

Anti-Money Laundering and Combatting the Financing of Terrorism, better known as AML/CFT, are covered by the Prevention of Money Laundering Act, Chapter 373 of the Laws of Malta and subsidiary legislation 373.01, Prevention of Money Laundering and Funding of Terrorism Regulations.

Currently, remote gaming operators are not subject persons or obliged entities under the Regulations. However, the remote gaming regulations do cover AML/CFT matters and quite seriously. The Malta Gaming Authority is also a supervisory authority.

Subject Persons / obliged entities are required to comply with the regulations and implementing procedures and directives issued by the Financial Intelligence Analysis Unit (FIAU). With the 4th AML Directive to be implemented by latest June 2017 all remote gaming operators shall become obliged entities and will have to follow the implementing procedures and regulations.

Verifying player identities can be achieved in a number of ways: a) namely documentation requests and control and, b) outsourcing to ID and Age verification entities. However, whilst this process satisfies an important aspect of the AML/CFT requirements, there are still quite a few other requirements that need to be satisfied, with some being more difficult than other to achieve without buying in the necessary tools or expertise. The main issue we see is the ongoing monitoring of the players' financial activity and identifying possible AML issues.

Remember, identifying and stopping criminal spend is also an AML requirement!

Kyte can assist you in complying with the regulations by providing training on-site or off-site with materials customised for your organisation. By carrying out risk assessments and auditing your AML/CFT procedures and by recommending tools and processes to enhance your compliance efforts.

AML & CFT



Data Protection Services

Maltese persons, legal or human, are required to comply with the Data Protection Act (DPA), Chapter 440 of the Laws of Malta whenever they collect, store or process personal data for commercial purposes.

The requirements of the current legislation are based on the 2nd EU Directive with the 3rd Directive just around the corner and should be implemented in 2017.

One of the requirements of the Data Protection Act is to notify the Commissioner for Data Protection about your data processing with information such as the purposes for processing, security in place, who has access to the data.

The core of the DPA are the following key principles:

- ▶ personal data is processed fairly and lawfully;

- ▶ personal data is always processed in accordance with good practice;

- ▶ personal data is only collected for specific, explicitly stated and legitimate purposes;

- ▶ personal data is not processed for any purpose that is incompatible with that for which the information is collected;

- ▶ personal data that is processed is adequate and relevant in relation to the purposes of the processing;

- ▶ no more personal data is processed than is necessary having regard to the purposes of the processing;

- ▶ personal data that is processed is correct and, if necessary, up to date;

- ▶ all reasonable measures are taken to complete, correct, block or erase data to the extent that such data is incomplete or incorrect, having regard to the purposes for which they are processed;

- ▶ personal data is not kept for a period longer than is necessary, having regard to the purposes for which they are processed.

If these principals are followed then a Data Controller will probably not have any issues with the DPA. The 3rd EU Directive will increase fines for non compliance and also imposes new requirements such as informing customers of breaches to their systems within 24 hours. The overall objective of these new regulations is "to give citizens back control over of their personal data, and to simplify the regulatory environment for business."

We can assist you to comply with the existing and future Data Protection requirements and can also act as your Personal Data Representative and ongoing compliance challenges.



Having worked with a large number of start-up's as well as established operators, we have extensive experience in assisting companies in starting their operation and obtaining remote gaming licenses. We can assist companies either throughout the entire process, or else through parts of the process itself.

Being a Maltese entity ourselves, this is the jurisdiction in which we specialise, but we have also assisted clients in obtaining licenses in other European jurisdictions. Our management and team are considered as experts in the Maltese Remote Gaming Regulations, as well as guidelines and directives published by the MGA.

One of our strong points is the drafting of documentation, such as business plans, policies, procedures, and technical documentation describing gaming systems. In such jobs, we either create documents from scratch, based on client feedback and requirements, or else review the client's documents and suggest changes to ensure they are in compliance with license requirements.

We have audited a large number of gaming companies, both directly as clients, or on behalf of regulators such as the **MGA** and the **UKGC**. Nowadays, we employ six fully qualified IT Auditors with a good background in various technologies and systems. This gives us with the experience necessary to provide adequate guidance on adherence to Policies, Procedures and technical requirements as well as controls.

Furthermore, this experience enables us to conduct mock audits on the operations of our clients. In these type of audits, gaps are identified and reported to management together with suggestions on how to rectify such shortcomings. This ensure that companies stay compliant to the ever stringent regulations of the various jurisdictions as well as the requirements of the different regulators. This also helps operators prepare themselves for the audits of the respective regulator.

Our exposure to various operations and gaming systems helps us quickly understand and gain familiarity with your systems and enables us to advise you on recommended implementations both from an operations point of view and more importantly on issues of compliance. This exposure, puts us in a unique position to assist clients in designing, improving and testing of their back office applications. These assignments would ensure that the back office application meets all the needs of the operator, does not hinder users from efficiently carrying out their duties, and that all reporting is integral and reliable.

We have also built relationship with a network of trustworthy and reliable service providers, and, for those services outside our core competencies, can assist you in selecting the right partners to benefit your business.

