Legal 500
Country Comparative Guides 2026

Malta

Data Protection & Cybersecurity

Contributor

Ganado Advocates

Paul Micallef Grimaud

Partner | pmgrimaud@ganado.com

Philip Formosa

Senior Associate | pformosa@ganado.com

Michela Zammit Lupi

Associate | mzlupi@ganado.com

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Malta.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Malta: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered; what sectors, activities or data do they regulate; and who enforces the relevant laws).

The GDPR applies directly into Maltese law and is supplemented by the Data Protection Act (the "DP Act"), Chapter 586, which addresses areas left to Member State discretion. The Processing of Personal Data (Electronic Communications Sector) Regulations, Subsidiary Legislation 586.01, implement the ePrivacy Directive, including its rules on cookies and direct marketing. The Office of the Information and Data Protection Commissioner (IDPC) is the main supervisory and enforcement authority in this area.

Cybersecurity is governed mainly by the Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order, Subsidiary Legislation 460.41 (NIS2 (Malta) Order), which transposes the NIS2 Directive and applies to essential and/or important entities across various sectors. Supervision is shared between the Critical Infrastructure Protection Directorate (CIPD), the Malta Communications Authority (MCA) and the Malta Information Technology Agency (MITA), each with distinct responsibilities. In parallel with NIS2, the Digital Operational Resilience Act (DORA)(Regulation (EU) 2022/2554) is implemented in Malta through the Malta Financial Services Authority Act (Digital Operational Resilience Act (DORA)) Regulations, 2024 (Legal Notice 166 of 2024) which is applicable for banks, insurers, investment firms, payment and e-money institutions.

The Critical Entities Resilience Directive (Directive (EU) 2022/2557)(CER Directive) is transposed into Malta through the Resilience of Critical Entities and Infrastructures (Identification, Designation and Protection) Order, 2026 (Legal Notice 5 of 2026).The Cybersecurity Act (Regulation (EU) 2019/881), which has direct effect in Malta is complemented by the Cybersecurity Certification Regulations (Subsidiary legislation 591.02) which establishes a national cybersecurity certification authority, administered via the Malta Digital Innovation Authority (MDIA) structures. This applies particularly to cloud, IoT, managed services and digital infrastructure providers.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

Key developments include the phased implementation of NIS2 in Malta, including a self-registration mechanism which has not yet been formally set up. The recent changes to the NIS2 (Malta) Order, which designated different roles to certain authorities, is likely to bring about change in enforcement practices. The Data Act has established new rules on data access and sharing, particularly for digital and cloud services. The EDPB DPIA template is currently under consultation and, once finalised, is expected to replace the current national template. With an ever-developing AI landscape and an EU Digital Omnibus package that puts into question the application of traditional data protection principles in an AI context, developments are bound to occur. Finally, on a purely domestic level, changes in data protection enforcement and policy direction may result from the recent appointment of a new Commissioner for Information and Data Protection.

3. Are there any identifiable trends or regulatory priorities in privacy, data protection and/or cybersecurity-related enforcement activity in your jurisdiction?

With regards to privacy and data protection, the period from 2024 to 2026 reflects a clear shift from predominantly reactive enforcement under the GDPR to a broader, multi-layered compliance framework incorporating the Data Act, the Artificial Intelligence Act, the NIS2 Directive and DORA. This shift is accompanied by increased coordination among national competent authorities and active participation in EU-level initiatives, including the Coordinated Enforcement Framework 2026, particularly in relation to transparency obligations and harmonised supervisory practices across EU data protection authorities.

On cybersecurity, Malta formally brought its NIS2 framework into force in January 2026, significantly strengthening cybersecurity obligations, particularly in

relation to risk management, incident reporting, and organisational resilience. In parallel, Malta is expected to align with emerging EU cybersecurity operational frameworks such as CyFun (Cyber Fundamentals), which functions as a practical compliance tool to support organisations in implementing the technical and organisational measures required under NIS2. The obligations of DORA are being enforced routinely by the Malta Financial Services Authority. These various frameworks have, amongst others, put adequate management frameworks and reporting obligations high on the agenda of licensed operators and undertakings across critical and important sectors.

4. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

There are no notification or authorisation requirements to the IDPC for personal data processing or transfers in or from Malta, with consultation limited to the specific cases in the GDPR. Entities within the scope of the Malta NIS2 Order are required to register, subject to limited exemptions. Non-compliance may result in fines and corrective measures. At present, an email may be sent to the CIPD to inform them of the intention to self register, following which the CIPD will issue the relevant form to complete.

5. What does "personal data," "personal information" or other equivalent terms (hereafter "personal data") mean under data protection laws in your jurisdiction? Does the definition broadly include information about all individuals? For example, would this include individuals acting in a personal or household capacity, as well as those acting in a business or commercial capacity (such as on behalf of a business or corporate entity or employer) or otherwise?

The GDPR applies directly in Malta and takes precedence over national law. "Personal data" is interpreted in accordance with the GDPR as any information relating to an identified or identifiable natural person. The DP Act does not expand this definition, but includes an exemption for processing carried out during purely personal or household activities, mirroring article 2(2)(c), GDPR.

6. Are certain types of personal data considered more sensitive or highly regulated under data protection laws in your jurisdiction? Please include the relevant defined terms for such data (e.g., special categories of personal data," "sensitive data" or "sensitive personal information"?

See above. The GDPR applies directly in Malta, and special categories of personal data (article 9), as well as data on criminal convictions and offences, are treated and protected as set out in the GDPR.

7. What principles apply to the processing of personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

In line with the GDPR, personal data must be processed lawfully, fairly and in a transparent manner, collected for specified, explicit and legitimate purposes, and be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, amongst other processing rules. Processing is permitted only where one of the lawful bases under article 6 (or 9, in cases of special categories of data) GDPR applies.

8. Are there any circumstances for which consent is required or typically obtained in connection with the processing of personal data? What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

Consent must be freely given, specific, informed, unambiguous and expressed through a clear affirmative act; it cannot be implied. In Malta, the GDPR applies directly and EDPB guidance is followed. Consent may be obtained in any form, provided it meets GDPR validity requirements, and written consent must be in clear, intelligible, and easily accessible language (Article 7(2) GDPR).

9. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

Processing requires a lawful basis under article 6, GDPR and, where special categories of data are involved, one of the conditions or derogations under article 9(2) GDPR must also apply. There are guardrails in place under Subsidiary Legislation 586.04 (the "Processing of Personal Data (Protection of Minors) Regulations) to allow for processing by teachers, schools and persons acting in loco parentis when it is in the best interest of the minor. In such cases, parental consent is not even required if this may be prejudicial to the best interests of the minor and the parent will not have access to the personal data held in relation to such minor. Whereas there are no ad hoc legal provisions, beyond the GDPR, relating to the primary processing of health data, the secondary processing of health data is regulated by the "Processing of Personal Data (Secondary Processing) (Health Sector) Regulations" (S.L. 528.10). These regulations list the instances in which secondary processing is authorised expressly providing that where the authorised purpose is for research, it must be in the public interest, if possible using anonymised data, and if not possible with the authorisation of the Health Ethics Committee or other Ethics Committee recognised by the Information and Data Protection Commissioner. Health Data can also be processed for Insurance Purposes under the "Processing of Data concerning Health for Insurance Purposes Regulations" (Subsidiary Legislation 586.10), where processing is authorised in circumstances where the processing is necessary and proportionate for issuing a policy; the data controller cannot reasonably be expected to obtain the data subject's consent and the controller is not aware that the data subject is withholding his/her consent.

10. Do the data protection laws in your jurisdiction have special or particular requirements, restriction, or rules regarding the collection, use, disclosure or processing of personal information from or about children or minors? If so, what is the age threshold and key requirements/restrictions that go beyond those applicable, generally?

