Feb 2023

Malta: Cybersecurity

Quardia / Essentials collection / istockphoto.com

1. GOVERNING TEXTS

1.1. Legislation

Malta does not have a specific law which regulates cybersecurity. Accordingly, several laws govern different aspects of cybersecurity, and such laws include both primary and secondary legislation.

Being a Member State of the EU, Malta transposed Directive on Security network and Information Systems (Directive (EU) 2016/1148) ('the NIS Directive') by means of Measures for High Common Level of Security of Network and Information Systems Order of 6 July 2018 (as amended) (Subsidiary Legislation 460.35) ('the NIS Order'). Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code ('the Electronic Communications Code Directive') has also been transposed into Maltese law through the Communications Laws (Amendment No. 2) Act, 2021,

which amended various pieces of primary legislation, including the Electronic Communications (Regulation) Act of 31 December 1997 (as amended) (Chapter 399 of the laws of Malta) ('ECA') and the newly enacted Electronic Communications Networks and Services (General) Regulations of 1 October 2021 (Subsidiary Legislation 399.48) ('the ECNS Regulations') which replaced and amended the previous Electronic Communications Networks and Services (General) Regulations 2011 (as amended) of 12 July 2011 (Subsidiary Legislation 399.28).

Other pieces of legislation which also address the topic of cybersecurity in Malta include the Criminal Code (Chapter 9 of the Laws of Malta) ('the Criminal Code'), the Data Protection Act (Act XX 2018) ('the Act'), the Processing of Personal Data (Electronic Communications Sector) Regulations of 15 July 2003 (as amended) (Subsidiary Legislation 586.01) ('the Personal Data Regulations'), and the Critical Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order of 18 November 2011 (Subsidiary Legislation 460.24) ('the Critical Infrastructures Order').

The NIS Directive is one of the most important pieces of legislation pertaining to cybersecurity in Malta. The aim of the NIS Directive (and likewise of the NIS Order) is to lay down measures so as to achieve a harmonised high level of security of network and information systems within the EU, in order to improve the functioning of the internal market.

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 ('the NIS 2 Directive') was adopted by the European Parliament and the Council on 14 December 2022. The review of the NIS Directive was carried out in response to the increased cybersecurity threats resulting from the ever-accelerating digitalisation (especially in the context of the COVID-19 pandemic). The NIS 2 Directive is intended to address the limitations of the previous NIS Directive and to make it suitable for current and future needs. Among the changes introduced by means of the NIS 2 Directive is the expansion of the scope of application to include new sectors based on their importance in terms of societal and economic activities within the internal market. The added sectors include, but are not limited to, entities operating in the sectors of health, public administration, manufacturing, and social media platforms. The NIS 2 Directive eliminates the current distinction between operators of essential services or digital service providers, by exploring a new approach to classification whereby entities are subjected to different supervisory and enforcement regimes based on the significance of the sector or service, and are designated as 'essential' or 'important'. The NIS 2 Directive also includes provisions to ensure a higher level of risk management by requiring entities to take an all-hazards approach with a minimum list of measures to be applied. Furthermore, the NIS 2 Directive provides national authorities with a minimum list of powers when exercising their supervisory and enforcement functions in respect of essential and important entities. The NIS 2 Directive entered into force on 16 January 2023. As with other Member States, Malta has until 17 October 2024 to transpose the provisions of the NIS 2 Directive into Maltese law.

The NIS Order includes the adoption of a national strategy on the security of network and information systems, and establishes the Critical Information Infrastructure Protection Unit ('CIIP Unit'), whose functions have been incorporated in the Critical Infrastructure Protection Directorate ('CIPD'). The CIIP Unit is the national competent authority with respect to the sectors and essential services delineated in the schedules to the NIS Order. Accordingly, it is the CIIP Unit which is overall responsible for monitoring the application of, among other things, the NIS Order.

The purpose of the Electronic Communications Code Directive was to revise and consolidate the directives forming part of the EU telecommunications regulatory framework, on which the domestic legal system for telecommunications is based. Among the objectives of the Electronic Communications Code Directive is to promote the interests of EU citizens by maintaining the security of networks and services. As defined in the Electronic Communications Code Directive itself, 'security of networks and services' refers to the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity, or confidentiality of those networks and services themselves, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those networks or services. The ECNS Regulations deal with security under Part VII. In particular, the ECNS Regulations are concerned with security incidents and require undertakings providing public electronic communications networks or publicly available electronic communications services, or gateway operators, to take certain measures to appropriately manage the risk involved and to ensure a level of security appropriate to that risk, so that the incidence of security incidents is prevented or minimised. The ECNS Regulations also state that an undertaking providing publicly available electronic communications services over public electronic communications networks must undertake all necessary measures to ensure the maximum availability of such services in the event of a catastrophic network breakdown or circumstances of *force majeure*.

As regards the scope of the ECNS Regulations, the definitions of 'electronic communications service' and 'electronic communications network' mirror those provided in the Electronic Communications Code Directive. The term 'electronic communications service' is defined as a service normally provided against payment through electronic communications networks and includes interpersonal communication services (a term introduced by the Electronic Communications Code Directive), as well as services consisting in the provision of internet access or the conveyance of signals. The definition of 'electronic communications network' broadly includes transmission systems and switching or routing equipment and other resources, which permit the conveyance of signals by wire, radio, optical, or other electromagnetic means. The ECNS Regulations (as contemplated in the Electronic Communications Code Directive) apply to providers of electronic communications networks and/or services, which are available to the public. The ECNS Regulations also provide for security requirements for gateway operators, i.e. undertakings engaged in the provision of, or authorised to provide, such electronic communications networks and/or services which include a submarine connection between the Maltese islands and/or include an international connection between Malta and other countries.

