WAHL

LAW FIRM

"Cybersecurity in the Republic of Croatia: Implementation Challenges"

November 07, 2025. I WAHL Legal Alert No 25 I Cybersecurity

In a digitized society, where state institutions, the economy, and the daily lives of citizens heavily rely on digital technologies, the issue of cybersecurity becomes a priority. Cybersecurity is no longer the exclusive responsibility of the IT sector - it is a shared concern across all sectors of society. Every individual, institution, and organization, regardless of their field of activity, plays a role in safeguarding digital security. Cooperation between technical experts, management structures, educational institutions, and legislative bodies is essential for creating a resilient and secure digital environment.

"The Concept of Cybersecurity and Why Is It Important?"

It is Monday morning. You have just arrived at work, and you are attempting to access your banking app to check the account balance - but the app is not functioning. You try to pay for coffee with your card - the POS terminal displays a declined payment message. You attempt to contact the bank's customer support - no one answers. News quickly spreads that a major cyberattack has occurred: banking systems have been hacked, data compromised, and transactions blocked.

What was once reserved for futuristic novels has now become reality. Increasingly frequent hacker attacks on critical infrastructure raise serious concerns about the vast potential consequences of a digital and globalized society.

In an era of complete societal dependence on ICT technologies and the widespread presence of sensitive personal data on platforms such as digital one-stop shops like "*e-Građani*" or "*e-Porezna*", cybersecurity must become a priority - not only for legislators but also for all of us who use these technologies daily.

Cybersecurity can be defined as a set of activities (processes, measures, and standards) designed to protect computer systems, networks, software, and data from unauthorized access, attacks, damage, or theft.[1]

Its purpose is not solely the technical protection of infrastructure, but also the preservation of public and economic trust in digital services.

Legislative Framework in the Republic of Croatia

In order to align with European standards, the Republic of Croatia has implemented Directive (EU) 2022/2555 of 14 December 2022

[1] https://mpudt.gov.hr/kiberneticka-sigurnost/28695?lang=hr

(commonly referred to as the NIS 2 Directive), which establishes a higher level of cybersecurity across the European Union. The NIS 2 Directive has been transposed into Croatian national law through the Cybersecurity Act ("*Narodne Novine"*, No. 14/24), which entered into force on 15 February 2024.

The Cybersecurity Act regulates the obligations and measures that public and private sector entities must implement to protect their information systems from cyber threats. It applies to a broader range of organizations, including essential and important entities in sectors such as energy, healthcare, transport, finance, digital services, and others.

The Act prescribes the obligation to implement:

- risk assessments,
- the establishment of security policies,
- the appointment of responsible persons for cybersecurity, and
- the reporting of significant incidents.

It is also important to note that on 21 November 2024, pursuant to Article 24 of the Cybersecurity Act, the Government of the Republic of Croatia adopted the Cybersecurity Regulation (*"NN" No. 14/24.*

The Cybersecurity Regulation sets out the criteria for classifying entities based on specific parameters for categorization, defines risk management measures in the field of cybersecurity and the manner of their application. It also regulates the procedure for conducting cybersecurity self-assessments, establishes the conditions for identifying significant cybersecurity incidents, the method of reporting such incidents, as well as other aspects essential for improving the overall level of cybersecurity.

An important component of the regulatory framework for cybersecurity in the Republic of Croatia is the National Cyber Crisis Management Program, adopted on 9 May 2025. The National Cyber Crisis Management Program is a bylaw adopted under the Cybersecurity Act, establishing a comprehensive system for responding to cyber crises in the Republic of Croatia. The Program defines objectives, capacities, resources, and procedures for effective crisis management in accordance with the European framework.

Differences Between the NIS 2 Directive and the Cybersecurity Act

Although the Cybersecurity Act is largely aligned with the European framework, it introduces additional obligations that go beyond the requirements of the NIS 2 Directive. For example, the Act explicitly mandates that important entities conduct a cybersecurity self-assessment at least once every two years, a requirement not expressly stipulated by the NIS 2 Directive. Furthermore, the Act provides more detailed provisions on supervisory mechanisms, including mandatory cybersecurity audits for essential entities at least once every two years, and oversight every three to five years.

