Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Artificial Intelligence 2026

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

Malta: Law & Practice

Paul Micallef Grimaud and Andrea Grima
Ganado Advocates

MALTA

Law and Practice

Contributed by:
Paul Micallef Grimaud and Andrea Grima
Ganado Advocates

Contents

Ganado Advocates is one of Malta's foremost law practices. It traces its roots to the early 1900's, where it was founded in Malta's capital city, Valletta. The firm has grown and adapted itself over the years to meet the changing needs of the international business and legal community. With a team of over 100 lawyers and professionals from other disciplines, it is consistently ranked as a top-tier firm in all its core areas, from corporate law to financial services, maritime, aviation, intellectual property, data protection, technology, litigation, employment and tax law. Ganado Advocates has over the past decades contributed directly towards creating and enhancing Malta's hard-won reputation as a reliable and effective international centre for financial and maritime services. Today, the firm continues to provide high standards of legal advisory services to support and enhance Malta's offering.

Authors

Paul Micallef Grimaud is a partner at Ganado Advocates and heads the firm's intellectual property, TMT and data protection practice groups. He is a warranted advocate with over 20 years' experience advising clients in the media, technology and entertainment space and representing them in court and arbitration proceedings. Paul has a keen interest in AI and innovative technology and is regularly involved in the drafting of laws, strategy and policies surrounding this area. He occupies the post of Vice President for the Professional Advancement of the Chamber of Advocates, is President of the Malta Institute of Privacy Law (MIPL) and is a member of ECTA's Law Committee.

Andrea Grima is an advocate within Ganado Advocates' intellectual property, TMT and data protection practice groups. He regularly assists clients with the protection, management, and enforcement of their intellectual property rights, including trade mark registrations, the drafting and negotiation of IP-related agreements, and brand protection strategies. Andrea has also researched and explored the regulatory challenges emerging within the digital landscape, particularly in the field of AI and innovative technology. Andrea also forms part of Ganado Advocates' corporate practice area, where he assists clients on a broad range of corporate transactional projects.

Ganado Advocates

171, Old Bakery Street
Valletta VLT 145
Malta

Tel: +356 2123 5406
Email: lawfirm@ganado.com
Web: www.ganado.com

1. Legal Framework

1.1 General Legal Background

In 2025, Malta enacted its first AI-specific regulations to implement the AI Act and formalise a domestic AI governance framework. Legal Notice 226 of 2025 (enacted under Chapter 591 of the Laws of Malta, the Malta Digital Innovation Authority Act) and Legal Notice 227 of 2025 (enacted under Chapter 586 of the Laws of Malta, the Data Protection Act) are the cornerstone instruments.

Notwithstanding these developments, Malta continues to rely primarily on existing civil, commercial and criminal law frameworks, supplemented by harmonised EU legislation, to regulate AI-related activity. Malta's mixed legal system – civil law in private and criminal matters, with common-law influences in public and administrative law – means that foreign jurisprudence, particularly from Italy, France and England, is likely to inform judicial interpretation in the absence of domestic case law.

Contractual and Tortious Lability

General principles of contract and tort law would continue to apply to the use of AI in Malta. These are covered by the Civil and Commercial Codes (Chapters 16 and 13 of the Laws of Malta, respectively).

Acting in good faith (in the manner of a bonus pater familias) is one of the underpinning principles of both contract law and tort law.

Article 1033 of the Civil Code, which establishes fault-based liability for damage caused by negligence, imprudence or lack of attention, is particularly relevant. The user cannot rely on ignorance of the effects of the use of the technology or the "black box" phenomenon to avoid liability. The duty of care applies equally in private and professional contexts.

IP, Data Protection, Product Safety and Consumer Affairs

Apart from its domestic laws, as an EU member state, Malta's laws adopt harmonised EU legislation in most of the areas that are relevant to AI, whether copyright and IP, data protection, use of medical devices, product safety or consumer protection law.

Consumer transparency is reinforced by Article 5 (1) (ea) of the Consumer Rights Regulations (Subsidiary Legislation 378.17), which requires that, prior to the conclusion of a distance or off-premises contract, or any corresponding offer, the trader must inform the consumer (clearly, comprehensibly, and in at least one of Malta's official languages) if the price has been personalised based on automated decision-making.

In addition, Legal Notice 225 of 2025 extended the Representative Actions (Consumers) Act (Act XVII of 2023) to cover breaches of consumer-facing obligations under the AI Act.

The use of personal data for AI in the health sector has been dealt with in the Processing of Personal Data (Secondary Processing) (Health Sector) Regulations (Subsidiary Legislation 528.10), which is discussed in further detail in **15.3 Healthcare**.

Employment Law

No Maltese employment statute specifically references AI, but the Digital Platform Delivery Wages Council Wage Regulation Order (Subsidiary Legislation 452.127) governs the employment conditions of couriers and delivery personnel operating through digital platforms and algorithmic management systems. In this legislation, algorithmic management is defined as the use by digital labour platforms of any automated systems.

Criminal Law

The Criminal Code (Chapter 9 of the Laws of Malta) does not distinguish AI-related offences as a separate category and has not been modified to cater for the use (or abuse) of AI systems. However, the unauthorised use of software, or use of software (which would include AI) to unlawfully access or render data inaccessible, constitutes an offence of "unlawful access to, or use of, information" under Article 337C of the Criminal Code. Similarly, using AI to commit fraud or forgery would render a person liable to the relevant offences under the Criminal Code.

In summary, traditional legal concepts are flexible enough to cover AI systems. AI is treated as a tool or method used by natural or legal persons, and those

persons remain accountable for compliance with the law.

2. Commercial Use of AI

2.1 Industry Use

AI is widely deployed across Malta's key industries, enhancing efficiency, decision-making and service delivery in various sectors:

- Transport: In the public sector, Transport Malta is piloting an AI-driven traffic-management system combining machine-learning models with real-time data analytics to optimise traffic flows and public transport scheduling, representing an early move towards semi-autonomous public-sector AI.
- Education: AI adoption in the education sector remains at an early stage but is recognised under the "Digital Education Strategy 2024–2030", with emphasis on learning analytics, digital literacy and ethical use.
- Healthcare: In healthcare, AI is used in diagnostics and resource planning. Maltese hospitals participate in the EU4Health BreastScan project, a pan-European initiative to support breast-cancer screening and radiological analysis, assisting clinicians by flagging anomalies. In parallel, the Central Procurement & Supplies Unit (CPSU) is piloting predictive analytics systems to forecast demand for medicines and medical supplies.
- Financial Services: Banks, insurers and fintech firms are likely to deploy machine-learning models for credit scoring, fraud detection, AML monitoring and risk management.
- iGaming: AI in the iGaming sector supports fraud detection, player protection and compliance monitoring, amongst other uses. In 2026, the Malta Gaming Authority (MGA) announced that it is developing a voluntary AI governance framework aligned with the AI Act.
- Tourism and Utilities: In the tourism sector, the Malta Tourism Authority (MTA) is spearheading data-driven initiatives to gain deeper insights into visitor behaviour and preferences. In the utilities sector, the Ministry for Energy, Enterprise and Sustainable Development (MESD) is deploying AI algorithms to analyse real-time data on water and energy usage.