Subtitle V of Title IX of Part II of the First Book of the Criminal Code, entitled 'Of Computer Misuse', was incorporated into the Criminal Code in 2001 and was subsequently amended in 2010 and 2015. Subtitle V incorporates various provisions of the Budapest Convention on Cybercrime 2001 ('Budapest Convention') which was fully ratified by Malta in April 2012. This section of the Criminal Code regulates, by virtue of Article 337C, the unlawful access to, or use of, information. Access to, or use of, information shall be considered unlawful when such access or use has been performed without authorisation by an entitled person. Unlawful access and use of information may result in an offence under Article 337F of the Criminal Code. The unlawful acts contemplated under Article 337C include, but are not limited to, the:

- use of a computer or any other device or equipment to access any data, software, or supporting documentation held in that computer or on any other computer, or the use, copying, or modification of any such data, software, or supporting documentation;
- copying of any data, software, or supporting documentation to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held; and
- disclosure of a password or any other means of access, access code, or other access information to any unauthorised person.

The misuse of hardware is regulated under Article 337D of Subtitle V of Title IX of Part II of the First Book of the Criminal Code which also lists a number of acts that should not be performed without obtaining the necessary authorisation. These acts include the modification of computer equipment or supplies that are used, or intended to be used, in a computer, computer system, or computer network. In addition, Article 337D criminalises the damaging, taking possession, and destroying of these same items.

The Data Protection Act, together with all of the subsidiary legislation issued thereunder, is another piece of legislation that plays a crucial role in the fight against cybercrime. The Data Protection Act implements the provisions and derogations in relation to the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). The GDPR and the Data Protection Act require data processing entities to implement appropriate technical and organisational measures with regard to the security of personal data to prevent such data from being accidentally or unlawfully processed.

The Personal Data Regulations implement the provisions and requirements of a number of EU directives and regulations, including, but not limited to, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector ('ePrivacy Directive') and Commission Regulation (EU) No 611/2013 of 24 June 2013 on the Measures Applicable to the Notification of Personal Data Breaches ('Notification of Breach Regulations'). The Personal Data Regulations are concerned with the secure processing of personal data in connection to the provision of publicly available electronic communications services in public communications networks. Furthermore, the Personal Data Regulations set out the rules pertaining to the processes to be observed in the case of a personal data breach, together with the relevant fines and sanctions.

Furthermore, the Critical Infrastructures Order defines critical infrastructure as 'an asset, system, or part thereof located in Malta which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'. The Critical Infrastructures Order caters for the establishment of the Malta CIP Unit, which falls under the responsibility of the Ministry for Home Affairs, Security, Reforms and Equality. The CIPU has a number of functions, including ensuring that a risk assessment is carried out by all owners or operators of critical infrastructures.

1.2. Regulatory authority

The CIIP Unit is tasked with the maintenance and monitoring of the application of the NIS Order. Such CIIP Unit functions include, but are not limited to, establishing the criteria for the identification and designation of operators of essential services and digital service providers, ensuring that a risk assessment is carried out by said operators, as well as monitoring security measures taken by such operators. The CIPD/CIIP Unit also have certain powers with respect to the requesting of information from operators of essential services.

As explained above, the CIPD has certain functions, including ensuring that a risk assessment is carried out by all owners or operators of critical infrastructures.

The Malta Communications Authority ('MCA') receives notifications by undertakings who intend to start or cease the provision of electronic communications networks and, or services, and has other powers associated with the grant of a general authorisation. The MCA also has specific powers in relation to compliance with the security requirements of Part VII of the ECNS Regulations, namely:

- to review security measures taken by providers of public electronic communications networks or of publicly available electronic communications services, or gateway operators, and issue recommendations on best practice concerning the level of security which such measures should achieve;
- to issue binding instructions as regards measures necessary to prevent or remedy a security incident where a significant threat has been identified and time-limits for implementation of such measures by providers of public electronic communications networks or of publicly available electronic communications services, or gateway operators; and
- to require a provider of public electronic communications networks or of publicly available electronic communications services, or gateway operators, to provide information or to submit to a security audit for the purposes of assessing matters, such as the security and integrity of its networks and/or services and compliance with any guidelines or binding instructions issued by the MCA.

The MCA is also empowered in terms of the ECNS Regulations to investigate cases of non-compliance and the effects thereof on the security of networks and services. The Malta Police Force set up a specialised Cyber Crime Unit in 2003 tasked with the provision of technical assistance for both the detection and investi-

gation of crimes where a computer is either the target or has been used to carry out a crime. The Cyber Crime Unit is also concerned with crime prevention and promoting awareness in relation to responsible computer use.

More generally, the Information and Data Protection Commissioner ('IDPC'), as established by the Data Protection Act, is responsible for monitoring and enforcing the application of the provisions of the GDPR, the Data Protection Act, and the Personal Data Regulations.

The MCA also has certain duties with respect to the protection of individuals' right to privacy, as well as the defence of national security, public safety, and the prevention of disorder or crime. The MCA is established by the Malta Communications Authority Act of 1 August 2000 (as amended) (Chapter 418 of the Laws of Malta) and has certain powers with respect to the issuance of administrative fines as part of the exercise of its regulatory functions in the field of communications.

