Image not found or type unknown

The Emergency Ordinance establishing a framework for cybersecurity of networks and IT systems in the civilian national cyberspace (the “Ordinance”) was published in the Official Journal of Romania, Part I, No. 1332 of 31 December 2024. The legislative act entered into force on the same date, with the exception of a small number of provisions which entered into force after the publication of the Ordinance in the Official Journal of Romania1 . By the Ordinance: • Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 published in the Official Journal of the European Union OJEU No. L. 333/80 of 27 December 2022 (“NIS 2 Directive”) is transposed. • Law No. 362/2018 on ensuring a high common level of network and IT system security (“Law No. 362/2018”), published in the Official Journal of Romania, Part I, No. 21 of 9 January 2019, is repealed, except for the measures adopted or imposed pursuant to the provisions of Chapters IV and V, which shall remain in force until their revision. The Ordinance imposes a number of new cybersecurity rules on important and critical activity sectors, incident reporting and management mechanisms and a number of sanctions for non-compliance with the obligations set out in such legislative act. The purpose of the Ordinance is to reduce the online activity of cyber actors that expose the infrastructure to numerous risks (such as hacker groups or hostile entities) and to increase technological interdependence (5G networks, artificial intelligence). The competent authority at national level is the National Cybersecurity Directorate (“DNSC”), with supervision, monitoring and sanctioning powers for entities that do not comply with the requirements of the Ordinance. DNSC cooperates in the field of cybersecurity with the National Authority for Administration and Regulation in Communications (“ANCOM”) and with the National Cybersecurity Incident Response Centre (“CERT-RO”). At European level, there is cooperation both with the European Commission and the European Union Agency for Cybersecurity (“ENISA”), and with the EU Member States through the Cybersecurity Incident Response Teams (the “CSIRT Network”). The institutions in the field of defence, public order and national security are excluded from the application of the provisions of the Ordinance. For the entities to which the provisions of Regulation (EU) 2022/2.554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (the “DORA Regulation”) are applicable, the rules of the Ordinance apply only partially, namely the legal provisions on the criteria for inclusion in the category of critical or important entities and the modalities to register them with DNSC. <h2>The main novelties and amendments brought by the Ordinance in the field of cybersecurity</h2> <u>a) Terminology</u> The definitions introduced by the Ordinance include: • Cyber threat - any circumstance, event or potential action that could cause damage or disruption to networks and IT systems, and to the users of such systems and to other persons, or that may otherwise have a negative impact on them; • Significant cyber threat - a threat that, due to its technical characteristics, may cause serious damage to an entity or its users; • • • Cybersecurity audit - an activity that systematically assesses all policies, procedures and protective measures implemented on networks and IT systems in order to identify malfunctions and vulnerabilities and provide solutions to remedy them; • Sectoral Cybersecurity Competent Authority - the public institution responsible for regulating and/or supervising security measures in various sectors; • Cyber crisis - a state of affairs that represents a real threat or deterioration of a cyber infrastructure, capable of causing damage to networks and IT systems that provide essential, digital, or nationally significant services; • Entity - a natural or legal person established and acknowledged as such under the domestic law of its place of establishment, which may, acting in its own name, exercise rights and be subject to obligations; • DNS service provider - entities that provide publicly accessible domain name resolution services to Internet end-users; • Incident - an event that compromises the availability, authenticity, integrity, or confidentiality of data that is stored, transmitted, or processed, or of the services provided by or accessible through networks and IT systems; • Major cybersecurity incident - an incident which exceeds the response capability of a single EU Member State or affects at least two EU Member States; • Online

marketplace – a service that uses software, including a website, a part of a website, or an application managed by or on behalf of the trader, allowing consumers to conclude remote contracts with other traders or consumers; • IT system security policy – a set of rules and measures for the protection of networks and IT systems to be adopted by a critical or important entity; • Risk - the potential for loss or disruption caused by an incident; it must be expressed as a combination of the magnitude of such loss or disruption and the likelihood of the incident occurring; • Cybersecurity - a state of normalcy resulting from the application of a set of proactive and reactive measures meant to ensure the confidentiality, integrity, availability, authenticity and non-repudiation of electronic information of public or private resources and services in the cyberspace; • Network and IT system security - protection against events that may affect the confidentiality, integrity and availability of data; • ICT service - a service consisting entirely or predominantly of the transmission, storage, retrieval or processing of information through networks and IT systems   <u>b) Activity sectors where compliance with cybersecurity rules is mandatory </u> • The Ordinance has broadened the sectors to which cybersecurity rules apply. CRITICAL SECTORS: <ul> Energy Transport Banking sector Financial market infrastructures Digital Infrastructure Health Drinking water Waste water Central public administration Space ICT service management SECTORS OF MAJOR IMPORTANCE: <ul> Postal and courier services Waste management Chemicals Food sector Manufacturing industry Digital Providers Research Local public administration Details of the fields related to the sectors mentioned above can be found in Annex 1 (Sectors of high critical importance) and Annex 2 (Other sectors of critical importance) of the Ordinance.   <u>c) Scope. Classification of entities relevant to cybersecurity</u> • The Ordinance applies to both public and private entities that are required to comply with cybersecurity rules and fall into the two categories covered by the Ordinance, namely critical entities and important entities. 1. Critical entities include central public administration entities, entities from sectors of high critical importance (see the table in section b) above), entities identified as critical entities under the legal provisions on the resilience of critical entities, DNS service providers, qualified trust service providers, TLD name registries. 2, Significant entities include large and medium-sized enterprises, providers of public electronic communications networks and providers of electronic communications services destined to the public, trust service providers, and other entities in sectors of high critical importance that do not meet the requirements to qualify as critical entities (sectors such as waste management, postal and courier services, food production). o For purposes of understanding the above-mentioned classification, please note that large enterprises are those enterprises that have at least 250 employees and a turnover of at least 50 million euro (RON equivalent) or a total annual balance sheet of over 43 million euro (RON equivalent), and medium-sized enterprises are those enterprises that have between 50 and 249 employees and have a net annual turnover of up to 50 million euro, RON equivalent, or total assets not exceeding the RON equivalent of 43 million euro. 3. An entity can be classified as critical or important according to the following criteria: o if it is the sole provider of a critical service; o if a potential disruption of its activity would affect the public safety or national security; o if the impact of such disruption would have cross-border consequences. 4. An entity is critical depending on its importance at national or regional level to the sector in which it operates or to other interdependent sectors. o Factors such as the impact on the fundamental rights and freedoms, the national economy, public health, national security and financial risks shall be taken into account when assessing the impact generated by a possible disruption of the activity of a critical entity. o The exact methodology for assessing these risks is to be established by an order of the Managing Director of DNSC. • The Ordinance applies, as a rule, only to entities established and registered in Romania. By way of exception, the providers of public electronic communications networks or the providers of electronic communications services destined to the public shall fall within the scope of the Ordinance when they provide services on the territory of Romania, regardless of their place of establishment or registration.   <u>d) Cybersecurity risk management

measures and incident reporting procedure </u> • Critical and important entities are required to conduct a risk analysis and implement appropriate technical, organizational and operational measures to protect networks and IT systems. • The Ordinance sets deadlines for entities to fulfil their cybersecurity obligations. Within 60 days following the official registration in the register managed by DNSC, critical and important entities are required to submit to the DNSC their risk level assessment, which must include the list of relevant assets and the list of identified risks. Subsequently, within 60 days following the submission of the risk assessment, the entities shall also conduct a self-assessment of the maturity level of their cybersecurity risk management measures. The entities are required to submit the self-assessment of the maturity of risk management measures on an annual basis. Following such self-assessment, within 30 days, a remediation plan for the identified deficiencies must be submitted to DNSC, approved by the entity's management, to ensure the continuous improvement of cybersecurity protection. • Security risk management measures must include clear risk analysis policies, the use of cryptography and, where applicable, encryption for data protection, effective incident management and the implementation of strategies to ensure business continuity in case of cyberattacks. o The entity's risk level shall be assessed according to the assessment methodology established by order of the Managing Director of DNSC o The assessment of cyber risk levels involves identifying and analysing threats that may impact the security of an organization. It is essential to identify critical assets such as IT systems, databases, network infrastructure and sensitive information that need to be protected. Then, both external and internal threats, as well as risks associated with suppliers and business partners are analysed. • As a novelty compared to previous regulations, the Ordinance also applies to the supply chain. Thus, in order to ensure compliance with security requirements, the provisions of the Ordinance also apply to suppliers and partners of economic operators in critical and major sectors, as can be identified in the table in Section b) above. The Ordinance provides that cybersecurity risks may also arise in contractual relationships with partners and suppliers, not only at the level of the entities concerned. • At the request of the DNSC, entities are required to provide information on the providers of essential services so as to ensure adequate protection against external risks. • By means of the Ordinance a number of obligations applicable to the management bodies of critical and important entities have been established, such as: ? the obligation to adopt cybersecurity risk management measures, to implement the orders adopted by the relevant competent authorities, to supervise their implementation and to answer for their breach; ? the obligation to attend accredited professional training courses to ensure a sufficient level of knowledge and skills for identifying risks and assessing cybersecurity risk