the operation of energy supply networks and energy plants include, in particular, the following:

- Pursuant to the German Energy Industry Act (*Energiewirtschaftsgesetz*), operators of energy supply networks and operators of certain energy plants (covering both electricity and gas supply networks and plants) are required to take adequate measures to protect their networks and plants against threats to telecommunications and electronic data processing systems necessary for secure network operation. The Federal Network Agency (*Bundesnetzagentur*) published IT security catalogues setting out the minimum requirements for adequate protection which have to be fulfilled by operators of energy supply networks and certain energy plants.
- Furthermore, operators of energy supply networks and certain energy plants are obliged to report disruptions to the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes to the Federal Office for Information Security (*Bundesamt für*

Sicherheit in der Informationstechnik) without undue delay via a specific contact point to be designated.

- Intentional or negligent violations of these requirements may lead to administrative fines against responsible individuals and, under certain circumstances, to corporate administrative fines against legal entities of up to EUR 100,000 (which can be exceeded if required to siphon off benefits generated from the offence).

SELECTED REQUIREMENTS FOR THE PROVISION OF TELEMEDIA SERVICES

Under the German Telemedia Act (*Telemediengesetz*), telemedia service providers must, amongst other requirements, take technical and organisational precautions to the extent technically possible and economically reasonable to protect the technical equipment used for their telemedia services from unauthorised access and attacks and to prevent violations of the protection of personal data. The term "telemedia service provider" covers, in particular, any persons operating a website. Intentional or negligent violations of this requirement may lead to, in particular, administrative fines against responsible individuals and, under certain circumstances, to corporate administrative fines against legal entities of up to EUR 50,000 (which can be exceeded if required to siphon off benefits generated from the offence).

ITALY

IMPLEMENTATION OF EU LAW

GDPR

The Italian Privacy Code, Legislative Decree no. 196 of 2003, as amended to ensure consistency with GDPR, sanctions criminal offences that may be committed alongside cybercrimes including:

- Unlawful processing of data;
- Unlawful communication or dissemination of personal data that is processed on a large scale; and
- Fraudulent acquisition of data that is processed on a large scale.

NIS DIRECTIVE

Italy implemented the NIS Directive by means of Legislative Decree no. 65 of 2018.

The Decree provides as follows:

- **Competent NIS authorities (Art. 7)**: Each Ministry in relation to the business sector it oversees (e.g. Ministry of Economic Development for Energy Oil and Gas and Digital Infrastructure, Ministry of Economy and Finance for Transports and Banking and Financial Markets Infrastructures). Each NIS authority (i) adopts specific security measures, (ii) supervises the involved operators and (iii) imposes penalties.
- **Computer security incident response team (CSIRT, Art. 8)**: The Italian CSIRT is established as a department of the Prime Minister's office and, together with the competent NIS Authority, is the recipient of security incident reports from OES and DSP (as defined below).
- **Operators of Essential Services (OES, Art. 4)**: As of 2020, the Italian NIS authorities have identified no. 465 OESs (both public and private entities) as actually providing services that qualify as essential for the country. These OESs have a duty to implement the measures aimed at ensuring compliance with the Decree in accordance with the Guidelines issued on July 2019 by the competent NIS authorities. The deadlines for the implementation of the Guidelines vary between four and twelve months from July 2019.
- **Digital Service Providers (DSP, Art. 14)**: DSPs providing online marketplace, search engine and cloud computing services must identify and implement security measures that are adequate to prevent the risks arising from the services they offer.

- **Penalties (Art. 21)**: Breaches of the Decree can result in penalties up to EUR 125,000 (and up to EUR 150,000 for non-compliance with instructions specifically provided to an operator by the competent Ministry).

PSD2

Italy has implemented the PSD2 primarily through Italian Legislative Decree no. 218 of 15 December 2017 (the **PSD Decree**), amending certain provisions of (i) the Italian Banking Act (Italian Legislative Decree no. 385 of 1 September 1993) and (ii) Italian Legislative Decree no. 11 of 27 January 2010, which had implemented PSD1 in Italy.

The PSD Decree provides for, amongst other things:

- the introduction of a strong customer authentication process, allowing payment service providers (**PSPs**) to verify the identity of payment service users or to assess the validity of the use of a specific payment instrument;
- additional specific rules governing the different types and categories of payment services; and
- additional requirements that PSPs shall observe when collecting data, in particular when there is a risk of fraud (actual or potential).

Competent Authority

Under the PSD Decree, the Bank of Italy is the main competent authority. In particular, the Bank of Italy is the competent authority for, amongst other things:

- authorising, monitoring and supervising PSPs and other market actors;
- prohibiting and removing unfair commercial practices, acting in concert with the Competition and Market Authority ("*Authorità Garante della Concorrenza ed il Mercato*"); and
- settling any dispute arising out of or in connection with payment services.

ITALIAN LEGISLATION ON ELECTRONIC SIGNATURES

Italian Legislative Decree no. 82 of 7 March 2005, as subsequently amended (the **Digital Administration Code** or **CAD**) and the EU Regulation no. 910 of 23 July 2014 (**eIDAS**) provide for:

- a definition of (i) "simple" electronic signature (*firma elettronica*), (ii) "advanced" electronic signature (*firma elettronica avanzata*); (iii) "qualified" electronic signature (*firma elettronica qualificata*) and (iv) digital signature (*firma digitale*);
- a definition of electronic document;
- a description of the legal value and evidential effectiveness of documents signed with electronic signatures; and
- a description of the evidential effectiveness of electronic documents that constitute copies of handwritten documents (and *vice versa*).

With reference to the **legal value** and to the **evidential effectiveness**, art. 20, para. 1-*bis*, of the CAD states that electronic documents signed with advanced or qualified electronic signatures or a digital signature meet the written form requirement and have the same legal effects of handwritten documents as provided for by **art. 2702 of the Italian civil code** ("**ICC**"). As regards "simple" electronic signatures, Italian Courts are entitled to conduct a case-by-case assessment of their legal value and evidential effectiveness, also based on the features of the electronic document submitted in Court.

Then, the CAD goes through the documents listed in art. 1350 of the ICC and makes the following distinctions:

- documents under art. 1350, nos. **1-12** of the ICC, must be signed with a **qualified electronic** or **digital signature** (see art. 21, para. 2-bis, of the CAD); and
- documents under art. 1350, no. **13** of the ICC, must be signed with an **advanced**, **qualified electronic** or **digital signature** (see art. 21, para. 2-bis, of the CAD).

Therefore, as of today, subject to the exceptions specified above, a document signed with advanced electronic signature has legal value and the effects specified under art. 20, para. 1-bis, of the CAD.

It has to be noted that Italian notaries are entitled to certify the authenticity of electronic signatures of a document. However, documents subscribed with electronic signatures – but not prepared in the form of a notarial deed, when this requirement is provided by Italian law – can never be considered as notarial deeds.

Although a signatory may in principle deny having executed a qualified electronic signature or a digital signature (as it may happen with a non-notarised wet ink signature), under art. 20, para. 1-ter, of the CAD, the use of the qualified or digital signature-creation device is assumed to be traceable back to its owner, unless there is proof to the contrary.

Art. 22, para 1, of the CAD states that electronic documents constituting a digital copy of notarised deeds, private writing or other documents originally prepared on paper-based formats have the same legal effects of handwritten documents as provided for by art. 2714 and 2715 of the ICC, provided that the requirements set forth under art. 20. para. 1-bis, of the CAD are met.

A paper-based document constituting a copy of an original electronic document, duly signed with an advanced, qualified electronic or digital signature, has the same legal effects as the original document if its conformity to the original document is certified by an authorised public official.

Glossary

Electronic signature: data in electronic form attached to or logically associated with other data in electronic form

Advanced electronic signature: data in electronic form attached to or logically associated with an electronic document, allowing the identification of the signatory of the document and providing a unique connection to the signatory

Qualified electronic signature: advanced electronic signature created by a qualified electronic signature creation device and based on a qualified certificate for electronic signatures

Digital signature: type of qualified electronic signature created through the use of encryption technology, which uses a qualified certificate-based digital ID that is awarded by a recognised trust service provider or certificate authority

Electronic document: an informatic representation of acts, facts or data that are legally relevant.

Relevant provisions of the ICC

Art. 1350 provides for a list of documents that must be made in writing under penalty of nullity

Art. 1350, nos. 1-12 includes, amongst others, contracts establishing, modifying or transferring the ownership of real estate property and/or other real property rights, and acts of division or renunciation of those rights

Art. 1350, no. 13 is a general clause that refers to "all other acts" for which the requirement of written form under penalty of invalidity is expressly provided by Italian law

Art. 2702 states that a private writing constitutes a full evidence of the declaration's origin set forth therein towards the counterparty, provided that (i) it is duly signed by the person executing the writing and (ii) the counterparty does not challenge the authenticity of the subscription

Art. 2714 and art. 2715 provide for the legal effectiveness of copies of notarial deeds and of private writings.

OTHER RELEVANT LAW AND REGULATION

CYBER LAW – RECENT DEVELOPMENTS IN ITALY

Italian Law No. 12 of 11 February 2019 provides:

- a definition of blockchain and smart contracts; and
- a description of the legal effects of blockchains and smart contracts.

Now, under Italian law, the **storage of an electronic document by means of blockchain technology** produces the same legal effects as electronic time stamps under Article 41 of the eIDAS Regulation, i.e., it **can qualify as evidence of the date and time of creation of electronic documents**. However, blockchain technologies must meet the requirements set out by the Agency for Digital Italy (**AGID**).

Smart contracts will meet the written form requirements. For this purpose, parties will need to be electronically identified in compliance with the guidelines which will be issued by the AGID.

Notification requirements under the NIS Directive may overlap with those under the GDPR. The Italian Data Privacy Authority recently highlighted the symmetry between data protection and cybersecurity and the importance of a responsible approach by business operators, to prevent "social" risk linked to information network and information systems.

Glossary

Blockchain: technologies and electronic protocols using a shared, distributed, replicable, simultaneously accessible, architecturally decentralised, cryptographically-based ledger, such as to allow the registration, validation, update and archiving of both unencrypted and encrypted data, which can be verified by each blockchain user, and cannot be altered or edited

Smart contracts: software operating on blockchains, whose execution automatically binds two or more parties and whose effects are predetermined by the same parties.

THE PERIMETER OF NATIONAL CYBERSECURITY

The Italian decree no.105 of 21 September 2019 (the **NCS Decree**), converted into Law No. 133 of 18 November 2019, set forth:

- urgent **provisions** on the perimeter of national cybersecurity;
- rules and **obligations** imposed upon private parties that provide services of strategic importance at the national level; and
- penalties.

In particular, the NCS Decree establishes the **perimeter of national cybersecurity** (the **Perimeter**) in order to ensure a high level of security of the networks, IT systems and IT services.

- Within four months of the date of entry into force of the conversion law (being 21 March 2020), a decree issued by the President of the Council of Ministers shall identify the public and private national entities and operators with registered offices in the national territory (the **Parties**) to be included within the Perimeter, which shall be under a duty to honour the obligations and provisions set forth in the Decree.
- The Decree sets forth the **criteria to identify** the Parties included in the Perimeter:
    - the party guarantees an essential service for the maintenance of civil, social or economic activities that are fundamental for the interests of the State; and
    - the exercise of such function or the performance of such service depends upon networks, IT systems and IT services.

As to the **obligations** imposed upon the Parties, the Decree provides for:

- a **duty of notification**: within six months of the entry into force of the decree identifying the Parties, such Parties are required to send to the Office of the President of the Council of Ministers and to the Ministry of Economic Development a list to be updated at least once each year, of the networks, IT systems and IT services respectively pertaining to them;
- a **duty of reporting cyber incidents**: the Parties will be required to report to the Italian Computer Security Incident Response Team (**CSIRT**) any incident that has had an impact on the networks, IT systems or IT services respectively pertaining to them. Such reporting obligations will be carried out through specific procedures to be defined by another decree by the President of the Council of Ministers, to be issued within ten months of the entry into force of the conversion law (i.e., by 21 September 2020);

- a **duty of implementation of measures aimed at ensuring high levels of security of the IT systems and IT services** pertaining to the Parties: through a decree to be adopted by 21 September 2020, the Office of the President of the Council of Ministers will elaborate the measures, taking into account the standards defined at the international and European Union levels.

As to the penalties imposed by the Decree, art. 1, paragraph 9, of the Decree introduces significant administrative sanctions for breaches of the obligations set forth in the Decree. In particular, the Ministry of Economic Development may apply the following sanctions to the Parties:

- **from Euro 300,000 to Euro 1,800,000** for the failure to report to the CVCN of the use of products or services on the IT networks or systems, or for the performance of IT services, in breach of the conditions or without passing the tests imposed by the CVCN;
- **from Euro 250,000 to Euro 1,500,000** for the failure to fulfil the reporting obligation in a timely manner; the failure to comply with the security measures mentioned above and the failure to collaborate in the performance of the tests imposed by the CVCN; the failure to fulfil the requirements imposed by the Ministry of Economic Development or the Office of the President of the Council of Ministers upon the completion of inspections; the failure to honour the requirements imposed by the CVCN;
- **from Euro 200,000 to 1,200,000**, for the breach of obligations to prepare and update the list of IT networks, systems and services.

CO-ORDINATION WITH THE "NIS" LEGAL FRAMEWORK

The operators of essential services (**OES**), digital service providers identified under the Italian legislative decree no. 65 of 18 May 2018, issued in accordance with the NIS EU Directive, and the businesses providing public communications networks or electronic communication services accessible to the public, referred to in the electronic communications code (Italian legislative decree 259/2003) will also be required:

To honour the cybersecurity measures provided under the respective legislative decrees of reference indicated above, if such measures are of a level at least equivalent to those adopted in accordance with the Decree. The Ministry of Economic Development has the task of identifying, for private parties, any additional measures that may be necessary in order to achieve the security levels provided under the Decree.

The notification of the cyber incidents made in accordance with the Decree serves to fulfil the obligation of reporting incidents having a material impact on the service provided, within the meaning set forth in arts. 12-14 of legislative

decree 65/2018 (**NIS notification**) and art. 16-ter of the Electronic Communications Code. To such end, the Italian CSIRT has the task of forwarding the notifications to the competent Ministry.

NETHERLANDS

GDPR

The provisions of the GDPR, including its security and breach notification requirements, apply directly in the Netherlands. In the implementation act of 16 May 2018 (*Uitvoeringswet algemene verordening gegevensbescherming,* the **mplementation Act**), certain elements of the GDPR which require or permit national implementation, were implemented, but these do not substantively touch on the security-related elements of the GDPR. In the Implementation Act, the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, **AP**) is established as the supervisory authority responsible for monitoring the application of the GDPR. Data breach notifications are to be made to the AP, within the timelines and under the further conditions set forth in the GDPR. Notifications can be made online through the AP's website. Pursuant to the Implementation Act, the requirement under the GDPR to notify data subjects of a data breach does not apply to financial service organisations. The latter are subject to separate security breach notification requirements under the Dutch Financial Supervision Act (discussed below).

ACT ON SECURITY OF NETWORK AND INFORMATION SYSTEMS (Wbni)

In the Netherlands, the NIS Directive has been implemented in the Act on the security of network and information systems of 17 October 2018 (*Wet beveiliging network- en informatiesystemen,* the "**Wbni**").

In line with the NIS Directive, the Wbni applies to operators of essential services designated by governmental decree and to digital service providers who offer online marketplaces, online search engines or cloud computing services (excepting micro and small enterprises). Pursuant to the NIS Directive, the Dutch Minister of Justice and Safety has been designated as the national single point of contact on the security of network and information systems in the Netherlands

Pursuant to the NIS Directive, the WBNI distinguishes a number of sectors in which providers of essential services can be designated, and appoints different competent authorities for the various sectors:

1. Energy and Digital Infrastructure – Competent authority: Minister of Economic Affairs and Climate;

2. Banking and Financial market infrastructures – Competent authority: the Dutch Central Bank (*De Nederlandsche Bank,* **DNB**);

3. Transport and Drinking water supply and distribution – Competent authority: the Minister of Infrastructure and Water Management;

4. Health Care – Competent authority: the Minister of Health, Welfare and Sport.

Additionally, the Dutch Minister of Economic Affairs and Climate is the competent authority responsible for digital services.

The Ministry of Justice and Safety harbours the computer security incident response team (**CSIRT**) for essential services, and the Ministry of Economic Affairs and Climate harbours the CSIRT for digital services (**CISRT-DSP**).

With regard to operators of essential services and digital service providers, the Wbni imposes obligations in accordance with the NIS Directive to implement security measures and to notify the appropriate authority of serious security breaches.

Failure to comply with the obligations imposed under the Wbni can result in fines of up to EUR 5 millionThe Minister of Justice and Safety has also established the National Cyber Security Centre (**NCSC**) which serves as a central information hub and centre of expertise for cybersecurity in the Netherlands. The NCSC regularly issues publications on its website (www.ncsc.nl) on the state of cybersecurity in the Netherlands, including cybersecurity alerts and guidelines. Recently, high-level guidelines were issued to draw attention to potential security vulnerabilities arising in the context of the COVID-19 virus, in particular in relation to the increased number of people working from home.

FINANCIAL SUPERVISION ACT

The Dutch Financial Supervision Act (*Wet op het financieel toezicht*, **Wft**) comprises specific security and breach notification obligations for financial service organisations. The security and authentication requirements for payment service providers introduced by PSD2 have been implemented in the Wft (and underlying governmental decrees) and in part also in the Dutch Civil Code (*Burgerlijk Wetboek*, **BW**). The security requirements are generally aimed at safeguarding controlled and sound business operations. Incident notification requirements apply, depending on the type of financial service organisation, to either DNB or the Dutch Authority for the Financial Markets (*Autoriteit Financiële Markten*, **AFM**). Payment service providers are required to notify DNB of serious security incidents.

TELECOMMUNICATIONS ACT

The Dutch Telecommunications Act (*Telecommunicatiewet*, "**Tw**") imposes specific security requirements on providers of public electronic communications networks and services, to safeguard personal data processed in the context of conducting electronic communications and to ensure the safety, continuity and integrity of the networks and services concerned. The requirements with regard to safeguarding personal data replicate those under the GDPR, and data

breaches are also to be notified to the AP. Any breach of security measures aimed at safeguarding the continuity and integrity of communications networks and services are to be notified to the Minister of Economic Affairs and Climate.