There are a number of sector-specific authorities, such as in the gaming and financial services sectors, which have certain powers in relation to licensing and the issuance of fines in the context of cybersecurity. These include the Maltese Gaming Authority ('MGA') and the Malta Financial Services Authority ('MFSA'). Sectoral regulatory authorities such as these have been vested with certain powers with respect to requesting and collecting such information that would allow them to ensure that stakeholders have implemented the necessary and appropriate technical and organisational security measures.

1.3. Regulatory authority guidance

The Maltese Government ('the Government') launched its first National Cyber Security Strategy ('the Strategy') as part of Digital Malta in 2016. The Strategy originally set the goals for the period 2014 to 2020, which included the establishment of a governance framework, the combating of cybercrime, and cybersecurity awareness and education. The aim was to:

- defend and protect national information infrastructure from cyber threats; and
- ensure the security, safety, and protection of users of cyberspace.

The National Cyber Security Strategy 2023-2026 ('the 2022 Strategy') was launched in 2022, with the aim to deliver further progress in the field by:

- ensuring compliance with specific domestic, EU, and international regulatory requirements; and
- taking into account present realities, challenges, and evolvements in cybersecurity on a national and global scale through strategic, operational, and cultural measures, beyond regulatory measures.

The 2022 Strategy has several objectives under the following key domains:

- Cybersecurity Governance Capacity;
- Cyber Defence Capacity;
- Cyber Competence and Culture; and
- International Cooperation.

These objectives are aimed at:

- strengthening the protection of digital infrastructure and its dependencies on a national scale, from the strategic, operational, legal, and regulatory, as well as technical perspectives;
- ensuring cyber risk assessment approaches across the business and economic sector;
- ensuring national cybersecurity consciousness and increased capabilities in cybersecurity; and
- fostering cooperation in cybersecurity on a national, European, and international scale.

The 2022 Strategy outlines four guiding principles underpinning the vision to make Malta more secure and resilient to cyber threats, whose principles call for a balanced, multi-disciplinary, and multi-stakeholder approach.

The scope and application of the Strategy is not sector-specific, but covers the breadth of Malta's economy and society.

The body responsible for overseeing and coordinating the implementation of the Strategy is the National Cyber Security Strategy Steering Committee, which falls under the Ministry for the Economy, European Funds and Lands.

As regards security measures, guidance is provided by the document published by the European Union Agency for Cybersecurity ('ENISA') entitled 'Guideline on Security Measures under the EECC' in July 2021. This document lists specific, detailed technical and organisational measures which could be implemented by electronic communications providers to manage the risks posed to the security of networks and services. It also provides examples of evidence which could indicate that security measures are actually in place. The MFSA published, in June 2019, its Guidance Notes on Cybersecurity ('the Guidance Notes'), described as a minimum set of best practices and risk management procedures to be followed in order to effectively mitigate cyber risks. The scope and applicability of the Guidance Notes are limited to professional investor funds investing in virtual currencies, the board of administration of Virtual Financial Asset ('VFA') agents, the board of administration of issuers, and the board of administration of VFA service providers. The practices and procedures set out within the Guidance Notes are to be adopted by the decision-making bodies of such regulated persons in order to establish and maintain a prudent operational governance framework.

In view of the increasing reliance on technology arrangements and the need for any organisation to have an effective cybersecurity framework, the MFSA published its Consultation Document on the Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements in June 2020. Later, in December 2020, the MFSA issued its Guidance on Technology Arrangements, ICT and security risk management, and outsourcing arrangements ('the ICT Guidance'), considering this as an opportunity to harmonise the approach across all sectors authorised by the MFSA. The purpose of the ICT Guidance is to provide general guidance to authorised firms, including, but not limited to, credit and financial institutions, insurance undertakings, investment services, and companies services providers. It is intended to outline the supervisor's expectations for ongoing compliance and is primarily based on the approach of the European supervisory authorities. The ICT Guidance deals with internal governance arrangements on ICT and security risk management, including cybersecurity and outsourcing, which licensed entities or prospective applicants should implement for technology arrangements. On 24 January 2022, the MFSA issued a circular, reminding authorised firms of their obligation to comply with the ICT Guidance.

Having identified supervisory ICT risk and cybersecurity as a cross-sectoral priority for the year 2021, the MFSA published the third volume of 'The Nature and Art of Financial Supervision' series, focussing on ICT risk and cybersecurity supervision on 28 January 2021. This document provides information on the applicable legal and regulatory framework and details the work of the MFA's supervisory ICT risk and cybersecurity function. It is addressed to regulated entities which must take note of the recommendations made in this publication and after conducting a self-assessment exercise and take any necessary corrective action with respect to the weaknesses identified in order to meet the MFSA's expectations in this field.

In its Circular of 17 March 2022 'Exercising Caution in Times of Heightened Cyber Threat' ('the Cybersecurity Circular'), the MFSA referred to the expectation of authorised firms to conduct proper situational awareness, to regularly assess their exposure to developing ICT and cybersecurity threats, and to take timely measures to address them. The Cybersecurity Circular sets out a number of practices which authorised firms are expected to implement, including:

- holding discussions on ICT and cybersecurity risks and ensuring that roles and responsibilities within the organisation are clearly set in connection with the management of such risks;
- keeping abreast of any developments from reputable sources, as well as revisiting and re-assessing ICT and security risks in light of emerging threats and vulnerabilities;
- ensuring that business continuity and disaster recovery plans are in place that address severe, but plausible scenarios;
- training of staff and releasing timely information to consumers about occurrences of cyber squatting; and
- reporting major ICT-related incidents to MFSA in a timely manner.

