



2026/0012(COD)

13.10.2026

AMENDMENTS

34 - 170

Draft report

Markéta Gregorová

(PE792.221v02-00)

Amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]

Proposal for a directive

(COM(2026)0013 – 2026/0012(COD))

Amendment 34

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Recital 2

Text proposed by the Commission

(2) To reduce the burden of compliance for entities and of supervision for competent authorities, a new category of small mid-cap enterprises should be introduced in Directive (EU) 2022/2555, in line with **Commission Recommendation (EU) 2025/1099**⁴. Entities of a type referred to in Annex I to Directive (EU) 2022/2555, which qualify as small mid-cap enterprises under that **Recommendation**, should as a main rule be designated as important entities. Further, to support the Commission's goal of cutting administrative costs by 25 % overall and by 35 % for small and medium-sized enterprises, the general size-cap rule set out in Directive (EU) 2022/2555, whereby all entities which qualify as medium-sized enterprises under Article 2 of the Annex to Commission Recommendation 2003/361/EC⁵, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, fall within the scope of Directive (EU) 2022/2555, should be applied to Domain Name System service providers.

⁴ **Commission Recommendation (EU) 2025/1099 of 21 May 2025 on the definition of small mid-cap enterprises (OJ L, 2025/1099, 28.5.2025, ELI: <http://data.europa.eu/eli/reco/2025/1099/oj>).**

⁵ Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36, ELI:

Amendment

(2) To reduce the burden of compliance for entities and of supervision for competent authorities, a new category of small mid-cap enterprises should be introduced in Directive (EU) 2022/2555, in line with **Regulation (EU) XXX/XXX [Proposal for Omnibus IV]**⁴. Entities of a type referred to in Annex I to Directive (EU) 2022/2555, which qualify as small mid-cap enterprises under that **Regulation**, should as a main rule be designated as important entities. Further, to support the Commission's goal of cutting administrative costs by 25 % overall and by 35 % for small and medium-sized enterprises, the general size-cap rule set out in Directive (EU) 2022/2555, whereby all entities which qualify as medium-sized enterprises under Article 2 of the Annex to Commission Recommendation 2003/361/EC⁵, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, fall within the scope of Directive (EU) 2022/2555, should be applied to Domain Name System service providers.

⁴ **Regulation (EU) XXX/XXX [Proposal for Omnibus IV]**

⁵ Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36, ELI:

Amendment 35

Andrea Wechsler, Christian Ehler

Proposal for a directive

Recital 4

Text proposed by the Commission

(4) In order to ensure proportionality as regards electricity producers within the meaning of Article 2, point (38), of Directive (EU) 2019/944 of the European Parliament and of the Council⁶, only those electricity producers with a total generation capacity of more than 1 MW should be considered to be essential or important entities under Directive (EU) 2022/2555, provided that they meet the size-cap rule. This should encompass electricity producers where a single electricity generation facility exceeds 1 MW as well as electricity producers that operate several generation facilities which together have a generation capacity of more than 1 MW. **Such** an approach enables a balance between the need to capture those entities where interference with their network and information system could imply a loss, non-controllability or external control of generation capacity that is on its own of relevance for the security and stability of the electricity grid, and the need not to place disproportionate administrative burden on undertakings under Directive (EU) 2022/2555.

Amendment

(4) In order to ensure proportionality as regards electricity producers within the meaning of Article 2, point (38), of Directive (EU) 2019/944 of the European Parliament and of the Council⁶, only those electricity producers with a total generation capacity of more than 1 MW should be considered to be essential or important entities under Directive (EU) 2022/2555, provided that they meet the size-cap rule. This should encompass electricity producers where a single electricity generation facility exceeds 1 MW as well as electricity producers that operate several generation facilities which together have a generation capacity of more than 1 MW. ***The application of the 1 MW threshold should take account of the principal activity of an undertaking providing services in several sectors. In particular, a municipal multi-utility undertaking should not be treated as an essential or important entity solely on the basis of its electricity-generation capacity where electricity generation is ancillary to its principal activity. Member States should be able to prevent multi-utility undertakings from becoming subject to additional energy-sector cybersecurity requirements solely because they generate electricity as an ancillary activity. The obligations applicable to their principal activity should remain unaffected.*** Such an approach enables a balance between the need to capture those entities where interference with their network and

information system could imply a loss, non-controllability or external control of generation capacity that is on its own of relevance for the security and stability of the electricity grid, and the need not to place disproportionate administrative burden on undertakings under Directive (EU) 2022/2555.