POLAND

CYBERSECURITY LAW IN POLAND

In Poland, cybersecurity is regulated by the Act on the National Cyber Security System (the "**Cyber Security Act**") of 5 July 2018. It is the first law in Poland in this respect and constitutes the implementation of the EU Directive on security of network and information services (the "**NIS Directive**") into the national legal system. The Cyber Security Act came into force on 28 August 2018.

Apart from complying with all the requirements imposed by the NIS Directive (described in the EU section), the Polish legislator has extended the reach of the Cyber Security Act by encompassing the public administration and the telecommunications sector (to some extent) in its scope.

The Cyber Security Act takes into account the regulations introduced by the General Regulation on the Protection of Personal Data (the "**GDPR**") and provides for fines of up to PLN 1,000,000 (approximately EUR 221,000).

Cybersecurity is also regulated to some extent by the amended Act on Payment Services (the "**Payment Services Act**") which transposes the EU's revised Payment Services Directive ("**PSD2**") into Polish law.

SCOPE

The Cyber Security Act defines the organisation of the national cybersecurity system and the tasks and responsibilities of its constituent bodies. The key entities are Key Service Operators, Digital Service Providers and certain public entities listed in the Act.

KEY SERVICE OPERATORS

Key Service Operators are companies and institutions providing services that are essential for maintaining critical social or economic activities. The Cyber Security Act indicates the sectors in which Key Service Operators are identified. These are:

- energy;
- transport;
- banking and financial market infrastructure;
- health protection;
- potable water supply (including distribution); and
- digital infrastructure.

OBLIGATIONS OF KEY SERVICE OPERATORS

Key Service Operators are required to implement a security management system in the information system used to provide the key service. The security management system requires systematic risk assessment and the adaptation of security measures (such as secure system operation), physical security of the system (including access control), security and continuity of service provision, maintenance of action plans enabling continuity of service provision, and continuous monitoring of the system providing the key service.

In addition, Key Service Operators are obliged to apply measures to prevent and limit the impact of incidents on the security of the information system, including the collection of information on cyber threats and vulnerabilities of the system. The Key Service Operator shall (i) designate a person responsible for maintaining contact with the entities of the national cybersecurity system; (ii) provide the key service user with access to the knowledge to understand cybersecurity threats and to apply preventative measures; and (iii) communicate certain data to the competent authority responsible for cybersecurity. Key Service Operators are also responsible for compiling, updating and maintaining documentation on the cybersecurity of the information system for at least two years.

In the event of an incident, a Key Service Operator shall remedy it by:

- classifying the incident on the basis of the criteria defined for each sector by an ordinance of the Council of Ministers determining thresholds for considering an incident to be serious based on (i) the number of users affected by the disruption of the key service, (ii) time impact of the incident, (iii) geographical reach and (iv) sector-specific factors;
- if the incident is classified as serious, reporting it to the relevant Computer Security Incident Response Team (the **CSIRT**) no later than 24 hours after its detection;
- interacting with the CSIRT to handle the incident and ensuring appropriate access to information; and
- removing system vulnerabilities.

DIGITAL SERVICE PROVIDERS

A Digital Service Provider is defined as a legal entity having its registered office or management in the territory of the Republic of Poland or a representative having an organisational unit in the territory of the Republic of Poland, providing a digital service (e.g. online trading platforms, cloud computing services, Internet search engines).

Micro and small legal entities are excluded from the scope of the Cyber Security Act.

OBLIGATIONS OF DIGITAL SERVICE PROVIDERS

Due to the cross-border nature of digital services and the international specificities of providers of such services, Digital Service Providers are subject to lighter regulation than Key Service Operators. They are required to apply security measures proportionate to the risk, taking into account in particular:

- security of information systems and facilities;
- incident handling (i.e. activities to detect, record, analyse, classify and prioritise incidents, taking corrective action and limiting the consequences of an incident);
- managing the business continuity of the provider to provide the digital service;
- compliance with international standards; and
- monitoring, audit and testing.

Digital Service Providers are also required to perform activities to detect, record, analyse and classify incidents. In the event of a significant incident, Key Service Providers are required to forward the information about the incident to the relevant CSIRT no later than 24 hours after its detection.

Digital Service Providers are supervised by the competent authorities, which have the power to conduct inspections and impose fines.

PUBLIC ENTITIES

The national cybersecurity system also includes public entities such as the National Bank of Poland (Narodowy Bank Polski), National Economy Bank (Bank Gospodarstwa Krajowego – a state-owned development bank), Office of Technical Inspection (Urząd Dozoru Technicznego), Polish Air Navigation Services Agency (Polska Agencja Żeglugi Powietrznej), Polish Centre for Accreditation (Polskie Centrum Akredytacji), the National Fund for Environmental Protection and Water Management (Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej), provincial environmental protection and water management funds, as well as research institutes and commercial law companies performing public utility tasks.

Each of the above-mentioned entities is obliged to appoint a person responsible for maintaining contacts with the entities of the national cybersecurity system within the scope of public tasks dependent on information systems.

Additionally, each of the public entities is obliged to manage incidents and report them to the relevant CSIRT. An incident must be reported within 24 hours from the moment of its detection.

STATE AUTHORITIES

Each key sector is supervised by a competent authority responsible for cybersecurity. The 11 sectors listed in the Cyber Security Act fall under the competence of the specific ministers responsible for the given departments of the administration. On the basis of an agreement, they may entrust the performance of certain tasks to subordinate or supervised entities.

The task of the body competent for cybersecurity is to analyse the entities operating in the given sector and to issue a decision on recognising a Key Service Operator. The authority also prepares recommendations for actions that will strengthen the sector's cybersecurity.

The competent authority is also responsible for:

- calling on the relevant entity to remove vulnerabilities that led or could have led to a serious incident;
- conducting inspections of Key Service Operators;
- co-operation with other EU Member States through Points of Single Contact; and
- participation in exercises and the processing of personal data necessary to perform the tasks.

At the government level, the Minister of Digital Affairs is responsible for (i) monitoring the implementation of the Cyber Security Strategy of Poland, (ii) recommending areas of co-operation with the private sector to increase cybersecurity, and (iii) preparing annual reports on serious incidents reported by Key Service Operators and Digital Service Providers. The Ministry of Digital Affairs is also responsible for implementing educational activities, sharing information and good practices related to cybersecurity.

SANCTIONS

Key Service Operators and Digital Service Providers may be punished with a fine from PLN 1,000 to PLN 1,000,000 (approximately from EUR 221 to EUR 221,000) for failing to fulfil their obligations under the Cyber Security Act. The financial penalty is imposed by way of a decision of the authority competent for cybersecurity, and the proceeds from the fines imposed constitute revenue for the state budget. More importantly, the financial penalty may also be imposed in cases where the entity has ceased the infringement or has remedied

the damage caused, if the competent cybersecurity authority considers that the duration, extent or effects of the infringement so warrant.

PSD2

Poland has implemented the PSD2 through the revised Payment Services Act, which imposes several important changes to its previous version.

Under the Payment Services Act, payment service providers (**PSPs**), as part of their risk management system, are required to take risk mitigation measures and provide control mechanisms to manage operational and security risks in regard to payment services, in particular by:

- maintaining an effective incident management procedure; and
- evaluating and updating procedures for the management of operational and security risks.

PSPs are required to provide the Polish Financial Supervision Authority (Komisja Nadzoru Finansowego, **KNF**) (or other relevant authority) with annual information regarding the evaluation and update of procedures in place with respect to the scope of operational risk management and security breach risks, as well as the evaluation of risk mitigation measures and control mechanisms.

A PSP is also obliged to immediately inform the KNF of any major operational or security-related incident, including those of an information and communication technology nature. If the incident has or may have an impact on the financial interests of users, PSP shall, without undue delay, notify users about the incident and inform them about the measures available, in order to limit the negative consequences of the incident.

Additionally, PSP is required to provide the KNF with annual data regarding any fraudulent activities related to payment services (e.g. cyber-attacks) which are provided by the PSP.

As part of counteracting cybercrime, PSP uses the so-called strong customer authentication whenever the payer:

- gains access to his/her on-line account;
- initiates an electronic payment transaction; and
- carries out, via a remote channel, an activity which may involve a risk of fraud or other misuse of the payment services provided.

PSP is obliged to take the appropriate security measures to protect the confidentiality and integrity of individual authentication data.

On 21 June 2019, the European Banking Authority (the **EBA**) published an Opinion on the elements of strong customer authentication (the **SCA**) under the PSD2. The Opinion addresses concerns about the preparedness and

compliance of some actors in the payments chain with the SCA requirements that apply as of 14 September 2019. Although the EBA is legally not able to postpone an application date that is set out in EU law, the Opinion accepts that, on an exceptional basis and in order to avoid unintended negative consequences for some payment service users after 14 September 2019, national competent authorities may decide to work with PSPs and the relevant stakeholders, including consumers and merchants, to provide limited additional time.

The Opinion was reflected in the KNF's Communication of 19 August 2019 on SCA in the case of certain means of payment using payment instruments. The KNF considers the application of the solutions proposed by the EBA with regard to card-based online payments and contactless payments executed using payment terminals to be acceptable. This means that no other supervisory measure relating to the failure to use strong customer authentication will be applied with regard to PSPs that notify the KNF before 14 September 2019 of the need to apply the solution regarding SCAs, and then submit an appropriate realistic "migration plan" which was previously agreed with the KNF. The risk associated with the failure to use SCA after 13 September 2019 is fully borne by the PSPs.

DRAFT AMENDMENT TO THE CYBER SECURITY ACT

A draft amendment to the Cyber Security Act was submitted for public consultation on 7 September 2020. It is aimed at strengthening the national cyber security system, implementing EU recommendations on the security of telecommunications networks and improving the functioning of the most important institutions in the national cyber security system.

The key aspects of the draft are:

- the regulation of electronic communications companies. The draft assumes the integration of electronic communications companies into the national cybersecurity system and defines their obligations with respect to, amongst other things, the handling of telecommunications incidents;
- giving the Cyber Security College (*Kolegium do Spraw Cyberbezpieczeństwa*) the competence to make a risk assessment of a supplier of hardware or software relevant to the security of the entities in the national cyber-security system. This competence is an implementation of the EU Toolbox 5G, a document issued in January 2020 by the NIS Cooperation Group, which contains recommendations addressed to Member States in the area of counteracting risks to the integrity and security of next-generation networks in Europe. The assessment by the Cyber Security College results in the possibility of equipment or software being used by entities in the national cyber security system. In the case of a moderate risk, these entities

do not use the equipment, software or services specified in the assessment of a given provider but may continue to use the equipment and software they already have or continue to use existing services. On the other hand, in the case of high risk, those entities shall not only refrain from bringing into use the equipment, software or services specified in the assessment of a given provider, but shall also decommission the equipment, software and services no later than five years from the date of publication of the assessment notice;

- the regulation of the Information Sharing and Analysis Center (**ISAC**) – a specialist organisation ensuring cooperation and exchange of information on incidents, threats, vulnerabilities and good practices in the field of cyber security protection;
- the regulation of the principles of operation of teams performing the function of security operations centre (**SOC**) in a given entity. Under the amendment, the provisions concerning the performance of obligations by Key Service Operators are to be made more detailed. Until now, the implementation of these obligations was the responsibility of a specialised outsourced entity or by internal structures responsible for cyber security of the Key Service Operators. According to the draft, the duties are to be performed by the internal SOC or provided by an entity rendering services in the field of cyber security;
- the clarification of the provisions on sectoral CSIRTs. The amendment also provides for changes aimed at enabling sectoral CSIRTs to play a greater role.

The draft is likely to change as a result of comments from industry organisations, and it may still enter into force, with some exceptions, in 2020.

ROMANIA

IMPLEMENTATION OF THE NIS DIRECTIVE

The NIS Directive was implemented in Romania in January 2019 by the Law No 362/2018 (the Romanian NIS Law).

NATIONAL COMPETENT AUTHORITY

The National Computer Security Incident Response Centre (**CERT-RO**) is the designated national competent authority and operates under the authority of the Ministry of Communications and Information Society. The national single point of contact and the Computer Security Incident Response Team (**CSIRT-RO**) are established within CERT-RO.

OPERATORS OF ESSENTIAL SERVICES

Designation as OES

The Romanian NIS Law identifies several key sectors vulnerable to cyber threats:

- energy (electricity, oil and gas);
- transport (air, rail, water and road);
- banking;
- financial markets (central counterparties, trading venue operators);
- healthcare (including private hospitals or clinics);
- water supply and distribution; and
- digital infrastructure (IXP, DNS and TLD).

Entities which operate in these sectors must perform an internal analysis to determine whether "essential" services are performed, as follows:

- is the service officially listed as essential or determined to be essential, following the entity's internal analysis?
- does the service depend on networks and information services?
- how is the service disrupted if an incident occurs?

If the service is determined as essential, the entity must notify CERT-RO, which, following its own assessment, may list the entity in the OES registry (**ROSE**), which is a classified document.

Obligations for OES

OES are subject to the following obligations:

- to meet minimum cybersecurity standards as requested by CERT-RO (from January 2021, a certified auditor must be retained to perform this analysis);
- to notify any incident with a material impact on the continuity of essential services; and
- to allow CERT-RO to audit compliance with cybersecurity standards and other obligations under the Romanian NIS Law.

SANCTIONS

Breaches of the Romanian NIS Law may trigger an administrative fine ranging from 0.5% to 5% of the annual turnover for the previous year, depending on the severity of the breach.

DIGITAL SERVICE PROVIDERS

The Romanian NIS Law also provides that DSP providing online market, online search engine and/or cloud computing services must notify CERT-RO which assesses whether their registration in the DSP registry is required (SMEs do not fall within the ambit of the Romanian NIS Law). In general, DSP listed by CERT-RO must comply with the same obligations as OES.

IMPLEMENTATION OF THE REVISED PAYMENT SERVICES DIRECTIVE (PSD2)

The cybersecurity obligations provisions under the Revised Payment Services Directive (**PSD2**) were implemented in Romania in November 2019 by the Law No 209/2019 (the **Romanian Payment Services Law**) and by the Regulation No 2/2020 of the National Bank of Romania (**NBR**).

NATIONAL COMPETENT AUTHORITY

The NBR is the designated national competent authority for the authorisation of payment services providers and for monitoring security incidents in the field of payment services.

POLICIES AND PROCEDURES

Payment services providers must set up mitigation and control mechanisms for addressing security risks and must maintain effective incident management procedures to detect and classify major operational or security incidents relating to payment services.

MAJOR INCIDENT REPORTING

Payment services providers must immediately notify NBR of any major operational or security incident in the manner set out in the NBR Regulation no 2/2020, which generally consists of:

- submitting an initial report within four hours after the occurrence of a major incident is identified or after a minor incident is requalified as major;

- submitting intermediate reports when additional relevant details about the incident and its possible consequences become available; and
- submitting a final report, when an analysis of the causes of the incident becomes available, irrespective of any implementation of mitigation measures, which must be submitted within 10 working days after the payment services operator has resumed the normal course of its activities, or immediately after a major incident is requalified as minor.

The criteria for qualifying an incident as major are provided by Appendix 1 to the NBR Regulation No 2/2020, and refer to the number and total value of affected payment operations, the number of affected customers, the duration of services malfunctions, the economic and reputational impact, the internal escalation processes of the relevant payment services provider, and the potential to impact other payment services providers or payments infrastructures and systems.

CUSTOMER NOTIFICATION OF MAJOR INCIDENT

Payment services providers must notify their customers directly, and without undue delay, if a security incident might impact the financial interests of those customers. The notification must include any measures the customers may undertake to mitigate the negative consequences of such incident.

ANNUAL RISK ASSESSMENTS

Payment services providers must submit to the NBR an annual assessment of the operational and security risks relating to the payment services they provide, and of the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

STRONG CUSTOMER AUTHENTICATION

Payment services providers must apply "strong customer authentication" (**SCA**) when a PSU accesses its payment account online, initiates an electronic payment operation, or carries out any action through a remote channel that may imply a risk of payment fraud or other abuse.

The SCA must be based on the use of two or more elements, categorised as:

- knowledge (something only the customer knows);
- possession (something only the customer possesses); and
- inherence (something the customer represents).

These elements must be independent, so that the breach of one element does not compromise the reliability of the other elements and they must be designed in such a way as to protect the confidentiality and integrity of the customer's personalised security credentials. Authentication of remote electronic payment

operations must include elements which dynamically link the operation to a specific amount and to a specific payee.

SANCTIONS

Breaches of the above obligations may trigger an administrative fine, ranging from RON 10,000 (approximately EUR 2,100) and RON 100,000 (approximately EUR 21,000), the temporary suspension of the payment services provider's activities until relevant remedies are implemented, the temporary suspension of access to payment systems until relevant remedies are implemented, or a fine ranging up to an amount representing twice the value of the profits actually obtained or up to an amount representing twice the losses actually avoided by the payment services provider responsible for the breach, in so far as such amounts can be determined.

RUSSIA

CRITICAL INFORMATION INFRASTRUCTURE LAW, PERSONAL DATA LAW, AND NATIONAL PAYMENT SYSTEM LAW

Cybersecurity issues became very important in light of successful cyber-attacks on Russian companies that were carried out several years back. The legislator recognised the importance of cybersecurity and, in addition to fragmentary regulations that previously existed in certain legal areas, adopted a new law regulating the general requirements of cybersecurity in most important spheres of Russian economy.

CRITICAL DATA INFRASTRUCTURE LAW (CDI LAW)

The main purpose of the CDI Law, which came into force on 1 January 2018, is to ensure that Russia's critical data infrastructure (that consists of "*critical data infrastructure facilities and telecommunications networks used for the interaction of such facilities*") is secure and stable in the face of cyber-attacks.

The CDI Law imposes certain obligations upon, amongst others, Russian entities and/or individual entrepreneurs (**CDI Operators**) that own, lease or have other legal rights to critical data infrastructure facilities (such as data systems, data and telecommunications networks and automated control systems) operating in the following areas: (i) healthcare; (ii) science; (iii) transport; (iv) communications; (v) energy; (vi) banking and other sectors of financial markets; (vii) oil & gas; (viii) nuclear; (ix) defence; (x) rocket and space;(xi) mining; (xii) metals; and (xiii) chemical industry (**CDI Facilities**).