2.2 Involvement of Governments in AI Innovation

The Malta AI Strategy and Vision 2030

Malta's approach to government involvement in AI innovation continues to be anchored in its National AI Strategy, "The Strategy and Vision for Artificial Intelligence in Malta 2030", first launched in 2019 and co-ordinated by the Malta Digital Innovation Authority (MDIA). The strategy was conceived as a holistic framework to position Malta as a trusted and competitive jurisdiction for AI development and deployment, structured around three strategic pillars – investment and innovation; public-sector adoption; and private-sector adoption. Within this framework, the original strategy set out a detailed programme of measures, including:

- 22 action points relating to education and workforce development;
- 6 actions addressing legal and ethical governance; and
- 11 actions focused on ecosystem infrastructure and enabling conditions for AI innovation.

Education and Workforce Measures

Government initiatives in the education and workforce space have focused on preparing Maltese society and the labour market for AI-driven transformation. The strategy's objectives include planning for the impact of technology and automation on the Maltese labour market; equipping the workforce with stronger digital competencies and new skills; and building awareness of AI, amongst other objectives.

These measures are reflected in sustained public investment in skills development and in collaboration with the University of Malta and the Malta College of Arts, Science and Technology (MCAST).

Legal and Ethical Governance Measures

From a legal-policy perspective, Malta was an early mover in embedding trustworthy AI principles into its innovation strategy. The legal and ethical objectives include the establishment of an ethical AI framework towards trustworthy AI; and the setting up of a regulatory sandbox for AI and a data sandbox for AI, amongst other objectives.

These objectives have materialised through the MDIA's Innovative Technology Arrangements (ITA) certification regime and the Technology Assurance Sandbox, which provide voluntary, structured pathways for AI developers to align systems with recognised standards and evolving EU regulatory requirements.

Ecosystem Infrastructure Measures

Government support for AI innovation has also focused on strengthening the enabling environment, including the establishment of a digital innovation hub (with a focus on AI), and identifying best practices for securing national AI solutions.

Realignment of the National AI Strategy

The MDIA is leading a realignment of Malta's National AI Strategy, with the process initiated through a public consultation launched in November 2025 and scheduled for completion during 2026. This realignment is being undertaken in response to several factors, including the fact that 80% of the objectives set out in the 2019 Strategy have already been partially or fully implemented, as well as the emergence of new areas of relevance and the declining importance of others, making a reassessment necessary.

The realigned strategy shifts away from a purely technology-first approach, placing societal well-being, sustainability, trust and legal accountability at its core, and introduces an expanded set of measures to support responsible innovation.

Other Initiatives

The Malta – European Digital Innovation Hub (DiHub-MT) has become a central mechanism through which government facilitates AI innovation. Led by the MDIA in collaboration with the Malta Council for Economic and Social Development (MCESD) and the University of Malta, DiHubMT operates as Malta's gateway to the EU-wide EDIH network, aligning innovation support with EU digital and AI policy objectives.

3. AI-Specific Legislation and Directives

3.1 General Approach to AI-Specific Legislation

The MDIA was established in 2018 by the MDIA Act (Chapter 591 of the Laws of Malta) with the objective of regulating and supporting innovative technologies through the issuance of recognition instruments, including mandatory and voluntary compliance certifications. While the Authority's initial focus was primarily on distributed ledger technologies (DLT), its remit has expanded to encompass other innovative technologies, including AI.

This expansion was formalised through the MDIA (Amendment) Act (Act XIX of 2024), which broadened the MDIA's statutory powers, modernised definitions of innovative technology, and strengthened enforcement and oversight mechanisms. The amendments expressly enable the Authority to perform expanded regulatory and supervisory functions in relation to AI and other emerging digital technologies. In parallel, the MDIA has been designated:

- the national cybersecurity certification authority under EU cybersecurity legislation;
- the competent authority for data intermediation services; and
- the authority responsible for the registration of data altruism organisations under the EU Data Governance Act.

Malta initially adopted a proactive and innovation-forward policy approach to AI regulation. In October 2019, it issued "The Strategy and Vision for Artificial Intelligence in Malta 2030", setting out a national policy agenda to "gain a strategic competitive advantage in the global economy as a leader in the AI field". The Strategy articulated a three-pillar vision, as mentioned in **2.2 Involvement of Governments in AI Innovation**.

The MDIA Technology Assurance Sandbox has remained a central element of Malta's regulatory philosophy. It enables AI systems to be developed, tested and refined in line with technology-driven control objectives and recognised standards, covering multiple stages of the AI life cycle.

A significant shift occurred in 2025, when Malta enacted its first AI-specific binding regulations to implement the AI Act and formalise a domestic AI governance framework, as mentioned in **1.1. General Legal Background** and as explored in **3.4 EU AI Act**.

3.2 Jurisdictional Law

Malta's AI-specific legislation is primarily concerned with implementing and enforcing the AI Act at national level, as mentioned in **1.1. General Legal Background** and as explored in **3.4 EU AI Act**.

3.3 Jurisdictional Directives

In October 2019, as part of "The Strategy and Vision for Artificial Intelligence in Malta 2030", the Maltese government published a non-binding Ethical AI Framework entitled "Malta – Towards Trustworthy AI". The Framework was developed by the Malta.AI Taskforce with the involvement of the MDIA and was expressly intended to supplement, rather than replace, existing legal and regulatory obligations.

The Ethical AI Framework sets out a series of governance and control practices grounded in four core guiding principles:

- Human Autonomy: AI systems should support, rather than undermine, human agency and decision-making.
- Prevention of Harm: AI systems should not cause harm to humans, the natural environment, or other living beings.
- Fairness: AI systems should avoid bias and discrimination and promote equitable outcomes.
- Explicability: The operation and outputs of AI systems should be understandable and capable of being challenged or reviewed by humans.

This AI framework reflected the Maltese policymakers' aspirations to strike a balance between endorsing the uptake of AI technology, whilst also ensuring its safe deployment within the relevant industries.

