THE MALTA CHAMBER

FEEDBACK BY THE MALTA CHAMBER

Consultation on the Transposition of Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity across the European Union (NIS 2 Directive)

Presented to : Ministry for Home Affairs, Security and Employment

Date : 07/10/2024

Classification : FINAL

THE MALTA CHAMBER

INTRODUCTION

The Malta Chamber has gathered input from businesses and stakeholders regarding the impact of the directive on their operations. The NIS2 Directive introduces new obligations to enhance cybersecurity across the EU, which although well intended, may result in increased compliance costs and operational burdens. The Malta Chamber seeks to safeguard the interests of its members by outlining key concerns, potential challenges and anticipated costs of implementation for Maltese firms.

This feedback prepared not only provides critical feedback on the draft legislation, but also highlights the broader implications for businesses and the economy. The Malta Chamber believes that this is imperative for authorities to understand to be in a better position to support and guide businesses through this regulatory transition, ensuring a smooth adaptation while minimising potential disruptions.

Notable salient points of interest in this respect are:

1. Implications for Business and the Economy
    a. Costs of doing business
    b. Impact on Competition
2. More clarity is required on:
    a. The specific implementation measures emerging from the legislation, both for business and national competent authorities.
    b. Regulated Entities based on the required market concentration and risk assessments; and
    c. Motivation behind personal liability of natural persons.

FEEDBACK & RECOMMENDATIONS

1. Implications for Business and the Economy

The Malta Chamber acknowledges that implementing the NIS2 Directive will enhance the capacity of public and private sectors to identify and mitigate cyber risks. However, these regulations may also impose significant costs on businesses and the broader economy,

impacting compliance expenses, consumer prices, trade, and innovation. Balancing enhanced cybersecurity with manageable economic impacts is crucial to ensure the directive does not hinder business growth and competitiveness.

A. Costs of Doing Business

According to a report by Frontier Economics, the direct costs of implementing the NIS2 regulation on firms across the EU is estimated to be €31.2 billion per year, split into €1.3 billion for sectors already regulated under NIS and €29.9 billion for sectors which didn't fall within the scope of NIS but now fall within the scope of NIS2.[1]

The report states that businesses will face expenses related to staffing, additional services, software and hardware. Companies will need to hire extra information security, IT security, and business continuity staff, and will likely require further assistance from legal consultants and advisory services. Additionally, investments in software and hardware will be necessary to support cybersecurity frameworks and systems, including firewalls, cabling, and other essential components to maintain internal security processes.

The burden each business faces will vary depending on several factors. New entities falling under NIS2 require sufficient time to consult, invest in technology, train in skills and align with the regulatory obligations, all of which will not happen by transposition date (18th October 2024).

Businesses already regulated under NIS will be impacted less but still need to address the additional requirements introduced by the expanded NIS2 Directive. Costs will depend on the current level of cybersecurity measures within the respective business since several firms already have systems and frameworks in place, hence the financial impact will largely depend on how closely these existing standards align with the new NIS2 requirements. Smaller business entities which now fall under essential / important businesses are likely to incur more costs as compared to larger ones due to economies of scale.

[1] Assessing the Economic Cost of EU Initiatives on Cybersecurity (July 2023)

These increased costs for businesses are likely to be passed on to consumers. This impact will extend beyond sectors directly regulated by NIS2, also affecting other industries that rely on trade with NIS2-regulated sectors.

B. Impact on Competition

While the directive promotes uniformity and harmonisation across EU member states, it may create a competitive disadvantage compared to non-EU countries.

As explained prior, higher compliance costs are likely to drive up prices for EU firms, reducing their global competitiveness. Moreover, higher costs may limit innovation as companies will have lesser resources for research and development, further exacerbating competitive disadvantages, and a higher risk-taking aversity.

As a result of the NIS2 directive, European imports are expected to decline by €13.4 billion, and exports are also expected to dip by €19.4 billion within the EU (Frontier Economics, 2023).

Additionally, given that NIS2 is a directive, each EU member state will implement it differently in their national laws. Although the substantial effect is expected to be equal, it is essential to monitor how other Member States plan to adopt the directive. We need to ensure that Maltese businesses are not placed at competitive disadvantage compared to their EU competitors.

2. Legislative provisions

Following discussions with its members, the Malta Chamber would like to highlight points which it believes should be further explained or rectified in the draft legislation. Some proposals in this regard are also being put forward. The scope of this exercise is to primarily provide more clarity for businesses and to ensure that the transition is as smooth and effective as possible.

A. Clarity

The Malta Chamber underscores the need for greater clarity in the transposition of the NIS2 Directive into national legislation. This includes specific guidance on the time frames and

deadlines businesses will have to comply with their obligations, such as grace periods for preparatory implementation and reporting. The absence of clearly defined timelines creates uncertainty, making it difficult for firms to plan and allocate resources effectively.

Further clarity is also required concerning key terms in the legislation, such as "major incident", to take one example. Without a uniform interpretation, businesses may face ambiguity, potentially leading to inconsistent reporting or enforcement. Standardised definitions are crucial to ensure businesses and regulators operate under a common framework, avoiding loopholes or conflicting interpretations.