The main obligation of any CDI Operator is to inform the Federal Security Service of the Russian Federation and the Central Bank of the Russian Federation, as the case may be, immediately of any "cyber incident". The definition of "cyber incident" is broad and does not necessarily come down to a cyber-attack, but rather includes "*any malfunction or stoppage of a critical data infrastructure facility or telecommunications network used for the interaction of such facilities, and/or a breach of the security of the data processed by such facilities, including as a result of a cyber-attack*".

In addition, the CDI Law focuses on the security of what is called "important critical data infrastructure facilities" (**Important CDI Facilities**). Important CDI Facilities will be determined by the CDI Operators in accordance with specific regulations on the basis of various criteria of importance (such as social, political, economic, and ecological importance, and their importance for national defence and law and order), and will be registered in a special register of important critical data infrastructure facilities (the **Register**). Any CDI Operator whose CDI Facility is on the Register will have additional obligations under the

CDI Law. In particular, such CDI Operator will be obliged to comply with specific security regulations for Important CDI Facilities and, in case of a cyber incident, to respond to the cyber incident in accordance with special procedures.

CDI Operators' compliance with requirements under the CDI Law will be monitored by the Federal Service for Technical and Export Control of the Russian Federation through scheduled and unscheduled audits. Scheduled audits will take place every three years.

Unscheduled audits will be carried out in the circumstances specified in the CDI Law (for example, in the event of a cyber incident with negative consequences for an Important CDI Facility). CDI Operators' officers may be criminally prosecuted for violations of the CDI Law, if the violation has resulted in damage to the critical data infrastructure.

PERSONAL DATA LAW

The Personal Data Law concerns anyone that processes the personal data of individuals (the **Personal Data Operators**). "Personal data" is extremely broadly defined and covers "*any information relating to a, directly or indirectly, identified or identifiable individual*".

The Personal Data Law requires any Personal Data Operator to apply all necessary legal, administrative and technical measures to protect the personal data from illegal or accidental access, destruction, modification, blocking, copying, transfer, dissemination or other illegal operations. In particular, they include, amongst others:

- detection of security threats;
- application of specific administrative and technical security measures stipulated by the personal data regulations for the purposes of compliance with the personal data security requirements;
- application of information security tools that have passed compliance verification;
- evaluation of efficiency of the personal data security measures in place before the personal data information system has been put into operation;
- adoption of the personal data access rules and recording of all operations with the personal data; and
- security measures control.

In the case of a security breach, the Personal Data Operators may face damage claims from individuals whose personal data has been breached. In addition, the Personal Data Operators may be subject to administrative fines of up to RUB 15,000 that potentially may be multiplied by the number of the relevant individuals affected.

NATIONAL PAYMENT SYSTEM LAW

Money transfer operators, banking paying agents, payment system operators and payment infrastructure service providers (the **Supervised Entities**) have the specific relevant security obligations with respect to bank secrecy and other information in the payment system. In particular, they are obliged to comply with specific security requirements, including, amongst others:

- design and implementation of the security system;
- application of information security measures (encryption (cryptographic) tools, security measures from unauthorised access, antivirus protection, firewalling measures, intruder detection systems, and protection control tools); and
- detection of incidents regarding violations of security requirements.

The National Payment System Law also requires uninterrupted operation of money transfers and, therefore, money transfer operators are obliged to apply specific measures to provide uninterrupted operation of money transfers, that include, amongst others:

- collection, systematisation, and accumulation of money transfer information by reducing the electronic money balance of the payer and increasing the respective balance of the receiver;
- prevention and, if it occurs, remedying of malfunction of operational and technical facilities engaged in recording of information with respect to electronic money balances and their transfer;
- analysis of causes of malfunction; and
- ongoing testing of operational and technical facilities.

In addition to the above, money transfer operators are required to adopt internal regulations that must contain, amongst others, the response plan in case of malfunction of the operational and technical facilities.

Sanctions for violation of the National Payment System Law depend on whether the operation of the money transfer was interrupted as a result of the violation. In case of interruption, the Russian Central Bank may limit or suspend operations of the relevant entity. In addition, fines of up to RUB 1,000,000 may be applied.

OTHER REGULATIONS

Specific regulations relating to information security can be applied to Russian companies operating in certain spheres of the Russian economy. For example, the most developed cybersecurity regulations in this regard are in the banking sphere. In particular, there are information security standards issued by the

Until you have experienced something like this, you don't realise just what can happen, just how serious it can be.

Søren Skou, CEO at A.P. Møller-Maersk

Bank of Russia to be followed by Russian banks. Although these standards are advisory in nature rather than mandatory, in practice most (if not all) Russian banks comply with them.

SLOVAK REPUBLIC

CYBER SECURITY ACT

In the Slovak Republic, cybersecurity was not comprehensively regulated at a national level until 2018. Certain issues concerning cybersecurity have been governed by the Act on Critical Infrastructure, the Act on Information Systems of Public Administration, and the Act on Trusted Services for Electronic Transactions in the Internal Market. Given that these fragmentary regulations did not ensure an appropriate level of security of network and information systems, the Slovak Parliament passed Act No. 69/2018 Coll. on Cyber Security (the **Cyber Security Act**) in January 2018, which implements the NIS Directive[4].

The Cyber Security Act, which came into effect on 1 April 2018, aims to ensure the security of cyberspace in the Slovak Republic. In line with the NIS Directive, it introduces obligations for operators of essential services and providers of digital services. In particular, operators of essential services must adopt general and sectorial security measures. These measures not only include technological security measures but also personal and organisational measures, such as internal security policies. In addition, operators of essential services and providers of digital services are subject to several notification obligations, including the obligation to notify the National Security Authority (**NBU**) of incidents via the cybersecurity integrated information system. While operators of essential services must notify all substantial incidents, providers of digital services are subject to the notification obligation only if an incident having an essential impact occurs, and they have sufficient information to identify it. Currently, notifications can be made by sending an email to the NBU's email address sk-cert@nbu.gov.sk (the NBU recommends PGP encryption) or by filling in a form available on the NBU's webpage https://www.sk-cert.sk/en/tips-and-tricks/report-an-incident/index.html

The above obligations, however, do not apply to all operators providing services in the selected sectors (energy, transport, banking, financial market infrastructure, etc.). The identification criteria for essential services are defined in a Decree of the National Security Authority No. 164/2018 Coll.. Operators providing services in the selected sectors become subject to the obligations once the service they provide meets the identification criteria, and the NBU registers them in the register of operators of essential services. Similarly, the

[4] Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

obligations only apply to the providers of digital services specified in the Cyber Security Act (such as online marketplaces, online search engines and cloud computing services) that employ at least 50 employees and have a turnover of more than EUR 10 million.

Compliance with the Cyber Security Act is monitored by the NBU which acts as the national computer security incident response team. The NBU is also in charge of preparing the national cybersecurity strategy. Current strategic documents concerning cybersecurity include the Cyber Security Concept of the Slovak Republic for 2015 to 2020, approved by the Slovak government under resolution No. 328/2015 and the Action Plan for Implementation of the Cyber Security Strategy of the Slovak Republic for 2015 to 2020 approved by the Slovak government under resolution No. 93/2016. While the first strategic document proposes a new institutional framework of cybersecurity, the latter proposes tasks to be undertaken to provide for an adequate protection of the state's cyberspace against potential dangers that could cause irreparable damage to the Slovak Republic.

Finally, the NBU has an important role in incident handling. Upon the occurrence of a serious incident or its threat, the NBU may give a warning of such incident via the cybersecurity integrated information system, and require operators of essential services and providers of digital services to take reactive measures. Operators of essential services and providers of digital services must then demonstrate, without undue delay, to the NBU that they have met the obligation imposed by the NBU.

In the event of a breach of obligations arising from the Cyber Security Act, operators of essential services and providers of digital services may be subject to administrative fines of up to EUR 300,000. The fine may be doubled for repeated breaches.

In the financial sector, an important piece of legislation concerning cybersecurity is the Act on Payment Services, into which the revised Payment Services Directive (**PSD2**)[5] was transposed. The Act on Payment Services requires payment service providers to comply with a number of cybersecurity obligations such as:

- **Policies and procedures:** Payment service providers must have a security policy with appropriate mitigation measures and control mechanisms in place to manage operational and security risks. They must also establish and maintain effective incident management procedures that should help to detect and classify major operational and security incidents. Details on the

[5] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

policy and security measures are laid down in the Guidelines on the Security Measures for Operational and Security Risks of Payment Services under PSD2 issued by the European Banking Authority (**EBA**).

- **Major incident reporting:** Payment service providers must notify the National Bank of Slovakia (**NBS**) of major operational or security incidents without undue delay. When reporting incidents, payment services providers should follow the Guidelines on Major Incident Reporting under PSD2, issued by the EBA. Notifications must be made in electronic form, using the Statistics Collection Portal (https://www.nbs.sk/en/statistics/information-for-reporting-subjects/statistics-collection-portal).
- **Customer notification of major incidents:** If a major operational or security incident could have an impact on the financial interests of customers, payment service providers must inform customers of the incident without undue delay. In addition, they must inform them of all measures they can take to mitigate the adverse effects of the incident.
- **Annual risk assessments:** Payment service providers must provide the NBS with an annual assessment of the risks relating to their payment services and the adequacy of the mitigation and control mechanisms implemented.
- **Strong customer authentication:** Payment service providers must apply strong customer authentication when a customer accesses its payment account online, initiates an electronic payment transaction, or carries out any other action through a remote channel that may imply a risk of payment fraud or other abuses. The strong customer authentication must be carried out by using two or more of the following elements, categorised as (i) knowledge (i.e. information that is known to the customer only); (ii) possession (i.e. a thing that the customer has in his/her possession); and (iii) inherence (i.e. biometric data of the customer). These elements must be independent so that if one of them is compromised the reliability of the others will not be affected. When applying strong customer authentication, payment service providers must have adequate security measures in place to protect the confidentiality and integrity of customers' personalised security credentials.

Under the Act on Payment Services, the NBS may impose a fine of up to EUR 300,000 upon payment services providers for breach of their obligations under the Act. The fine may be doubled for repeated breaches.

UNITED ARAB EMIRATES (UAE)

CYBER CRIMES LAW

The Cyber Crimes Law has been in force since 27 August 2012 and comprises 51 articles, most of which set out specific cybercrimes, and prescribe the applicable penalty for each crime. The Cyber Crimes Law penalises: hacking; phishing; unauthorised access to electronic sources, including laptops and emails; obtaining/ intercepting communications (including emails) intentionally; unlawfully accessing banking details (including any form of electronic payment like PayPal) or secure details (such as passwords) using information technology; forging electronic documents or credit/debit cards; and capturing an asset, benefit or right through fraudulent means or by taking a false name or capacity via an electronic source.

Apart from these, the Cyber Crimes Law also penalises acts such as:

- using a Virtual Private Network (**VPN**) to commit a crime or prevent its discovery;
- inciting, tempting or assisting in committing prostitution or debauchery by using information technology (it is questionable if dating apps might fall foul of this);
- insulting another person or attributing an incident to a person via information technology that may make that person subject to contempt or punishment (akin to defamation);
- calling for donations or promoting the same using information technology without a licence (e.g. raising monies for charities through the internet); and
- crimes related to morality and public order committed through the internet, including pornography, blackmail, or gambling or materials prejudicing public morals, criticism of the State or its Rulers or insulting one of the monotheistic religions.

In addition to the Cyber Crimes Law, Article 29 of Federal Law No.1 of 2006 concerning e-transactions and e-commerce penalises the committing of a crime under any other applicable law by electronic means.

The Cyber Crimes Law is intended to penalise the perpetrators of the crime and does not place any obligations on individuals or entities to protect themselves from cybercrimes, or penalise them for lack of such protection.

PENALTIES

All the crimes under the Cyber Crimes Law carry a penalty of imprisonment and/or a fine, with prison sentences ranging from temporary imprisonment to no minimum sentence, and fines ranging from AED 100,000 to AED three million, subject to any more severe punishment that is applicable under any other law. An attempt to commit any of the cybercrimes enumerated by the Cyber Crimes Law is punishable by half the penalty prescribed for the relevant crime. Other measures the courts can take include confiscating devices, erasing information and closing sites, deporting convicted foreigners, and supervising, controlling or prohibiting a convict's use of electronic sources. The courts can reduce or waive the prosecution of any individual who informs the authorities of a cybercrime relating to the security of the State (a list of which is included in Article 44), based on a request from the public prosecutor.

The UAE's free zones – the Dubai International Financial Centre (**DIFC**) and the Abu Dhabi Global Markets (**ADGM**) – do not have specific cybersecurity laws. However, the DFSA (a regulator in the DIFC) and the ADGM have signed memorandums of understanding with the Telecommunications Regulatory Authority (**TRA**) to co-operate in the aim of preventing cybercrimes. In addition, the UAE Central Bank is in the process of setting up a department dedicated to cybercrime but has been actively issuing circulars on cyber security since 2019.

UAE DATA PRIVACY

Under Article 31 of the UAE Constitution, the right of confidentiality of communication is entrenched. At present, onshore UAE does not have a federal data protection law or a national data protection regulator, although we understand a new law might be implemented in due course. Instead, there are various UAE Federal Laws that contain provisions relating to privacy and protection of personal data, including the Penal Code, the Cyber Crimes Law, and some sector-specific laws discussed below. The DIFC and ADGM (which are free zones in the UAE) have their own comprehensive data protection laws and data protection regulators. The DIFC data protection law was revised in June 2020 and borrows various concepts from the GDPR. We understand that the ADGM may also update its data protection law soon. In addition, Dubai Healthcare City (another free zone) also maintains its own data protection system. The data protection regulations in these free zones are generally consistent with laws in other developed jurisdictions.

THE PENAL CODE

The Penal Code sets out a number of defamation and privacy offences, including: (a) publishing anything which could expose the victim to public hatred

> **Only through collective action can we hope to meet the global challenge of cyber security**.
>
> Daniel Dobrygowski,
> Project Lead for Cyber Resilience
> at the World Economic Forum.

or contempt (Article 372); (b) false accusations that could dishonour or discredit a person (Article 373); (c) recording or publishing of any news, pictures or comments which may reveal the secrets of people's private or family lives, even if the published material is in the public interest and true (Article 378); and (d) disclosing a secret that a person is entrusted with by reason of his profession or circumstance, without consent, unless permitted by law.

THE CYBER CRIMES LAW

Article 21 of the law makes it an offence to "assault the privacy of a person" online by recording or transmitting communications, audio-visual materials, pictures or electronic news or information, even if they were correct and true. Social media posts, for example, might fall foul of the UAE's privacy laws, as they could theoretically constitute a breach of privacy, and defamation, and be an offensive publication all at once. We understand from media stories that people have been convicted for posting videos, without consent, of a friend sleeping, or of road rage incidents, and for posting a picture of an illegally parked car. These examples highlight the need for sensitivity to such laws. The TRA issues guidance on the appropriate usage of social media and online platforms which users should familiarise themselves with.

SECTOR-SPECIFIC LAWS

Telecoms

On 10 January 2017, the TRA issued consumer protection regulations (that were updated in 2019) that require telecoms companies in the UAE to take all reasonable measures to prevent the unauthorised disclosure or use of a subscriber's information, which includes their personal details, service usage, call/message records, payment history and credit rating. Disclosure is permitted where the subscriber has consented, or is required, to disclose to law enforcement agencies any such information which might aid criminal investigations. A subscriber's consent can be recorded in their contract, provided they have a right to subsequently opt out. The TRA also launched the National Cyber Security strategy in 2019, pursuant to which further cybersecurity regulations may be issued.

Banking

The UAE Banking Law (Federal Law No. 14 of 2018) codifies rules on confidentiality of customer information for banks. Article 120 confirms that written permission is needed from customers for Licensed Financial Institutions to share their data with third parties (other than in a small number of cases, such as AML/CFT compliance and institutions establishing their rights in litigation). The confidentiality rules in the UAE Banking Law cover a broad range of information, being "all data and information related to customers' accounts, deposits… and related transactions". A breach of such confidentiality can result in criminal sanctions against the relevant personnel and the financial institution.

While there are no data localisation requirements in the UAE Banking Law, we understand that the UAE Central Bank was considering draft outsourcing regulations that might include localisation requirements. While such regulations are yet to be issued, it is anticipated that the transfer of confidential data outside the UAE might require notification to the UAE Central Bank and the bank may need to satisfy the Central Bank that the relevant jurisdiction has adequate safeguards to protect such data.

Healthcare

The UAE Healthcare law (Federal Law 2 of 2019) regulates the use of medical data. Onshore and free zone entities that directly or indirectly provide services in the healthcare sector (including health insurance and healthcare IT) are prohibited from transferring medical data outside of the UAE except with UAE Health Authority and Ministry of Health approval. Such entities could disclose this data with the written approval of the patient or where disclosure is for preventive procedures related to public health or treatment of the patient or those in contact with the patient. In practice, healthcare providers are likely to limit disclosure of such data to health authorities in the UAE. The Cyber Crimes Law also makes it a crime to disclose or damage confidential information relating to medical treatment without permission.

UAE Government Entities

NESA, The National Electronic Security Authority, is a federal body tasked with protecting the UAE's critical information infrastructure and improving national cybersecurity. To achieve this, it has produced a set of standards and guidance for government entities in critical sectors. Compliance with these standards is mandatory for such government and government-linked entities. In Dubai, the Government has created an Information Security Committee which has a similar role to NESA. We understand there are information security regulations that require UAE government data to be stored within the UAE and some of these regulations are at Emirate level. Moreover, Cabinet Resolution No. 21 of 2013 imposes requirements in respect of governmental information systems, and on governmental employees to take various measures to prevent cybercrimes.

Insurance

The Insurance Authority has mandated all insurance companies in the UAE to comply with the NESA standards issued in 2017, with companies to be compliant by the end of 2020. Separately, the UAE Insurance Authority issued outsourcing regulations in 2019 that require insurance companies to store information that is received electronically (through its website or other mediums) in the UAE.