⁶ Directive (EU) 2019/944 of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125; ELI: <http://data.europa.eu/eli/dir/2019/944/oj>).

⁶ Directive (EU) 2019/944 of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125; ELI: <http://data.europa.eu/eli/dir/2019/944/oj>).

Or. en

Justification

The 1 MW threshold may also capture organisations whose principal responsibility lies in another municipal service and whose electricity generation arises only in support of that service. Applying the threshold without regard to that context could extend energy-sector cybersecurity requirements beyond the entities for which they are intended. The clarification promotes a proportionate application of NIS2.

Amendment 36

Morten Løkkegaard, Bart Groothuis, Barry Andrews, Elisabetta Gualmini

Proposal for a directive

Recital 7

Text proposed by the Commission

(7) In order to enable entities providing services across several Member States to benefit from more coherent and less burdensome supervisory approaches across the internal market, such entities should be able to demonstrate compliance with specific or all cybersecurity risk-management obligations laid down in Directive (EU) 2022/2555 by obtaining a certificate on the cyber posture under a European cybersecurity certification scheme. The development of such a scheme will benefit from the adoption of

Amendment

(7) In order to enable entities providing services across several Member States to benefit from more coherent and less burdensome supervisory approaches across the internal market, such entities should be able to demonstrate compliance with specific or all cybersecurity risk-management obligations laid down in Directive (EU) 2022/2555 by ***voluntarily*** obtaining a certificate on the cyber posture under a European cybersecurity certification scheme ***that shall be recognised across the Union***. The

implementing acts on the technical and methodological as well as sectoral requirements concerning the cybersecurity risk-management measures under Directive (EU) 2022/2555 which are based on maximum harmonization.

development of such a scheme will benefit from the adoption of implementing acts on the technical and methodological as well as sectoral requirements concerning the cybersecurity risk-management measures under Directive (EU) 2022/2555 which are based on maximum harmonization. ***Where compliance has been demonstrated via such certificates, competent authorities should avoid duplicating assessments of those requirements, except where proportionate supervisory measures are necessary due to reasonable doubt that relevant requirements continue to be fulfilled.***

Or. en

Amendment 37

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Recital 7

Text proposed by the Commission

(7) In order to enable entities providing services across several Member States to benefit from more coherent and less burdensome supervisory approaches across the internal market, such entities should be able to demonstrate compliance with specific or all cybersecurity risk-management obligations laid down in Directive (EU) 2022/2555 by obtaining a certificate on the cyber posture under a European cybersecurity certification scheme. The development of such a scheme will benefit from the adoption of implementing acts on the technical and methodological as well as sectoral requirements concerning the cybersecurity risk-management measures under Directive (EU) 2022/2555 which are based on maximum harmonization.

Amendment

(7) In order to enable entities providing services across several Member States to benefit from more coherent and less burdensome supervisory approaches across the internal market, such entities should be able to demonstrate compliance with specific or all cybersecurity risk-management obligations laid down in Directive (EU) 2022/2555 by obtaining a certificate on the cyber posture under a European cybersecurity certification scheme. The development of such a scheme will benefit from the adoption of implementing acts on the technical and methodological as well as sectoral requirements concerning the cybersecurity risk-management measures under Directive (EU) 2022/2555 which are based on maximum harmonization. ***The preparation of European cybersecurity certification schemes relating to the cyber posture of***

entities should benefit from the expertise of relevant stakeholders, including the NIS Cooperation Group, competent authorities, industry representatives and the entities concerned.

Or. en

Amendment 38

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Recital 8

Text proposed by the Commission

(8) Given the continuously increasing reliance of our society and the economy on digital technologies, it is necessary to take mitigation measures against the quantum threat. The possibility of ‘harvest now - decrypt later attacks’, likely occurring already now, and the future risks induced by quantum attacks on forging signatures, as well as the planned deprecation of certain algorithm implementations and full disallowance of current public-key cryptographic algorithms, increase the urgency of initiating actions for the migration to post-quantum cryptography (PQC). Therefore, Member States should be required to adopt policies for the migration to PQC as part of their national cybersecurity strategy. Such policies should facilitate the acceleration of strategic planning and the creation of support measures and tools to assess the exposure of cryptographic assets to the risks posed by quantum computers. Further, they should assist in creating a migration plan and in testing the roll-out of PQC in digital applications and networks, while simultaneously fostering the emergence and uptake of formally verified and evaluated European PQC solutions adhering to compliance frameworks in products and services. Those policies