Malta has implemented article 8, GDPR, setting an age threshold of 13. Outside of this, there is no other statutory age limit in Malta for a minor to be able to consent to processing. Refer to the reply to the previous question in relation to the processing of persona data relating to minors by teachers, schools, other professionals or persons acting in loco parentis.

11. Do the data protection laws in your jurisdiction include any derogations, exemptions, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

Malta has implemented article 23, GDPR, through the Restriction of the Data Protection (Obligations and Rights) Regulations (S.L. 586.09), which allow for limited restrictions to the rights of data subjects. These cover inter alia situations relating to the prevention, detection, investigation and prosecution of criminal offences; the safeguarding and maintaining of national security, public security, defense and international relations; the administration of tax and social security benefits; the establishment, exercise or defence of legal claims and proceedings and health emergencies.

12. Does your jurisdiction require or recommend privacy risk or impact assessments in connection with personal data processing activities and, if so, under what circumstances? How are these assessments typically carried out?

A Data Protection Impact Assessment (DPIA) is mandatory in the cases set out in article 35, GDPR. The IDPC has also issued guidance identifying a non-exhaustive list of processing operations, including the use of innovative technologies and employee monitoring, that require a DPIA, available here: https://idpc.org.mt/for-organisations/data-protection-impact-assessment/.

13. Are there any specific codes of practice, or self-regulatory codes applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

Most particularly, GDPR-related guidelines are available for both the Maltese banking and gaming sectors. These are not official guidelines issued by the IDPC; rather, they were developed by the respective stakeholders following

prior consultation with the IDPC.

14. Are organisations required to maintain any records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

Yes, as set out in article 30, GDPR each controller shall maintain a record of processing activities which shall contain the minimum information covered in the said provision. No further relevant local guidance has been issued by the IDPC in this regard.

15. Do the data protection laws in your jurisdiction specifically impose data retention limitations? If so, please describe such requirement(s).

Yes, the storage limitation principle in article 5(1)(e), GDPR applies. Record-keeping obligations arise in different scenarios under different provisions of Maltese law, such as anti-money laundering legislation.

16. Under what circumstances is it required or recommended to consult with the applicable data protection regulator(s)?

In addition to where the GDPR points at this, e.g. where a DPIA indicates a high-risk notwithstanding measures taken, the IDPC has, to date, been willing to provide clarity and perspective in cases of lack of published guidance or clarity in the law.

17. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, what are their legal responsibilities?

The GDPR regulates these matters. The IDPC has issued guidance on the role and expected responsibilities of the DPO, in the form of FAQs (https://idpc.org.mt/for-organisations/data-protection-officers/). These largely summarise the more detailed guidance issued by the EDPB.

18. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s) or recommendation(s).

While not an explicit legal requirement, training is strongly recommended as part of an organisation's accountability obligations. Such training should be proportionate to the nature, scope, and extent of the processing activities carried out.

19. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

Yes, compliant privacy notices must be provided in accordance with articles 13 and 14, GDPR.

20. Do the data protection laws in your jurisdiction distinguish between the responsibilities of "controllers" and those of "processors" (or equivalent terms) of personal data? If so, how are such terms defined and what are the key distinctions between the obligations of controllers and processors (or equivalent terms)?

Yes, the distinction between controllers and processors, both in terms of responsibility and liability, in Malta is as set out in the GDPR.

21. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these or any similar terms defined?

Individuals have the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects, subject to the limited exceptions under the GDPR. Monitoring, profiling, and the use of tracking technologies such as cookies must comply with the GDPR and the ePrivacy rules as implemented into Maltese law, and will commonly require a DPIA.

22. Do the laws in your jurisdiction include specific rules, requirement or regulator guidance regarding the use of cookies, pixels, online tracking and/or targeted advertising? Please describe any restrictions on targeted advertising and/or cross context behavioral advertising. How are these terms or any similar terms defined?

In Malta, tracking cookies are only lawful where prior, informed consent is obtained through a clear affirmative action. The IDPC has indicated that cookie walls, pre-ticked boxes, and implied consent (e.g. scrolling) are generally non-compliant, as they do not meet GDPR consent standards. Consent is also typically required for other cookies and tracking technologies, except for those that are strictly necessary.

