Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

TMT

Malta
GTG Advocates

chambers.com

2019

Law and Practice

Contributed by GTG Advocates

Contents

GTG Advocates has a TMT team composed of two partners, three senior associates, three junior associates and two trainees. Its primary practice areas are blockchain and virtual currencies, gaming and betting, data protection and privacy, FinTech, IP, e-commerce and telecommunications. The firm advises the Government of Malta, the Malta Financial Services Authority and the Malta Digital Innovation Authority in relation to blockchain, DLTs and cryptocurrencies; other clients include the Malta Gaming Authority, GO plc (Malta's largest quad-play telecommunications operator), RS2 plc, ApcoPay, BitBay, Kyber Network, Iconomi, AG Tech, Golden Race, BtoBet, and BMTI. The founders of GTG Advocates also founded sister company Afilexion Alliance, which provides corporate and advisory services to the technology, FinTech, DLT and gaming sectors, and Caledo, a joint venture between Afilexion Alliance and Wyzer which acts as a one-stop shop for all services related to blockchain and virtual currencies, including legal, technical, corporate, economics and marketing services.

Authors

Dr Ian Gauci is a partner of the firm and Head of its TMT department. He was one of the founders of the Malta IT Law Association, and his clients include the Malta Financial Services Authority (MFSA), the Malta Digital Innovation Authority (MDIA) and the Malta Gaming Authority. Ian is the legal expert on the National Blockchain Taskforce, which was entrusted with reviewing proposals and making recommendations to the Government of Malta to implement its National Blockchain Strategy, resulting in the promulgation of the Virtual Financial Assets Act (Cap 590 of the Laws of Malta), the Malta Digital Innovation Act (Cap 591 of the Laws of Malta) and the Innovative Technology Arrangements and Services Act (Cap 592 of the Laws of Malta). He has also advised the Maltese Government on e-commerce and eTrust certification, and is a co-founder of Afilexion Alliance and Caledo Group. In addition to his work at GTG Advocates, Ian regularly lectures on Legal Futures & Technology Law and Communications Law at the University of Malta.

Dr Michele Tufigno is a senior associate within the TMT department, active in the areas of TMT, data protection and privacy, gaming and betting, blockchain and cryptocurrencies, consumer law and M&A. He lectures on data protection law, with a particular focus on its practical applications within the sphere of employment law, as well as delivering seminars on the subject. He is also regularly involved in matters of alternative dispute resolution, negotiation and mediation.

Dr Terence Cassar is a senior associate at the firm and is experienced in matters relating to TMT, IP, blockchain and cryptocurrencies, FinTech, data protection and privacy, gaming and betting, e-commerce, and cybercrime. He is a frequent headline speaker on technology laws in Malta, particularly on blockchain, IP and data protection, including at the Malta Stock Exchange, FinanceMalta and the Malta Institute of Management. He was a key expert on the Malta IP Hub, an initiative to amend local IP laws, and has represented various clients before the European Intellectual Property Office. He has also led the GDPR compliance of various organisations, including Malta's foremost utility provider, and was one of the first lawyers in Malta to advise on virtual currencies and blockchains. He is currently advising various major exchanges in relation to licensing under the Virtual Financial Assets Act.

Dr Bernice Saliba is a junior associate at the firm with particular expertise in blockchain and virtual currencies, and has delivered lectures on the subject at SkillsMalta and to a number of major local banks. She is currently involved in assisting with the licensing of major cryptocurrencies exchanges.

1. Cloud Computing

1.1 Laws and Regulations

Maltese laws apply in a technology-neutral manner, except for legislation in respect of distributed ledger technologies (DLTs). Accordingly, there is no legislation which specifically regulates the processing of data within a cloud computing environment, or the use of cloud computing technology generally. Naturally, general legislation applies to cloud computing and, in this context, it should be noted that as an EU Member State, Malta's Data Protection Act (Cap 586 of the Laws of Malta) is compliant with EU data protection laws including the General Data Protection Regulation (EU) 2016/679 (GDPR).

Typically, the primary relevant legislation with respect to cloud computing is the Electronic Commerce Act (Chapter 426 of the Laws of Malta) which regulates electronic commerce and matters ancillary thereto. Other laws that are generally relevant include the Commercial Code (Cap 13 of the Laws of Malta), the Electronic Communications (Regulation) Act (Cap 399 of the Laws of Malta) (ECRA), the Consumer Affairs Act (Cap 378 of the Laws of Malta) and the Copyright Act (Cap 415 of the Laws of Malta).