ENFORCEMENT

We understand that the UAE has appointed public prosecutors specifically tasked with prosecuting cybercrimes. Complaints in respect of cybercrimes first need to be made to the relevant Emirate's police department. Most Emirates have a designated cybercrimes department which will investigate such crimes and, based on its report, the public prosecutor then decides whether a criminal case should be filed or not. As with cybersecurity, the unauthorised disclosure of private data attracts criminal sanctions, and the data subject could lodge a complaint with the police in the relevant Emirate. Other bodies in the UAE with cybersecurity responsibilities include: (a) National Electronic Security Authority, a federal authority; (b) the TRA; (c) the UAE Computer Emergency Response Team (**aeCert**), a subsidiary of the TRA; and (d) the Dubai Electronic Security Centre. Article 274 of the UAE Penal Code requires any individual who has knowledge of a crime to report it to the competent authorities or risk a fine of up to AED 1,000. However, in practice, we understand that this might not be strictly applied. A victim of cybercrime or data breaches could also bring parallel civil proceedings against the perpetrator if they can prove that the crime caused them damage. If successful with a criminal complaint, there is a presumption of liability in UAE civil proceedings.

GUIDANCE FOR UAE COMPANIES

The restriction in Article 379 of the Penal Code could apply to personal data of employees. Where possible, companies should seek an employee's consent prior to disclosure of his/her data. Law No.2 of 2015 concerning Commercial Companies requires directors and employees to act in their organisation's best interests and with reasonable skill and care. In the DIFC and ADGM, entities are also obliged to implement adequate operating systems and controls. Failure to maintain adequate cybersecurity, or to prevent unauthorised disclosure of data, may constitute a breach of those duties, opening the doors to liability for compensation and regulatory sanctions against such persons. If the directors or employees of UAE companies were found guilty of cybercrimes or data privacy breaches while performing their duties, it might also expose the company to vicarious liability under UAE law. It is advisable for companies to adopt international best practices in relation to cybersecurity and data protection systems, and to instate adequate training for its personnel.

UNITED KINGDOM

IMPLEMENTATION OF EU LAW

E-PRIVACY DIRECTIVE

The Privacy and Electronic (EC Directive) Regulations 2003 (**PECR**) implement the e-Privacy Directive[6] in the UK.

Under the PECR (s.5(1), public electronic communications service (**PECS**) providers must take appropriate technical and organisational measures to safeguard the security of its services to:

- ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;
- protect personal data stored or transmitted against:
  - accidental or unlawful destruction;
  - accidental loss or alteration; and
  - unauthorised or unlawful storage, processing, access or disclosure; and
- ensure the implementation of a security policy regarding the processing of personal data.

The **Information Commissioner's Office (ICO)** has powers (Regulation 31) for enforcing and overseeing the requirements of PECR, including: to audit PECS providers; to impose enforcement notices, information notices and monetary penalty notices; conduct a dawn raid; and prosecute for failure to comply with a notice.

GDPR

The GDPR,[7] as a Regulation, has direct effect in EU member states (which the UK was at the time it came into force), but in addition the Data Protection Act 2018 (**DPA**) which, replaced the Data Protection Act 1998 which had created criminal offences that may be committed alongside cyber-dependent crimes including:

- obtaining or disclosing personal data;
- procuring the disclosure of personal data; and

---

6 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

7 Regulation (EU) 2016/679 (General Data Protection Regulation)

- selling, or offering to sell, personal data.

This provision was most typically/commonly used to prosecute those who had accessed healthcare and financial records without a legitimate reason but, for example, could also be used in a scenario such as where Trojans can appear as legitimate computer programs but facilitate illegal access to a computer in order to steal personal data without a user's knowledge.

The new DPA (at s.170) builds on this, to add the offence of:

- knowingly or recklessly retaining personal data (which may have been lawfully obtained) without the consent of the data controller.

There are some exceptions, such as where the obtaining, disclosing, procuring or retaining of personal data was necessary for the purposes of preventing or detecting a crime.

The **ICO** is the supervisory authority for data protection in the UK, and its role includes providing guidance, monitoring compliance, conducting audits and taking enforcement action. As set out in more detail below, the ICO also covers a broad range of other UK legislation.

FRAMEWORK DIRECTIVE

The Communications Act 2003 (**CA 2003**) implements Article 13a of the Framework Directive 2002,[8] which sets a common regulatory framework for electronic communications networks and services.

The CA 2003 provides that public electronic communications network (**PECN**) providers and public electronic communications service (**PECS**) providers must take technical and organisational measures appropriately to manage risks to the security of PECNs and PECSs, taking all appropriate steps to protect, as far as possible, the availability of PECNs (s. 105A). These measures include:

- the prevention or minimisation of the impact of security incidents on end-users; and
- the prevention or minimisation of the impact of security incidents on interconnection of PECNs.

The **Office of Communications (Ofcom)** is responsible for enforcing breaches of the CA 2003 and ensuring that telecommunications network providers implement the cybersecurity measures required to secure their communication networks. It has enforcement powers including to: notify regulated providers of contraventions; gather information from, and audit, regulated providers; issue

[8] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services

directions suspending the entitlement to provide networks or services; and impose substantial fines.

A PECN provider is under an obligation (s. 105B) to notify Ofcom of:

- any breach of security that has a significant impact on the operation of a PECN; and
- any reduction in the availability of a PECN that has a significant impact on the network.

NIS DIRECTIVE

The Network and Information Systems Regulations 2018 (**NIS Regulations**) came into force on 10 May 2018.These implement the NIS Directive[9], which aims to raise levels of the overall security and resilience of network and information systems across the EU. The NIS Regulations apply to those sectors which are vital to the economy and society: Energy; Transport; Health; Drinking Water Supply and Distribution; and Digital Infrastructure.

While listed as a sector in the NIS Directive, the NIS Regulations (in line with Recital 9 and Article 1(7) of the NIS Directive) do not set out any criteria for identifying and regulating those in the Financial Market Infrastructure sector, as a different framework –for example, PSD2 - already applies.

The NIS Regulations:

- require publication of a UK's national network and information systems strategy;
- identify the UK's single point of contact (**GCHQ**);
- identify the UK's Computer Security Incident Response Team (the NCSC, part of GCHQ);
- identify the criteria in each subsector for identifying operators of essential services (**OES**);
- identity what a relevant digital service provider (**RDSP**) is;
- set out the requirements of an OES or RDSP to notify cyber incidents;
- set out the enforcement regime and penalties for failure to comply; and

[9] Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

- identify the UK's national Competent Authority (**CA**) or authorities for the sectors, who have the power to issue guidance, inspect organisations and take enforcement action where necessary.

Organisations are designated as an OES by the relevant CA. An OES is required to:

- take appropriate and proportionate measures to manage risks posed to the security of network and information systems on which their essential service relies;
- those measures must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed;
- take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services;
- have regard to any relevant guidance issued by the relevant CA when carrying out the above duties.

A RDSP is a provider of digital services – an online search engine,[10] online marketplace[11] or cloud computing service[12] - (either alone or in combination) that:

- provides the digital services to external customers (i.e. to individuals or organisations, not internally maintained services);
- is not a small or micro business (fewer than 50 staff and a turnover and/or balance sheet of less than EUR10 million, noting that if the service is part of a larger group, include the staff and turnover size of the group when assessing whether the small business exemption applies); and
- has either a head office in the UK or has a nominated UK representative.

A RDSP must identify and take appropriate and proportionate measures to manage the risks posed to the security of network and information systems on which it relies to provide, within the European Union: online marketplace; online search engine; or cloud computing services. These measures must:

10 a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found

11 a digital service that allows consumers and/or traders […] to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace

12 a digital service that enables access to a scalable and elastic pool of shareable computing resources

- (having regard to the state of the art) ensure a level of security of network and information systems appropriate to the risk posed;
- prevent and minimise the impact of incidents affecting their network and information systems with a view to ensuring the continuity of those services; and
- take into account the following elements: the security of systems and facilities; incident handling; business continuity management; monitoring, auditing and testing; and compliance with international standards.

For RDSPs, the Implementing Regulation[13] (also known as the 'DSP Regulation), and technical guidelines produced by ENISA (European Union Agency for Network and Information Security), is also relevant.

The National Cyber and Security Centre (**NCSC**), as the UK's national technical authority for information assurance, and which provides advice and assistance on cyber security, has provided cyber security guidance to the CAs and OES on meeting the requirements of the NIS Directive, notably its Cyber Assessment Framework (**CAF**).

OVERSIGHT & MONITORING

For CAs regulating OES, active oversight is expected. In its guidance to CAs, the Department for Culture, Media and Sport (**DCMS**) states that CAs should proactively engage with industry, publish guidance, meet with representatives from OES, and implement an assessment framework, including an audit programme. CAs are also required to consult and co-operate with the ICO when addressing incidents that result in breaches of personal data.

This is different for RDSPs, where the CA and the ICO is limited to post-ante oversight. The DCMS guidance still recommends that the ICO should provide guidance and support to RDSPs.

The NCSC has no regulatory role but provides cyber security advice and guidance and acts as a source of technical expertise. However, the NCSC's CAF contains guidance which will be used by CAs to assess compliance during mandatory audits. In addition, as the designated CSIRT for the UK, NCSC must take actions including to: monitor incidents in the UK; and provide early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents.

[13] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018

ENFORCEMENT & PENALTIES

According to the DCMS guidance, CAs should not rush to take action just because an incident has been reported. An incident is not by itself an infringement of the NIS Regulations, and the key factor for determining enforcement action is whether or not appropriate and proportionate security measures and procedures were in place and being followed.

CAs have a lot of flexibility under the NIS Regulations when it comes to the exact form that any enforcement action takes. In addition to the power to impose fines, CAs have the power to:

- conduct inspections: to assess if the organisation has met its obligations under the NIS Regulations;
- serve information notices: to require an organisation to provide information to enable the regulator to assess the organisation's compliance with the NIS Regulations; and
- serve enforcement notices: which shall set out the steps that the organisation must take to rectify identified failures by the organisation.

The DCMS guidance recommends that CAs should implement a stepped process of enforcement in which OES and RDSPs are given warnings, and that CAs publish their enforcement policy so that OES and RDSPs are clear as to the approach being taken.

The NIS Regulations set out the following tiered system of financial penalties, capping the potential fines that CAs can impose for different breaches of the NIS Regulations:

- penalty not exceeding GBP 1 million any contravention which the enforcement authority determines could not cause a network and information systems incident;
- penalty not exceeding GBP 3.4 million for a material contravention which the enforcement authority determines has caused, or could cause, an incident resulting in a reduction of service provision by the OES or RDSP for a significant period of time;
- penalty not exceeding GBP 8.5 million for a material contravention which the enforcement authority determines has caused, or could cause, an incident resulting in a disruption of service provision by the OES or RDSP for a significant period of time; and
- penalty not exceeding GBP 17 million for a material contravention which the enforcement authority determines has caused, or could cause, an incident resulting in an immediate threat to life or significant adverse impact on the UK economy.

COMPETENT AUTHORITY (CA) GUIDANCE

A key part of the functioning of the NIS Regulations will be how the sector CAs assesses and enforces them. CAs are strongly encouraged to use the NCSC's CAF as part of their toolkit in order to provide consistency across sectors and the UK.

DIGITAL INFRASTRUCTURE

Ofcom, is the CA for OES in the Digital Infrastructure sector, although the ICO is the CA for RDSPs. Ofcom, published interim guidance for OES in May 2018, which:

- gives a high-level introduction to the NIS Regulations;
- sets out Ofcom's initial views on the immediate steps it expects an OES in the sector to take, as a minimum, to meet its obligations under the NIS Regulations;
- provides information about the types of operators on which duties have been imposed under the NIS Regulations;
- sets out the processes and thresholds for reporting relevant security incidents; and
- introduces Ofcom's intended initial enforcement approach.

OES that are "deemed to be designated" for the Digital Infrastructure subsector are:

- Top Level Domain Name Registries (who service an average of 2 billion or more queries in 24 hours for domains registered within the Internet Corporation for Assigned Names and Numbers);
- Domain Name Service Providers (which service an average of 2,000,000 or more requesting DNS clients based in the United Kingdom in 24 hours; or which are servicing 250,000 or more different active domain names); and
- Internet Exchange Point Operators (IXP Operators who have 50% or more annual market share amongst IXP Operators in the United Kingdom, in terms of interconnected autonomous systems, or who offer interconnectivity to 50% or more of Global Internet routes).

Anyone meeting the criteria after 10 May 2018 has a duty to notify Ofcom within three months after the date the criteria was met.

Ofcom states that it currently expects enforcement to be broadly in line with the approach set out in its June 2017 Enforcement guidelines for regulatory investigations, and that it will review in due course whether this approach needs adapting.

The ICO provides living guidance to RDSPs in a dedicated section of its website, which summarises the obligations of RDSPs under the NIS

Regulations and explains the ICO's role as the CA for these organisations. It also provides more information on the requirements of the Implementing Regulation[14] (**DSP Regulation**) and provides links to relevant sections of guidance produced by others, such as the technical guidelines produced by ENISA (European Union Agency for Network and Information Security) in respect of the DSP Regulation. The ICO also sets out its approach to notifications and enforcement, as well as providing guidance on the interaction between the NIS Regulations and GDPR. RDSPs were required to register with the ICO by 1 November 2018.

Drinking Water Supply and Distribution: The Department for Environment, Food & Rural Affairs (**Defra**) is a CA for this sector, but has conferred its CA function to the Drinking Water Inspectorate (**DWI**). The DWI guidance states that:

- each water company must take appropriate and proportionate measures to manage risks to their network and information systems and to prevent and/or minimise the impact of incidents to those systems; and
- water companies must understand their own network and information systems and the level of security required and therefore should be capable of taking informed, balanced decisions about how these measures are managed.

As a result, the DWI is of the view that a principles-based approach is the most effective way of driving improvements around the resilience of cyber security in the context of the NIS Regulations rather than an approach based on prescriptive rules.

Water companies should also take into account the information and guidance outlined in the Defra Water Sector Cyber Security Strategy, which summarises what water and sewerage companies need to do to reduce the risks of cyber attacks, and Water UK's Cyber Security Principles for the Water Sector, a set of principles and recommendations produced to help its members address the risks posed to water and waste water services by cyber related threats.

Energy: The Energy sector is split into three subsectors – electricity, oil and gas. The Office of Gas and Electricity Markets (**Ofgem**) has, in its role as a joint CA with The Department for Business, Energy and Industrial Strategy (**BEIS**), produced guidance for the Downstream Gas and Electricity subsectors to help OES in those sectors understand their duties and to set out Ofgem's initial approach to NIS implementation. The guidance sets out that OES are expected

[14] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018

to perform self-assessments against the NCSC's CAF, and work with Ofgem to establish improvement plans where necessary.

Health: The DHSC is one of the CAs for the Health sector and has published guidance:

- NHS Trusts and Foundation Trusts are considered OES for the health sector in England for the purposes of the NIS Regulations. The DHSC will also designate other NHS healthcare providers as OES and those organisations will be individually notified.
- The DHSC has incorporated the NIS Regulations into its approach to implementing the National Data Guardian's 10 data security standards. These data security standards apply to all health and care organisations to ensure that systems and data are protected. While the NIS Regulations will only apply to organisations considered OES, the 10 data security standards and wider regulatory framework, including the GDPR, apply to all health and care organisations.
- NHS Digital guidance on implementing the 10 data security standards is accessible through the Data Security and Protection Toolkit, which will be updated over time and reflect relevant guidance from the NCSC. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practicing good data security and that personal information is handled correctly. Such organisations are required to carry out self-assessments of their compliance against the assertions and evidence contained within the toolkit.

Transport: The DfT is one of the CAs for the Transport sector and has published guidance which:

- sets out the responsibilities of OES;
- sets out as the roles and responsibilities of the CA and how these will be carried out;
- sets out the process and thresholds for mandatory incident notifications; and
- contains specific guidance for each transport mode and provides clarity on how the NIS Regulations will align with any existing guidance, standards or regulations related to network and information system security.

The types of organisations in scope within the sector are:

- owners or managers of airports; air navigation service providers; air carriers;
- harbour authorities; shipping companies; operators of port facilities; operators of vessel traffic services;

- operators of railway assets (trains, networks, stations and light maintenance depots) for domestic and international rail plus some light rail and metro/underground services; and
- roads authorities and operators of intelligent transport systems.

Specific thresholds will apply to many of the above types of entities, which are generally based on the scale of the operation in terms of annual passenger numbers or freight tonnage. For domestic and international rail there are no specific thresholds and so any entity that meets the definitions will be in scope.

PAYMENT SERVICES DIRECTIVE PSD2)

The UK has implemented PSD2[15] primarily through the Payment Services Regulations 2017 (**PSRs**).

Under the PSRs, the **Financial Conduct Authority (FCA)** is the competent authority for most of the provisions (including being responsible for authorising and supervising payment service providers (**PSPs**)), although the **Payment Systems Regulator (PSR**) is the competent authority for monitoring and enforcing compliance with certain requirements relating to payment systems.

The PSRs and related changes to FCA rules introduce the following new requirements on PSPs relating to security and fraud risks:

- PSPs are required to establish a framework to manage the operational and security risks relating to the payment services they provide, including effective incident management procedures that allow PSPs to detect and classify **major operational** and **incidents** (such as a cyber-attack on an IT system that prevents consumers using their bank accounts). PSPs must provide the FCA with an assessment of these operational and security risks and the adequacy of related risk mitigation and control measures, at least annually.
- If a major operational or security incident occurs, PSPs must report the incident to the FCA within four hours of detection under new reporting rules in Chapter 15 of the Supervision manual (**SUP**) of the FCA Handbook. PSPs must also make intermediate notifications at least every time there is a relevant status update to the incident, and a final notification when the root cause analysis has taken place. The FCA requires PSPs to comply with the European Banking Authority (**EBA**) Guidelines on major incident reporting under PSD2, which specify the criteria for assessing whether a major operational or security incident has occurred, as well as the notification format and procedures.

[15] Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

- PSPs are required to implement adequate security measures to protect the confidentiality and integrity of customers' personalised security credentials, and to allow them to apply strong customer authentication (**SCA**) and communicate securely with customers and other PSPs. Regulatory technical standards on SCA[16] set out the detail of these requirements, including requirements for periodic testing, evaluation and audit of these security measures.
- PSPs are required to have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions, and must collect and report fraud data to the FCA annually. EBA Guidelines on fraud reporting under PSD2 specify the data to be reported.
- Note that banks have to allow TPPs (Third Party Providers, authorised online service providers that have been introduced as part of open banking) access to customers' payment account data under PSD2. This involves processing of customers' personal data and is subject to the GDPR. As such, bear in the mind that the ICO, as well as the FCA and PSR, is also potentially a relevant regulator in the event of a cyber incident.