Following the recent discovery of two malware families, the Advisory of 1 March 2022 'Best practices to be implemented' ('the Advisory') was issued by the national Computer Security and Incident Response Team ('CSIRT Malta') on 1 March 2022. In the Advisory, the CSIRT Malta (which forms part of the CIPD structure) shared a list of best practices which entities are encouraged to implement in order to strengthen the resilience of their network systems.

2. SCOPE OF APPLICATION

2.1. Network and Information Systems

Network and information systems are covered by the NIS Order. Article 2 of the NIS Order defines a 'network and information system' as:

- an 'electronic communications network' within the meaning of Article 2 of the ECA;
- any device or group of interconnected or related devices, one or more of which, pursuant to a programme, perform automatic processing of digital data; or
- digital data stored, processed, retrieved, or transmitted by elements covered under the above two points for the purposes of their operation, use, protection, and maintenance.

In terms of the ECA, an electronic communications network includes transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical, or by other electromagnetic means, including satellite networks, fixed (circuit-switched and packet-switched, including the internet), and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.

2.2. Critical Information Infrastructure Operators

The NIS Order does not expressly define the term 'critical information infrastructure operator'. That being said, Article 2 of the NIS Order defines 'critical information infrastructure' or 'CII' as an ICT asset, system, network, or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic, or social well-being of people, and the disruption or destruction of which would have a significant impact in Malta as a result of the failure to maintain those functions.

2.3. Operator of Essential Services

Article 2 of the NIS Order defines an 'operator of essential services' as a public or private entity of a type referred to in the Second Schedule to the NIS Order which meets the criteria laid down in Article 9(2) of the same.

The Second Schedule to the NIS Order lists various entities that operate in certain sectors (such as energy, transport, banking, and so on). These entities are all deemed to provide essential services, ranging from air carriers to healthcare providers, as well as credit institutions. Additionally, such operators must meet the criteria of Article 9(2) of the NIS Order which deals with the identification of operators of essential services by the CIPD/CIIP Unit. The criteria are as follows:

- the entity provides a service which is essential for the maintenance of critical, societal, economic activities, or both;
- the provision of that service depends on network and information systems; and
- an incident would have significant disruptive effects on the provision of that service.

2.4. Cloud Computing Services

Article 2 of the NIS Order defines 'cloud computing service' as a digital service that enables access to a scalable and elastic pool of shareable computing resources. Cloud computing services are one of the services (along with the online marketplace and online search engine) making up a digital service as provided for by the Third Schedule to the NIS Order. A cloud computing service provider must therefore comply with the requirements of a digital service provider as set out within the NIS Order.

2.5. Digital Service Providers

Article 2 of the NIS Order defines a 'digital service provider' as any legal person that provides a digital service. The NIS Order also defines 'digital service' as a 'service' within the meaning of Regulation 2 of the Notification Procedure Regulations of 21 November 2003 and 1 May 2004 (as amended) (Subsidiary Legislation 419.06) ('the Notification Regulations') which can be of three types: a cloud computing service, online marketplace, and/or online search engine.

The Notification Regulations define the term 'service' as any information society service normally provided for remuneration, at a distance, by electronic means, and at the individual request of a recipient of services. The Notification Regulations go on to define the elements of such definition as follows:

- 'at a distance' means that the service is provided without the parties being simultaneously present;
- 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and en-

tirely transmitted, conveyed, and received by wire, radio, optical, or other electromagnetic means; and
- 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual requests.

The Third Schedule of the Notification Regulations also provides a non-exhaustive list of services that are not covered by the above definition of 'service'.

Under the NIS Order, digital service providers are given certain responsibilities, including the identification and taking of appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems that they use in the context of offering services within Malta. Digital service providers are also obliged to prevent, as well as minimise the impact of any incidents affecting their network and information systems, with a view to ensuring the continuity of those services.

2.6. Other

Online marketplace

The NIS Order states that an 'online marketplace' refers to a digital service which allows consumers, traders, or both, as respectively defined in Paragraphs (a) and (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR), to conclude online sales or services 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.

Online search engine

The NIS Order states that an 'online search engine' is a digital service that allows users to perform searches of, in principle, all website 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.

3. REQUIREMENTS

3.1. Security measures

The term 'risk' is defined by the NIS Order as any reasonably identifiable circumstance or event having a potential effect on the security of network and information systems and leading to uncertainty on the objectives of an asset, system, network, or part thereof. The NIS Order goes on to state that risk is often charac-

terised by reference to potential events and consequences, or a combination of these. Moreover, risk is often expressed in terms of a combination of the consequences of an event, including changes in circumstances, and the associated likelihood of occurrence.

The CIIP Unit is tasked with ensuring that a risk assessment is carried out by operators of essential services and digital service providers. Accordingly, the CIIP Unit must ensure that operators of essential services take the appropriate measures to both prevent, as well as minimise the impact of any potentially disruptive incidents which threaten the security of network and information systems. This observatory function is facilitated through the appointment of a security liaison officer. Moreover, operators of essential services are subject to certain responsibilities with respect to the notification of any disruptive incidents.