Additionally, the coordinating entity Critical Infrastructure Protection Department (CIPD) needs to be more specific on which entities are subject to the NIS2 Directive. Guidance is required, for instance, on whether holding companies fall within the scope of the directive if one of their subsidiaries qualifies as an essential or important entity. Similarly, the overlap between NIS2 and other regulatory frameworks, such as the Digital Operational Resilience Act (DORA) for financial services, needs to be addressed to prevent conflicting compliance obligations.

To aid businesses in understanding and implementing the directive, the Malta Chamber proposes the publication of a comprehensive guidebook detailing the steps which impacted companies are required to follow. This guidebook, along with simplified versions of the criteria issued by the CIPD, would help businesses quickly identify whether (a) they fall under the scope of NIS2 and (b) what specific actions are required against what implementation / reporting deadlines.

By offering clear, accessible resources, the government can better ensure effectiveness of implementation by supporting businesses in navigating the complexities. At the same time, due consideration should be devoted to ensuring that compliance with national and EU-wide standards does not create excessive bureaucracy or unlevel competition locally and internationally.

B. Legislative criteria

The Malta Chamber believes that the current criteria for determining whether an entity falls within the scope of the NIS2 Directive lacks sufficient proportionality. Under the current draft legislation, businesses that meet specific employee or revenue thresholds, whether they just qualify or exceed these limits significantly, are subject to the same responsibilities and obligations. This approach does not account for the varying degrees of impact that cybersecurity risks might have on smaller versus larger businesses. Not all companies pose the same level of risk to the economy, especially those operating in highly competitive sectors. A blanket approach may also inadvertently disadvantage smaller businesses, creating an uneven playing field and hampering their competitiveness. Any impact assessment to determine whether a business entity qualifies as 'essential' or 'important' entity in the ambit of the LN should consider not only size of business transactions but also the economic impact and role within its respective industry. This would ensure that the Directive is applied fairly and proportionately to its mandated intentions, thus creating a more balanced and equitable framework.

C. Regulating Entities

The Malta Chamber emphasises the importance of clearly defining the roles and responsibilities of each regulatory entity involved in the implementation. The NIS2 Directive places responsibilities on Critical Infrastructure Protection Department (CIPD), the Malta Communications Authority (MCA) and the Malta Financial Services Authority (MFSA) as national competent authorities. These roles must be explicitly outlined in the legislation itself to avoid ambiguity, rather than relying on non-binding intra-Governmental Memoranda of Understanding (MoUs). This approach ensures that each regulator has the authority to oversee its designated sectors holistically and effectively while the impacted operators would understand to whom they should respond.

Moreover, the Malta Chamber stresses the need for ensuring that regulators are adequately resourced to manage the portfolios assigned to them. The introduction of NIS2 brings significant new responsibilities and regulators must be equipped with the expertise, personnel and technical capabilities to handle their oversight obligations effectively. Without sufficient resources, there is a risk that the regulatory framework may not be applied consistently or efficiently, hindering the overall objectives of the directive and pushing impacted business off their timelines.

D. Personal Liability of Natural Persons

The provision in Section 19(1) of the LN states that "*The natural persons composing the management bodies may jointly and severally be held liable for infringements*". This raises significant concerns regarding personal liability for executives and managers within organisations. While accountability is a fundamental aspect of corporate governance, the potential for individual liability in cases of cyber incidents may create an environment of fear and hesitation among leaders. This could, in turn, discourage decisive leadership and proactive decision-making, which are essential for fostering innovation and robust cybersecurity practices.

It is crucial to recognise that cyber-attacks can occur despite the implementation of stringent security measures. Holding individuals, such as CEOs or managers, personally liable for incidents is on various counts disproportionate to their control and therefore, excessively punitive. Such a stance may not only undermine the confidence of those in leadership roles but could also pushes companies into supplementary unnecessary levels of safeguards which cost money and hinder the overall effectiveness of cybersecurity strategies within businesses.

It is there essential for authorities and stakeholders to facilitate access to appropriate cybersecurity insurance products that cover personal liability for executives. By ensuring that insurance solutions are available, individuals can protect themselves against potential legal repercussions stemming from incidents despite their adherence to best practices and due diligence.

CONCLUSION

The transposition of the NIS2 Directive into national legislation represents a pivotal step towards enhancing cybersecurity across the EU, however, it is essential to approach this transition with careful consideration of the potential implications for businesses and the economy.

The Malta Chamber urges policymakers to prioritise clarity in the ever-increasing legislative framework being placed on businesses as part of their digital transition, ensure equitable regulatory practices and foster an environment that encourages innovation and effective leadership, not the opposite.

By addressing the concerns outlined in this document, authorities can create a robust and supportive regulatory landscape that safeguards the interests of businesses while effectively mitigating cyber risks. Collaboration among regulators, stakeholders and businesses will be vital to achieving a balanced approach that enhances resilience in the face of evolving cyber threats.

THE MALTA CHAMBER

www.maltachamber.org.mt

+356 2203 2304

The Malta Chamber of Commerce,
Enterprise and Industry 64, Republic
Street Valletta, VLT 1117