3.4 EU AI Act

Legal Notice 226 of 2025 (Artificial Intelligence Regulations, 2025) designates the MDIA as Malta's lead authority for the purposes of the AI Act. In particular, the MDIA is assigned multiple, central roles:

- Market Surveillance Authority (MSA) for AI systems in general;
- National Single Point of Contact, responsible for co-ordination with other member states and EU-level bodies;
- Notifying Authority, tasked with accrediting, supervising, and withdrawing approval from conformity assessment bodies that will certify high-risk AI systems under the AI Act; and
- the authority responsible for establishing and operating Malta's AI Regulatory Sandbox on a permanent footing.

The MDIA is also empowered to exercise enforcement powers, including inspections, information requests, corrective measures, and the imposition of administrative penalties.

Legal Notice 227 of 2025 complements this framework by assigning a specialised oversight role to the Information and Data Protection Commissioner (IDPC). The IDPC is designated as:

- MSA for specific categories of high-risk AI systems that heavily implicate fundamental rights or sensitive personal data; and
- Malta's Fundamental Rights Authority (FRA) for the purposes of the AI Act, with responsibility for safeguarding privacy, data protection, and related fundamental rights in AI contexts.

The IDPC also supervises AI systems listed in Annex III of the AI Act relating to:

- biometric identification and categorisation of natural persons;
- law enforcement AI systems (including criminal risk assessment and predictive policing tools);
- migration, asylum and border-control AI systems; and
- AI systems used in the administration of justice and democratic processes.

Malta has not introduced additional substantive national requirements beyond those prescribed by the AI Act. Instead, its approach is one of alignment with the EU's risk-based model.

That said, Maltese law introduces procedural and institutional safeguards to give practical effect to certain AI Act prohibitions and restrictions. Notably, the deployment of real-time remote biometric identification in publicly accessible spaces for law enforcement purposes, which the AI Act generally prohibits subject to narrow exceptions, is subject in Malta to prior judicial authorisation. Under the national framework, a Magistrate's warrant is required before such systems may be deployed and in urgent cases where deployment occurs without prior authorisation, ex-post judicial approval must be sought within 24 hours. This safeguard, introduced through Legal Notice 227 of 2025, reinforces Malta's commitment to the AI Act's strict stance on biometric surveillance and other intrusive AI practices, while remaining within the bounds of the AI Act.

3.5 US State Law

This is not applicable in Malta.

3.6 Data, Information or Content Laws

Malta has not enacted AI-specific amendments to its data protection, copyright, or content laws beyond the implementation of EU-level instruments.

3.7 Proposed AI-Specific Legislation and Regulations

We are not aware of proposed legislation and regulations addressing AI-specific rules in Malta. Any further developments are expected to arise from EU-level initiatives, such as potential amendments flowing from the Digital Omnibus proposals, rather than unilateral national legislation.

4. Case Law

4.1 Precedent-Setting Judicial Decisions

The Maltese courts have not had the opportunity to address the legal challenges being posited by AI, particularly in relation to intellectual property rights, data protection, consumer protection, competition law and damages resulting from the use of AI solutions.

Given Malta's mixed legal system, Maltese courts traditionally look to foreign jurisprudence for guidance where domestic case law is lacking. This approach is particularly relevant in the AI context. Thus, EU and UK court judgments on intellectual property rights and Italian and French court judgments in relation to tort and contractual damages resulting from the use of AI would be of interest to the courts in Malta.

5. AI Regulatory Oversight

5.1 Regulatory Agencies

MDIA and IDPC

The MDIA is the central public authority for AI governance in Malta. It leads national AI initiatives, advises the government on AI policy and strategy, and is responsible for implementing Malta's National AI Strategy and its associated action points in collaboration with public and private stakeholders.

As mentioned in **3.4 EU AI Act**, Legal Notice 226 of 2025 designates the MDIA as Malta's lead authority for the purposes of the AI Act, and under Legal Notice 227 of 2025, the IDPC is also designated as MSA for specific categories of high-risk AI systems listed in Annex III of the AI Act.

MFSA

The Malta Financial Services Authority (MFSA) remains the single regulator for financial services in Malta. While it has not adopted standalone AI-specific legislation, it is expected to play a key sectoral role in supervising the use of AI by licensed entities in banking, insurance, investment services and fintech, particularly where high-risk AI systems are deployed. The MFSA co-ordinates with the MDIA in respect of AI systems used in regulated financial activities and continues to issue supervisory guidance on digitalisation and technology risk within the financial sector.

MGA

The MGA regulates Malta's gaming and iGaming sectors, which are among the most AI-intensive industries in the jurisdiction.

Other

Where a non-EU person or undertaking intends to invest in an AI-related activity in Malta, clearance may be required from Malta's National Foreign Direct Investment Screening Office (NFDISO). Under the

National Foreign Direct Investment Screening Office Act (Chapter 620 of the Laws of Malta), investments involving critical technologies, expressly including AI, may be subject to notification and screening on grounds of security or public order.

Transport Malta will likewise be instrumental in regulating the use of autonomous vehicles and AI-enabled means of transport, including drones.

5.2 Regulatory Directives

In practice, much of the non-binding guidance relevant to Malta continues to originate at EU or pan-European supervisory level, with national regulators adopting, endorsing or referencing such guidance when exercising their supervisory functions.

In financial services, the MFSA has followed this approach by issuing a 2024 circular explaining the European Securities and Markets Authority (ESMA) Public Statement on the use of AI in the provision of retail investment services under the Markets in Financial Instruments Directive II (MIFID II), clarifying how existing organisational, conduct-of-business and client-interest obligations apply where AI is used. The MFSA has indicated that it will continue to monitor developments and assess the need for national supervisory measures.

The MDIA plays a central role in providing soft-law guidance, particularly where multiple regulatory regimes intersect. To address the combined application of the AI Act, Digital Operational Resilience Act (DORA), the Network and Information Security 2 (NIS 2) and the Cyber Resilience Act (CRA), the MDIA operates a regulatory sandbox framework. The MDIA works closely with other regulators, most notably the MFSA, reflecting their stated shared commitment to ensuring a secure and trustworthy digital environment.

The MGA, as stated in **2.1 Industry Use**, has announced a voluntary AI governance framework tailored specifically to gaming operators, focusing on transparency, fairness, data protection, robustness and human oversight. While non-binding, this framework is intended to complement EU-level AI obligations and provide practical guidance to MGA licensees.

5.3 Enforcement Actions

To date, no publicly reported enforcement actions or administrative fines have been imposed in Malta specifically related to AI systems.