Digital service providers are required to undertake certain measures so as to manage any risks which may potentially threaten the security of the network and information system in use. Article 13 of the NIS Order describes the elements which these respective measures are required to consider, including the security of systems and facilities, incident handling, and business continuity management. Digital service providers are also required to undertake certain measures, intended to minimise the impact of the incidents, as well as ensure the continuity of the services provided in Malta.

Like digital service providers, electronic communications providers have an obligation to take appropriate and proportionate technical and organisational measures to appropriately manage the risk posed to the security of networks and services. In terms of Regulation 28(1) of the ECNS Regulations, electronic communications providers are required to implement state of the art measures, and in particular measures, including encryption, where appropriate, in order to prevent and minimise the impact of security incidents on users and on other networks and services. Such security measures should ensure the protection of personal data against, for instance, unauthorised access, accidental or unlawful destruction, accidental loss, or alteration, and the implementation of a security policy with respect to the processing of personal data. Under the ECNS Regulations, gateway operators are similarly obliged to take certain measures so as to safeguard the integrity and resiliency of the network elements utilised to provide connectivity.

Furthermore, within the CIPD, there is also the CSIRT Malta which is responsible for risk and incident handling in accordance with a well-defined process. The CIIP Unit is also expected to adopt a national strategy plan which shall incorporate a risk assessment plan for the identification of risks.

Within the context of personal data protection, the GDPR requires the data controller and data processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to the potential risk of breach. Such measures include the pseudonymisation and encryption of personal data, and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, amongst others.

The Critical Infrastructures Order also requires operators of a critical infrastructures to draw up and maintain an operator security plan which involves, *inter alia*, carrying out a risk analysis based on major threat scenarios, the vulnerability of each asset, and potential impact.

3.2. Notification of cybersecurity incidents

The NIS Order requires operators of essential services to notify the CIIP Unit, without undue delay, of any incidents which may have a significant impact on the continuity of the essential services they provide. An equivalent obligation applies to digital service providers. The NIS Order lists the contents of the notification to be submitted to the CIIP Unit which shall include information enabling the CIIP Unit to determine the significance of the impact, in particular the number of users affected, the duration of the respective incident, the geographical spread with respect to the affected area, the sectors affected, and the dependency of the critical infrastructure or critical information infrastructure on the disruption of essential services. Once such information has been provided to the CIIP Unit, the latter shall inform any affected EU Member States if the respective incident has a significant impact on the continuity of essential services in that Member State. The NIS Order provides that where a designated operator of essential services provides a service to an undertaking providing electronic communications networks and/or services in terms of the ECA, the MCA shall also be notified by the relevant CSIRT. Lastly, following any consultation with the notifying operator of essential services, the CIPD/CIIP Unit may also inform the public about such incidents where this is deemed beneficial for the prevention or treatment of an ongoing incident.

In terms of the NIS Order, notification is not limited to operators of essential services and digital service providers as described therein. Other entities may also notify, on a voluntary basis, any incident having a significant impact on the continuity of the services which they provide. Whilst the same procedure is utilised for both mandatory and voluntary notifications, the CIIP Unit may prioritise the processing of mandatory notifications over voluntary ones.

The Personal Data Regulations also impose notification obligations on the provider of publicly available electronic communications services in the case of a personal data breach. In such instances, the data breach is to be notified to the IDPC without undue delay. Furthermore, where the breach may also negatively affect the personal data or privacy of a subscriber or individual, the provider shall also notify such individuals without any undue delay.

The GDPR is to be read in conjunction with the Notification of Breaches Regulation, specifically Article 2. Accordingly, providers of publicly available electronic communications services are obliged to notify any personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible.

Article 33 of the GDPR obliges the data controller to notify the IDPC of any personal data breach without undue delay and, in any event, no later than 72 hours after becoming aware of a data breach that is likely to result in a risk to the rights and freedoms of data subjects. The same legal provision continues by outlining the format of the notification, which is to include, *inter alia*, the nature of the breach, its likely consequences, as well as any measures taken or proposed to be taken by the controller to address it. Any of the information outlined and required by the GDPR when carrying out such notification obligations can be provided in phases where it is impossible to provide it all together at the same time.

In terms of Regulation 28(2) the ECNS Regulations, providers of electronic communications must notify the MCA without undue delay where there is:

- (i) any security incident that significantly impacts the operation of networks or services; or
- (ii) failure or serious degradation of connectivity provided by a gateway operator.

Further to (i), the significance of the impact of a security incident is to be determined by reference to the geographical spread and number of users affected by the security incident, and the duration of the security incident, among other things. Incidents should be reported to the MCA in accordance with the Technical Guidelines on Reporting Incidents (August 2013) as published by the MCA. In the case of a particular and significant threat of a security incident, providers of electronic communications must inform any users who may be potentially affected of possible protective measures or remedies which they can take.

The MCA is also required to inform the national regulatory authorities in other Member States and ENISA of any security incidents, where this is deemed appropriate. Moreover, the MCA may also notify the public of any security incident where such disclosure is considered to be in the public interest.

3.3. Registration with a regulatory authority

The CIIP Unit is tasked with the maintenance of a register of the CSIRTs, operators of essential services, and digital service providers that provide such services in Malta.

In accordance with the ECA and the ECNS Regulations, undertakings are required to obtain a commercial general authorisation to be entitled to provide electronic communications networks and/or services. Accordingly, undertakings must notify the MCA of their intention to start providing, or when they cease to provide such networks and/or services. This enables the MCA to keep a register of authorised electronic communications providers.