Industry-specific legislation may, however, give rise to industry-specific obligations in relation to the use of cloud technology. For example, the Technical Infrastructure and Hosting Gaming and Control Systems Guidelines ('Technical Infrastructure Guidelines') issued by the Malta Gaming Authority (MGA) impose information security standards regarding the use of cloud technologies by gaming licensees. Hosting critical components of a gaming licensee's architecture, such as the random number generator, the jackpot servers, the player database servers, the financial database servers and the gaming database servers, within a cloud environment is permitted subject to a risk assessment and MGA approval. The MGA would be satisfied that a proposed architecture meets the required regulatory principles set out under the Technical Infrastructure Guidelines when the critical components are hosted on a private cloud environment which is not shared with other tenants on the same cloud. Virtual private cloud environments are allowed if the MGA is satisfied that the integrity and security of critical components is not at risk. The architecture can be located in Malta, in any EEA member state and, or in any other third-country jurisdiction wherein the MGA is satisfied that the same principles required under Maltese law and the Technical Infrastructure Guidelines can be obtained. However, if the architecture is located abroad, live replication to a server located in Malta is required. Similarly, in terms of Chapter 2 of the Virtual Financial Assets Rulebook, issuers of virtual financial assets (VFAs) whose IT infrastructure is located in a cloud environment must ensure that the data is replicated in real time by virtue of a live replication server located in Malta.

Inherently, the features of cloud technology give rise to issues of a cross-border nature. On this front, it should be noted that as a jurisdiction where GDPR applies, the transfer of personal data (whether through the cloud, or any other technology) within the EU/EEA is permitted without any additional requirement. Transfers of personal data to third countries may, however, only lawfully take place on the basis of the same grounds provided by the GDPR; namely, if the third country is subject to an adequacy decision issued by the EU Commission; or the transfer is subject to appropriate safeguards; or the transfer is to an entity(s) which has adopted binding corporate rules; or a derogation for a specific situation applies.

1.2 Regulations in Specific Industries

See **1.1 Laws and Regulations**.

1.3 Processing of Personal Data

See **1.1 Laws and Regulations**.

2. Blockchain

2.1 Risk and Liability

Malta has promulgated a first-of-its-kind legal framework regulating DLTs, including blockchains, smart contracts, cryptocurrencies (defined as VFAs), and related service providers, leading the jurisdiction to become dubbed the 'Blockchain Island'. From a high-level perspective, this new legal framework consists in the following pieces of legislation (each substantiated by various rules, guidelines and subsidiary legislation):

- the Malta Digital Innovation Authority Act, Cap 591 of the Laws of Malta ('MDIA Act') which sets up the Malta Digital Innovation Authority (MDIA) – namely, the Maltese Authority primarily responsible for promoting digital innovation; and
- the Innovative Technology Arrangements and Services Act, Cap 592 of the Laws of Malta (ITASA) which provides for certification by the MDIA of innovative technology arrangements (ITAs) and authorisations for innovative technology service providers (ITSPs); and
- the Virtual Financial Assets Act, Cap 590 of the Laws of Malta (VFAA) which establishes regulations in relation to initial coin offerings, VFAs and related services providers.

MDIA Act and ITASA

It should be noted that ITAs which can be certified by the MDIA under the ITASA, as at today, consist in:

- software and architectures which are used in designing and delivering DLT which, ordinarily but not necessarily:
  - (a) uses a distributed, decentralised, shared and, or replicated ledger;
  - (b) may be public or private or hybrids thereof;

(c) is permissioned or permissionless or hybrids thereof;
(d) is secure to a high level against retrospective tampering, such that the history of transactions cannot be replaced;
(e) is protected with cryptography; and
(f) is auditable.

- smart contracts and related applications, including decentralised autonomous organisations, as well as other similar arrangements.;
- any other ITA which may be designated by the relevant minister, on the recommendation of the MDIA, by notice from time to time.

Certification of ITAs is a voluntary endeavour and which (among others) requires a positive assurance from a systems auditor. That said, where an ITA is used in the context of an initial offering of VFAs (IVFAO), as regulated by the VFAA the auditing by a systems auditor becomes mandatory.