6. Standard-Setting Bodies

6.1 National Standard-Setting Bodies

While the MDIA and other sectoral regulators (such as the MFSA, MGA and IDPC) set regulatory expectations within their respective domains, no binding national technical standards for AI systems have been formally adopted. That said, Malta has taken early steps in voluntary standardisation and assurance, most notably through the MDIA's ITA certification framework, which expressly encompasses AI systems.

Similarly, while some representative bodies of professionals in Malta (such as those representing the legal and medical professions) have issued statements on the use of AI, none has, to date, adopted profession-specific AI standards.

6.2 International Standard-Setting Bodies

Until standards are harmonised across jurisdictions, it is expected that any standards that may be in line with what is applied in one jurisdiction will not automatically be accepted by regulatory bodies in other jurisdictions.

European harmonised standards, developed by the European Committee for Standardisation (CEN) and European Committee for Electrotechnical Standardisation (CENELEC), will provide a presumption of conformity with key AI Act obligations once cited in the Official Journal of the EU. Once adopted at EU level, such harmonised standards will be relied upon by Maltese regulators when assessing compliance.

7. AI and the State

7.1 Government Use of AI

As discussed in **2.1 Industry Use**, the government's use of AI continues to be primarily pilot-based, experimental and policy-driven, rather than operational at scale.

7.2 Judicial Decisions

To date, no judicial decisions have been issued by the Maltese courts concerning the use of AI by government agencies.

7.3 National Security

The use of AI in national security or defence by Maltese authorities has not been publicly disclosed.

8. Generative AI

8.1 Generative AI: Key Legal Issues and Regulatory Approaches

To date, Maltese courts and regulators have not issued decisions or guidance dealing specifically with generative AI systems. The legal treatment of generative AI in Malta therefore continues to rely on existing national law, together with directly applicable EU legislation.

Foundation Models and General-Purpose AI

The AI Act's dedicated regulatory regime for general-purpose AI models has applied since August 2025.

Copyright in Training Data and AI-Generated Outputs

Malta has not introduced AI-specific copyright rules. Copyright issues relating to generative AI continue to be governed by the Copyright Act (Chapter 415 of the Laws of Malta) and harmonised EU law.

Licensing terms applicable to generative AI are expected to be enforceable under general contract law. In the absence of licensing terms, copyright protection for AI-generated outputs depends on originality and the extent of human intervention in the generated works.

Should the AI-generated work constitute a substantial copy of an original work and this is used by the entity that, through its prompts, generated the work using a third-party model, the said entity would be in breach of the copyright of the original work's author, irrespective of the entity's knowledge or intention in creating a copy of the original work. The only exception to this is where the exhaustive exceptions to copyright protection found in Article 9 of the Copyright Act apply. These include acts of reproduction of literary works by public libraries which are not for economic advantage, the reproduction of works for purposes of teaching or illustration without compensation, the reproduction or translation of works to render them accessible to disabled persons without compensation.

Similarly, unauthorised training of generative AI models on copyrighted material may expose developers to infringement claims.

Where a work that would ordinarily qualify for copyright protection is created wholly by an autonomous process without meaningful intervention in the creation of the work, copyright would not arise. This is because copyright arises where the author or any of the joint authors of the artistic, literary or audiovisual work that qualifies for copyright protection is a citizen of, or is domiciled or permanently resident in, or in the case of a body of persons, is established in, Malta or a state in which copyright is protected under an international agreement to which Malta is also a party. The term "author" is defined as "the natural person or group of natural persons who created the work eligible for copyright". The creation of a work by an autonomous process would eliminate the presence of an "author" and, consequently, copyright could not arise in such a work.

See also **16 Intellectual Property** for further information.

Data Protection Issues in Generative AI

Generative AI systems pose significant data-protection risks, both in the training phase (use of large datasets) and the deployment phase (user prompts and outputs).

However, under Maltese law, there are no derogations from the GDPR specific to generative AI. The use of personal data to train generative AI models must comply with Article 6 of the GDPR (lawful basis) and Article 9 of the GDPR where special categories of data are involved.

In practice, compliance is often challenging, particularly where models are trained on large, scraped datasets. Maltese law does not provide blanket exceptions for AI training. A limited, sector-specific exception exists under the Processing of Personal

Data (Secondary Processing) (Health Sector) Regulations (Subsidiary Legislation 528.10), which permit secondary use of health data for specified purposes (including research and system improvement), subject to anonymisation or ethics-committee approval. This remains the only Maltese legislative instrument that explicitly contemplates AI-related secondary data use.

There are no Maltese-specific exceptions to Article 22 of the GDPR (automated individual decision-making). Data subjects retain the right to object to solely automated processing producing legal or similarly significant effects, and all data-subject rights under Articles 12–22 of the GDPR continue to apply.

See also **17 Data Protection** for further information.

Liability for Harmful or Infringing Outputs

Maltese law has not adopted AI-specific liability rules for generative AI. Liability continues to be assessed under contract law, tort law and criminal law.

Malta's civil liability for non-contractual damages is fault-based, making it difficult for civil liability to arise unless an element of fault in a harmful or infringing output can be attributed to a specific human or legal person.

In addition, the Criminal Code contains general provisions on participation in, or facilitation of, criminal offences. Depending on the circumstances, these may apply to users who leverage generative AI to generate infringing outputs for criminal purposes. Furthermore, the use of generative AI systems to commit specific acts of fraud or forgery may render a person liable under the existing relevant offences of the Criminal Code.

See also **1.1 General Legal Background** for further information.

Transparency Requirements

Transparency has emerged as a central theme for generative AI, under the AI Act. The transparency obligations under the AI Act apply directly in Malta, affecting generative AI systems used or deployed.

9. Legal Tech

9.1 AI in the Legal Profession and Ethical Considerations

To date, Maltese regulators and professional bodies have not issued AI-specific guidance for the legal profession. The use of AI, including generative AI tools, is therefore governed by existing professional ethics rules, confidentiality obligations and data protection law. AI may be used as a support tool for legal work, but it does not diminish lawyers' responsibility to act independently, ethically and in accordance with professional secrecy and procedural obligations. AI does not change the level of responsibility of lawyers to act ethically in accordance with the Code of Ethics that regulates the profession and their legal obligations resulting from, amongst other pieces of legislation, the Professional Secrecy Act (Chapter 377 of the Laws of Malta) and the Code of Organisation and Civil Procedure (Chapter 12 of the Laws of Malta).