3.4. Appointment of a 'security' officer

In terms of the NIS Order, the CIIP Unit is bound to ensure that operators of essential services appoint a security liaison officer with the necessary expertise. The duties of the security liaison officer include:

- the facilitation of the development, maintenance, and review of the operator of essential services (with respect to its preparedness, processes, and solutions);
- ensuring that the operator of essential services carries out appropriate risk assessments, as well as maintains and exercises an operator security plan; and
- serving as a point of contact between the operator of essential services and the CIIP Unit to ensure the fulfilment of the obligations laid down in the NIS Order.

The NIS Order also requires CSIRTs to be adequately staffed with computer security incident response officers ('CSIROs'), which are to be available at all times.

Additionally, the Critical Infrastructures Order provides that the CIPU shall assess and ensure that every designated European Critical Infrastructure ('ECI') located in Malta possesses a security liaison officer or equivalent. This security officer is to act as the point of contact for security-related issues between the owner or operator of the ECI and the CIPU.

3.5. Other requirements

Not applicable.

4. SECTOR-SPECIFIC REQUIREMENTS

Cybersecurity in the health sector

Healthcare settings (including hospitals and private clinics) and healthcare providers as defined in Article 3(g) of Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare fall within the Second Schedule to the NIS Order and therefore, if they meet the criteria of Article 9(2) of the NIS Order, they are considered to be operators of essential services under Article 2 of the same order. In this way, such operators must abide by the provisions applicable to such operators of essential services under the NIS Order (as detailed above), in addition to the general provision on cybersecurity set out within the Criminal Code and the GDPR.

Cybersecurity in the financial sector

Professional investor funds investing in virtual currencies, the board of administration of VFA agents, the board of administration of issuers, and the board of administration of VFA service providers are advised to follow the Guidance Notes issued by the MFSA. These Guidance Notes stipulate how such persons should go

about effectively mitigating cyber risks.

The Innovative Technology Arrangements and Services Act of 1 November 2018 (as amended) (Chapter 592 of the Laws of Malta) ('the Innovation Act') provides a framework for the certification of several innovative technology arrangements and innovative technology services. The Innovation Act defines an 'innovative technology arrangement' as being an arrangement listed in the First Schedule to the Innovation Act, meaning the software and architectures which are used in designing and delivering Distributed Ledger Technology ('DLT') which ordinarily, but not necessarily:

- uses a distributed, decentralised, shared, and/or replicated ledger;
- may be public or private or hybrids thereof;
- is permissioned or permissionless, or hybrids thereof;
- is secure to a high level against retrospective tampering, such that the history of transactions cannot be replaced;
- is protected with cryptography; and
- is auditable for such arrangements.

The First Schedule to the Innovation Act was amended by virtue of Legal Notice 389 of 2020, Innovative Technology Arrangements and Services Act (Amendment) Regulations to include software and other architectures, not necessarily used in the context of DLT, smart contracts, and related applications which are used, or are meant to be used, as a stand-alone, or part of a solution in risky or critical sectors, where their failure of misuse could for example result in loss of life, grave prejudice to the well-being and rights of individuals, significant loss or damage to assets, and harm to the environment. Moreover, smart contracts and related applications, including decentralised autonomous organisations, as well as other similar arrangements and any other innovative technology arrangement which may be designated by the minister responsible for the digital economy, on the recommendation of the Malta Digital Innovation Authority, by notice from time to time are considered innovative technology arrangements under the First Schedule.

The term 'DLT' is defined under Article 2(1) of the Malta Digital Innovation Authority Act of 15 July 2018 (Chapter 591 of the Laws of Malta) as a database system, in which information is recorded, consensually shared, and synchronised across a network of multiple nodes as further described in the First Schedule to the Innovation Act , whereby the term 'node' means a device and data point on a computer network. 'Innovative technology service' is defined by Article 2(2) of the Innovation Act as a service relating to an innovative technology arrangement listed in the Second Schedule, namely:

- the review or audit services referred to in the Innovation Act with reference to innovative technology arrangements provided by the system auditors; and
- the technical administration services referred to in the Innovation Act with reference to innovative technology arrangements provided by technical administrators.

In the context of an Initial Virtual Financial Asset Offering ('IVFAO') under the Virtual Financial Assets Act of 1 November 2018 (as amended) (Chapter 590 of the Laws of Malta), the whitepaper of an issuer must contain at least, amongst other things, a description of the security safeguards against cyber threats to the underlying protocol, to any off-chain activities, and to any wallets used by the issuer together with other information. Section 10 of the VFA Rulebook Frequently Asked Questions, published by the MFSA on 10 October 2018 (as amended), sets out further information on the systems audit and IT audit requirements. An IVFAO is defined as a method of raising funds whereby an issuer is issuing virtual financial assets and is offering them in exchange for funds.

Any stakeholder forming part of the financial sector would also need to comply with the provisions of the GDPR on the protection of personal data against a personal data breach, as well as the more general terms of the NIS Order and the Criminal Code.