Amendment

(8) Given the continuously increasing reliance of our society and the economy on digital technologies, it is necessary to take mitigation measures against the quantum threat. The possibility of ‘harvest now - decrypt later attacks’, likely occurring already now, and the future risks induced by quantum attacks on forging signatures, as well as the planned deprecation of certain algorithm implementations and full disallowance of current public-key cryptographic algorithms, increase the urgency of initiating actions for the migration to post-quantum cryptography (PQC). Therefore, Member States should be required to adopt policies for the migration to PQC as part of their national cybersecurity strategy. ***Those policies should include, in particular, the identification and prioritisation of use cases according to their criticality, an inventory of relevant cryptographic assets, migration plans with appropriate implementation timelines, and risk mitigation measures for cases where timely migration is not feasible.*** Such policies should facilitate the acceleration of strategic planning and the creation of support measures and tools to assess the exposure of cryptographic assets to the risks posed by quantum computers.

should align with the milestones set out in Union legal acts and Union policies as well as documents adopted by the NIS Cooperation Group, in particular the Coordinated Implementation Roadmap for the transition to PQC, adopted by the NIS Cooperation Group in June 2025, thus achieving the migration to PQC by 2030 for critical use cases and by 2035 for medium and low level use cases.

Further, they should assist in creating a migration plan and in testing the roll-out of PQC in digital applications and networks, while simultaneously fostering the emergence and uptake of formally verified and evaluated European PQC solutions adhering to compliance frameworks in products and services. Those policies should align with the milestones set out in Union legal acts and Union policies as well as documents adopted by the NIS Cooperation Group, in particular the Coordinated Implementation Roadmap for the transition to PQC, adopted by the NIS Cooperation Group in June 2025, thus achieving the migration to PQC by 2030 for critical use cases and by 2035 for medium and low level use cases.

Or. en

Amendment 39
Markus Buchheit

Proposal for a directive
Recital 8

Text proposed by the Commission

(8) Given the continuously increasing reliance of our society and the economy on digital technologies, it is necessary to take mitigation measures against the quantum threat. The possibility of ‘harvest now - decrypt later attacks’, likely occurring already now, and the future risks induced by quantum attacks on forging signatures, as well as the planned deprecation of certain algorithm implementations and full disallowance of current public-key cryptographic algorithms, increase the urgency of initiating actions for the migration to post-quantum cryptography (PQC). Therefore, Member States should be required to adopt policies for the migration to PQC as part of their national cybersecurity strategy. Such policies should facilitate the acceleration of

Amendment

(8) Given the continuously increasing reliance of our society and the economy on digital technologies, it is necessary to take mitigation measures against the quantum threat. The possibility of ‘harvest now - decrypt later attacks’, likely occurring already now, and the future risks induced by quantum attacks on forging signatures, as well as the planned deprecation of certain algorithm implementations and full disallowance of current public-key cryptographic algorithms, increase the urgency of initiating actions for the migration to post-quantum cryptography (PQC). Therefore, Member States should be required to adopt policies for the migration to PQC as part of their national cybersecurity strategy. Such policies should facilitate the acceleration of

strategic planning and the creation of support measures and tools to assess the exposure of cryptographic assets to the risks posed by quantum computers. Further, they should assist in creating a migration plan and in testing the roll-out of PQC in digital applications and networks, while simultaneously fostering the emergence and uptake of formally verified and evaluated **European** PQC solutions adhering to compliance frameworks in products and services. Those policies should align with the milestones set out in Union legal acts and Union policies as well as documents adopted by the NIS Cooperation Group, in particular the Coordinated Implementation Roadmap for the transition to PQC, adopted by the NIS Cooperation Group in June 2025, thus achieving the migration to PQC by 2030 for critical use cases and by 2035 for medium and low level use cases.

strategic planning and the creation of support measures and tools to assess the exposure of cryptographic assets to the risks posed by quantum computers. Further, they should assist in creating a migration plan and in testing the roll-out of PQC in digital applications and networks, while simultaneously fostering the emergence and uptake of formally verified and evaluated PQC solutions adhering to compliance frameworks in products and services, ***including those based on internationally recognised standards. The concepts should be technology-neutral and should not favour any particular suppliers or regions of origin.*** Those policies should align with the milestones set out in Union legal acts and Union policies as well as documents adopted by the NIS Cooperation Group, in particular the Coordinated Implementation Roadmap for the transition to PQC, adopted by the NIS Cooperation Group in June 2025, thus achieving the migration to PQC by 2030 for critical use cases and by 2035 for medium and low level use cases.