management practices, and their impact on the services provided by the entity. This obligation is also applicable to the entity’s staff; ? the obligation to establish permanent contact channels, allocate the necessary resources for implementing cybersecurity risk management measures and, where applicable, appoint network and IT systems security officers responsible for implementing and supervising cybersecurity risk management measures within the entity. The security officer must have managerial authority and be independent of the entity's IT structures so that he/she can make objective decisions on cyber protection. He/she must complete an accredited specialized course, recognized by DNSC, in the field of cybersecurity, within 12 months of his/her appointment. o The general meeting of shareholders is not the management body of critical and important entities within the meaning of the Ordinance. • If the management bodies fail to comply with their obligations under the Ordinance, the DNSC may refer the matter to the competent authorities in order to impose a temporary ban on holding executive director or legal representative positions. • The Ordinance requires entities to report significant incidents, while adhering to the following deadlines and guidelines: ? reporting in the event of an incident with possible cross-border impact must be made within a maximum of 6 hours of becoming aware of it ? the early warning must be given within a maximum of 24 hours of becoming aware of the significant incident; ? incident information updates must be made no later than 72 hours after discovery of the incident; ? the interim report, with all updated information, is carried out at the request of the national incident response team (“National CSIRT”); ? the final report shall be submitted no later than one month after the initial notification of the incident. • All reports are

made to the National CSIRT using the National Platform for Reporting Cybersecurity Incidents (“PNRISC”). o DNSC serves as the National CSIRT. • For incident reporting purposes, entities are required to provide details such as: o detailed description of the incident, including its severity and impact; o the type of threat or root cause that probably triggered the incident; o mitigation measures in place and ongoing; o where appropriate, the cross-border impact of the incident. • An incident is considered significant if: o it causes serious business disruption or significant financial loss; o it has affected or is likely to affect other natural or legal persons, causing substantial material or non-material damage.   <u>e) Entity registration procedure </u> • DNSC keeps a register that includes critical and important entities. They must notify DNSC for registration within 30 days of the Ordinance coming into force or from the time its provisions apply to them. • The previously mentioned notification must include details such as: ? identification data; ? field of activity; ? Member States of the European Union in which they provide services; ? IT infrastructure used; ? documents attesting to its status as a critical or important entity. • The registration decision is issued by DNSC within 60 days for critical entities and 150 days for important entities. • Entities must notify DNSC within 3 months of any changes concerning: the person appointed as the entity's representative, his/her address and contact details, if the entity is not established in the European Union; the Member States in which they provide services, if applicable; the entity's public IP address ranges, in the case of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, content delivery network operators, data centre service providers, managed service providers, managed security service providers and digital service providers; the entity's public IP address ranges, for entities other than those listed above. Any other changes to the other information to be included in the aforementioned notification must be communicated to DNSC within 2 weeks. • If an entity no longer meets the necessary conditions set out in the Ordinance, it must notify DNSC and provide supporting documents within 30 days. The DNSC reviews the documents and issues a decision on deregistration.   <u>f) Security incident response </u> • Critical entities, important entities and sectoral competent authorities may set up cybersecurity incident response teams (“CSIRT”). • CSIRT has a number of responsibilities, including: o Monitoring and analysing cyber threats, vulnerabilities and incidents; o Providing early warning mechanisms, alerts, announcements and dissemination of information to critical and important entities; o collecting and analysing cybersecurity data. • CSIRTs serving critical entities or important entities are authorized by DNSC.   <u>g) Supervision and control</u> • The ordinance assigns DNSC the role of supervision, verification and control authority over entities to ensure compliance with the legal provisions on cybersecurity. • In order to accomplish these duties, DNSC carries out the following activities: o checks on cybersecurity measures carried out by designated staff; o having ad-hoc security audits carried out by certified auditors; o requesting information on risk management measures taken; o requesting access to data, documents and other relevant information, such as the results of the audits carried out by certified auditors.   <u>h) Exchange of information on cybersecurity </u> • Critical entities, important entities, their partners and suppliers may exchange information on cybersecurity in order to prevent or detect security incidents and to minimize their potential impact. • The main objective with regard to information exchange is to increase the level of cybersecurity by detecting, limiting and preventing the possible spread of potential threats, by remedying vulnerabilities and by promoting collaboration between public and private entities in the field of cyber threat research. • Cybersecurity information exchange agreements are notified to DNSC, which has the role of assisting entities in concluding such agreements, and which may limit the scope of such an exchange agreement if the information is made available by competent authorities or by CSIRT.