Financial entities are subject to a higher level of harmonisation within the EU, in comparison with the requirements laid down in the NIS 2 Directive, by virtue of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 ('DORA'). DORA consolidates and upgrades the regulatory framework on digital operational resilience for financial entities with a view to ensure that financial entities have the capability to withstand, respond to, and recover from cyber and other ICT risks and disruptions, which would help preserve the stability and integrity of the EU financial market. DORA lays down requirements concerning the security of network and information systems supporting the business processes of financial entities, including requirements on:

- ICT risk management;
- reporting of major ICT-related incidents;
- testing of ICT systems, controls, and processes;
- information and intelligence sharing between financial entities; and
- contracts concluded with ICT third-party service providers.

DORA has a broad coverage to include nearly all financial entities (with the exception of those listed in Article 2(2) thereof), but the application of certain rules depends on the size and overall risk profile of the financial entity, and the nature, scale, and complexity of its services, activities, and operations. DORA shall become applicable on 17 January 2025.

Cybersecurity practices for employees

Employees would be required to adhere to any policies which their employer issues in relation to the mitigation of any cybersecurity breaches. One such policy is issued by the employer in accordance with Article 5(2) of the GDPR. However, other than the general obligations in ensuring that confidential information and trade secrets are kept confidential, Maltese law does not provide for specific regulations or practices in this regard.

Employees would also need to comply with the more general terms of the NIS Order and the Criminal Code.

Cybersecurity in the educational sector

Schools and other educational institutions are required to adhere to the provisions of the GDPR on the prevention of personal data breaches. There also exists the Processing of Personal Data (Education Sector) Regulations of 9 January 2015 (as amended) (Subsidiary Legislation 586.07) which set out the manner in which educational institutions may process personal data.

Persons within the educational sector would also need to comply with the more general terms of the NIS Order and the Criminal Code.

5. PENALTIES

Various pieces of legislation provide for different penalties which depend on the unlawful act carried out. The NIS Order imposes an administrative fine where an operator of essential services fails to comply with certain security and notification obligations as delineated therein. The CIIP Unit is tasked with the enforcement and imposition of the administrative fine in accordance with a pre-determined procedure as described in the NIS Order. The respective amounts of such fines are dependent on the nature of the failure. For example, any undertaking that fails to implement appropriate and proportionate security measures and/or fails to cooperate with the CIIP Unit when exercising its monitoring obligations shall be liable to an administrative fine of not less than €1,000 and not more than €100,000 for individual violations. Moreover, an additional fine of €100 shall be imposed on the undertaking for each day during which such violation persists.

A different administrative fine of not less than €500 and not more than €50,000 is imposed where an undertaking fails to:

- notify an incident where it ought to have notified the incident;
- comply with a lawful instruction from the CIIP Unit; or
- comply with the provisions of the NIS Order.

Likewise, an additional fine of €50 shall be imposed on the undertaking for each day during which such violation persists.

The Criminal Code also provides for a fine of not more than €23,293.73 and/or a term of imprisonment not exceeding four years where any person is found guilty of an offence listed in Subtitle V of Title IX of Part II of the First Book of the Criminal Code. The law also lists instances where both the fine and term of imprisonment may be increased.

The GDPR describes the manner and nature of administrative fines to be imposed by the supervisory authorities of EU Member States, as well as when such fines are to be imposed. An infringement of, *inter alia*, Article 32 of the GDPR, which sets out the requirement for data processing entities to implement technical and organisational security measures, could result in an administrative fine of up to €10 million, or in the case of an undertaking, up to 2% of the undertaking's total worldwide annual turnover of the preceding financial year, whichever is higher. On the other hand, a breach of, *inter alia*, Article 5 of the GDPR, which sets out the basic principles for processing of personal data, would be subject to administrative fines up to €20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Penalties may also be imposed by sector-specific regulatory authorities as is the case with the MFSA. These penalties range from an administrative fine to the revocation of a licence.

6. OTHER AREAS OF INTEREST

Open invitations for 5G networks

The MCA launched a discussion paper and survey entitled '5G Demand and Future Business Models: Towards a Feasible 5G Deployment', in May 2019. The MCA is currently inviting any entity interested in evaluating the potential impact of 5G to apply for the MCA's test and trial licensing scheme. Any entity, including, although not limited to, mobile network operators, academics, and non-governmental organisations, can apply for a test or trial licence. The test and trial licensing framework consists of a light-weight licensing framework, providing the licensee temporary frequency authorisation to a particular frequency band. Further information on the test and trial licensing framework can be found here.

BSecure Scheme

In June 2019, the Parliamentary Secretary for Financial Services, Digital Economy and Innovation announced that the Government was set to launch a scheme referred to as the BSecure Scheme, which is a government investment of €250,000 for businesses to educate their personnel, and evaluate, plan, and enhance their cybersecurity and is the first of its kind. This scheme was opened on 23 October 2019 during the first edition of the Cyber Security Summit and applications were accepted until 24 November 2019. The implementation

process is focussed on the delivery of services consisting in training and risk assessments, which started being offered as of January 2020. In particular, the scheme was designed to target 220 people by providing a total of 330 hours of training and 123 hours of risk assessments.

Malta National Cyber Security Challenge

The Malta National Cyber Security Challenge ('the National Challenge') which was first held between 31 July 2021 and 1 August 2021, took place again between 18 June and 9 July 2022. This time round, the National Challenge consisted in solving 12 jeopardy-style challenges, varying in nature and difficulty. It was hosted online through the Hacking-Lab platform. The event catered for all levels of participants between the ages of 16 and 25, including information security aspirants, as well as information security professionals. The aim of the National Challenge is principally to instil the culture of information security among youths. Although the purpose of the event was for participants to gain knowledge and experience, there was a cash prize for the first three runners-up. Once scores from the National Challenge are final, a group of shortlisted participants will be given the opportunity to attend online and on-site training by local and international cybersecurity professionals. Ten participants will be chosen by the MITA to represent Malta in the seventh edition of the European Cyber Security Challenge which was held in Vienna, Austria, between 13 and 16 September 2022.