The service of a systems auditor reviewing an ITA for the purposes of the ITASA as well as technical administration services are considered to constitute an ITSP and qua an ITSP require an authorisation from the MDIA to be able to render services in terms of the ITASA.

Locally, it is probable and expected that in the medium to short-term future, the ITASA is extended to also include within scope ITAs relating to artificial intelligence (AI) and Internet of things (IoT) technologies.

As opposed to the ITASA, the VFAA falls within the remit of the Malta Financial Services Authority (MFSA) and the new legal framework caters for instances wherein the two authorities, that is the MDIA and the MFSA, need to interface.

VFAA

In terms of the VFAA, no issuer may offer a VFA to the public in or from within Malta, nor apply for a VFAs' admission to trading on a DLT exchange, unless a white paper drawn up in accordance with the VFAA has been registered with the MFSA. Furthermore, VFA Services, meaning services in relation to VFAs, cannot be provided by a service provider in or from within Malta unless that service provider holds the appropriate license in terms of the VFAA.

The following four classes of VFA Licences are available:

- *Class 1* – licence holders authorised to receive and transmit orders and, or provide investment advice in relation to one or more VFAs and, or the placing of VFAs. Class 1 Licence Holders are not authorised to hold or control clients' money.
- *Class 2* – licence holders authorised to provide any VFA Service but not to operate a VFA exchange or deal for their own account. Class 2 Licence Holders may hold or control clients' money in conjunction with the provision of a VFA Service.
- *Class 3* – licence holders authorised to provide any VFA Service but not to operate a VFA exchange. Class 3 Licence Holders may hold or control clients' money in conjunction with the provision of a VFA Service.
- *Class 4* – licence holders authorised to provide any VFA Service. Class 4 Licence Holders may hold or control clients' money in conjunction with the provision of a VFA Service.

An application for a VFA Licence can only be made through what is known as a 'VFA Agent'; namely, an agent who is duly registered with the MFSA. Likewise, an issuer is required to appoint, and have at all times in place a VFA Agent. In simplistic terms, the VFA Agent's role and function is to generally advise and guide his client, perform a fitness and properness assessment prior to onboarding the client, act as a point of liaison between the MFSA and his or her client, and co-operate with the MFSA as may be required.

In the case of an IVFAO, 'key information' must be provided to investors with a view of enabling them to understand the nature and the risks of the proposed project, the issuer and the VFAs that are being offered. For a white paper to be compliant with the VFAA, it is mandatory to include a detailed description of the risks associated with the VFA and the investment therein as well as information on associated challenges, risks and mitigating measures thereof.

'Prudential requirements' imposed on VFA Licence Holders also include requirements on risk management. The Board of Administration of a VFA Services License Holder must approve and periodically review the strategies and policies for taking up, managing, monitoring and mitigating the risks that the VFA Licence Holder is or might be exposed to, including those posed by the macroeconomic environment in which it operates in relation to the status of the business cycle.

The following actions are expected to be taken by VFA Licence Holders, with a view of managing their risks:

- establishing, implementing and maintaining adequate risk management policies and procedures, which identify risks relating to the VFA Licence Holder's activities, processes and systems, and where appropriate, set the level of risk tolerated by the VFA Licence Holder;
- adopt effective arrangements, processes and mechanisms to manage the risks relating to the VFA Licence Holder's activities, processes and systems, in light of that level of risk tolerance;
- monitor the following:

(a) the adequacy and effectiveness of the VFA Services Holder's risk management policies and procedures;
(b) the level of compliance by the VFA Services Licence

Holder and its relevant persons with the arrangements, processes and mechanisms adopted; and

(c) the adequacy and effectiveness of measures taken to address any deficiencies in those arrangements and procedures, including failures by the relevant persons to comply with such arrangements or follow such procedures.

- take into consideration the internal capital adequacy assessment process (if applicable).

An independent risk management function must also be appointed by the VFA Licence Holder. However, the MFSA may allow the VFA Licence Holder to establish a risk management function that does not operate independently, if such does not give rise to conflicts of interest and the VFA Licence Holder demonstrates to the MFSA that the establishment of an independent risk management function is not appropriate and proportionate in view of the nature, scale and complexity of its business and the nature and range of the VFA services undertaken in the course of that business.

It should be noted that the above information on risk in the context of VFA services is based upon Chapter 3 of the VFA Rulebook, which as at the date of writing remains subject to change.