23. Do the data protection laws in your jurisdiction specifically restrict or regulate the "sale" of personal data and/or "data brokers"? How is "sale" and/or "data broker" or (similar/related terms) defined?

There are no specific rules in Malta regulating the sale of "personal data" or "data brokers". In principle, any transfer, whether a "sale" or otherwise, constitutes processing. Any transfer or disclosure of personal data to third parties must therefore comply with the GDPR, including the requirement to have a valid legal basis, transparency obligations, and respect for data subject rights.

24. Do the data protection laws in your jurisdiction specifically regulate or restrict marketing and electronic communications, including telemarketing/telephone solicitations and 'robocalls', email marketing, SMS/text messaging or other direct marketing? Please provide an overview.

As a general rule, electronic communications for direct marketing (via email, fax, or automated calling systems) require prior consent from the subscriber or user (irrespective of whether a natural or legal person). There is a limited "soft opt-in" exception, allowing email marketing where: (i) contact details were obtained in the context of a prior sale; (ii) the marketing concerns similar products or services; and (iii) the recipient is given a clear, free, and easy opt-out at collection and in every message.

25. Do the data protection laws in your jurisdiction regulate, restrict or impose specific obligations on the processing of biometric data, such as facial recognition. If so, how are the relevant terms defined? Are these obligations focused on the collection, use and processing of unique biometric 'identifiers' (rather than any sort of biometric measurements) ?

Biometric data used for identification is a special category of personal data and is generally prohibited unless an article 9, GDPR condition applies. Its processing typically requires a prior DPIA.

26. Are there any data protection laws in your jurisdiction that specifically address or apply to artificial intelligence or machine learning ("AI"). If so, do these laws specifically apply to the processing of personal information related to AI, or more broadly?

At present, there are no AI-specific data protection rules in Malta. However, AI systems remain subject to the general GDPR framework where personal data is processed and the EU Artificial Intelligence Act applies in Malta directly as an EU Regulation. The EDPB's Opinion 28/2024 on AI models acts as guidance. Moreover, the IDPC has been designated as Fundamental Rights Authority (FRA) and Market Surveillance Authority (MSA) for certain high risk applications for Malta under the AI Act.

27. Are there any data localization requirements in your jurisdiction? In other words, are there any circumstances where some or all personal data is required to be stored locally, or prohibited from being transferred to or stored in certain jurisdictions?

There are no general data localisation requirements under the GDPR or Maltese data protection law (subject to any sector-specific rules). Transfers of personal data from Malta or elsewhere in the EU to third countries must comply with the GDPR, including reliance on an adequacy decision or, failing that, use of appropriate safeguards such as standard contractual clauses or binding corporate rules.

28. Is the transfer of personal data outside your jurisdiction restricted, under certain circumstances? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

Cross-border transfers to third countries do not require prior notification to or authorisation from the IDPC but require a GDPR-compliant transfer mechanism, such as standard contractual clauses, supported by a transfer impact assessment. In line with EDPB guidance, supplementary measures may be required to ensure a level of protection essentially equivalent to the EU/EEA.

29. What personal data security obligations are imposed by the data protection laws in your jurisdiction?

Controllers and processors must implement appropriate technical and organisational measures under Article 32 GDPR, proportionate to risk, including encryption, access controls, resilience measures, and regular testing. NIS2 and DORA impose additional security obligations on in-scope entities.

30. Are there more specific security obligations for certain types of personal data (e.g., sensitive data or special categories of personal data)?

Under the GDPR (as directly applicable in Malta), there are no specific security measures tied to categories of personal data. Article 32 instead requires risk-based technical and organisational measures, with higher risk processing (e.g. special category data) generally requiring stronger safeguards.

31. Do the data protection laws in your jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances and within what timeframe must such a breach be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

"Personal data breaches" are as defined in the GDPR. Where the IDPC is the competent supervisory authority, the controller must notify it within 72 hours of becoming aware of the breach, unless it is unlikely to result in risk to individuals. Affected data subjects must be informed without undue delay where the breach is likely to result in a high risk.