10. Liability for AI

10.1 General Theories of Liability

As noted in **1.1 General Legal Background** and **8.1 Generative AI: Key Legal Issues and Regulatory Approaches**, liability for AI systems in Malta continues to be governed by the general principles of contract, tort and criminal law.

Liability in relation to the use of AI will continue to be governed by the principles of tort and contract law under the Civil Code (Chapter 16 of the Laws of Malta) and the Commercial Code (Chapter 13 of the Laws of Malta).

As regards criminal law, the Criminal Code (Chapter 9 of the Laws of Malta) does not distinguish AI-related offences as a separate category and has not been modified to cater for the use (or abuse) of AI systems. However, certain provisions could be applicable to AI-caused harm.

Under Maltese law the technology itself would not have legal personality. It would therefore be the deployer or developer that would be ultimately responsible for harm caused by the use of AI. The determining factor

would be the cause of the damage suffered by the injured party, whether this was a result of the wrongful use of the technology or a defect in the technology itself.

The new Product Liability Directive (Directive 2024/2853), adopted on 23 October 2024 and in force since December 2024, expressly extends the concept of "product" to software and AI systems, including standalone and embedded AI. It also broadens the range of recoverable damage (including damage to data and psychological harm) and the categories of potentially liable economic operators (including manufacturers, importers, authorised representatives, platforms and certain service providers). However, member states have until 9 December 2026 to transpose the new Product Liability Directive into national law. To date, Malta has not yet completed transposition, and the existing product-liability regime continues to apply to products placed on the market before that date.

See also **1.1 General Legal Background** and **8.1 Generative AI: Key Legal Issues and Regulatory Approaches** for further information.

10.2 Regulatory Approaches to Liability for AI

The proposed AI Liability Directive, which sought to harmonise non-contractual civil liability rules for AI and introduce presumptions of causation and disclosure obligations, was formally withdrawn by the European Commission in 2025 due to lack of political consensus. As a result, there is no EU-level harmonised fault-based liability regime for AI, and liability outside the scope of product liability remains governed by national law, subject to general EU law principles and the obligations imposed by the AI Act.

At present, there are no Maltese legislative proposals introducing a bespoke AI liability regime and liability continues to be addressed through existing legislation.

However, Malta will be required to transpose the new Product Liability Directive (Directive 2024/2853) by December 2026.

11. Agentic AI Systems and Autonomous Decision-Making

11.1 Agentic AI Systems: Legal Framework and Governance

Agentic AI systems are not regulated as a distinct category under Maltese law. Instead, they are assessed under existing legal frameworks, including directly applicable EU legislation such as the GDPR and the AI Act.

Where such systems involve automated decision-making based on personal data, Article 22 of the GDPR applies. As clarified by the CJEU in the SCHUFA judgment, data subjects must be clearly informed of the use of fully automated decision-making, including profiling, and retain the right to object where such processing produces legal effects or similarly significant consequences.

The AI Act imposes mandatory human oversight, logging, and governance requirements in relation to agentic high-risk AI systems. However, agentic AI systems not considered to be high-risk would only be subject to minimal transparency requirements.

11.2 Liability Allocation for Autonomous AI Systems

Malta does not recognise autonomous AI systems as legal persons. As a result, liability for harm caused by autonomous AI systems is allocated to human or legal actors involved in the design, deployment or use of the system. The applicable framework combines general principles of contract, tort and criminal law, with directly applicable EU legislation, most notably the AI Act and the new Product Liability Directive, once it is transposed.

See also **1.1 General Legal Background** and **8.1 Generative AI: Key Legal Issues and Regulatory Approaches** and **10 Liability for AI** for further information.

12. Specific Legal Issues With AI

12.1 Algorithmic Bias and Fairness

Algorithmic bias is one of the identified and well-documented risks of AI. Although no standards have been mandated by Maltese regulators and/or law to avoid the risk of algorithmic bias, developers of AI are guided by best industry practice.

The transparency obligations imposed by the AI Act also serve to minimise these risks in a harmonised fashion. The AI Act also permits, under strict safeguards, the processing of special categories of personal data solely for bias monitoring, detection and correction in high-risk AI systems.

Where bias in the algorithm creates prejudice and damages are suffered, the liability principles mentioned in **1.1 General Legal Background** and **8.1 Generative AI: Key Legal Issues and Regulatory Approaches** and **10 Liability for AI** will apply.

12.2 Biometric Technologies and Emotion Recognition

The use of AI for emotion recognition and biometrics is known to be one of the more sensitive uses of this technology and brings with it inherent risks to the privacy of the individuals. Biometric data is treated as a special category of personal data under Article 9 of the GDPR, requiring a particularly high level of protection. The use of biometric AI systems engages not only data-protection law but also the fundamental right to respect for private and family life under Article 8 of the European Convention on Human Rights.

The AI Act has introduced a clear regulatory structure for biometric AI systems. Certain uses are prohibited outright, including untargeted scraping of facial images from the internet or CCTV, emotion recognition systems in the workplace or educational institutions (save for narrow medical or safety exceptions) and certain forms of biometric categorisation and manipulative surveillance.

Other biometric uses, including facial recognition, are classified as high-risk under Annex III of the AI Act and are subject to strict compliance obligations.

Given the direct applicability of the AI Act, biometric AI regulation and enforcement in Malta is expected to be highly harmonised with the rest of the EU.

12.3 Deepfakes and Synthetic Media

Deepfakes and other forms of synthetic media are primarily regulated under the transparency obligations set out in the AI Act, particularly Article 50. This provision requires that users of AI systems generating synthetic content disclose that certain content has been AI-generated or manipulated, thereby ensuring transparency for end-users.

These obligations are further supported by the forthcoming EU Code of Practice on Transparency of AI-Generated Content, expected to be finalised in 2026. The Code provides practical guidance on implementation measures such as watermarking, metadata tagging, and disclosure mechanisms to help platforms and content creators comply with Article 50.

Where deepfakes result in harm, existing civil remedies under Maltese law remain applicable. These include actions for defamation, depending on the nature and impact of the synthetic content.

12.4 Transparency and Disclosure

Transparency obligations arise from a patchwork of EU laws, including the AI Act and GDPR. As mentioned above, Article 50 of the AI Act sets out transparency obligations, which include informing users that they are interacting with AI systems, such as chatbots (unless this is obvious), and making individuals aware when certain content is AI-generated or manipulated.

Data subjects retain the right, under the GDPR, to understand how personal data has been processed and how results affecting them were produced. The “black box” risk associated with opaque automation therefore remains a key compliance concern. Deployers of AI systems remain liable for outcomes and resulting damage, notwithstanding the use of complex or autonomous technologies.