From a liability perspective, it should be noted that an issuer and a VFA Licence Holder would be deemed to be guilty of an offence if they breach the VFAA and, on conviction, they generally may be liable to a fine not exceed EUR10 million or up to three times the profits made or losses avoided by virtue of the offence (whichever is the greater), or to imprisonment for a term not exceeding six years or both such fine and imprisonment. On the other hand, a VFA Agent guilty of an offence under the VFAA is generally liable for a fine not exceeding EUR500,000 or to imprisonment for a term not exceeding six months, or both such fine and imprisonment.

Additionally, the MDIA also has the power to impose administrative fines of up to EUR350,000 for each infringement or failure to comply, or EUR12,000 for each day of infringement or non-compliance as the case may be (unless a specifically provided otherwise). If the MDIA considers that an unlawful act or omission has especially significant effects on the market to the detriment of competitors and, or consumers, the amount that may be imposed as an administrative fine may be increased to an amount that is not more than 5% of the turnover of the undertaking in the calendar year immediately preceding the year when the infringement was committed, provided further that any daily fine imposed by the MDIA may be back-dated to the date of commission or commencement of the infringement.

Legislation of a generic nature, such as the Criminal Code (Chapter 9 of the Laws of Malta) and the Civil Code (Chapter 16 of the Laws of Malta) are expected to be updated also in light of DLTs and digital innovation generally.

2.2 Intellectual Property

Intellectual property considerations are to date not addressed under Malta's novel DLT legal framework. However, the registration of intellectual property in Malta is one of the factors which are taken into consideration by the MDIA when determining whether an ITA is considered as operating in or from within Malta.

2.3 Data Privacy

To date there are no specific laws or precedents in Malta in relation to data privacy in the context of DLTs and blockchains. Nor have guidelines been issued as yet by the Information and Data Protection Commissioner (IDPC) in Malta.

However, it should be noted that for the purposes of a systems audit certifying an ITA under the IRASA, the systems audit control objectives of security, processing integrity, availability, confidentiality and protection of personal data need to be followed.

2.4 Service Levels

There are no specific service level requirements imposed to date by Maltese legislation in relation to blockchain and DLTs. However, it should be noted that the local legislation is still in an embryonic stage, having become effective in November 2018.

2.5 Jurisdictional Issues

Authorisations issued in terms of the VFAA are not pass-portable to other states in light of the fact that the VFAA is a local legislation and thus does not derive from an EU law on the basis of which pass-portability would be permitted across the EU.

Furthermore, it should be noted that if a VFA Licence Holder wishes to establish a branch or provide services in a Member State or in an EEA state, other than Malta ('European Right'), it must notify the MFSA of its intention to do so in writing prior to the provision of, or to holding itself out as providing, a VFA service in another Member State. In such case, an internal assessment must be carried out by the VFA Licence Holder so as to determine whether the laws of the target states allow for the provision of such services. Obtainment of a legal opinion from a lawyer in such state is required and must also be submitted to the MFSA as part of the submission of a statement of intent to exercise a European Right.

3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence

3.1 Big Data

Unless a fully anonymised data set is used, the use of big data in Malta faces the challenge of compliance with applicable data protection laws, including the GDPR, which among others require that an appropriate legal ground is in place

for any processing of personal data. For marketing analytics purposes, it should also be noted that if consent is relied upon as the ground for legitimately processing personal data, such must be of the quality required under GDPR including that it is granted via a specific opt-in approach.

Patenting of inventions related to big data can be very challenging in Malta, especially if the novelty or inventive step of the invention relies on the execution of computer code, as programs for computers are excluded from the scope of patentability of inventions under the Patents and Designs Act, Cap 417 of the Laws of Malta.

3.2 Machine Learning

In the absence of local precedents and guidance, it is currently unclear whether works produced by artificially intelligent machines can qualify for intellectual property protection, including for copyright, as Maltese intellectual property laws seem to confer protection exclusively to intellectual property created by a natural person.

Algorithmic decision-making methods which are taken on the basis of personal data need to be compliant with data protection laws, including the GDPR. Where the algorithmic decision may produce legal or similarly significant effects, the data subject has, among others, a right not to be subject to such processing, a right to obtain human intervention on the part of the controller, express his or her point of view and contest the decision. The existence of such algorithmic decisions, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing, must be disclosed to the data subject.