<u>i) Audit obligations</u> • The Ordinance sets out a number of obligations relating to the audit of critical and important entities. • There are two possibilities for the audit: ?The periodic audit, which is carried out on a regular basis in order to assess the security measures in place, identify deficiencies and propose remedial solutions. o During the regular cybersecurity audit, a systematic assessment of all policies, procedures, and protection measures implemented within networks and IT systems is conducted to identify dysfunctions and vulnerabilities and recommend remedial measures. o Within maximum 15 business days from the date of receipt of the audit report, the entities are required to draw up and submit to NSCD and, as applicable, to the sectoral competent authority, based on the recommendations issued by the auditor, the plan of measures to remedy all deficiencies found and the deadlines for their implementation. ? The ad-hoc audit, which is exceptionally ordered by DNSC in specific cases, such as: o the occurrence of a significant security incident; o major changes in the audited entity's IT infrastructure, but no later than 180 days after the change occurs; o reasonable suspicion of a breach of the cybersecurity regulations established by the Ordinance. ? In case of an ad hoc audit, DNSC shall communicate the reasons for and the objectives of the audit. • The cybersecurity audit can only be performed by DNSC certified auditors.   <u>j) Sanctions for non-compliance with obligations</u> • The Ordinance sets out a number of misdemeanours and fines that can be imposed for non-compliance with the provisions of the Ordinance. • In case of non-compliance with key obligations established by the Ordinance (such as the obligation to notify service recipients; the obligation to adopt technical, operational and organizational measures; the obligation to implement vulnerability management processes; the obligation to submit the data requested by DNSC), DNSC and other competent authorities may impose misdemeanour-related fines up to EUR 7,000,000 (in RON equivalent) or 1.4% of the annual turnover (for important entities), and up to EUR 10,000,000 (in RON equivalent) or 2% of the annual turnover (for critical entities). The higher value between the percentage of turnover and the fixed monetary amount shall be considered for sanctioning non-compliance with the obligations and perpetration of the misdemeanours stipulated in the Ordinance. • Also, complementary measures may be ordered, such as temporary suspension of certain activities, temporary prohibition from exercising certain management positions, or ordering the entity to remedy the vulnerabilities and to inform the entity's customers. • For newly established legal entities and legal entities that have not recorded turnover in the financial year preceding the sanction, the fine for non-compliance with the obligations is set at a minimum of 1 and a maximum of 50 gross minimum wages at national level. • Fines are statute-barred in 3 years from the date of the offense. • The sanctioning decision can be appealed in court, but filing an appeal only suspends payment of the fine, not the obligation to comply with the imposed measures. k) Transitional provisions • Transitional provisions have been laid down stating that the provisions on sanctions entered into force 30 days after the publication of the Ordinance in the Official Journal of Romania. • By order of the Managing Director of DNSC the following are approved and published in the Official Journal of Romania: o the criteria and thresholds for determining the degree of disruption of a service and the methodology for assessing the risk level of the entities, within 20 days from the date of entry into force of the Ordinance o the requirements regarding the notification process for registration and the method of submitting the information, within 15 days from the date of entry into force of the Ordinance; o the risk management measures, within 120 days from the date of entry into force of the Ordinance; o the methodological rules on incident reporting, within 120 days from the date of entry into force of the Ordinance; o the national cybersecurity crisis management plan in peacetime, within 180 days from the date of entry into force of the Ordinance; o the implementing rules and the methodology for risk-based prioritization of supervisory, verification and control activities, within 120 days from the date of entry into force of the Ordinance