32. Do the data protection laws in your jurisdiction establish specific rights for individuals, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, and any exceptions.

In Malta, individuals are entitled to the data subject rights set out in Chapter 3 of the GDPR (access, rectification, erasure, restriction etc.). Requests must be addressed by the controller without undue delay and within one month, subject to limited extensions. Controllers must facilitate the exercise of these rights and ensure transparent communication. These rights are subject to the limitations in the GDPR (e.g. excessive or manifestly unfounded requests) and the restrictions adopted in Maltese law (see Q.11.).

33. Do the data protection laws in your jurisdiction allow or provide for a private right of action for violations? If so, does your jurisdiction also allow "class action" litigation (i.e., on behalf of a class or ('many') claimants)? Please explain under what circumstances in which a private right of action applies and/or a class action may be brought, and whether types of claims/violations present a higher risk of a private right of action or class action (e.g., are there statutory damages or presumed harm for certain violations)?

Individuals may bring an action for compensation under Article 30(2) DP Act for material or non-material (moral) damage resulting from an infringement. In Malta, such actions are instituted by sworn application before the First Hall of the Civil Court against the controller or processor concerned and must be filed within 12 months from when the data subject became aware, or should reasonably have become aware, of the infringement, whichever is earlier. Representative actions are also permitted under article 80, GDPR.

34. Are individuals entitled to monetary damages

or compensation if they are affected by breaches of data protection law? Does the law require actual and material damage to have been sustained, or is non-material injury to feelings, emotional distress or similar sufficient for such purposes?

The right to compensation is not limited to financial loss and includes non-material damage such as distress, anxiety, reputational harm, or loss of control over personal data. However, mere infringements of the GDPR, without the existence of damage suffered (whether material or non-material), are not sufficient to confer a right to compensation (see e.g. Case C 300/21).

35. How are data protection laws in your jurisdiction typically enforced? What regulatory body(ies) have enforcement authority?

The IDPC is the national supervisory authority responsible for monitoring and enforcing the GDPR and the Data Protection Act in Malta. Its decisions are subject to a two-tier appeal process: first to the Information and Data Protection Appeals Tribunal, and subsequently to the Maltese Court of Appeal (Inferior Jurisdiction).

36. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction? Are there any guidelines or rules for the calculation of such fines or the imposition of sanctions?

UNDRE Part Y of the DP Act and in accordance with article 58, GDPR, the IDPC has investigative, corrective and advisory powers , including the power to impose administrative fines. With the exception of public authorities or bodies, per article 83, GDPR, fines may reach €10 million or 2% of turnover, and €20 million or 4% for more serious infringements. EDPB Guidelines require consideration of factors such as the nature, gravity and duration of the infringement, prior breaches, and data affected. The DP Act also provides further fines and criminal sanctions for knowingly providing false information to the IDPC or failing to comply with a lawful request. The maximum fine that may be imposed on a public authority or body by the IDPC is twenty-five thousand euro (€25,000) for each violation and, additionally, the Commissioner may impose a daily fine payment of twenty-five euro (€25) for each day during which such violation persists.

37. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

See response to Q.35. Appeals to the Tribunal may be brought on the grounds of a material error of fact, procedure, or law, or other material illegality.Bottom of Form

38. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide an overview of these obligations and explain their scope/applicability. For example, are all organizations subject to the requirement or only to certain organizations (e.g., based on size, sector, critical infrastructure designation, public company)? Are there specific and/or additional regulations for different industries (e.g., finance, healthcare, government)?.

Yes. In Malta, specific cybersecurity risk management obligations apply depending on the applicable legal framework.

Under the NIS2 framework, the Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order requires in-scope essential and important entities to implement appropriate and proportionate technical, operational, and organisational cybersecurity risk management measures. These include risk analysis and information system security policies, incident handling procedures, business continuity and disaster recovery planning, supply chain security, vulnerability handling, encryption, access control, and regular testing and training. The obligations apply to designated entities operating in critical or important sectors, rather than to all organisations generally.Obligations apply to “essential” and “important” entities across sectors such as energy, transport, health, waste, and ICT.