Or. de

Amendment 40

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a directive

Recital 8 a (new)

Text proposed by the Commission

Amendment

(8a) Providers of general-purpose AI models with systemic risk and the operators of the compute infrastructure on which such models are trained and run have become a dependency of for essential and important entities, comparable to cloud computing and data centre services, and the compromise of a

model, of its parameters or of the infrastructure on which it runs can propagate to every entity relying on it. Such providers and operators should therefore be subject to Directive (EU) 2022/2555 regardless of their size. AI systems operating autonomously can circumvent containment measures and act on the network and information systems of third parties; such AI high risk security incidents, and events of the same kind involving AI systems built on other AI models, should be notified like significant incidents and forwarded to ENISA and to the AI Office, and essential and important entities should address the secure integration of AI systems in their cybersecurity risk management measures.

Or. en

Amendment 41
Diego Solier

Proposal for a directive
Recital 8 a (new)

Text proposed by the Commission

Amendment

(8a) *The following is added as 8a new*
The migration to post-quantum cryptography should be completed as rapidly as technically and economically feasible, taking into account the availability of post-quantum cryptographic solutions that are certified under European cybersecurity certification schemes and interoperable standards. Member States should work towards the migration of critical use cases by 31 December 2030 and of all other use cases by 31 December 2035, in line with the Coordinated Implementation Roadmap for the transition to PQC adopted by the NIS Cooperation Group. Member States should notify the Commission where migration within those

timelines is not technically or economically feasible for specific systems or use cases, providing reasons and a revised timeline.

Or. en

Justification

Hard migration deadlines that cannot be met in practice damage regulatory credibility and create perverse incentives. PQC-certified products meeting the necessary assurance levels may not be available in sufficient quantity by 2030 for all critical use cases, and legacy systems in energy, water, transport and defence-adjacent sectors may have multi-decade operational lifetimes. Converting the deadlines into targets with a notification mechanism maintains ambition while ensuring operational realism.

Amendment 42

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Recital 9

Text proposed by the Commission

(9) Pursuant to Article 21(2), point (d), of Directive (EU) 2022/2555, essential and important entities are to ensure an appropriate level of security in their supply chain. In practice, that obligation has led many entities to request extensive information from their suppliers through heterogeneous questionnaires, formats, and processes. While such requests aim to support due diligence and risk management, they may also create a significant administrative burden for suppliers to essential and important entities, particularly when similar information must be provided repeatedly in divergent forms. To alleviate that burden and promote a consistent, proportionate and efficient approach to supply chain security assessments, the Commission should develop guidelines to recommend an appropriate level of detail, structure, and format for such information requests. Such guidelines should facilitate harmonisation,

Amendment

(9) Pursuant to Article 21(2), point (d), of Directive (EU) 2022/2555, essential and important entities are to ensure an appropriate level of security in their supply chain. In practice, that obligation has led many entities to request extensive information from their suppliers through heterogeneous questionnaires, formats, and processes. While such requests aim to support due diligence and risk management, they may also create a significant administrative burden for suppliers to essential and important entities, particularly when similar information must be provided repeatedly in divergent forms. To alleviate that burden and promote a consistent, proportionate and efficient approach to supply chain security assessments, the Commission should develop guidelines to recommend an appropriate level of detail, structure, and format for such information requests. Such guidelines should facilitate harmonisation,

reduce unnecessary duplication, and support both entities and their suppliers in complying effectively with their obligations under Directive (EU) 2022/2555.

reduce unnecessary duplication, and support both entities and their suppliers in complying effectively with their obligations under Directive (EU) 2022/2555. ***The Commission should ensure the close involvement of relevant stakeholders, including representatives of affected industries, in the preparation of those guidelines. Those guidelines should be published without undue delay in order to facilitate their consistent implementation across the Union.***