The proposal for a global treaty to counter cybercrime

In December 2019, the UN General Assembly adopted Resolution 74/247 that initiated the process to elaborate a comprehensive international convention on countering the use of ICT for criminal purposes. An *ad hoc* committee was established to that end. While there exists a regional cybercrime treaty, this would be a global treaty dealing with cybercrime. Russia spearheaded the proposal, with 79 states voting in favour of the 2019 resolution while it was strongly opposed by the UN, US, EU, and many state parties to the Budapest Convention. This reflects the wide disagreements on what constitutes cybercrime and how it should be addressed. Russia's draft convention has been criticised as extremely vague and open to abuse. The *ad hoc* committee held a one-day meeting on organisational matters on 24 February 2022, and its first session from 28 February to 11 March 2022, where it approved the roadmap and mode of work. Since its first session, the *ad hoc* committee met twice again in 2022 and the three remaining negotiating sessions are scheduled to take place over the course of 2023.

National Coordination Centre for Malta and National Cybersecurity Community

On 20 May 2021, the European Commission ('the Commission') adopted Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres ('the Founding Regulation'). The mission of the European Cybersecurity Industrial, Technology and Research Competence Centre ('the Competence Centre') and the Network of National Coordination Centres ('the EU

Network') involves, amongst other things, supporting EU technological capabilities and knowledge in relation to the resilience and reliability of the infrastructure of network and information systems. In February 2022, the MITA officially joined the EU Network, as the national coordination centre ('NCC') for Malta. The tasks of an NCC under the Founding Regulation include:

- promoting, encouraging, and facilitating the participation of civil society, industry, in particular start-ups and small- and medium-sized enterprises ('SMEs'), the academic and research communities, and other stakeholders at national level in cross-border projects and in cybersecurity actions funded by relevant EU programmes;
- providing technical assistance to stakeholders by supporting them in the application phase for projects managed by the Competence Centre in relation to its objectives; and
- seeking to establish synergies with relevant activities at national, regional, and local level, such as national policies on research, development, and innovation in the area of cybersecurity.

The NCC for Malta was launched on 26 October 2022 at the fourth edition of the Cyber ROOT 2022 Conference organised by MITA. Its mission is to invest in securing the Maltese and EU cyber space by bringing together knowledge, competency, and experience within one community, while encouraging active participation and contribution in research and educational programmes to build next generation cybersecurity solutions.

One of the main responsibilities of the NCC is that of fostering a National Cybersecurity Community ('the Community'). The Community brings together professionals and entities involved in the field of cybersecurity. It is governed by a dedicated Consultation Council in terms of policies, initiatives, market actions, memberships, and acceptable behaviour. It operates through working groups focused on a specific area of interest or technology, where Community members can collaborate and share expertise and experiences to address common challenges.

It has been announced that the NCC will be organising a series of business breakfast events intended specifically for Community members, which will consist in information sharing and training sessions on emerging cybersecurity topics. These will take place bi-monthly throughout 2023 and quarterly for 2024, with the first 'CYBER Breakfast' event scheduled for 7 February 2023.

Cybersecurity campaigns

MITA recently organised two campaigns to raise awareness on cybersecurity when it comes to making purchases online, and more generally in our everyday digital life. The online shopping campaign was organised in December 2021 and it tackled various points, including fake websites, scams, passwords, and secure wi-fi. In January 2022, MITA joined forces with the organisers of Malta Song Contest, to create features, which appeared during the days preceding the final night of this year's Malta Song Contest, where participating

singers highlighted numerous elements of cybersecurity. Another campaign called '12 Days for Christmas' was organised by the newly launched NCC in December 2022. The campaign was targeted towards the general public and work professionals to create awareness on scams and fake news, as well as to provide password tips.

Commission proposal for Cyber Resilience Act

In her 2021 State of the Union Address, President von der Leyen referred to the EU's aim to not simply address cyber threat, but also strive to become a leader in cybersecurity, whereby the development of cyber defence tools occurs here in Europe. It is then that she announced a new initiative: a new Cyber Resilience Act, which will take the form of an EU regulation. Between March and May 2022, the Commission carried out a consultation exercise to gather views and experiences of all relevant parties that will shape the forthcoming Cyber Resilience Act. On 15 September 2022, the Commission adopted its Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. The new Cyber Resilience Act will complement the EU cybersecurity acquis, which includes the recent review of the NIS framework, by establishing common rules which will apply to all products with digital elements whose intended and reasonably foreseeable use includes a direct or logical or physical data connection to a device or network. Amongst the objectives of the new Cyber Resilience Act is to ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life. As at 9 February 2023, the procedure for adoption of the new Cyber Resilience Act is ongoing, with this proposal currently being considered by the Council of the European Union, in the first reading stage.

Steven Decesare Partner
steve.decesare@camilleripreziosi.com
Alexia Valenzia Associate
alexia.valenzia@camilleripreziosi.com
Kristina Abela Junior Associate
Kristina.abela@camilleripreziosi.com
Camilleri Preziosi Advocates, Valletta