In addition, financial entities are subject to the Digital Operational Resilience Act (Regulation (EU) 2022/2554), as implemented in Malta, which imposes detailed and prescriptive requirements relating to ICT risk management, incident classification and reporting, digital resilience testing, ICT third party risk management, and governance, supervised by the MFSA.

Separately, all organisations processing personal data are subject to the GDPR, which requires the implementation of appropriate technical and organisational security measures to protect personal data irrespective of sector or designation. The Cybersecurity Act establishes a certification framework but does not itself impose mandatory risk management measures.

39. Do the cybersecurity laws in your jurisdiction impose formal cybersecurity audit or certification requirements? If so, please provide an overview.

At present, cybersecurity laws in Malta do not impose a general mandatory cybersecurity certification regime. The Malta NIS2 Order establishes a supervisory, risk based compliance regime under which the competent authorities may require entities to demonstrate compliance, including through inspections, audits and assessments, but it does not mandate certification by default.

Certification schemes established under the EU Cybersecurity Act and implemented locally remain voluntary, although they may be used as evidence of compliance or required contractually or by regulators in specific contexts.

By contrast, DORA imposes mandatory resilience testing and audit type obligations on financial entities, including periodic ICT risk assessments, resilience testing (and, for certain entities, advanced threat led penetration testing), and regulatory review by the MFSA.

40. Do the cybersecurity laws in your jurisdiction impose specific requirements regarding vendor and supply chain management? If so, please provide details of these requirements.

Yes. The Malta NIS2 Order imposes supply chain and vendor risk management requirements on essential and important entities. In-scope entities must implement proportionate technical and organisational measures to manage risks arising from suppliers and service providers, including ICT supply chains and, where relevant, subcontractors. This includes identifying, assessing, and mitigating third-party cybersecurity risks, and may be reflected in contractual safeguards such as security requirements, incident notification obligations, audit rights, and business continuity and resilience provisions.

These obligations are supplemented for financial entities falling in scope of DORA, which contains detailed ICT third party risk management requirements, including contractual content, subcontracting oversight, and exit strategies.

41. Do the cybersecurity laws in your jurisdiction require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, please provide an overview of the requirement, including whether there are any formalities that must be observed regarding such appointment (e.g., board-approval, reporting line structure, notification to regulatory body).

While Maltese law does not mandate the appointment of a CISO by title, the Malta NIS2 Order requires essential and important entities to designate a Security Liaison Officer (SLO). The SLO is responsible for supporting compliance and acting as the interface with the competent authority. Key functions include facilitating the development and review of business continuity (and, where relevant, termination) plans, ensuring appropriate risk assessments are carried out, overseeing the maintenance and testing of the operator security plan, and acting as the point of contact with the competent authority (e.g. the CIPD) to ensure fulfilment of the entity's obligations.

Financial entities subject to DORA must also establish clearly defined governance and accountability arrangements for ICT risk management at both management and board level.

42. Do the cybersecurity laws in your jurisdiction impose specific reporting or notice obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and what are the reporting and notification requirements (please also note whether these laws require reporting of certain cyber security incidents, regardless of whether there has been a 'breach of personal data')?

In-scope entities under the Malta NIS2 Order must report cybersecurity incidents. An "incident" is broadly defined as any event compromising the availability, authenticity, integrity, or confidentiality of data or services provided via network and information systems. Essential and important entities must notify the CSIRT Malta without undue delay of incidents with a significant impact on their

services. Reporting is staged, typically involving an early warning (within 24 hours of becoming aware of the incident), a subsequent notification with initial assessment (by latest 72 hours), possibly (upon CSIRTMalta's request) an intermediate report and a final report (within one month from the incident notification). The report must highlight the nature of the incident, the type of identified threat, the mitigation measures applied and if there is any cross-border impact. Similar timelines apply under DORA, as specified in Article 5 of the Commission Delegated Regulation 2025/301 of 23 October 2024.