Or. en

Amendment 43

Morten Løkkegaard, Bart Groothuis, Barry Andrews, Elisabetta Gualmini

Proposal for a directive

Recital 9

Text proposed by the Commission

(9) Pursuant to Article 21(2), point (d), of Directive (EU) 2022/2555, essential and important entities are to ensure an appropriate level of security in their supply chain. In practice, that obligation has led many entities to request extensive information from their suppliers through heterogeneous questionnaires, formats, and processes. While such requests aim to support due diligence and risk management, they may also create a significant administrative burden for suppliers to essential and important entities, particularly when similar information must be provided repeatedly in divergent forms. To alleviate that burden and promote a consistent, proportionate and efficient approach to supply chain security assessments, the Commission should develop guidelines to recommend an appropriate level of detail, structure, and format for such information requests. Such guidelines should facilitate harmonisation, reduce unnecessary duplication, and support both entities and their suppliers in

Amendment

(9) Pursuant to Article 21(2), point (d), of Directive (EU) 2022/2555, essential and important entities are to ensure an appropriate level of security in their supply chain. In practice, that obligation has led many entities to request extensive information from their suppliers through heterogeneous questionnaires, formats, and processes. While such requests aim to support due diligence and risk management, they may also create a significant administrative burden for suppliers to essential and important entities, particularly when similar information must be provided repeatedly in divergent forms. To alleviate that burden and promote a consistent, proportionate and efficient approach to supply chain security assessments, the Commission should, ***while taking into account existing European and international standards,*** develop guidelines to recommend an appropriate level of detail, structure, and format for such information requests. Such guidelines should facilitate harmonisation,

complying effectively with their obligations under Directive (EU) 2022/2555.

reduce unnecessary duplication, and support both entities and their suppliers in complying effectively with their obligations under Directive (EU) 2022/2555.

Or. en

Amendment 44

Morten Løkkegaard, Bart Groothuis, Barry Andrews

Proposal for a directive

Recital 10

Text proposed by the Commission

(10) Ransomware attacks in which malware encrypts data and systems and demands a ransom payment for release remain one of the prime threats to essential and important entities. Harmonising and improving the collection of data on ransomware attacks from affected essential and important entities would provide insights to computer security incident response teams (CSIRTs) and national authorities enabling them to ensure that future ransomware interventions are appropriate and effective, to support entities in growing their resilience and preventing future attacks, and to compile the intelligence and evidence that law enforcement agencies need to disrupt and dismantle ransomware gangs and sanction their operatives. Given the potentially sensitive nature of information to be shared regarding ransomware attacks, in particular whether an entity has paid a ransom, and if so, what amount and to whom, such information should only be submitted to CSIRTs or, where applicable, competent authorities upon their request. For the purpose of such information exchange, essential and important entities are encouraged to appoint a person that acts as a point of contact and ensures the confidentiality and trustworthiness of the information exchange. In the context of the

Amendment

(10) Ransomware attacks in which malware encrypts data and systems and demands a ransom payment for release remain one of the prime threats to essential and important entities. Harmonising and improving the collection of data on ransomware attacks from affected essential and important entities, ***where this information is available to those entities***, would provide insights to computer security incident response teams (CSIRTs) and national authorities enabling them to ensure that future ransomware interventions are appropriate and effective, to support entities in growing their resilience and preventing future attacks, and to compile the intelligence and evidence that law enforcement agencies need to disrupt and dismantle ransomware gangs and sanction their operatives. Given the potentially sensitive nature of information to be shared regarding ransomware attacks, in particular whether an entity has paid a ransom, and if so, what amount and to whom, such information should ***be subject to strict protection and only be submitted to CSIRTs or, where applicable, competent authorities upon their request. Information submitted should be subject to relevant retention limits***. For the purpose of such information exchange, essential and important entities

International Counter Ransomware Initiative, the Union has endorsed a non-binding international policy statement whereby relevant institutions under the authority of the participating national governments should not pay ransomware extortion demands.

are encouraged to appoint a person that acts as a point of contact and ensures the confidentiality and trustworthiness of the information exchange. In the context of the International Counter Ransomware Initiative, the Union has endorsed a non-binding international policy statement whereby relevant institutions under the authority of the participating national governments should not pay ransomware extortion demands.