THE BREXIT EFFECT

The UK left the EU on 31 January 2020. A transitional period is in place until 31 December 2020, during which substantially all of the EU legislation which previously applied in the UK remains in force. At the end of the transition period, this EU legislation will be "onshored" into UK domestic law under the European Union (Withdrawal) Act 2018 (**EUWA**), as it applies at that date. This means that substantially all of the EU legislation which previously applied in the UK will continue to apply after the end of the transition period, subject to the UK government's powers under the EUWA to amend this retained EU legislation to ensure it works in a post-Brexit context.

In respect of the GDPR, GDPR will continue to have direct effect in the UK during the transition period, alongside the data protection regime in the DPA 2018. After that time, the GDPR, will be onshored into UK domestic law under the EUWA and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 will act to merge the UK GDPR and the DPA to form a single general processing regime for the UK.

In the context of the NIS Directive, large RDSPs headquartered outside the UK which offer digital services within the UK will have to nominate a representative within the UK by 20 April 2021, so that they can be contacted by the ICO for compliance purposes. Likewise, RDSPs based in the UK but offering services

[16] Commission Delegated Regulation (EU) 2018/389

in the EU will need to appoint a representative in the EU to act on its behalf with regulators and notify the ICO of such appointment.

Minor consequential amendments to drafting will take effect for the DPA on 31 December 2020, and for the NIS Regulations on 20 January 2021.

OTHER RELEVANT LAW AND REGULATIONS

LEGISLATION

There are a number of pieces of UK domestic legislation which can have application in the context of a cyber incident or attack.

COMPUTER MISUSE ACT 1990 (CMA)

The CMA is the main piece of UK legislation relating to offences or attacks against computer systems, such as hacking or denial of service (**DoS**) attacks.

Offences under the CMA include those relating to:

- unauthorised access (ss.1, 2);
- unauthorised acts with the intent to impair the operation of a computer (relevant, for example, to cases involving distributed denial of service (**DDoS**) attacks, such as those launched against Lloyds Banking Group and Barclays in 2017) (s.3);
- unauthorised acts causing, or creating a risk of, serious damage, for example, to human welfare, the environment, economy or national security (aimed at those who seek to attack critical national infrastructure) (s.3ZA); and
- making, supplying or obtaining articles for use in offences contrary to section 1, 3 or 3ZA (deals with those who make or supply malware) (s.3A).

As well as the usual criminal authorities, the ICO also has the power to take action under the CMA, which it used for the first time in 2018 when it successfully prosecuted an individual on a charge of securing unauthorised access to personal data after the ICO found he had used colleagues' log-in details to access software containing thousands of customer records.

INVESTIGATORY POWERS ACT 2016 (IPA)

The IPA repealed part of the Regulation of Investigatory Powers Act 2000 (**RIPA**) and merged what were previously two separate offences in s.1 of RIPA, replacing them with one offence. Under s.3(1) IPA, a person commits an offence if he intentionally intercepts a communication in the course of its transmission without lawful authority by means of:

- a public telecommunication system;
- a private telecommunication system; or

- a public postal service.

This offence could apply in a hacking case, where content has been unlawfully intercepted through cyber-enabled means, and offenders may be charged under the IPA instead of or in addition to the CMA. The IPA would usually be used where material was unlawfully intercepted in the course of its transmission, and the CMA would usually be used where material is acquired through unauthorised computer access.

OFFICIAL SECRETS ACT 1989 (OSA)

The OSA criminalises the disclosure of (or failure to secure) information which is damaging to the armed forces, security or intelligence services (or their work), or endangers the lives of British citizens or British interests abroad. The OSA generally applies to the Government or Crown, but s.8(1) could potentially cover cybersecurity issues for third party Government contractors providing services which relate to energy, policing, prisons or immigration. It is an offence if, in relation to any "document or article" which it would be an offence to disclose without lawful authority, a person fails to "take such care to prevent the unauthorised disclosure of the document or article as a person in his position may reasonably be expected to take".

CYBER-ENABLED CRIME

There is a wealth of UK legislation to address crimes which do not depend on computers or networks, but have been transformed in scale or form by the use of the internet and communications technology. These include the category of economic-related cybercrime, including fraud and intellectual property crime (piracy, counterfeiting and forgery).

Economic-related cybercrimes include unauthorised access, sabotage or use of computer systems with the intention to cause financial gain to the perpetrator or financial loss to the victim. They may involve computer fraud or forgery, hacking to steal personal or valuable data for commercial gain, or the distribution of viruses.

Offences under the Fraud Act 2006 are applicable to a wide range of cyber-frauds by focusing on the underlying dishonesty and deception. The nature of the offending will dictate the appropriate charges, and prosecutors may also consider offences under the Theft Act 1968, Theft Act 1978, Forgery and Counterfeiting Act 1981 and Proceeds of Crime Act 2002.

FINANCIAL AND PRUDENTIAL REGULATION

The statutory objectives of the financial and prudential regulators in the UK, the FCA and the PRA, mean that the cyber resilience of regulated financial services firms is of key significance. The FCA has a strategic objective to ensure that relevant markets function well, as well as operational objectives which include the protection of consumers and protection of financial markets. One of the

PRA's statutory objectives is to promote the safety and soundness of the firms it regulates.

Key FCA principles and rules relevant to firms' resilience to cyber issues include:

- Principles for Businesses, Principle 3: A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems;
- Senior Management Arrangements, Systems and Controls handbook (**SYSC**) 3.1.1: A firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business; and
- SYSC 3.2.6: A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system, and for countering the risk that the firm might be used to further financial crime.

The Senior Managers and Certification Regime (**SMCR**) creates a Chief Operations Senior Management Function (SMF 24), and the regulators have made it clear that this will be the individual responsible for the resilience of operations and technology of the firm – and so responsible for the firm's cyber resilience.

Firms must report a material cyber incident to the FCA under Principle 11 of the Principles for Businesses and the rules set out in Chapter 15 of the Supervision manual (**SUP**). Firms may consider an incident material if it:

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

The PRA similarly has key rules relevant to a firm's resilience to cyber issues, including:

- Fundamental Rule 5: A firm must have effective risk strategies and risk management systems;
- Fundamental Rule 6: A firm must organise and control its affairs responsibly;
- PRA Rulebook, Risk Control: A firm must establish, implement and maintain adequate risk management policies and procedures, including effective procedures for risk assessment, which identify the risks relating to the firm's activities, processes and systems, and, where appropriate, set the level of risk tolerated by the firm; and a firm must adopt effective arrangements, processes and mechanisms to manage the risk relating to its activities, processes and systems, in light of that level of risk tolerance; and

- PRA Rulebook, Group Risk Systems: A firm must have adequate, sound and appropriate risk management processes and internal control mechanisms for the purpose of assessing and managing its own exposure to group risk, including sound administrative and accounting procedures; and ensure that its group has adequate, sound and appropriate risk management processes and internal control mechanisms at the level of the group, including sound administrative and accounting procedures.

Operational resilience more broadly has been a focus of the FCA and PRA for some time, and the material which both regulators have put out is highly relevant to cyber security and resilience. In December 2019, the FCA, PRA and the Bank of England published joint discussion papers proposing the introduction of new requirements for financial services firms to strengthen their operational resilience. Under the proposals, firms and financial market infrastructures (**FMIs**) would be required to:

- identify their important business services that, if disrupted, could cause harm to their consumers (retail and wholesale) or market integrity, threaten the viability of firms or cause instability in the financial system;
- set impact tolerances for each important business service (i.e. thresholds for maximum tolerable disruption, to help achieve consumer protection and market integrity);
- identify and document the people, processes, technology, facilities and information that support their important business services (mapping);
- test their ability to remain within their impact tolerances through a range of severe but plausible disruption scenarios;
- conduct lessons-learnt exercises to identify, prioritise, and invest in their ability to respond and recover from disruptions as effectively as possible; and
- develop internal and external communications plans for when important business services are disrupted.

The deadline for the responses was 1 October 2020.

THE VIEW FROM REGULATORS AND INDUSTRY

DATA

In July 2019, the ICO issued two notices of intention to impose record-breaking fines for infringements of the GDPR.

- A GBP183.4 million fine against British Airways Plc (**BA**) relating to a cyber incident, believed to have begun in June 2018, in which the personal data of approximately 500,000 BA customers was compromised. The fine would have equated to 1.5% of BA's global turnover for 2017; ; however, on 16

October 2020, and having considered representations from BA and the economic impact of COVID-19, the ICO issued its penalty notice against BA in a significantly smaller sum – GBP 20 million.

- A GBP99.2 million fine against Marriott International, Inc (**Marriott**). The proposed fine relates to a cyber incident whereby approximately 339 million global guest records relating to residents in 31 countries in the European Economic Area, including credit card details, were exposed by malicious actors. Seven million of the compromised records related to UK residents. The incident was notified to the ICO by Marriott in the same month of the attack.

In December 2019, the ICO concluded its first enforcement action under the GDPR, fining a London-based pharmacy (Doorstep Dispensaree Ltd) GBP275,000 for failing to ensure the security of special category data.

The ICO has also taken a number of enforcement actions under the old (DPA 1998) regime for conduct before the GDPR was in force. These include:

- In March 2019, the ICO prosecuted two employees who had accessed or shared personal data obtained from their employer without a valid reason. Faye Caughey had to pay fines and costs totalling GBP1,640 after she viewed personal data held on the systems of a National Health Service foundation trust. Jayana Morgan Davis forwarded several work emails containing personal data of customers and other employees to her personal email account and had to pay fines and costs of GBP820. Mike Shaw, who heads up the criminal investigations team at the ICO, said: *"People expect that their personal information will be treated with respect and privacy. Unfortunately, there are those who abuse their position of trust and the ICO will take action against them for breaking data protection laws."*
- In April 2019, the ICO fined the London Borough of Newham GBP145,000 after an employee sent an email with the personal information of more than 200 people who featured on a police intelligence database which records information in respect of alleged gang members.
- In January 2020, the ICO fined DSG Retail Limited the maximum fine of GBP500,000 under the GDPR after a point of sale computer system was compromised as a result of a cyber attack, affecting at least 14 million people.
- In March 2020, the ICO also levied the maximum fine of GBP500,000 against Cathay Pacific Airways Limited, the computer system of which the ICO found lacked appropriate security measures. This led to the personal details (including names, passport and identity details, dates of birth, postal and email addresses, phone numbers and historical travel information) of 111,578 UK customers, and approximately 9.4 million more individuals

worldwide, being exposed. Steve Eckersley, the ICO Director of Investigations, said: *"This breach was particularly concerning given the number of basic security inadequacies across Cathay Pacific's system, which gave easy access to the hackers. The multiple serious deficiencies we found fell well below the standard expected. At its most basic, the airline failed to satisfy four out of five of the National Cyber Security Centre's basic Cyber Essentials guidance."*

FINANCIAL SERVICES

In October 2018, the FCA fined Tesco Personal Finance plc (**Tesco Bank**) GBP16,400,000 for failing to exercise due skill, care and diligence in protecting its personal current account holders against a cyber-attack which took place in November 2016.

The FCA found that cyber-attackers exploited deficiencies in Tesco Bank's design of its debit card, its financial crime controls and in its Financial Crime Operations Team to carry out the attack. Those deficiencies left Tesco Bank's personal current account holders vulnerable to a largely avoidable incident that occurred over 48 hours, and which netted the cyber-attackers EUR2.26million.

The FCA found that Tesco Bank breached Principle 2 of the FCA's Principles for Businesses because it failed to exercise due skill, care and diligence in:

- designing and distributing its debit card;
- configuring specific authentication and fraud-detection rules;
- taking appropriate action to prevent the foreseeable risk of fraud; and
- responding to the cyber-attack with sufficient rigor, skill and urgency.

The level of the penalty could have been higher – a 30% credit for mitigation and settlement at the first stage of the FCA's executive settlement procedure meant that it came down from a starting figure of GBP33,562,400.

In 2017 and 2018, the FCA surveyed 296 firms to assess their technology and cyber capabilities to gain a better understanding of the industry's resilience. The survey looked at key areas such as governance, delivery of change management, managing third party-risks and effective cyber defences. Firms self-assessed their capabilities, and the FCA then analysed the responses for each firm and across sectors.

Firms' responses highlighted cyber weaknesses in three areas: people; third-party management; and protecting their key assets. Many firms reported that they have mature IT change management functions, but the FCA noted in its report that failed IT changes caused 20% of the operational incidents reported to the FCA between October 2017 and September 2018. The FCA expects all

firms to consider the report's findings and feedback, and its relevance to their business. The FCA reiterated that, under Principle 11, it expects firms to report major technology outages and cyber-attacks to the FCA, and noted that evidence suggests that firms are under-reporting.

In March 2019, the FCA published a document bringing together industry insights on cyber resilience, with the objective of aiding cybersecurity practices. This highlighted the importance of ensuring that cyber risk is on firms' executive agenda, systematically reviewing the linkage between risk and controls to monitor effectiveness, planning for incidents, and testing internal and external communications. In July 2019, an FCA FOIA request revealed that the number of declared cyber incidents rose from 69 in 2017 to 819 in 2018, an increase of over 1,000%.

The focus of the **PRA** has been more on cyber insurance, and the industry's response to it. In January 2019, it published a 'Dear CEO' letter to specialist general insurance firms it regulates (which include insurance companies and Lloyd's of London) setting out areas where it thinks firms could do more to ensure the product management of cyber risk exposures (having Supervisory Statement on Cyber insurance underwriting risk in July 2017).

PAYMENT SERVICES

In respect of the resilience of payment, the view of the PSR is that, in view of the roles of the Bank of England and the FCA, the PSR would not expect to take the lead in the event of any incident, but would expect to be informed and involved in any discussions regarding regulatory action.

The **Payment Card Industry Security Standards Council (PCI SSC)**, has published a number of payment card and account security standards, including the PCI Data Security Standards (**PCI DSS**) and cyber security framework.

The PCI DSS is aimed at merchants and payment processors, representing good practice for any business handling sensitive financial data. Although guidance represents best practice, when issuing a monetary penalty for any regulatory failures, the ICO has made it clear they will consider any breach of applicable PCI DSS standards to be an aggravating factor.

PENSIONS

The consequences of a cybersecurity breach for a pension scheme and its members could be severe. The destruction or loss of data, or the disruption of computer systems, could leave a scheme unable to calculate benefits or pay pensions. Although pension schemes have not yet been the subject of a high-profile cybersecurity breach, trustees should not be complacent, and the **Pensions Regulator (PR)** has increased its focus on cyber resilience. In April 2018, the PR published guidance for trustees which considers the steps needed to build a scheme's cyber resilience as well as those required when a cybersecurity incident strikes a scheme, which included:

- Pension schemes should fully understand their scheme's cyber risk, not least through developing an awareness of the scheme's "cyber footprint" (that is, the extent of the digital presence of all parties involved in the scheme).
- Ensure sufficient controls are in place to minimise the risk of cyber incidents. Cyber risk should appear on a scheme's risk register and be regularly reviewed. In addition, trustees should assure themselves that their third-party suppliers have sufficient cybersecurity controls in place.
- Maintain an incident response plan, designed to help the scheme to recover swiftly after a cyber incident. This should include details of the necessary formalities for reporting incidents to the PRA, the FCA or the ICO, as appropriate.

MOBILE SERVIES

Businesses that operate in the mobile industry can process data of a sensitive nature and must meet all regulatory requirements in its preservation and use. The **Mobile Marketing Association (MMA) Code of Conduct** applies to any business involved in the mobile ecosystem and, in addition to indirect cybersecurity obligations, the Code of Conduct imposes a duty to implement reasonable technical administrative and physical procedures to protect user information collected in connection with mobile marketing programs from unauthorized use, alteration, disclosure, distribution, or access. the **Groupe Speciale Mobile Association (GSMA)** has also published a voluntary Code of Conduct for Mobile Money Providers which includes security, governance and risk management obligations.

PUBLIC COMPANIES

Publicly listed companies are subject to certain governance obligations under the **UK Corporate Governance Code (CGC)**, the **FCA Listing Rules** and **Disclosure and Transparency Rules**. Although the provisions of the CGC are not specific to cybersecurity, they would encompass cybersecurity requirements. Relevant provisions include:

- Provision 29 of the CGC concerning risk management and internal controls, requires companies to conduct, at least annually, a risk review covering "all material controls, including financial, operational and compliance controls".
- Provision 28 of the CGC requires companies to carry out an assessment of the company's emerging and principal risks and provide an explanation in its annual reports of how these risks will be mitigated or managed.

- The Disclosure and Transparency Rules require listed companies to disclose information that may affect its share price, including cybersecurity risks and breaches that have or could potentially affect the company. Failure to disclose may lead to investor compensation claims under s.90 of the Financial Services and Markets Act 2000.

ACCOUNTING AND CORPORATE FINANCE

In 2014, the **Institute of Chartered Accountants for England and Wales (ICAEW)** issued guidance on cybersecurity in corporate finance. The publication provides step-by-step guidance dealing with the six stages of a corporate transaction from initial preparation through to completion. The guidance is supported by an online cybersecurity resource centre, which provides ICAEW members with guidance on small firm cybersecurity standards, auditing, training and compliance.

THE VIEW OF THE COURTS

Whilst the majority of claims brought before the English courts in respect of cyber issues relate to cyber-enabled crime, the courts are seeing an increasing number of civil claims, particularly in relation to loss of control over data.

- In August 2020, a representative action (an "opt-out" class-type action) was commenced against Marriott International on behalf of millions of claimants whose personal data was allegedly exposed as a result of a data breach which is believed to have first taken place as early as 2014, and to have continued until 2018. The claimants seek damages for loss of control of personal data resulting from breaches of the GDPR and / or statutory duty under the Data Protection Act 1998.
- In May 2020, proceedings were issued by a group of claimants (under a group litigation order – an "opt-in" class-type action) against easyJet for breach of statutory duty under the GDPR, breach of contract, breach of confidence and misuse of private information. The claims are said to arise out of a data breach suffered by easyJet in January 2020 affected the personal data of approximately nine million customers.
- In April 2020, the UK Supreme Court in *WM Morrison Supermarkets plc v Various Claimants* [2020] UKSC 12 allowed an appeal by supermarket chain Morrisons against a decision by the Court of Appeal that it was vicariously liable for the actions of a disgruntled employee who had copied mass employee data and published it on the internet, thereby breaching Data Protection legislation (in this case, the Data Protection Act 1998). The Supreme Court found instead that the disgruntled employee was pursuing a "personal vendetta". The scope of vicarious liability described by the Supreme Court remains broad, however, and so businesses remain at risk

of being held vicariously liable when employees' actions are connected with the business, even if those actions are illegal.