13. AI Procurement and Supply Chain Accountability

13.1 AI Procurement Standards and Contracting

Deployers of AI are ultimately responsible for using the technology within their business practice. Consequently, AI procurement contracts should include tailored risk-allocation provisions that address regulatory non-compliance, model performance, audit rights, etc. These protections can be further reinforced by service level agreements (SLAs) that include performance thresholds, incident remediation, and human-oversight support. Given the requirements of the GDPR and the AI Act, contracts must also define data governance. This includes clear regulation of ownership and usage rights for training and inference data, as well as restrictions on the secondary use of deployer data by suppliers.

Furthermore, certain sector-specific laws and regulatory directives may impose obligations on licensed entities in relation to the outsourcing agreements they have with third parties, including AI suppliers. This is the case, for instance, with DORA and the "Guidance on Technology Arrangements, ICT and Security Risk Management and Outsourcing Arrangements" issued by the MFSA in relation to licensed financial service providers, where certain obligations would need to be inserted in the outsourcing agreements.

13.2 AI Supply Chain Accountability and Due Diligence

AI supply-chain accountability has been imposed by the AI Act's provisions, including different obligations for providers, deployers, importers and distributors of AI systems.

14. Employment

14.1 Hiring and Termination Practices

The use of AI in employment-related decisions, particularly in hiring and termination, is subject to scrutiny under both the GDPR and the AI Act. Article 22 of the GDPR prohibits fully automated decision-making, including profiling, that produces legal effects or similarly significant impacts on individuals, unless specific conditions are met. In the employment context, this means that relying on fully automated processes that lead to the selection of candidates for a job is legally risky and could give rise to discrimination, legal challenges and ultimately damages being borne by the employer.

Under the AI Act, AI systems used for recruitment, selection, and termination of employment are explicitly classified as high-risk in Annex III. As a result, they are subject to strict requirements, including obligations around transparency, human oversight, data governance, and risk management.

14.2 Employee Evaluation and Monitoring

The same concerns that arise with regard to hiring and termination practices may also apply to employment performance analysis and monitoring.

Under the AI Act, AI systems used to monitor and evaluate employee behaviour and performance are classified as high-risk in Annex III. As a result, they are subject to strict compliance obligations. Employers must ensure that such systems do not operate in a fully automated manner without meaningful human intervention, especially where outcomes may affect employment conditions or career progression.

Moreover, the AI Act explicitly prohibits certain practices, including the use of AI systems for emotion recognition in the workplace. This prohibition reflects concerns about privacy intrusion, and the potential for discriminatory or manipulative outcomes.

15. AI in Industry Sectors

15.1 Digital Platform Companies

The use of AI in digital platforms is a given in today's world. These platforms rely heavily on user-generated data, making data protection legislation and its enforcement essential to preventing misuse. When platforms integrate AI systems, such as chatbots or content moderation tools, the AI Act becomes directly relevant. In particular, the Act imposes transparency obligations, requiring that users be clearly informed when they are interacting with an AI system.

In addition to the AI Act, several other EU legislative instruments are shaping the regulatory landscape for digital platforms. The Digital Markets Act (DMA), the Digital Services Act (DSA), and the Data Act, in their own ways and from their own angle, seek to mitigate the conglomeration and control of data by gatekeepers.

15.2 Financial Services

The financial services sector is among the most advanced adopters of AI, using it across functions such as customer onboarding, credit scoring, fraud detection and AML monitoring. The MFSA has identified key AI-related risks in its "FinSights: Enabling Technologies" series, including accountability, opacity of algorithms, data quality, regulatory fragmentation, competition concerns and discrimination.

These risks are reflected in the AI Act, which classifies creditworthiness-assessment systems as high-risk under Annex III, subjecting them to enhanced transparency, human oversight and documentation requirements.

Data protection remains central to AI compliance, with the GDPR imposing strict obligations on transparency, purpose limitation, data minimisation and the right to object to fully automated decision-making, particularly in high-impact contexts such as insurance.

Moreover, DORA obligations would apply, as will the MFSA Guidance on Technology Arrangements, ICT and Security Risk Management (subject to modification in order to supplement DORA obligations.)

Confidentiality and professional secrecy considerations also impact the licensed providers' interaction with generative AI and large language models, whilst the Data Act obligations relating to the data owner's control rights, where the IoT is being deployed, may also apply.

It is for this purpose, given the complexity of regulation in this industry, that sector players are advised to take a global view of the regulatory implications resulting from their use of AI.

15.3 Healthcare

Healthcare is known to be another high-risk scenario for the use of AI. Under the AI Act, there are a number of healthcare-adjacent public-interest applications designated as high-risk. In particular, high-risk classification applies to emergency healthcare patient triage systems, as well as to AI systems used by public authorities to evaluate the eligibility of natural persons for healthcare services. In addition to the Annex III use cases, AI software that is itself a medical device, or a safety component of one, and which is subject to third-party conformity assessment under the Medical Device Regulation (MDR), the In Vitro Diagnostic Regulation (IVDR), will also be considered high-risk under the AI Act.

In Malta, the Processing of Personal Data (Secondary Processing) (Health Sector) Regulations (Subsidiary Legislation 528.10) provides a legal basis for the secondary use of health data by public health providers for purposes beyond the original intent – such as research, innovation, and system planning. This secondary use is permitted subject to the application of anonymisation techniques or approval by an established Ethics Committee. This framework has enabled the development and testing of AI solutions in the health sector within a controlled and ethically supervised environment.

Patient rights, professional responsibility, and the risks of culpable negligence remain central considerations. The use of AI must also comply with professional secrecy obligations and data protection requirements under the GDPR, particularly where special categories of data are processed.

15.4 Autonomous Vehicles

Autonomous vehicles on Maltese roads remain at an early stage of testing in the public transport sector, alongside an AI-driven traffic management system. Transport Malta does not seem to have proposed any changes to the highway code or laws that require vehicles to be driven by persons that have a licence issued in accordance with the law.

15.5 Retail and Consumer

The retail and consumer sector may implement AI solutions across a broad range of functions, includ-

ing dynamic pricing, customer service chatbots and inventory management.

AI is increasingly deployed across the retail and consumer sector, supporting functions such as dynamic pricing, customer service chatbots, personalised marketing, and inventory optimisation. While most AI systems used in this context are not classified as high-risk under the AI Act, they are nonetheless subject to specific regulatory obligations. The AI Act imposes transparency requirements on limited-risk AI systems, including those that interact directly with consumers.