Or. en

Amendment 45

Morten Løkkegaard, Bart Groothuis, Barry Andrews, Elisabetta Gualmini

Proposal for a directive

Recital 11 a (new)

Text proposed by the Commission

Amendment

(11a) Reporting the same incident under different Union legal acts, and through different national procedures, places an undue administrative burden on entities. Therefore, entities should not be required to submit the same information more than once. To facilitate this, Member States should reuse existing documentation whenever possible. Where all required information has been submitted through the single-entry point, within relevant deadlines, separate national reporting should not be required.

Or. en

Amendment 46

Morten Løkkegaard, Bart Groothuis, Barry Andrews, Elisabetta Gualmini

Proposal for a directive

Recital 12

Text proposed by the Commission

Amendment

(12) Given the cross-border dimension of many essential and important entities across the internal market and the need to ensure coherence and promote convergence and efficiency in relation to supervisory approaches, ENISA should support Member States in carrying out mutual assistance for essential and important entities which provide services in more than one Member State or which provide services in one or more Member States and have their network and information systems located in one or more other Member States. For that purpose, Member States should submit additional information to the registry of entities maintained by ENISA. Based on the information contained in the registry of essential and important entities, ENISA should conduct a comprehensive analysis on cross-border cybersecurity risks relating to essential and important entities. The analysis should be based on a methodology developed together with the Commission and the NIS Cooperation Group. That methodology could take into account the degree to which essential and important entities deploy their services on a wide cross-border basis, rely on cross-border services, are exposed to a supply chain concentration risk, can be identified as a source of supply chain concentration risk, are exposed to incidents that could have significant disruptive effects to cross-border services, or rely on network and information systems for the provision of their services that are located across different Member States and outside the Union. Based on the risk analysis report, ENISA should recommend to the relevant competent authorities to set up joint examination teams to support the supervision of entities with a higher degree of risk for the smooth functioning of the internal market in case of incidents and assist the competent authorities in the execution of joint supervisory actions upon their request.

(12) Given the cross-border dimension of many essential and important entities across the internal market and the need to ensure coherence and promote convergence and efficiency in relation to supervisory approaches, ENISA should support Member States in carrying out mutual assistance for essential and important entities which provide services in more than one Member State or which provide services in one or more Member States and have their network and information systems located in one or more other Member States. ***Where it is necessary*** for that purpose, Member States should submit additional information to the registry of entities maintained by ENISA. Based on the information contained in the registry of essential and important entities, ENISA should conduct a comprehensive analysis on cross-border cybersecurity risks relating to essential and important entities. The analysis should be based on a methodology developed together with the Commission and the NIS Cooperation Group. That methodology could take into account the degree to which essential and important entities deploy their services on a wide cross-border basis, rely on cross-border services, are exposed to a supply chain concentration risk, can be identified as a source of supply chain concentration risk, are exposed to incidents that could have significant disruptive effects to cross-border services, or rely on network and information systems for the provision of their services that are located across different Member States and outside the Union. Based on the risk analysis report, ENISA should recommend to the relevant competent authorities to set up joint examination teams to support the supervision of entities with a higher degree of risk for the smooth functioning of the internal market in case of incidents and assist the competent authorities in the execution of joint supervisory actions upon their request.

Amendment 47
Katri Kulmuni, Eero Heinäluoma

Proposal for a directive
Recital 12 a (new)

Text proposed by the Commission

Amendment

(12a) The registry maintained by ENISA should comply with the principle of data minimisation. The information on the entities' IP ranges is not necessary at Union level for the purposes of the registry and should remain with the national competent authorities. Noting principle of data minimization, only information on IP ranges that the entity continuously uses should be submitted to the national competent authorities. The registry should be protected by state-of-the-art technical and organisational measures designed in consultation with the European Data Protection Supervisor.

Or. en

Justification

Submission and updating information of dynamic IP ranges or IP ranges that are used only for short period of time is not feasible for the purposes of NIS2. It's also in conflict with the principle of data minimisation. Currently it is not clear whether NIS2 requires that, and therefore adding it to new recital would give valuable guidance to both competent authorities and NIS2 entities for application.