Malta is currently aiming to develop a National Strategy for the regulation of AI and a taskforce has been set up for this purpose. A pilot project to explore the citizenship rights for artificially intelligent robots was also announced in November 2018 and some form of regulatory intervention in the area is expected in the future. In fact, as noted above, the ITASA was purposefully drafted in a forward-looking manner, to enable it to eventually be extended to also cover AI and IoT.

However, to date there are no specific regulatory or insurance requirements imposed specifically as a result of the use of machine learning and AI (generic laws still apply).

3.3 Artificial Intelligence

See **3.2 Machine Learning**.

4. Legal Considerations for Internet of Things Projects

4.1 Restrictions Affecting a Projects' Scope

IoT technologies which rely on personal data inputs must process personal data in compliance with data protection laws, including the GDPR. In this respect, it is worth noting the obligation that appropriate security measures need to be in place to protect the security of personal data especially since IoT can be a pervasive technology and in practical terms might not always be as secure as other technologies.

Technical regulation and standards under the purview of the Malta Competition and Consumer Affairs Authority might apply in relation to IoT products.

Spectrum authorisations may also be required. In this respect, it should be noted that a spectrum-allocation exercise meant to support IoT technologies has been undertaken recently by the Malta Communications Authority (MCA).

As noted above, it is expected that regulation specific to IoT will be forthcoming in the future in Malta and most likely via the extension of coverage of the ITASA.

5. Challenges with IT Service Agreements

5.1 Specific Features

When entering into an IT service agreement with a Maltese organisation, entities need to give careful consideration to the transfer of copyright and undertakings in this respect. In Malta, copyright vests by default under the Copyright Act with the author of the creative work (except for computer programs and databases created in the course of employment with an employer). Case law precedents in fact confirm that unless specifically assigned in writing, the copyright vests with the author even in a service relationship. Furthermore, to date, the Maltese Industrial Property (intellectual property) register does not cater for the registration of security over IPRs.

From a contract negotiations perspective, it should also be noted that the Maltese courts have developed two opposing schools of thought in relation to the interpretation of penalty clauses in agreements and some uncertainty as to the precise interpretation expected from a court in respect of penalty clauses is in place.

Lastly, the provision of certain IT services in Malta might give rise to regulatory requirements, for example, provision of IT services in the gaming area need to be carefully reviewed as they may trigger the requirement of obtaining an authorisation from the MGA.

5.2 Rules and Restrictions
See **5.1 Specific Features**.

6. Key Data Protection Principles

6.1 Core Rules Regarding Data Protection
In Malta, the core rules regarding data protection are found within the Data Protection Act, Cap 586 of the Laws of Malta, along with its subsidiary legislation and guidance issued by the IDPC. As an EU jurisdiction, EU legislation such as the General Data Protection Regulation (2016/679) also applies and forms part of the core applicable data protection rules in Malta.

6.2 Distinction Between Companies/Individuals
Maltese data protection laws exclusively apply in respect of the processing of personal data; namely, data rendering a natural person identifiable.

Data relating to companies and other legal entities does not fall within the scope of Maltese data protection laws.

6.3 General Processing of Data
General processing of data which does not qualify as personal data is typically unregulated; that is, except for obligations arising from industry-specific legislation.

6.4 Processing of Personal Data
Given that the GDPR has direct effect in Malta, the processing of personal data must be undertaken in compliance with the GDPR, which (among others) provides that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. Monitoring & Limiting of Employee Use of Computer Resources

7.1 Employees' Restrictions on Computer Use
Monitoring and limiting the use by employees of company computer resources is permitted in Malta, insofar as it is undertaken in accordance with data protection laws which, among others, impose that such is carried out in an adequate, relevant and non-excessive manner and in the least intrusive way possible.

If employers wish to monitor employee's use of computer resources such as email or roll out web traffic monitoring technologies which can personally identify the employee's web use, as a minimum, employers need to ensure that employees have been notified in advance and made aware regarding such processing, including the purposes for which it is being carried out.

It is generally accepted that an employer can restrict employees from utilising company computer resources for private purposes although there are no known local precedents. In fact, in general terms and notwithstanding the proliferation of computer resources in the workplace, case law precedents in this area remain somewhat scarce. In practical terms, it would be expected that the principles established by the European Court of Human Rights in Barbalescu v Romania (61496/08) would be upheld by the courts.