Separately, the GDPR imposes mandatory personal data breach notification obligations on all controllers, regardless of NIS2 or DORA status – refer to the reply to Q.31.

43. Can individuals bring a private right of action for cybersecurity incidents or other violations of cybersecurity laws? If so, does your jurisdiction also allow "class action" litigation (i.e., on behalf of a class or ('many') claimants)? Please explain under what circumstances in which a private right of action and/or a class action may be brought?

Maltese law does not currently provide a standalone private right of action specifically for breaches of cybersecurity obligations under the NIS2 or DORA framework. Enforcement of NIS2 and DORA obligations is primarily administrative and regulatory.

However, individuals may bring private claims arising out of cybersecurity incidents under other legal bases, such as contract law, where applicable, and general tort principles. Malta also permits representative actions in certain contexts, including collective redress mechanisms under EU consumer and data protection law, although class action litigation as understood in common law jurisdictions remains limited.

44. How are cybersecurity laws in your jurisdiction typically enforced? What regulatory body(ies) have enforcement authority?

The primary enforcement authority under Malta's NIS2 framework is the CIPD, which functions as the national supervisory authority and is responsible for overseeing compliance and enforcing corrective measures. Within the CIPD, CSIRT Malta is responsible for handling cyber incident reporting, analysis, and coordination. Legal Notice 89 of 2026 introduced an Enforcement Committee empowered to impose administrative fines and penalties upon referral by the CIPD or competent authorities. Sectoral regulators, including the Malta Communications Authority and Malta Financial Services Authority, support enforcement within their domains. The MFSA is the regulator entrusted with enforcing DORA.

45. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

Under Malta's NIS2 framework, the CIPD (or other competent authority, where designated) has broad supervisory powers. These include on-site and off-site inspections, targeted and ad hoc security audits (including independent audits), security scans, and risk-based checks. The authority may request information, access documents and systems, and require evidence of cybersecurity policies, risk management measures, CSIRT monitoring, and business continuity arrangements. The MFSA's powers in relation to DORA are equally broad and stem from the Malta Financial Services Authority Act. The MDIA, acting as the NCCA, has supervisory and enforcement powers in relation to cybersecurity certification schemes.

46. What is the range of sanctions (including fines and penalties) for violations of cybersecurity laws in your jurisdiction? What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction? Are there any guidelines or rules for the calculation of such fines or the imposition of sanctions?

Under NIS2, the competent authority may impose a range of enforcement measures on essential and important entities, including administrative penalties. Penalties may reach up to €10 million or 2% of global annual turnover for essential entities, and up to €7 million or 1.4% for important entities, whichever is higher. Prescribed factors include the seriousness and duration of the breach, prior infringements, harm caused, intent or negligence, remedial actions, cooperation, and compliance with codes or certification schemes. The IDPC may impose fines for breach of data protection laws that range between 2% and 4% of annual turnover and €10 million and €20 million, depending on the type of breach, its seriousness and repercussions. The MDIA may also impose penalties under Maltese law for infringements of the Cybersecurity Act, in line with its article 65, and

require the immediate cessation of any such infringements.

47. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Enforcement decisions, save for fines, under Malta's cybersecurity framework (NIS2) are generally subject to appeal before the Administrative Review Tribunal, which may confirm, vary, or annul the decision. A further appeal from the decision of the Tribunal on points of law lies with the Court of Appeal. Fines are imposed, upon the commencement of proceedings by the CIPD or other competent authority (where designated), and following due process, by the Civil Court. Under DORA, appeals from the decisions of the MFSA are filed before the Financial Services Tribunal with a further appeal available before the Court of Appeal.

Contributors

Paul Micallef Grimaud
Partner
pmgrimaud@ganado.com

Philip Formosa
Senior Associate
pformosa@ganado.com

Michela Zammit Lupi
Associate
mzlupi@ganado.com