Consumer protection law plays a central role in regulating AI-driven practices. Article 5 (1)(ea) of the Consumer Rights Regulations (Subsidiary Legislation 378.17) requires traders to disclose when a price has been personalised based on automated decision-making. Furthermore, the inclusion of the AI Act in the Schedule to the Representative Actions (Consumers) Act (Act XVII of 2023) enables consumer associations to bring representative actions in cases of non-compliance with AI-related consumer obligations.

Data protection remains a cornerstone of compliance. By way of example, the use of personal data to personalise offers must comply with the GDPR. This includes ensuring a lawful basis for processing, respecting data subject rights, and conducting data protection impact assessments where required.

Finally, AI-driven practices that may distort competition or mislead consumers may also be subject to scrutiny by the Malta Competition and Consumer Affairs Authority (MCCAA) and the IDPC.

See also **1.1 General Legal Background**.

15.6 Industrial AI and Robotics

The use of AI-enabled robotic systems in industrial contexts raises a number of legal considerations.

Under the AI Act, AI systems intended to be used as safety components of machinery or other regulated products, and where the products are required to undergo a third-party conformity assessment, classified as high-risk. Industrial AI systems often fall within the intersection of the AI Act and existing EU product safety legislation, such as the Machinery Regulation (EU Regulation 2023/1230). While the AI Act addresses risks specific to algorithmic behaviour and system autonomy, traditional product safety rules continue to apply to the mechanical and operational aspects of the underlying machinery. This layered compliance framework requires manufacturers and deployers to ensure that both sets of obligations are met in parallel.

Where industrial AI systems process personal data, data protection obligations under the GDPR also apply.

16. Intellectual Property

16.1 IP Protection for AI Assets

AI systems, being computer programs and algorithms, are afforded copyright protection. Under Article 2 of the Copyright Act, a computer program is defined as a literary work and, subject to it having an original character, is afforded copyright up to 70 years after the end of the year in which the author dies.

The data compiled for the purpose of training an AI model may also enjoy sui generis protection rights relating to databases under Article 25 of the Copyright Act, where substantial investment in obtaining, verifying or presenting the data can be demonstrated.

As generative AI models become more precise, the manner in which a user prompts the model becomes a valuable element that the user may wish to protect. This protection may be achieved by treating the prompts as trade secrets under the Trade Secrets Act (Chapter 589 of the Laws of Malta). A trade secret is defined as information that:

- is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- has commercial value because it is secret; and
- has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Under the Maltese Copyright Act, in order for copyright protection to arise an "author" would need to be a natural person. Consequently, AI-generated works would not qualify for copyright protection unless a natural person can evidence, if challenged, that he or she did substantively participate in the creation process. Currently there are no Maltese court judgments to go by on this matter.

A similar interpretation would apply to the notion of an inventor under the Patents and Designs Act (Chapter 417 of the Laws of Malta) whereby the right to a patent will apply to the "inventor" and only a "natural person or legal entity may file an application for a patent" (Article 9).

See also **8.1 Generative AI: Key Legal Issues and Regulatory Approaches**.

16.2 AI as Inventor/Author

Under Maltese law, the concept of authorship is strictly limited to natural persons. The Copyright Act (Chapter 415 of the Laws of Malta) defines an "author" as "the natural person or group of natural persons who created the work eligible for copyright". As a result, works generated entirely by autonomous AI systems, without meaningful human input, do not qualify for copyright protection under current law.

Similarly, under the Patents and Designs Act (Chapter 417) the notion of "inventor" is understood to refer to a human creator. This position is consistent with the approach taken by the European Patent Office and courts in other jurisdictions, which have uniformly rejected the notion of AI systems being named as inventors.

There are currently no Maltese judicial or administrative decisions addressing this issue directly, and no legislative proposals have been tabled to extend authorship or inventorship to AI systems. However, the discussion at both EU and international levels will be relevant to Malta, particularly in light of the growing use of generative and agentic AI systems.

See also **8.1 Generative AI: Key Legal Issues and Regulatory Approaches** and **16.1 IP Protection for AI Assets**.

16.3 Copyright and AI Training Data

Where AI models are trained on copyrighted works without authorisation and no applicable exception applies, the developer of the model may be liable for copyright infringement. Under the Copyright and Related Rights in the Digital Single Market Regulations (Subsidiary Legislation 415.8), two key exceptions may apply to AI training. These being the text and data mining (TDM) exception for scientific research, and the general TDM exception for other purposes (which may be overridden by rights holders).

The AI Act reinforces this position by requiring general-purpose AI providers to adopt and implement copyright-compliance policies and to respect opt-out mechanisms available under EU copyright law.

Liability may also arise where AI-generated outputs substantially reproduce protected elements of training data. Although such reproduction may be unintentional, it can still constitute infringement if the output is deemed to be a derivative or unauthorised copy of the original work. This is particularly relevant in the context of generative AI systems trained on large volumes of copyrighted material.

See also **8.1 Generative AI: Key Legal Issues and Regulatory Approaches** and **16.1 IP Protection for AI Assets**.

16.4 AI-Generated Works of Art and Works of Authorship

Under the current legal framework, copyright protection in Malta is limited to works created by a natural person. As a result, works generated autonomously by AI systems, without meaningful human input, do not qualify for copyright protection under the Copyright Act (Chapter 415 of the Laws of Malta). Ownership and moral rights are similarly tied to human authorship, and there is no provision for recognising AI systems as authors or rights holders.

There is currently no Maltese case law or pending litigation that addresses the copyright status of AI-generated works. However, the issue remains under discussion, particularly in light of developments in generative AI technologies and ongoing policy debates at the EU level.

See also **8.1 Generative AI: Key Legal Issues and Regulatory Approaches** and **16.1 IP Protection for AI Assets**.

16.5 Foundation Models and Open-Source AI: IP Considerations

Using foundation models and open-source AI raises several IP issues, especially concerning licensing and ownership, and compliance.

Foundation models can be offered under different licences. Proprietary models are usually accessed via APIs and come with strict terms. Open-weight models share the model's internal data (the model weights) but may limit how they're used. Open-source models are more flexible but may still include conditions, such as limits on commercial use.

The distinction between API-based access and self-hosted models has important IP implications. API users typically do not receive a copy of the model and are bound by the provider's terms of service, which may include limitations on use or IP ownership of outputs. In contrast, self-hosted models, particularly open-source ones, allow greater control but shift the burden of compliance, risk management, and IP due diligence to the user.

17. Data Protection

17.1 AI Training and Data Protection

In Malta, AI training activities involving personal data are governed primarily by the GDPR, which applies directly and uniformly.