Amendment 48
Bart Groothuis, Morten Løkkegaard, Barry Andrews, Ivars Ijabs

Proposal for a directive
Recital 14 a (new)

Text proposed by the Commission

Amendment

(14a) Managed security service providers (MSSPs) process real-time telemetry, sensor and logging data from

the essential and important entities they serve. That data is often decisive for early threat detection and cross-sector situational awareness, but it is not always available to CSIRTs, who may have additional cyber threat intelligence. Regulation (EU) 2025/38 provides for the voluntary sharing of such data between MSSPs and CSIRTs. To complement it, a CSIRT should be able, by means of a duly reasoned request, to require MSSPs to provide such data concerning the essential and important entities that operate within the respective Member State, where this is necessary and proportionate for a CSIRT's tasks of monitoring significant cyber threats or significant incidents and for issuing early warnings and alerts. Such requests should be targeted and limited in time. The data requested should be limited to what is strictly necessary, giving priority to indicators of compromise and to aggregated or pseudonymised data, and should not include the content of communications. In case of a potential or ongoing cyber incident, the CSIRT should, in return and where possible, provide the managed security service provider with relevant cyber threat intelligence concerning the essential or important entity they serve.

Or. en

Justification

Corresponding recital to the changes in Article 11 of NIS2.

Amendment 49
Christophe Grudler, Morten Løkkegaard

Proposal for a directive
Recital 14 a (new)

Text proposed by the Commission

Amendment

(14a) The increasing dependence of

essential societal and economic activities on space-based services calls for broader cybersecurity coverage of the space sector. The scope of Directive (EU) 2022/2555 should therefore be extended, beyond the operators of ground-based infrastructure already covered, to space operators, including those operating Union-owned assets, collision avoidance space services providers and primary providers of space-based data. Ownership of the assets concerned by the Union should not, in itself, exclude their operators from the scope of that Directive.

Or. en

Amendment 50

Bart Groothuis, Morten Løkkegaard, Barry Andrews, Ivars Ijabs

Proposal for a directive

Recital 14 b (new)

Text proposed by the Commission

Amendment

(14b) Providers of internet access services are well placed to reduce malicious traffic before it reaches connected networks of essential and important entities. They should therefore take appropriate and proportionate traffic management measures aimed at the mitigation of distributed denial-of-service attacks and protective measures at the level of the domain name system against phishing and other malicious domain names. Those measures should be limited to serve cybersecurity purposes and should rely only on traffic data, not on the content of communications. They should be based on objective, documented and regularly reviewed criteria and on reliable threat information, and should be maintained only for as long as necessary. They should be transparent and respect end-users' freedom to choose a DNS resolver, allow end-users to deactivate DNS-level protection easily and free of

charge. To ensure a consistent approach across the Union, the Commission may lay down the technical and methodological requirements for those measure by means of implementing acts, after consulting ENISA and BEREC.

Or. en

Justification

Corresponding recital to the changes in Article 7 and 21 of NIS2.

Amendment 51

Christophe Grudler, Morten Løkkegaard

Proposal for a directive

Article 1 – paragraph 1 – point 1 – point a – point ii – introductory part

Text proposed by the Commission

Amendment

(ii) the following points (iv) **and (v)** are added:

(ii) the following points (iv), **(v) and (va)** are added:

Or. en

Amendment 52

Christophe Grudler, Morten Løkkegaard

Proposal for a directive

Article 1 – paragraph 1 – point 1 – point a – point ii

Directive (EU) 2022/2555

Article 2 – paragraph 2 – point a

Text proposed by the Commission

Amendment

(va) entities of a type referred to in point (11) of Annex I;

Or. en

Justification

Even a small company may control satellites or ground infrastructure whose compromise could have serious consequences. This amendment ensures that all types of entity listed in the

space sector are covered regardless of size, while preserving proportionate obligations and the distinction between essential and important entities.

Amendment 53

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 1 – point a – point ii a (new)

Directive (EU) 2022/2555

Article 2 – paragraph 2a (new)

Text proposed by the Commission

Amendment

(iia) The following part is added to Article 2 – paragraph 2a (new)

Article 2 of Directive (EU) 2022/2555 establishes the scope of the Directive, including definitions of essential and important entities based on size thresholds set out in Article 3. Member States may exempt from the obligations of this Directive entities with fewer than 10 employees and an annual turnover or annual balance sheet not exceeding EUR 2 million, where such entities do not provide services critical to the continuity of essential or important services.

Or. en

Justification

The NIS2 Directive already raised thresholds beyond NIS1. A further amending directive must not expand compliance burdens without a proportionality impact assessment. Micro-enterprises face disproportionate compliance costs with negligible systemic risk reduction. This amendment allows Member States to apply proportionate exemptions for the smallest entities that do not pose systemic risk.