- Also in April 2020, generic particulars of claim were served on behalf of a group of claimants bringing claims (under a group litigation order) against British Airways following a data breach in 2018 that is said to have affected some 400,000 customers, and resulted in the loss of log in, payment card and travel booking details, as well as passenger name and address information.
- In October 2019, a claimant (on behalf of a class of other claimants) was granted, on appeal, permission to serve proceedings in the form of a representative action on Google in California (Lloyd v Google LLC [2019] EWCA Civ 1599). The proceedings concern allegations that Google had secretly collated browser-generated information from iPhone users and sold it to advertisers. The judgment is important as the Court of Appeal recognised that compensation can be awarded for a breach of data protection legislation resulting in loss of control of personal data even where the claimant provides no evidence of pecuniary loss or emotional harm. It also opens the door to claims of a significant quantum, allowing a large number of alleged victims of a data breach to seek redress. Permission has been granted for an appeal to the Supreme Court.
- In July 2018, the Commercial Court granted a worldwide freezing injunction against a group of unknown defendants who were suspected of having perpetrated a cyber-attack on an English company's email system, causing the Bank of China to transfer monies to a number of jurisdictions around the world (CMOC v Persons Unknown [2017] EWHC 3599 (Comm)). Damages were subsequently ordered for the full amount of the loss, on the basis of successful claims for, amongst other things, "unlawful means" conspiracy (with the unlawful means including breaches of the CMA).
- In June 2016, in another case concerning damages under the Data Protection Act 1998 (TLT & others v Secretary of State for the Home Department and the Home Office [2016] EWHC 2217), it was determined that family members of data subjects who have their data misused can bring statutory and common law claims where their identities can also be readily inferred from published data.
- In Vidal-Hall v Google Inc [2014] EWHC 13 (QB), a prior case involving the collation of browser-generated information from iPhone users, the High Court in January 2014 found that claimants could be awarded damages for "distress" caused by a breach of the Data Protection Act 1998 even where pecuniary (i.e. monetary) loss had not been suffered. This effectively decoupled claims for distress from claims for financial loss, and opened the

door to claims by victims of data misuse who had not suffered any financial loss as a result.

The English courts are also prepared to act quickly and grant injunctive and other interim relief to seek to recover and prevent further dissemination of data and/or funds which are the subject of a cyber incident, even where the perpetrators are unknown. They have also shown themselves willing to facilitate applications for interim relief by being open to innovative methods of effecting service on respondents, including service via email and social media.

CONTACTS

Czech Republic

Daniela Bencova
Associate

T +420 222 55 5280
E daniela.bencova
@cliffordchance.com

Michal Jašek
Counsel

T +420 222 55 5229
E michal.jasek
@cliffordchance.com

France

Julia Martres
Avocat

T +33 14405 2493
E julia.martres
@cliffordchance.com

Jérémy Guilbault
Avocat

T **+33 14405 2480**
E jeremy.guilbault
@cliffordchance.com

Alexandre Manasterski
Avocat

T +33 14405 5971
E alexandre.manasterski
@cliffordchance.com

Dessislava Savova
Partner

T +33 14405 5483
E dessislava.savova
@cliffordchance.com

Germany

Grégory Sroussi
Avocat

T +33 14405 5248
E gregory.sroussi
@cliffordchance.com

Heiner Hugger
Partner

T +49 697199 1283
E heiner.hugger
@cliffordchance.com

Ines Keitel
Partner

T +49 697 199 1250
E ines.keitel
@cliffordchance.com

David Pasewaldt
Partner

T +49 697 199 1453
E david.pasewaldt
@cliffordchance.com

Gerson Raiser
Senior Associate

T +49 697199 1450
E gerson.raise
@cliffordchance.com

Dr. Thomas Voland
Partner

T +49 211 4355 5642
E thomas.voland
@cliffordchance.com

Italy

Carlo Felice Giampaolino
Partner

T +39 064229 1356
E carlofelice.giampaolino
@cliffordchance.com

Alessandro Sciarra
Associate

T +39 064229 1384
E alessandro.sciarra
@cliffordchance.com

Andrea Tuninetti Ferrari
Senior Associate

T +39 028063 4435
E andrea.tuninettiferrari
@cliffordchance.com

Iolanda D'Anselmo
Associate

T +39 028063 4294
E iolanda.danselmo
@cliffordchance.com

Middle East

Daniel Royle
Counsel

T +966 11481 9756
E daniel.royle
@cliffordchance.com

Arun Visweswaran
Senior Associate

T: +971 50455 9270
E: arun.visweswaran
@cliffordchance.com

Netherlands

Andrei Mikes
Associate

T: +31 20711 9507
E: andrei.mikes@cliffordchance.com

Jaap Tempelman
Counsel

T: +31 20711 9192
E: jaap.tempelman@cliffordchance.com

Poland

Marcin Ciemiński
Partner

T: +48 22429 9515
E marcin.cieminski@cliffordchance.com

Krzysztof Hajdamowicz
Counsel

T: +48 22429 9620
E: krzysztof.hajdamowicz@cliffordchance.com

Paweł Pogorzelski
Counsel

T: +48 22429 9508
E: pawel.pogorzelski@cliffordchance.com

Russia

Ekaterina Makarova
Senior Associate

T:+7 495 725 6435
E: ekaterina.makarova@cliffordchance.com

UK

Evgeny Soloviev
Counsel

T:+7 495 725 6420
E: evgeny.soloviev@cliffordchance.com

Jamie Andrew
Senior Associate

T:+44 20 7006 1367
E: jamie.andrew@cliffordchance.com

Jonathan Kewley
Partner

T:+44 20 7006 3629
E: jonathan.kewley@cliffordchance.com

Simon Persoff
Partner

T:+44 20 7006 3060
E: simon.persoff@cliffordchance.com

Kate Scott
Partner

T:+44 20 7006 4442
E: kate.scott@cliffordchance.com

Samantha Ward
Partner

T:+44 20 7006 8546
E: samantha.ward@cliffordchance.com

Ellen Lake
Senior Associate

T: +44 20 7006 8345
E: ellen.lake@cliffordchance.com

Haafiz Suleman
Senior Associate

T:+44 20 7006 4348
E: haafiz.suleman@cliffordchance.com


ASIA
PACIFIC

AUSTRALIA

CYBER SECURITY STRATEGY

. On 6 August 2020, the Australian Government released "Australia's Cyber Security Strategy 2020" which is the successor to the 2016 Cyber Security Strategy. The 2020 Strategy, which involves a $A1.67 billion investment in cyber security initiatives over the next 10 years, has been introduced with the stated aim of creating "a more secure online world for Australians, their businesses and the essential services upon which we all depend". Central to the 2020 Strategy is the need for governments, businesses and the community to work collaboratively in order to achieve effective cyber security.

Some of the key initiatives outlined in the 2020 Strategy include:

- Strengthening the critical infrastructure regulatory framework (as further detailed below).
- Considering the introduction of new laws that establish a minimum cyber security baseline across the entire economy which could result in changes to privacy, consumer and data protection laws as well as the duties of company directors.
- Developing new powers accompanied by appropriate safeguards that allow the governments to take action against sophisticated cyber attacks.
- Releasing the "Code of Practice: Securing the Internet of Things for Consumers", a voluntary Code of Practice containing 13 principles to inform businesses of the cyber security features expected of internet-connected devices available in Australia.

PRIVACY ACT 1988 (CTH)

The Privacy Act imposes some obligations in relation to cybersecurity:

- Entities subject to the Australian Privacy Principles (**APPs**) (each an APP entity) must have a clearly expressed and up-to-date policy in relation to the management of personal information.
- Entities that hold personal information (or credit-reporting information) are required to implement appropriate measures to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.
- Recipients of individuals' tax file numbers (**TFNs**) must take reasonable steps to protect TFN information from misuse and loss, and from

unauthorised access, use, modification or disclosure, and ensure that access to records containing TFN information is restricted to individuals who need to handle that information for taxation law, personal assistance law or superannuation law purposes.

- Generally, if an entity holding personal information, credit reporting information or an individual's TFN no longer requires the information, the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.
- An APP entity must take such steps as are reasonable in the circumstances to ensure that an overseas recipient of personal information from the entity does not breach the APPs in relation to the information (for example, through contractual provisions), unless an exception applies (such as where consent is given or the recipient of the information is subject to a law that has the effect of protecting the information in a way that is substantially similar to the way in which the APPs protect the information, and there are mechanisms that the individual can access to take action to enforce that protection).

It is also important to note that, by virtue of its extraterritorial effect, the Privacy Act applies to the acts and practices of foreign organisations with an 'Australian link'. To this end, proceedings commenced in March 2020 by the Australian Information Commissioner against Facebook Inc, and Facebook Ireland Ltd. This will set an important precedent for determining the scope of the extra-territorial effect of the Privacy Act. Conversely, the extraterritorial effect of the EU's GDPR will mean that certain Australian businesses are subject to the GDPR in addition to local law requirements.

NOTIFIABLE DATA BREACHES SCHEME (NDB SCHEME)

The NDB Scheme came into effect on 22 February 2018, as an amendment to the Privacy Act.

The NDB Scheme imposes mandatory investigation and notification obligations in respect of eligible data breaches on a number of agencies and organisations including APP entities, credit reporting bodies, credit providers and TFN recipients. Under the NDB Scheme, an entity covered by the scheme which is subject to an eligible breach is required to notify the Office of the Australian Information Commissioner (**OAIC**) and any individuals likely to be at risk of serious harm as a result of the breach. The notice must include:

- The identity and contact details of the organisation
- A description of the data breach
- The kind of information that has been disclosed
- Recommendations about the steps individuals should take in response to the data breach.

AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY (APRA)

APRA's Prudential Standard "CPS 234 Information Security" came into effect on 1 July 2019. This Standard applies to authorised deposit-taking institutions (**ADIs**), general insurers, life insurers, private health insurers, licensees of registrable superannuation entities (**RSE licensees**) and authorised or registered non-operating holding companies. The Standard aims to ensure that APRA-regulated entities are resilient against information security incidents (including cyber-attacks) by requiring that each such entity maintains an information security capability that is commensurate with information security vulnerabilities and threats. The Standard requires, inter alia, that APRA-regulated entities have clearly defined information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals, and that APRA is promptly notified of any material information security incidents. Other relevant APRA standards and guidelines include:

- APRA Prudential Standards – CPS 220 (Risk Management) and CPS 231 (Outsourcing)These Standards require APRA-regulated entities to have proper risk management strategies, including IT systems, and to ensure that they properly manage outsourcing risk in relation to material business activities
- APRA Prudential Practice Guides – CPG 234 (Management of Security Risk in Information and IT) and CPG 235 (Managing Data Risk)These Guides provide guidance to senior management and risk management and technical specialists (both management and operational) about data and security risks and specifically target areas where APRA continues to identify weaknesses as part of its ongoing and supervisory activities

- APRA Information Paper – Outsourcing involving Cloud Computing Services
  - This paper, released on 24 September 2018, provides an update to APRA's July 2015 publication which outlined prudential considerations and key principles that should be considered when adopting the use of cloud computing services.

AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION (ASIC)

In June 2019, ASIC released Consultation Paper 314 (Market Integrity Rules for Technological and Operational Resilience) seeking feedback on proposed new market integrity rules for securities and futures market operators and market participants to promote the resilience of their critical systems. If introduced, the rules will require, amongst other things, that market operators and participants:

- Maintain adequate arrangements to ensure the resilience, reliability and integrity of their critical systems.
- Implement appropriate controls in respect of outsourcing arrangements for the provision, support or operation of critical systems.
- Implement procedures and policies to protect the confidentiality, integrity and security of data.
- Maintain records of any unauthorised access to, or use of, their critical systems or market-sensitive, confidential or personal information for no less than seven years.
- Implement an incident management plan and business continuity plan to enable the continued operation or timely restoration of critical systems following incidents or major events which affect critical systems.
- Notify ASIC as soon as practicable on becoming aware of any unauthorised access to, or use of, critical systems (where the functioning of those systems is impacted) and market sensitive, confidential or personal information.

Comments in respect of the Consultation Paper closed in August 2019. ASIC has yet to release its response to the consultation process and the market integrity rules in a final form.

Further, in addition to continuous disclosure obligations which may require a company to disclose a breach of data security, ASIC's Cyber Resilience Health Check 2015 set out ASIC's expectation that company Boards participate in cybersecurity issues, recommending that companies (i) adopt the US Department of Commerce's National Institute of Standards and Technology Cyber Security Framework, (ii) engage with cybersecurity bodies and (iii) involve directors and the Board in managing cybersecurity to foster a strong culture of cyber resilience. In December 2019, ASIC released a report on the cyber resilience of firms in Australia's financial markets, which revealed that the cyber resilience of firms operating in Australia had improved by an average of 15% across all cyber resilience functions since the previous report on cyber resilience had been published in November 2017.

ASIC's increased focus on cybersecurity in recent years is reinforced by the commencement of proceedings on 21 August 2020 against RI Advice Group Pty Ltd (RI) alleging that RI's failure to have and implement adequate cybersecurity measures contravened its obligations under the Corporations Act 2001 (Cth). This is the first time that litigation has been initiated by ASIC in respect of deficient cybersecurity practices.

ASIC has published good practice guidance, key questions for boards to ask in relation to cyber resilience and other resources to help organisations improve

Hostile states, terrorists and criminals use… instant connectivity and encrypted communications… to undermine our national security, attack our interests and, increasingly, commit crime.

Jeremy Fleming,
Head of GCHQ

their cyber resilience: https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/resources-on-cyber-resilience/

CYBERCRIME ACT 2001 (CTH)

This Act establishes offences that are consistent with those required by the Council of Europe Convention on Cybercrime. The provisions are drafted in technology-neutral terms to accommodate advances in technology. The Act establishes cybercrime offences, including serious offences which are defined as offences punishable by imprisonment for five years or more, including life sentences.

SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018 (CTH)

This Act seeks to strengthen the Australian Government's ability to respond to national security threats, particularly sabotage, espionage and coercion, that may be brought about by cyber-attacks. The Act captures approximately 165 assets in the electricity, gas, water and ports sectors, and creates a Register of Critical Infrastructure Assets, gives the Government greater information-gathering powers with respect to these assets, and creates a Ministerial directions power to allow the Minister for Home Affairs to issue directions to owners or operators of these critical assets in order to mitigate national security risks.

As noted above, a key initiative of the 2020 Strategy is the enhancement of the critical infrastructure regulatory framework by way of legislative amendments to the Act. To this end, the Government is proposing to:

- Expand the range of sectors which are subject to the Act to include the following sectors: banking and finance; communications; data and the cloud; defence; education, research and innovation; food and grocery; health; space; and transport.
- Introduce a positive security obligation that will apply to all critical infrastructure entities and consist of both a principles-based set of security outcomes as well as sector-specific guidance and requirements to be designed by entities in conjunction with the relevant regulator in each sector.
- Introduce enhanced cyber security obligations that will apply to entities that are considered to be involved with critical infrastructure of national significance.
- Facilitate Government assistance or intervention if necessary to effectively respond to and manage cyber attacks on the networks and systems of critical infrastructure entities.

The Australian Government has signalled its intention to engage in extensive consultation on the proposed reforms that will inform the development of legislative amendments to the Act.

CHINA

CYBERSECURITY LAW OF THE PEOPLE'S REPUBLIC OF CHINA

The *Cyber Security Law of the People's Republic of China* (2016) (the "**Law**") came into force on 1 June 2017 with the aim of strengthening the protection of network operation and information security. The Law states that China takes steps to monitor, defend and address cybersecurity risks both from within and outside China. The Law applies to everyone who operates networks in the PRC, including multinational corporations. It applies to the construction, operation, maintenance and use of networks as well as the regulation of cybersecurity within the PRC. It also applies to both the internet and individual intranets as long as there is any network-related activity taking place in the PRC.

The Law comprises 79 articles within seven chapters. Amongst other things, the Law focuses on network operation security and network information security.

NETWORK OPERATORS

Network operators are the main entities regulated under the Law. According to Article 76 of the Law, the term "network operators" refers to an entity or person that owns or administers a network and/or provides services through a network. By definition, therefore, any person or entity in China who has access to a network may become a network operator. In addition to traditional telecom and internet operators, network operators may also include financial institutions that provide online services, such as banks and insurance companies.

NETWORK OPERATION SECURITY

Network operators must observe the following security requirements:

- network operators must take technical and other necessary measures to safeguard network operations, respond effectively to cybersecurity

incidents, prevent cybercrime and maintain the integrity, confidentiality and accessibility of network data (Article 10); and

- network operators must set up network security governance and safeguard networks from interference, destruction or unauthorised access, must retain network logs for at least six months, and prevent network data from being leaked, tampered with or stolen by following applicable cybersecurity requirements set out under a grading protection system (Article 21).

OPERATION SECURITY OF THE CRITICAL INFORMATION INFRASTRUCTURES (CIIs)

CIIs include critical information infrastructures for public communication and information services, utilities (such as energy, transportation and water), finance and public services, as well as other infrastructures that may result in damage to state security, public welfare and public interests if they were destroyed, disabled or subject to data breaches (Article 31). If a network operator operates a CII, it will be subject to more stringent rules and requirements. CII operators must carry out an assessment of their facilities' cybersecurity at least once a year, and report potential risks and proposed remediation measures to the authorities (Article 38).

On 10 July 2017, the Cyberspace Administration of China (**CAC**) published the *Regulations on Security Protection of Critical Information Infrastructures (Consultation Draft)*. Although the Consultation Draft has not yet been finalised, it echoes the Law and clarifies relevant issues and requirements concerning the security protection of CIIs, including: (i) specifying the scope of CIIs; (ii) prescribing security protection obligations for CII operators in a more structured way; and (iii) in principle requires the operation and maintenance of CIIs to be carried out only in China. According to the consultation draft, competent authorities will issue a further guideline regarding the scope and identification of CIIs at a later stage.

PROTECTION OF PERSONAL INFORMATION

The Law contains strict requirements regarding the protection of personal information controlled by network operators. Personal information protected under the Law includes all types of information recorded electronically or otherwise that may identify a person, including, for example, name, date of birth, telephone number(s) and address(es).