8. Scope of Telecommunications Regime

8.1 Technologies within Local Telecommunications Rules
Malta's telecommunications laws are technology-neutral and thus apply irrespective of the type of technology utilised. The content of telecommunications does not, however, fall within the scope of Malta's telecommunications laws. Such would fall within the scope of other laws – principally, laws in confidentiality and data protection.

From a high-level perspective, Malta's current telecommunications authorisations regime is divided into three broad categories; namely:

- general authorisation (GA) for the provision of networks and, or, services;

- spectrum licensing; and
- radio communications equipment licensing.

In terms of ECRA, a GA is required for the provision of electronic communications networks and, or, services. The respective categories of GAs include the establishment and operation of:

- Public Communications Networks;
- Publicly Available Telephone Services;
- Television and Radio Distribution Services;
- Other Publicly Available Electronic Communications Services;
- Non-Public Electronic Communications Services;
- Publicly Available Telephone Directories and Directory Enquiry Services; and
- Private Electronic Communications Networks and, or, Private Electronic Communications Services.

In terms of requirements for the obtainment of a GA, the GA is a notification rather than a licensing process. Upon completion of all GA notification requirements, the notifying undertaking is deemed to be authorised to provide an electronic communications network or service, subject to the conditions of the GA, applicable laws, as well as MCA decisions. Subject to ongoing compliance, a GA is conferred for an unlimited duration.

Radio frequency spectrum management is carried out by the MCA and licences for a right to use radio frequencies are required. The spectrum licensing process to be undertaken with the MCA and licence duration and specificities depend on the spectrum licence sought.

ECRA also requires that the installation or use of radio communications equipment is authorised by the MCA on an individual licence basis. Light-licensing under a GA is also in place in relation to radio communications equipment covered by the General Authorisations (Radiocommunications Apparatus) Regulation, Subsidiary Legislation 399.40 of the Laws of Malta, whereas radio communications equipment falling within the scope of the Radiocommunications Apparatus Exemption Order, Subsidiary Legislation 399.42 of the Laws of Malta, is exempt from the requirement of an authorisation from the MCA.

Telephony services which are powered by the Internet such as voice-over-IP and instant messaging services are typically deemed to fall out of the scope of local telecommunications laws. For such services to fall within the scope of the Maltese telecommunications regime, they must (among other requirements) utilise a public switched telephone network (PTSN) and, in such case, a GA from the MCA would then be required as a minimum.

9. Audiovisual Services and Video channels

9.1 Main Requirements

The Broadcasting Authority (BA) is the Maltese authority entrusted with regulating the broadcasting of content which originates from Malta. Its remit covers radio and television and such services require a licence from the BA.

In terms of the Broadcasting Act, Cap 350 of the Laws of Malta, the BA may issue licences for nationwide radio and television broadcasting services, digital radio broadcasting services, community radio stations and for nationwide television teleshopping broadcasting services. Each different type of licence is subject to its own specificities in terms of procedures, payments and requirements; however, it should be noted that in terms of Article 10(5) of the BA, a broadcasting licence may only be issued to a company incorporated in Malta.

Online audiovisual content falls beyond the remit of the BA. Indeed, online video channels and services similar to YouTube are typically unregulated (unless they trigger sector-specific legislation, such as responsible gaming and advertising under the Gaming Act).

9.2 Online Video Channels

See **9.1 Main Requirements**.

10. Encryption Requirements

10.1 Legal Requirements Governing the Use of Encryption

Maltese law does not impose any general obligation to use encryption technology. However, using cryptographic or similar techniques for an illegal purpose is deemed to constitute an offence under the Electronic Commerce Act, Cap 426 of the Laws of Malta.

The use of encryption does not exempt an entity from any legal obligations in Malta. However, given that GDPR applies in Malta, encryption is specifically recognised as a technical measure for the purposes of securing personal data against breaches.

It should also be noted that protection with cryptography is one of the features considered under the VFAA for the purposes of determining whether a technology amounts to a DLT and likewise for the purposes of the determining an ITA's definition in terms of the ITASA. Cryptography is also taken into consideration in the System Control Objectives pursued by a systems auditor auditing an ITA for the purposes of certifying that ITA under the ITASA.

10.2 Exemptions

See **10.1 Legal Requirements Governing the Use of Encryption**.

GTG Advocates
66, Old Bakery Street
Valletta
VLT 1454
Malta

Tel: +356 2124 2713
Email: info@gtgadvocates.com
Web: www.gtgadvocates.com