The following is a list of services we provide our gaming customers:

- ▶ Full licensing assistance on all compliance matters
- ▶ Corporate services including company incorporation, opening of bank accounts, registered office
- ▶ Company Secretary and Directorship service
- ▶ Accounting
- ▶ Key Official Services
- ▶ Data Protection
- ▶ Anti Money Laundering
- ▶ PCI DSS compliance
- ▶ Sourcing of suppliers

Gaming



IT Audit and Assurance

Information Technology is at the core of the modern organisation's business model, often driving mission critical systems which necessitate monitoring and control to avert information leaks and vulnerabilities. The modern organisation must increasingly comply with legislative and regulatory compliance applicable to the industry they operate on.

Kyte was one of the first companies to become an approved systems and compliance auditor for the Malta Gaming Authority and also one of the first to become a Qualified Security Assessor Company for the PCI Standards Council.

Kyte's specialisation of IT Audit for Governance, Risk and Compliance (GRC) include:

- ▶ PCI DSS
- ▶ ISO27001:2013
- ▶ Remote Gaming
- ▶ COBIT

Apart from IT Audits for Governance, Risk and Compliance, Kyte can assist you in identifying control gaps in your systems and procedures by reviewing them and comparing them with best practice so that risks are appropriately categorised and managed. Kyte can carry out a specific audit of only your IT systems and/or your operational procedures as a one off assignment. Alternatively, Kyte can be engaged to develop and implement an Internal Audit plan. This would ensure that your organization is constantly being assessed for new risks and also be in a position to implement the necessary controls in a timely manner to mitigate such risks.

IT audits are carried out by our personnel with several years' of experience in the IT industry worldwide across several business verticals and industry qualifications such as CISA, ISO27001:2013 Lead Auditor, CISSP, SSCP, PCI QSA, Microsoft and more. Based on the outcome of the IT Audit, we also provide consultancy services implementing industry best practices to enable compliance and maximising the potential of the client's IT infrastructure.

Kyte is also in a position to assist you in achieving compliance to ISO27001:2013. We can assist in several ways, based on the availability and experience of client resources. We can leverage our experience in information security to offer you:

- ▶ Full Risk Assessment in accordance with requirements
- ▶ Assistance in compiling documented policies and procedures
- ▶ General consultancy on understanding and interpreting requirements
- ▶ Performing your Internal Audit function as a requirement of ISO27001
- ▶ Engage and manage the Certification process

In the unfortunate event of a security incident Kyte can also assist in investigating the root cause of the incident and to design controls to ensure weaknesses are identified and mitigated.



Explosive growth in the amount of credit (and debit) card transactions worldwide require compliance with the Visa / MasterCard / JCB and American Express mandated PCI Data Security Standard (PCI-DSS). Kyte Consultants has been a Qualified Security Assessor (QSA) company providing certification for PCI-DSS since 2008.

Rather than just relying on automated tools, we leverage our experience and attention to detail during the assessment as we assist our clients with achieving compliance in a timely and cost effective manner. We recognise that PCI Compliance has to be tailored to each individual's environment and available resources. For every onsite visit, we involve key players to ensure that:

- ▶ sensitive data is only retained for as long as required
- ▶ the network is adequately protected
- ▶ all applications are properly secured
- ▶ systems are monitored effectively
- ▶ any stored cardholder data is protected; and
- ▶ all controls are in place to satisfy compliance requirements

Furthermore, through robust methodologies, direct and constant contact with your assigned QSA, we are sure that your audit will go smoothly. Discussions on present and future setups, policies and procedures are encouraged so that PCI-DSS is taken on board by all within your company.

Through our ancillary services, and via a trusted network of long standing partners, we help you with the compliance efforts. Services to support your compliance efforts include:

- ▶ external and internal vulnerability scanning
- ▶ penetration and segmentation testing
- ▶ ongoing compliance monitoring
- ▶ assistance with documentation
- ▶ secure coding training

Whether you are a payment gateway in Europe, a merchant in the Middle East, an issuing bank in the US, an electronic money institution in Eastern Europe, or something in between, we are able to help you navigate PCI-DSS safely.

PCI DSS



Training

Very often we underestimate the importance of training within our organization. Ensuring that our employees have the necessary skills to perform their job function is crucial for every employee to succeed and for the department he/she forms part of, to deliver results. In some instances, providing training to certain key roles within an organization is a regulatory requirement and hence mandatory.

Kyte works very closely with companies in regulated markets and for this reason has good understanding of the training requirements of these companies. We are also aware of the fact that training in specialized areas of information security is not widely available and/or may be very expensive. Having tailor made training sessions is not something many training centers provide. Some courses in the market are basic computer based training which may not meet the training needs of the respective organization.

Kyte attempts to bridge this gap by providing specialized training in those areas which are required for compliance and for which ready-made courses are not available. We provide regular training in the following subject matters:

- ▶ Information Security Awareness

- ▶ Secure Coding

- ▶ AML procedures

- ▶ PCI DSS compliance

- ▶ Data Protection

Training is provided either on premise or in the form of webinars and the course content can be tailored to the needs of the company and the number of attendees.