In principle, personal information can only be collected when individuals have been informed and have agreed to the purpose and scope of the collection. The Law explicitly provides that:

- network product and service providers that collect users' information are required to inform and obtain consent from the users (Article 22);

- in collecting and using personal information, network operators must adhere to the principles of legality, fairness and necessity, disclose their rules of collection and use, explicitly indicate the purposes, means and scope of collecting and using the information, and obtain consent from the persons whose information is collected (Article 41);
- network operators shall neither collect personal information irrelevant to the services provided by them, nor collect or use personal information in violation of the provisions of laws, administrative regulations or the agreement with users, and should process personal information controlled by them in accordance with the provisions of laws, administrative regulations and user agreements (Article 41);
- network operators must not disclose, tamper with or destroy personal information they have collected (Article 42); and
- individuals are entitled to request the operator to delete personal information where it has been obtained in breach of the provisions of laws, administrative regulations and user agreements (Article 43).

There is a non-compulsory national standard regarding personal information security (the **National Standard**), which was implemented on 1 May 2018 and further updated on 6 March 2020 (the updated version came into effect on 1 October 2020). Under the 2018 National Standard, personal information may be classified as personal information and personal sensitive information. The latter mainly refers to information that may endanger physical or property security, cause damage or discriminative treatment to personal reputation and/or physical and mental health in the event of data leakage, illegal provision or misuse. Moreover, the personal information of children aged 14 or younger is classified as personal sensitive information. When collecting personal sensitive information, expressed and distinct consent is always required. The 2020 National Standard adds further detailed guidance for network service providers to protect personal information (such as the best practice to obtain consent).

In addition to requirements prescribed under the Law and the National Standard, following extensive enforcement activities against mobile internet application programs (**Apps**) which collected personal information illegitimately, on 28 November 2019, PRC regulators issued the *Measures on Identifying Illegitimate Collection and Usage of Personal Information by Apps (2019)* (the "**Apps Data Measures**"). The Apps Data Measures reflect the latest developments for implementing the Law and provide further practical guidance on the requirements regarding consent, and regulators have further illustrated typical activities/behaviours that constitute illegitimate collection and usage of personal information by Apps.

The outbreak of COVID-19 does not undermine the determination of regulators to protect personal information. CAC issued the Circular on the Protection of Personal Information and Utilisation of Big Data to Support the Prevention and Control of the Novel Coronavirus (2020) on 4 February 2020, which emphasises the principles of lawfulness, necessity and minimalism when collecting and processing personal information for epidemic prevention and control during the COVID-19 outbreak. In particular:

- unless properly authorised by competent authorities or by law, an entity/person may not collect personal information without acquiring the consent of the data subject even for the purpose of prevention and control of COVID-19;
- the scope of personal information to be collected must be kept at a minimum and targeting specific groups, such as patients/suspected patients suspected of having COVID-19 and people who have had close contact with them; and
- the personal information collected may not be used for any other purpose or disclosed without the data subject's consent, unless to the extent required for the prevention and control of COVID-19 and after anonymisation.

Data and the internet have turned our business on its head.

Alex Younger, Head at MI6

DATA STORAGE AND EXPORT

Personal information and important data collected and generated by CIIs must be stored within China. Where information and data are to be transferred overseas, a security assessment must be conducted according to rules to be jointly formulated by China's cyberspace administrative bodies and relevant departments under the State Council (Article 37). These restrictions apply to both personal information and non-personal data that constitute "important data". Latest consultation papers indicate that regulators want to extend this security assessment obligation to the operators of non-CIIs.

Regarding export of important data, on 28 May 2019, CAC issued the *Administrative Measures on Data Security (Consultation Draft)*, which emphasise that if any network operator intends to export any important data, a security assessment shall be carried out. Such export activities shall be approved by the competent industrial authorities or the competent provincial counterpart of CAC (where applicable).

Regarding the export of personal data, CAC issued the *Security Assessment Measures on Export of Personal Data (Consultation Draft)* on 13 June 2019, which provides that:

- security assessment is mandatory for any transfer of personal information without any safe harbour or exemption;
- security assessment should be carried out on a periodical basis (at least every two years) or be reassessed if any material change occurs;
- the agreement between the network operator and the non-PRC data recipient should be submitted for security assessment and incorporate prescribed clauses;
- export of personal information is prohibited if the security assessment indicates that such activity may endanger State security or public interest, or the safety of personal information cannot be sufficiently protected; and
- the transfer of personal information must be suspended or terminated if (i) any data leakage or data abuse incident occurs to the network operator and/or the non-PRC data recipient; (ii) the data subject is unable to exercise legitimate rights or obtain legitimate interest (or experiences difficulty in doing so); and (iii) the network operator and/or the non-PRC data receiving party is unable to protect the safety of personal information.

CERTIFICATION OF SECURITY PRODUCTS

Vendors can only sell critical network equipment, products or services after the equipment, the products or services have been certified by a qualified institution according to mandatory national standards (Article 23). CII operators purchasing network products and services that might affect national security must pass a national security review by CAC (Article 35).

PENALTIES

There are monetary penalties for companies and individuals found to be in breach of the Law. Business licences may be revoked, websites shut down and offenders detained. Note that the network operators and network products or services providers may be subject to a fine of one to ten times the illegal gains made in respect of certain non-compliance, including infringement upon the rights concerning personal information (Article 64). This penalty rule empowers regulators to impose significant penalties.

REGULATION OF SOCIAL MEDIA AND CHAT ROOMS

On 25 August 2017, CAC issued two new regulations concerning internet forums and chat rooms: the *Administrative Provisions on Internet Forum Community Services (2017)* and the *Administrative Provisions on Online Comment Threads Services (2017)*. Both provisions took effect on 1 October 2017. In addition, CAC issued the *Administrative Provisions on Microblogs Information Services (2018)* on 2 February 2018, which took effect on 20 March 2018. These three provisions complement the "real name registration" requirement and require providers of internet forums, community boards, chat

rooms and microblogs to verify the identity of their users. Only those who have their real names and identify information registered and verified are able to use these services and post comments. The provisions also impose requirements on service providers to:

- create a robust system for information censorship, real-time inspection, emergency responses, complaints and data protection;
- provide necessary information and technical support to the authorities for inspection;
- dispose of illegal information in a timely fashion; and
- establish a mechanism for refuting unsubstantiated rumours (for microblog service providers only).

On 20 December 2019, CAC issued the *Provisions on Ecological Management of Internet Information (2019)*, which came into effect on 1 March 2020. These new provisions further clarify the permitted and prohibited scope of internet information and reinforce regulatory requirements on internet information, which must be complied with by network information producers, network information service providers and network information service users.

HONG KONG

INDUSTRY-SPECIFIC GUIDANCE

There is no overarching legal framework for cybersecurity in Hong Kong. Entities regulated by the Hong Kong Monetary Authority (**HKMA**),Securities and Futures Commission (**SFC**) and the Insurance Authority (**IA**) must abide by the **regulatory guidance issued, including** the various **guidelines and circulars** concerning cyber risk management, resilience testing and management accountability. The Office of the Government Chief Information Officer (**OGCIO**) has issued guidelines in relation to cybersecurity controls to government departments and runs awareness campaigns for the wider community. The Personal Data Privacy Ordinance, Cap. 486 (**PDPO**) addresses the security of personal data, including data storage and security measures. There are a number of offences under Hong Kong law targeting cybersecurity-related crimes, including "unauthorised access to a computer by telecommunications" under the Telecommunications Ordinance, Cap. 106, "access to a computer with criminal or dishonest intent" and criminal damage under the Crimes Ordinance, Cap. 200.

THE HONG KONG MONETARY AUTHORITY

An HKMA Circular dated 14 October 2014, issued to all Authorised Institutions ("**AIs**"), required a review of existing controls and compliance with the PDPO, and addressed reporting requirements and failure to report. The circular stated that AIs should implement "layers" of security controls (covering both IT and non-IT) to prevent and detect any loss or leakage of customer data. AIs should be prepared to implement additional stringent controls related to Bring-Your-Own-Device (**BYOD**) devices in accordance with their data classification and risk assessment results whenever there is a need to protect systems and networks. AIs should have in place effective incident handling and reporting procedures.

A subsequent HKMA Circular, issued on 15 September 2015, dealt specifically with cyber risk management. It pinpointed areas of cyber risk management, including risk ownership and management accountability, periodic evaluations and monitoring of cybersecurity controls, increased industry collaboration and contingency planning and regular independent assessment and tests. It stated that senior management should evaluate periodically the adequacy of the AI's cybersecurity controls, having regard to emerging cyber threats and a credible benchmark of cybersecurity controls endorsed by the Board.

> **We're seeing an increase in nation state-sponsored computer intrusions. And we're also seeing a "blended threat"—nation states using criminal hackers to carry out their dirty work. We're also concerned about a wide range gamut of methods, from botnets to ransomware.**
>
> Christopher Wray,
> Director of the FBI

In December 2016, the HKMA launched a Cyber Security Fortification Initiative consisting of three pillars, namely a Cyber Resilience Assessment Framework ("**C-RAF**"), a Professional Development Programme and a Cyber Intelligence Sharing Platform.

In addition, the HKMA's Supervisory Policy Manual on Business Continuity Planning requires AIs to have a business contingency plan (**BCP**) in place, which may be triggered in the event of a cyber-attack. The Board of Directors and senior management of AIs have ultimate responsibility for the implementation and effectiveness of their BCP.

SECURITIES AND FUTURES COMMISSION

On 27 October 2017, the SFC published the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (the "**Guidelines**") following a consultation, requiring all licensed corporations engaged in internet trading to implement 20 baseline requirements as minimum standards. These covered,preventive controls (to protect internet brokers' internal networks and internet trading systems, as well as client accounts, from cyber-attacks), detective controls (to detect suspected hacking activities and alert internet brokers and clients on a timely basis to mitigate their impact and reduce financial losses) and internal governance-related controls (to strengthen overall cybersecurity governance and management of internet brokers and the cybersecurity awareness of both brokers and their clients). One key control, the implementation of two-factor authentication (**2FA**) for clients to log in to their internet trading accounts, took effect on 27 April 2018, while all other requirements took effect on 27 July 2018.

In September 2020, the SFC published a report after conducting a survey of 55 internet brokers and onsite inspections of 10 of them. The survey results and inspection findings revealed that most firms complied with the SFC's key regulatory requirements. Nevertheless, the SFC noted deficiencies and instances of non-compliance in the protection of clients' internet trading accounts (including the implementation of 2FA, data encryption, and monitoring and surveillance to identify suspicious unauthorised transactions), infrastructure security and user access management, as well as cybersecurity management and incident reporting. Firms are reminded to comply with the Guidelines and encouraged to implement a number of good practices.

Similar to the HKMA requirements, under the Management, Supervision and Internal Control Guidelines of the SFC, firms are required to implement an effective BCP appropriate to their size to ensure that they are protected from the risk of interruption to its business continuity, which may arise from a cyber-attack. Key processes include: a business impact study, identification of likely scenarios involving interruptions (e.g., breakdown of its data processing

> **It still never fails to [illegible] that some governmen[illegible] sa[illegible] we don't have cybercrime in our country, we don't see any threat here.**
>
> Neil Walsh, Chief of Cyber and Emerging Crime at UN Office on Drugs and Crime

systems), and documentation and regular testing of the firm's disaster recovery plan.

INSURANCE AUTHORITY

In June 2019, the IA published a guideline on cybersecurity which sets out the minimum standard for cybersecurity that authorized insurers are expected to have in place and the general guiding principles which the IA uses in assessing the effectiveness of an insurer's cybersecurity framework. The areas which an insurer should pay attention to include its cybersecurity strategy and framework; governance; risk identification, assessment and control; continuous monitoring; response and recovery; and information sharing and training. The guideline came into effect on 1 January 2020.

OFFICE OF THE GOVERNMENT CHIEF INFORMATION OFFICER

On 1 September 2020, a partnership programme for cyber security information sharing, also known as Cybersec Infohub, was formalised. This programme launched by the OGCIO in 2018. It was designed to encourage the cross-sector sharing of cyber security information with a view to further enhancing Hong Kong's overall defensive capabilities and resilience against cyber attacks. Under the formalised arrangement, the OGCIO will partner with Hong Kong Internet Registration Corporation Limited, a non-profit-distributing organisation, to administer the programme and to encourage more public and private organisations to take part. As of September 2020, the programme had 259 organisation members, covering a wide range of sectors including finance and insurance, innovation and technology and information security.

PERSONAL DATA (PRIVACY) ORDINANCE

The PDPO requires all practicable steps to be taken to ensure that personal data held by a data user is protected against unauthorised or accidental access, processing, erasure, loss or use, having particular regard to:

- the nature of data and the damage that could result from unauthorised or accidental access, processing, erasure, loss or use;
- the physical location where the data is stored;
- any security measures used for the equipment where the data is stored;
- any measures taken for ensuring the integrity, discretion and competence of persons having access to the data; and
- any measures taken for ensuring the secure transmission of the data (Data Protection Principle 4(1)).

The PDPO does not require that personal data security breaches be notified, either to data subjects or the Privacy Commissioner. However,while not a legal requirement, the Privacy Commissioner does encourage notification of breaches.

There are a range of criminal sanctions for breach of the PDPO. If a data user is found to have breached the Data Protection Principles of the PDPO, the Privacy Commissioner may issue an enforcement notice requiring the data user to take steps to rectify the breach. A breach of the enforcement notice constitutes a criminal offence, punishable by a fine of up to HK$50,000 (doubled for any subsequent convictions) and imprisonment for up to two years. Contravention of other requirements of the PDPO is also an offence.

In addition, it is an offence for a person to obtain personal data from a data subject without the data subject's consent, and to disclose that personal data with the intent to obtain a gain or cause loss to the data subject, or in circumstances where the disclosure causes psychological harm to the data subject. The offence is punishable by a fine of up to HK$1 million and up to five years' imprisonment. Lesser contraventions of the PDPO are punishable by fines of up to HK$10,000 and up to six months' imprisonment. In addition to criminal sanctions, a data subject who suffers a loss due to a breach of the PDPO is entitled to seek compensation from the data user through civil action, including for emotional distress.

JAPAN

JAPANESE CYBER SECURITY LAW

The existing cybersecurity-related laws in Japan include the Basic Act on Cyber Security, the Act on the Protection of Personal Information and the Act on the Prohibition of Unauthorised Computer Access. The regulator of financial institutions has also promulgated regulations to deal with cybersecurity issues in each of the financial sectors as part of its supervising activities. Certain cyber-attacks are criminalised in Japan.

In the wake of the coronavirus (**COVID-19**) pandemic, the principal agency of Japanese cybersecurity strategy, the National Center of Incident Readiness and Strategy for Cybersecurity (**NISC**), published a Q&A handbook about cybersecurity law in Japan on 2 March 2020. This Q&A covers cybersecurity measures that should be taken by corporates as well as legal matters that may arise due to accidents (available only in Japanese).

THE BASIC ACT ON CYBER SECURITY (ACT NO 104 OF 2014) (THE BAC)

The BAC was enacted in 2014 and came into force on 1 April 2016. The relevant regulator is the Ministry of Internal Affairs and Communications (the "**MIC**"). Mandatory obligations are imposed on different categories of entities: CII operators (operators of businesses that provide vital infrastructure), cyber space-related business entities and other business entities. The Cyber Security Council, involving governmental bodies, educational institutions and service providers to improve communication between these parties and to enhance cybersecurity, was established under the BAC.

The BAC stipulates the following responsibilities:

- CII operators are to make efforts to deepen their awareness and understanding of the critical value of cybersecurity, ensure cybersecurity voluntarily and proactively, and co-operate with the measures on cybersecurity taken by the national government or local governments.
- Cyberspace-related business entities and other business entities are to make efforts to ensure cybersecurity voluntarily and proactively in their businesses and to co-operate with the measures on cybersecurity taken by the national or local governments.

However, the BAC is enacted as a basic act indicating general government policy; it does not necessarily cover specific activities and incidents related to cybersecurity. For example, any sanction for breach of the above-mentioned obligations is not stipulated under the BAC.

THE ACT ON PROTECTION OF PERSONAL INFORMATION (ACT NO. 57 OF 2003) (THE APPI)

The APPI is the legislation in respect of protection of personal data in Japan and applies to all private sectors. Major amendments to the APPI came into force on 30 May 2017, in order to raise the level of protection of personal data to the same level as that in the EU. The relevant regulator is the Personal Information Protection Commission (**PIPC**), which was established on 1 January 2015 as the sole regulatory body under the APPI and now regulates and supervises all private industries, in co-operation with other regulators, such as the Financial Services Agency (**FSA**).

All businesses that handle, collect or process personal information (such as information that can identify the specific individual by name, date of birth, certain kinds of biological information and ID numbers) would be subject to the regulations and the APPI.

Various obligations will apply under the APPI to secure the protection of personal information, and some regulations and/or obligations would be relevant to cybersecurity, for example:

- Information handlers shall specify the purpose of use of personal information as much as possible and shall not handle personal information of an individual, without obtaining the prior consent of such individual, beyond the scope necessary to achieve the purpose of use
- The handlers principally shall not provide personal information to a third party without obtaining the prior consent of the individual
- The handlers shall promptly notify the PIPC and other relevant supervising authorities if the personal information has been disclosed or leaked (including in case of cyber-attack by other parties and breach of cyber regulations by itself or relevant parties) to others in an unauthorised way
- The handlers shall take necessary and proper measures for the security control of personal information, and shall exercise necessary and appropriate supervision over both their own employees and those outsourced entities to ensure the security control of personal data
- The handlers shall endeavour to process complaints appropriately and promptly about the handling of personal information.

Under the APPI, if the handler breaches the requirements under the APPI and breaches the improvement order, criminal sanctions of up to six months' imprisonment or a fine of JPY 300,000 could be imposed on the handler. If the handler is a representative, an agent or an employee of a legal entity, such legal entity could also be imposed with the fine. In addition, if the handler files a false report, a criminal sanction up to JPY 300,000 could be imposed.

Cybercrime is ultimately preventable. If you know what the risk is, you're less likely to become a victim.

Neil Walsh, Chief of Cyber and Emerging Crime at UN Office on Drugs and Crime

Please note that an amendment to the APPI was promulgated on 12 June 2020 and is to be enacted within 2 years of promulgation. The amended APPI will introduce more severe penalties for legal entities compared with those for natural persons.