AI training requires a valid lawful basis under Article 6 GDPR. In practice, the most commonly relied-upon bases are consent (although this is often difficult to obtain or manage at scale, particularly for historical or web-scraped datasets), legitimate interests (subject to a balancing test and transparency obligations) and scientific or statistical research (where the conditions of Articles 5 (1)(b) and 89 GDPR are met).

The absence of a specific AI-training lawful basis means that controllers must justify training activities under existing GDPR grounds, on a case-by-case basis.

The purpose-limitation principle presents a key challenge for AI training. Personal data collected for one purpose may only be reused for AI training if the new purpose is compatible with the original one, or a new lawful basis is established. In addition, data subjects retain their full GDPR rights in the context of AI training, including the rights of access, rectification, erasure, and objection.

The use of special category data in AI training is prohibited unless a specific exemption applies. While the AI Act permits limited processing of such data for bias monitoring in high-risk systems, this does not override the GDPR's strict requirements.

Anonymisation is a key safeguard, as truly anonymised data falls outside the scope of the GDPR. However, anonymisation must be effectively irreversible in practice. Pseudonymised data, by contrast, remains subject to the GDPR.

17.2 AI Deployment and Data Subject Rights

In Malta, these obligations are governed by the GDPR, which applies directly, and are interpreted in line with EU jurisprudence and guidance.

All AI-driven processing must be based on a valid lawful basis under Article 6 GDPR. In high-impact use cases, such as credit scoring, recruitment, or fraud detection, controllers often rely on legitimate interests. However, this basis requires a documented balancing test and the implementation of appropriate safeguards to protect data subjects' rights and freedoms.

Article 22 GDPR is particularly relevant in the deployment phase. It grants individuals the right not to be subject to decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects, unless one of the limited exceptions applies (eg explicit consent). AI systems must also comply with the storage limitation principle under Article 5 (1)(e) GDPR.

With regards to children's personal data, this may only be collected and processed with the consent of a parent or guardian under GDPR.

17.3 AI Data Governance and Cross-Border Transfers

AI data governance in Malta is mainly regulated by the GDPR. The Maltese regulator, the IDPC, follows EU-level enforcement and guidance closely in this area.

Data Protection Impact Assessments (DPIAs) are mandatory under Article 35 of the GDPR where AI systems are likely to result in a high risk to individuals' rights and freedoms. Most high-risk AI systems under the AI Act will also trigger the need for a DPIA, reinforcing the importance of early-stage risk assessment.

Given the layered nature of AI supply chains, which often involve multiple parties, it is important to clearly define controller and processor roles. This is typically achieved through contractual arrangements that allocate responsibilities.

Cross-border data transfers remain a key challenge, particularly where third-country service providers are involved. Such transfers must comply with Chapter V of the GDPR, relying on mechanisms such as adequacy decisions and Standard Contractual Clauses (SCCs).

As the AI Act moves toward full application, its governance provisions – such as documentation, record-keeping, and post-market monitoring – will further reinforce the GDPR's accountability framework, particularly for high-risk AI systems.

See also **17.1 AI Training and Data Protection**.

18. Antitrust

18.1 Emerging Antitrust Issues in AI

While there is no dedicated Maltese legislation specifically addressing AI-related antitrust issues, Malta operates under EU and local competition laws, which are applicable to AI technologies and practices. We expect the Maltese regulators to adopt a similar approach to that which the EU takes on such matters.

Emerging antitrust issues may fall under the responsibility of one or various sector regulators. Primarily, the Office for Competition within the MCCAA will continue to be tasked with addressing anti-competitive behaviour, including collusion, even when this results from the use of AI, such as AI-driven pricing strategies. Other sector regulators, namely the MFSA (for licensed entities within the financial services sector, such as banks, payment service providers and insurers) and the MCA (for telecommunications and postal service providers) will also have a remit in ensuring that their licensed entities will not adopt abusive and market-distorting behaviour.

See also **15.5 Retail and Consumer**.

19. Cybersecurity

19.1 Applicability of Cybersecurity Legislation to AI

Cybersecurity obligations applicable to AI systems in Malta arise from a layered and fully EU-aligned legislative framework, rather than from AI-specific cybersecurity legislation. Malta applies a convergent regulatory approach, whereby AI-related cyber risks are addressed through the combined operation of the AI Act, DORA, NIS 2 (as transposed into Maltese law) and GDPR, where personal data is affected.

Incident reporting obligations applicable to AI systems arise from multiple legal sources:

- DORA requires financial entities to detect, classify and report major ICT-related incidents, including those involving AI systems, to competent authorities.
- NIS 2, which came into force in Malta in January 2026, expands mandatory incident-reporting obligations to entities classified as essential or important.
- GDPR breach-notification requirements apply where AI-related cyber incidents result in personal-data breaches.

20. ESG

20.1 ESG Dimensions of AI

Malta does not impose AI-specific environmental-impact obligations, but environmental considerations arise indirectly through EU sustainability legislation.

In February 2026, Malta transposed the Corporate Sustainability Reporting Directive (EU Directive 2022/2464) through the enactment of the Corporate Sustainability Reporting Regulations (CSRR), requiring in-scope entities to disclose material information on energy use, climate impacts and sustainability risks, which may include AI systems where material to the business. While no standalone AI carbon-disclosure obligation exists, organisations deploying AI at scale are likely to be expected to account for AI-related energy consumption within broader ESG reporting.

At the policy level, Malta's "AI Strategy and Vision 2030" reinforces ESG objectives through its focus on innovation and start-ups; public-sector AI adoption to enhance social well-being and access to services; and private-sector adoption grounded in transparent and accountable governance.

Malta's ESG-AI approach is further shaped by international engagement, including participation in initiatives such as the UN-led AI for Good Innovation Factory, which, while non-binding, underscores Malta's commitment to aligning AI development with global ESG standards.

21. AI Governance and Compliance

21.1 AI Governance Frameworks and Implementation

AI governance in Malta is now grounded in the mandatory, risk-based framework established by the AI Act and national implementing legislation. Organisations are expected to adopt AI governance structures, conduct risk and impact assessments, and integrate AI oversight into existing compliance and risk-management frameworks. Proportionate governance, robust documentation, third-party oversight and effective incident-response mechanisms are central to compliant AI deployment, supported by ongoing training and awareness programmes.

At the public-sector level, Malta has recently strengthened its institutional AI-governance capacity through the designation of specialised Chief AI Officer, who is tasked with acting as a central co-ordinator for AI-related projects across all government ministries.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Luke.Wilson@Chambers.com