In terms of scope, the Act retains the criteria set out in the NIS 2 Directive but places additional emphasis on entities registered in the Republic of Croatia. An exception is made for providers of public electronic communications networks and services, who are subject to the Act only if they provide services within Croatia, regardless of their place of registration. The Act also stipulates that the competent authority must notify essential and important entities by February 2025, and those entities must comply within one year of receiving the notification.

Regarding penalties, the Cybersecurity Act imposes stricter sanctions than the NIS 2 Directive.

Essential entities may be fined:

- Between €10,000 and €10,000,000, or 0.5% to 2% of annual turnover, whichever is higher

- Members of senior management may be fined between €1,000 and €6,000.

Important entities may be fined:

- Between €5,000 and €7,000,000, or 0.2% to 1.4% of annual turnover.
- Members of senior management may be fined between €500 and €3,000.

Who Are Essential and Important Entities?

Under the Cybersecurity Act, entities are classified as essential or important. Essential entities include, for example, hospitals, energy companies, and banks, while important entities include digital service providers or logistics companies. The classification is based on the type, size, activity, and impact of the entity, with the primary distinction being the potential impact of a cybersecurity incident on society, the economy, and national security.

Challenges in Implementing the NIS 2 Directive

Every implementation process brings certain challenges, and the transposition of the NIS 2 Directive is no exception. Key challenges include:

- *Financial and organizational burdens for small and medium-sized enterprises (SMEs)*
- *National infrastructure available only in the Croatian language*
- *Obtaining credentials for system access*

Financial and Organizational Challenges for SMEs

The adoption of the Cybersecurity Act imposes numerous obligations on organizations, including the appointment of responsible persons, risk assessments, incident response planning, IT audits, employee training, and investments in technical protection. SMEs are particularly affected, as they often lack the necessary expertise and financial resources. Despite their limited capacity, they are increasingly targeted by cyberattacks due to weaker defenses. Therefore, legislative measures must be accompanied by concrete support, education, and financial assistance to enable smaller entities to meet legal requirements and enhance their resilience.

National Infrastructure in the Croatian Language

The establishment of a national platform for reporting cybersecurity incidents introduces two key roles: platform administrator and platform user. The administrator must be an employee of the company, access the platform via e-Business, and manage authorizations through e-Authorizations. The user, who may be an employee or an external service provider, is responsible for reporting incidents.

A problem arises when directors or employees are foreign nationals who do not speak Croatian, as the platform is available exclusively in Croatian. In today's digital environment, directors play a crucial role in ensuring organizational readiness for cyber threats. Although the Act does not prohibit foreigners from performing these roles, the language barrier significantly hinders their ability to fulfill legal obligations, increasing the risk of fines.

The Security and Intelligence Agency (SOA) has acknowledged the issue and confirmed that a solution is being developed, including the potential introduction of English-language support on the platform.

Obtaining Credentials for Access

A growing practical issue in implementing the Cybersecurity Act relates to obtaining credentials for accessing national digital systems such as e-Authorizations, e-Citizens, NIAS, and Pixi. Although technical in nature, this issue significantly impedes access, particularly for foreign nationals in executive roles within Croatian companies.

Access requires Croatian credentials (e-ID card, Croatian bank mToken, or FINA certificate), which are generally unavailable to foreign nationals without residence in Croatia. As a result, they are unable to formally assume authority or implement legally mandated measures. Additionally, the fact that all systems are available only in Croatian presents a further obstacle.

Given the increasing presence of foreign investors and international personnel, this shortcoming represents a serious systemic challenge. It is urgently necessary to consider amendments to the legal framework, enable alternative authentication methods, and introduce multilingual support to ensure lawful and effective compliance for organizations with international staff.

Deadlines Set by the Cybersecurity Act

The Cybersecurity Act clearly defines key deadlines that obligated entities must comply with.

The first obligation concerns the initial categorization of entities, which had to be completed by 4 April 2025. Following this, the notification of categorization must be delivered by the competent authority to the entities no later than 5 May 20251.