SECTOR-SPECIFIC FINANCIAL REGULATORY LEGISLATION RELATING TO CYBER SECURITY

Since 2015, in accordance with the implementation of the BAC, the FSA has adopted rigorous policies and measures to strengthen cybersecurity in the financial sector (updated in 2018), and in June 2020, further published a "Report on Cybersecurity across the Financial Sector", which reflects the current state and common issues of cybersecurity in the financial sector. The supervisory guidelines for commercial banks, securities firms, insurance companies and licensed moneylenders, published by the JFSA, were updated in February 2015, in order to include check-points on cybersecurity. These require regulated financial institutions to take appropriate measures to protect customer data and to ensure cybersecurity.

In addition, since 2016, the FSA has been organising financial industry-wide cybersecurity drills (so-called "Delta Wall"). The number of participants in these drills has increased year-by-year, with around 120 financial institutions participating in drills in 2019.

WORK FROM HOME AND CYBER SECURITY

On 13 April 2018, as part of its business contingency plan and to encourage various working styles, the MIC published "Telework Security Guidelines". These MIC Guidelines aim to set a standard for cybersecurity when corporates arrange for their employees to work from home or to access their work PCs remotely.

CRIMINALISATION OF CYBER ATTACKS

Under the Act on the Prohibition of Unauthorised Computer Access and the Penal Code, certain cyber-attacks may be subject to criminal sanctions.

SINGAPORE

THE CYBER SECURITY ACT, THE PERSONAL DATA PROTECTION ACT AND THE COMPUTER MISUSE ACT

Cybersecurity ranks high on the Singapore Government's agenda, and the seriousness with which it views cybersecurity threats can be seen in, amongst others, the establishment of the Cyber Security Agency (**CSA**) of Singapore as the central agency to oversee and co-ordinate all aspects of cybersecurity for the nation.

In February 2018, the Singapore Parliament passed a Cyber Security Act which purports to be a broad, omnibus cybersecurity law. The Cybersecurity Act came into operation on 31 August 2018, and applies to organisations that are designated as operating "critical information infrastructure" in Singapore, which includes organisations in the energy, telecoms, water, health, banking, transport and media sectors.

The Cyber Security Act exists alongside other Singapore legislation that deal with information security, such as the Personal Data Protection Act. Aside from that, the regulators of some sectors which are deemed to be critical information infrastructure (**CII**) sectors (e.g., financial services providers) have also promulgated regulations dealing with cybersecurity incidents.

THE CYBER SECURITY ACT

The Cyber Security Act takes a holistic approach towards Singapore's resilience against cyber-attacks.It focuses on ensuring that the country is prepared and can respond effectively and promptly when an attack occurs. It seeks to establish a framework for the oversight and maintenance of national cybersecurity in Singapore, and empower the CSA to carry out its functions.

The Act has four objectives:

- To provide a framework for the regulation of sectors considered CII sectors. This is with the intention of formalising the duties of owners of CII in ensuring the cybersecurity of their respective CIIs.
- To provide the CSA with powers to manage and respond to cybersecurity threats and incidents. The intention is to enhance the existing powers related to cybersecurity which are provided for in the Computer Misuse Act, and to specifically vest the officers of the CSA with sitting powers.
- To establish a framework for the sharing of cybersecurity information with and by CSA, and the protection of such information.
- To establish a light-touch licensing framework for cybersecurity service providers.

Under the Cyber Security Act, organisations which have been designated as CII owners will be subject to various duties, including:

- to report certain cybersecurity incidents;
- to disclose certain information;
- to undertake periodic cybersecurity audits and risks assessments, and could be further required to adhere to codes of practice or standards; and
- to notify changes in the legal or beneficial ownership of the CII.

THE PERSONAL DATA PROTECTION ACT (PDPA)

It is acknowledged that cybersecurity is related to personal data protection, and in connection with that, the PDPA requires organisations, in relation to personal data in its possession or under its control, to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Further, legislative amendments to the PDPA will soon make compulsory the notification of a personal data breach that "results in, or is likely to result in, significant harm to an affected individual" or "is, or is likely to be, of a significant scale". The notification should be made to the affected individuals as soon as practicable, and to the Personal Data Protection Commission as soon as practicable, and no later than 3 calendar days of its occurrence

THE COMPUTER MISUSE ACT (CMA)

The CMA was enacted in 1993 to secure computer material against unauthorised access or modification. It was amended in April 2017 to address the changing nature of computer offences and the growing threat of cybercrime.

Under the CMA, it is an offence to:

- Use a computer to secure unauthorised access to any program or data held in any computer.
- Cause an unauthorised modification of the contents of any computer.
- To knowingly secure unauthorised access to any computer to obtain any computer service.
- To obstruct the use of or prevent access to a computer without authority.
- To knowingly and without authority, disclose any password, access code or any other means of gaining access to any program or data held in any computer for wrongful gain, any unlawful purpose or with the knowledge that it is likely to cause wrongful loss to any person.

In 2017, the CMA was amended to criminalise the use of personal data obtained via an act in breach of the CMA, where the person knows or has reason to

There's no silver bullet solution with cybersecurity, a layered defence is the only viable defence.

James Scott, Senior Fellow at the Institute for Critical Infrastructure Technology

believe that the personal information was so obtained. It is not an offence if the personal information was obtained or retained for a purpose other than for use in committing, or in facilitating the commission of any offence. It was clarified that this exception was created to allow journalists or researchers who use information derived from hacks for their news reports or research, so long as they do not circulate the personal details that were disclosed through the hack.

The CMA was also amended to:

- Criminalise the act of obtaining and the act of dealing in tools which may be used to commit an offence under the CMA.
- Extend the territorial scope of offences under the CMA to cover any offence committed by any person who was in Singapore at the material time, any offence where the computer, program or data was in Singapore at the material time, and any offence which causes or creates a significant risk of serious harm in Singapore.
- Allow prosecutors to amalgamate cybercrime charges against a perpetrator instead of having to bring separate charges for each instance of a distinct act.

CONTACTS

Australia

Tim Grave
Partner

T +61 2 8922 8028
E tim.grave
@cliffordchance.com

Sharfah Mohamed
Associate

T +61 2 8922 8516
E sharfah.mohamed
@cliffordchance.com

China

Kimi Liu
Counsel

T +86 10 6535 2263
E kimi.liu
@cliffordchance.com

Hong Kong

Ling Ho
Partner

T +852 2826 3479
E ling.ho
@cliffordchance.com

Donna Wacker
Partner

T +852 2826 3478
E donna.wacker
@cliffordchance.com

William Wong
Consultant

T +852 2826 3588
E william.wong
@cliffordchance.com

Anita Lam
Consultant, HK Head of Employment

T +852 2825 8952
E anita.lam
@cliffordchance.com

Japan

Satoshi Nomura
Counsel

T +81 3 6632 6312
E satoshi.nomura
@cliffordchance.com

Hitomi Kurokawa
Senior Associate

T +81 3 6632 6632
E hitomi.kurokawa
@cliffordchance.com

Singapore

Luke Grubb
Partner

T +6 56 506 2780
E luke.grubb
@cliffordchance.com

Lena Ng
Partner

T +65 6410 2215
E lena.ng
@cliffordchance.com


UNITED
STATES

UNITED STATES

CYBERSECURITY REGULATION

In the US, cybersecurity enforcement is split between a number of federal agencies and state governments. While there is no single cybersecurity regulatory regime, several regulatory agencies have been active in this area in recent years in response to the steady stream of high-profile data breaches and cybersecurity incidents that have arisen in the past few years. Thus, most companies operating in the US will be subject to cybersecurity oversight by some combination of state attorneys general, the Federal Trade Commission, and one or more sector-specific agencies, such as the Securities and Exchange Commission and the New York Department of Financial Services.

FEDERAL CYBERSECURITY ENFORCEMENT

Two federal regulators – the Federal Trade Commission (**FTC**) and the Securities and Exchange Commission (**SEC**) – have asserted primary roles in enforcing federal cybersecurity standards.

STATE CYBERSECURITY ENFORCEMENT

State governments are also key players in the US cybersecurity regulatory arena, through their attorneys general offices and through sector-specific state regulators, such as the New York Department of Financial Services (**NYDFS**). In addition, several US states have recently passed new comprehensive data privacy statutes.

FTC

The FTC is the self-described "nation's leading privacy enforcement agency" and has sought to hold companies accountable for breached cyber defences and other violations based on its general authority to regulate "unfair or deceptive acts or practices in or affecting commerce" under Section 5 of the FTC Act. The FTC has interpreted Section 5 to prohibit both failing to abide by public representations (e.g. a privacy policy promising adequate cybersecurity protections for data) as well as failure to provide basic protections for data that consumers would expect (e.g. storing sensitive medical data without cybersecurity protections).

FTC settlements and enforcement actions against first-time offenders typically do not include financial penalties because the FTC can only collect monetary penalties for knowing violations of its rules, consent orders or cease and desist orders. However, repeated or subsequent violations can lead to significant financial penalties.

SEC

Separately, the SEC has authority to bring enforcement actions against registered entities (e.g., investment advisers and broker-dealers) and public companies. Registered entities are obliged to protect their customers from cyber-threats by Regulation S-P, which requires that they adopt policies that are reasonably designed to safeguard customers' non-public personal information, protect that information against anticipated threats, and prevent unauthorised access and use of non-public material information that could result in significant harm to the customer.

The SEC has also recently focused on cybersecurity disclosures by public companies, stating that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.

UPDATED SEC GUIDANCE ON CYBERSECURITY MARKET DISCLOSURE

In February 2018, the SEC released updated guidance on cybersecurity market disclosure. The Guidance specifically references the requirements of Regulation S-K and Regulation S-X, which impose obligations on issuers to disclose cybersecurity risks and incidents in the following manner:

- **Periodic Reports**: Issuers are expected to provide timely and ongoing information in their reports regarding material cybersecurity risks and incidents that trigger disclosure obligations;
- **Securities Act and Exchange Act Obligations**: Issuers should ensure they are providing adequate cybersecurity-related disclosure in connection with Sections 11, 12, and 17 of the Securities Act and Section 10(b), as well as Rule 10b-5 of the Exchange Act; and
- **Current Reports**: Issuers are encouraged to utilise current reports in Form 8-K or Form 6-K to ensure their shelf registration statements remain current with regard to the costs and other consequences of material cybersecurity incidents.

Issuers are also expected to disclose "such further material information, if any, as may be necessary to make the required statements, in the light of the circumstances under which they are made, not misleading". Omitted information about cybersecurity risks or incidents may be material, depending on the nature, extent, and potential impact of the event. Finally, the guidance also "encourage[s] companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly".

SEC CYBER ENFORCEMENT UNIT

Following the announcement of its own data breach, on 25 September 2017, the SEC announced the creation of a new enforcement initiative – the Cyber Unit – to target cyber-related threats.

The Cyber Unit is part of the SEC's Enforcement Division and focuses on conduct, including:

- Spreading false information through electronic and social media to manipulate the market;
- Hacking to obtain material non-public information;
- Violations involving distributed ledger technology and initial coin offerings;
- Misconduct perpetrated using the dark web;
- Intrusions into retail brokerage accounts;
- Cyber-related threats to trading platforms and other critical market infrastructure.

OCIE SWEEPS

In addition to enforcement actions, the SEC's Office of Compliance Inspections and Examinations (**OCIE**) has made cybersecurity a specific area of focus in its Annual Examination Priorities in recent years.

One of the key issues that OCIE has focused on is deficiencies in policies and procedures related to Rule 30(a) of Regulation S-P, which requires firms to adopt written policies and procedures reasonably designed to safeguard client information (the **Safeguards Rule**), and failure to enforce those policies and procedures. Amongst the issues OCIE has identified are:

- **Inadequate policies and procedures**. Policies and procedures cannot merely restate the Safeguards Rule, but instead must discuss administrative, technical, and physical safeguards for client personally identifiable information (**PII**). According to OCIE, these policies should prohibit sending unencrypted client PII and ensure that employees protect client PII on personal laptops. The policies should also ensure that hard copy PII is protected in secure storage (e.g., locked cabinets).
- **Inadequate employee training and monitoring**. Employees should receive training on the firm's obligations to protect client PII and the firm must enforce its rules regarding client PII.
- **Failure to limit access**. Employees can only access PII when necessary and should only share customer log-in information as permitted by its policies. The firm should also take steps to ensure that departing employees cannot access and retain client PII when they leave.

- **Failure to inventory PII**. The firm should identify what client PII it holds and where it is kept.
- **Inadequate incident response plans**. The firm needs to ensure that it has an incident response plan that addressees: (i) who is responsible for the plan; (ii) how the firm will address a cybersecurity incident; and (iii) how the firm will identify potential system vulnerabilities.

In addition to concerns related to policies and procedures, OCIE has also identified concerns regarding the failure to provide accurate privacy notices to customers and failure to provide privacy notices that inform customers of their right to opt-out of sharing non-public client PII.

STATE ATTORNEYS GENERAL

State attorneys general offices are also key players in the US cybersecurity regulatory space. These state regulators have pursued data breach actions under state unfair and deceptive trade practice statutes (often deemed "little FTC Acts"), or dedicated privacy statutes and regulations. In addition, many state unfair and deceptive trade statutes permit a right of enforcement by private claimants, which is not available under Section 5 of the FTC Act, and provide for attorneys' fees for successful litigants.

All state statutes also include data breach notification requirements, requiring notification to affected individuals and/or state government agencies when a company suffers a data breach involving certain enumerated categories of personally identifying information (**PII**). Which state statutes apply to a breach depends on the state(s) in which the affected data subjects reside, meaning a company whose data has been breached will often have to comply with multiple state statutes, depending on the geographic distribution of the data subjects affected by the breach.

THE NEW YORK DEPARTMENT OF FINANCIAL SERVICES

The New York Department of Financial Services (**NYDFS**) has issued a particularly stringent cybersecurity regulation that requires insurance companies, banks and other covered entities who operate in New York State to maintain department-approved plans to deter cyber-attacks and report any significant attacks to the NYDFS within 72 hours of their occurrence. .

The regulation came into effect on 1 March 2017. Covered entities had 180 days in which to implement most requirements. The following are some of the key provisions of the rule:

- **Programme, policies and procedures**: Based on a risk assessment, entities are expected to establish written cybersecurity policies and procedures to protect their information systems (including in-house developed applications) and sensitive non-public data;

- **Periodic Risk Assessment**: Entities must conduct periodic risk assessments to address any changes in the entity's information systems, non-public information or business operations;
- **Chief Information Security Officer (CISO)**: Each entity must designate a qualified individual to serve as the CISO, who is responsible for implementing, overseeing and enforcing the cybersecurity programme and policy; and
- **Notification of cyber events to NYDFS**: Entities must notify NYDFS no later than 72 hours from a determination that a reportable cybersecurity event has occurred.

INSURANCE DATA SECURITY MODEL LAW

In October 2017, the National Association of Insurance Commissioners (**NAIC**) approved an Insurance Data Security Model Law. The NAIC's model law establishes a legal framework for requiring insurance organisations to operate complete cybersecurity programmes, including everything from planned cybersecurity testing and board-level involvement in the information security programme to incident response plans and specific breach notification procedures.

The model law substantially follows the earlier NYDFS cybersecurity regulation. Although it is currently only a model law and not enforceable until approved and adopted by individual states, the NAIC actively worked to encourage state legislatures to adopt the model law.

The first state, South Carolina, adopted the model law in May 2018 and as of October 2020, the law has been implemented in ten other states: Alabama, Connecticut, Delaware, Indiana, Louisiana, Michigan, Mississippi, New Hampshire, Ohio and Virginia.

CALIFORNIA CONSUMER PRIVACY ACT

The California Consumer Privacy Act of 2018 became effective on 1 January 2020, and offers California residents wide-ranging privacy rights that are similar to the GDPR, including a right to be informed about personal data collected by a business and rights to access and delete that information, as well as a right to prevent personal information from being sold to third parties.

The law applies to all businesses that carry out business in California, so long as they meet at least one of three thresholds: annual gross revenue of $25 million; processing of 50,000 or more consumers, households, or devices for commercial purposes; or derivation of at least half of annual revenue from selling consumers' personal information.

The California Attorney General may bring actions for civil penalties of up to US$7,500 per violation and there is a limited private right of action for individual

victims of data breaches allowing for statutory damages ranging between US$100-750 per violation (or actual damages).

Regulations providing guidance on compliance with the law became effective on 14 August 2020, and the California Attorney General has signalled that it plans to continue to update and supplement these regulations as compliance and enforcement efforts continue.

NEW YORK SHIELD ACT

Effective on 21 March 2020, the New York Stop Hacks and Improve Electronic Data Security (**SHIELD**) Act requires any person or business that owns or licenses data that includes private information of a resident of New York to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information.

The SHIELD Act specifies that reasonable safeguards includes:

Administrative safeguards, such as:

- designating one or more employees to co-ordinate the security programme;
- identifying reasonably foreseeable internal and external risks;
- assessing the sufficiency of safeguards in place to control the identified risks;
- training and managing employees in the security programme practices and procedures;
- selecting service providers capable of maintaining appropriate safeguards and requiring those safeguards by contract; and
- adjusting the security programme in light of business changes or new circumstances;

Technical safeguards, such as:

- assessing risks in network and software design;
- assessing risks in information processing, transmission and storage;
- detecting, preventing, and responding to attacks or system failures; and
- regularly testing and monitoring the effectiveness of key controls, systems and procedures; and

Physical safeguards, such as:

- assessing risks of information storage and disposal;
- detecting, preventing, and responding to intrusions;

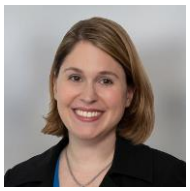
- protecting against unauthorised access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
- disposal of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

The law also states that any company in compliance with the data security rules and regulations of the federal or New York state government will also be deemed to be in compliance with the SHIELD Act.

A violation of the SHIELD Act is deemed to be a violation of the state's consumer protection act. The New York Attorney General may bring injunctions as well as an action for civil penalties of up to US$5,000 per violation. There is no private right of action.

CONTACTS

US



Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver@cliffordchance.com

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin@cliffordchance.com

Ben Berringer
Associate

T +1 212 878 3372
E benjamin.berringer@cliffordchance.com

CLIFFORD
CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