Upon receiving the categorization notice, entities are required, within 30 days, to establish an incident reporting system via the national platform and begin reporting incidents to the national CSIRTs (Computer Security Incident Response Teams).

Entities then have one year from the date of receiving the categorization notice to implement the initial measures prescribed by the Cybersecurity Act—specifically, by 4 April 2026.

The Act also mandates the enhancement of cybersecurity measures through risk management, including the first self-assessment for important entities or audit for essential entities. These must be conducted every two years, with the first round to be completed by 4 April 2028.

Furthermore, the Act requires regular expert supervision by competent authorities, to be carried out at least once every three to five years.

These deadlines reflect a strictly structured implementation plan for cybersecurity measures, requiring timely preparation and active management of obligations by all entities. Failure to meet these deadlines may result in serious consequences, including financial penalties and regulatory sanctions. Therefore, it is crucial that entities begin preparations immediately to ensure full compliance within the prescribed timeframes.

Key Deadlines:

- *Submission of entity categorization: by 4 April 2025*
  (notification by the competent authority must be delivered no later than 5 May 2025)

- *One year from receipt of the categorization notice – obligation to implement initial cybersecurity measures by 4 April 2026*

Initial Categorization Statistics in the Republic of Croatia

As part of the implementation of the Cybersecurity Act, an initial categorization of entities in the Republic of Croatia was carried out, forming the foundation for further implementation of the measures and obligations prescribed by the legal framework.

According to available statistical data, the categorization encompassed a total of 702 entities, of which 140 were identified as essential entities and 562 as important entities. This categorization spans 41 sectors, subsectors, and types of entities, indicating the broad scope of the Cybersecurity Act across various areas of the economy and public sector.

A specific segment of the categorization relates to 28 registries of Croatian internet domains, authorized by CARNET TLD. Although not directly covered by the Cybersecurity Act, these registries are required to submit data to the registry of special entities, thereby indirectly contributing to the cybersecurity system.

Changes to the registry of categorized entities are expected in the future, in two forms: permanent and one-time.

Permanent changes refer to a smaller number of new categorizations or decategorizations, typically resulting from legislative amendments, business expansion, or mergers and acquisitions.

One-time changes are anticipated by the end of 2025, primarily concerning small entities in the ICT service management sector.

The data indicates that the Republic of Croatia has approached the implementation of the Cybersecurity Act in a systematic and comprehensive manner, taking into account the complexity of the digital environment and the diversity of stakeholders. The initial categorization thus represents a key step toward more effective risk management and improved resilience to cyber threats. Continuous updating of the registry and active inclusion of additional entities will ensure that the legislation keeps pace with technological developments and changes in the business and institutional landscape.

Conclusion

It is evident that in a digitized society, cybersecurity has become a fundamental pillar of stability, resilience, and public trust in digital services—among citizens, businesses, and institutions alike. It is no longer merely a technical issue concerning IT professionals, but a strategic challenge requiring the engagement of all societal stakeholders—from legislators, management, and operational teams to end users.

Through the implementation of the Cybersecurity Act and alignment with the NIS 2 Directive, Croatia has taken a significant step toward a systematic approach to protecting digital infrastructure, with clearly defined requirements, deadlines, and penalties for non-compliance.

However, alongside normative progress, the Republic of Croatia faces numerous practical implementation challenges, particularly in the context of language barriers, technical accessibility, and limited resources among smaller entities. For the legislative framework to be effective, it is essential to ensure operational infrastructure, targeted education, and ongoing support for all entities involved in the cybersecurity system.

Only through such an approach can the primary goal be achieved: the creation of a secure and resilient digital environment capable of responding to increasingly sophisticated cyber threats.

Ultimately, only through synergy between the state, the private sector, and the expert community can a secure digital future be built.

Contact:

Neven Marić
+385 1/5629-767
n.maric@wahl.hr

Matea Miljuš Beranek
+385 1/6535 327
m.miljus-beranek@wahl.hr

** Attorney trainee Valentina Štih contributed to the preparation of the publication.*