Amendment 54

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a directive

Article 1 – paragraph 1 – point 1 – point a – point ii a (new)

Text proposed by the Commission

Amendment

(iia) (iia) the following point (vi) is added:

‘(vi) providers of general-purpose AI models with systemic risk within the meaning of Article 51 of Regulation (EU) 2024/1689 and operators of AI compute infrastructure, including AI Factories established pursuant to Council Regulation (EU) 2021/1173;’

Or. en

Amendment 55
Christophe Grudler, Morten Løkkegaard

Proposal for a directive
Article 1 – paragraph 1 – point 1 – point a a (new)
Directive (EU) 2022/2555
Article 2

Text proposed by the Commission

Amendment

(aa) (b) the following paragraph 2a is inserted:

‘2a. The references to Regulation (EU) [...] in point (11) of Annex I identify the types of entity concerned.^{1a}

For space objects launched before [the date of application of this amending Directive], the measures required under Article 21 shall not require onboard hardware or software modifications where these are technically impossible.

The entities concerned shall document those technical constraints and implement appropriate and proportionate compensating measures. Their obligations concerning the ground segment, governance and incident reporting remain applicable.’;

^{1a} Regulation (EU) [...] [Proposal for a Regulation on the safety, resilience and sustainability of Space activities in the Union.].;

Or. en

Justification

The reference to the Space Act identifies the types of actor concerned. For space objects launched before the new rules apply, this amendment avoids requiring technically impossible onboard modifications.

Amendment 56

Katri Kulmuni, Eero Heinäluoma

Proposal for a directive

Article 1 – paragraph 1 – point 1 – point b

(EU) 2022/2555

Article 1 – paragraph 3a

Text proposed by the Commission

Amendment

Regardless of their size, this Directive applies to entities identified as owners, managers and operators of strategic dual-use infrastructure under Regulation (EU) [...]**.

deleted

Or. en

Justification

It is sufficient that NIS2 applies to owners, managers and operators of strategic dual-use infrastructure where they are designated as critical entities under the CER Directive, whose provisions are already in force. An open reference to this definition and Regulation could create legal uncertainty regarding the scope of NIS2, particularly for SMEs. Therefore, this paragraph should be removed.

Amendment 57

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Article 1 – paragraph 1 – point 1 a (new)

Directive (EU) 2022/2555

Article 2, paragraph 1, new subparagraph

Text proposed by the Commission

Amendment

(1a) in paragraph 1, the following subparagraph is added:

For the purposes of determining whether an entity falls within the scope of this Directive, Member States shall have regard to the entity's main activity. Ancillary or purely internal activities shall not in themselves bring an entity within scope unless they constitute the provision of a service referred to in Annex I or Annex II.

Or. en

Amendment 58
Markus Buchheit

Proposal for a directive
Article 1 – paragraph 1 – point 2 – point a – point i
Directive (EU) 2022/2555
Article 1 – paragraph 1 – point 2 – point a i

Text proposed by the Commission

Amendment

(a) entities of a type referred to in Annex I which exceed the ceilings for small mid-cap enterprises;

(a) entities of a type referred to in Annex I which exceed the ceilings for small mid-cap enterprises ***within the meaning of Article 6(42);***

Or. de

Amendment 59
Markéta Gregorová
on behalf of the Verts/ALE Group
Jens Geier
on behalf of the S&D Group

Proposal for a directive
Article 1 – paragraph 1 – point 2 – point a – point i
Directive (EU) 2022/2555
Article 3(1), point (b)

Text proposed by the Commission

Amendment

(b) qualified trust service providers, providers of European Digital Identity Wallets, providers of European Business Wallets and top-level domain name registries, regardless of their size;;

(b) qualified trust service providers, providers of European Digital Identity Wallets, providers of European Business Wallets, ***providers of general-purpose AI models with systemic risk, operators of AI compute infrastructure*** and top-level domain name registries, regardless of their size;;

Or. en

Amendment 60

Katri Kulmuni, Eero Heinäluoma

Proposal for a directive

Article 1 – paragraph 1 – point 2 – point a – point ii

(EU) 2022/2555

Article 1 – Paragraph 2(a)(ii)

Text proposed by the Commission

Amendment

(h) entities identified as owners, managers and operators of strategic dual-use infrastructure under Regulation (EU) [...] [Proposal for a Regulation of the European Parliament and of the Council on establishing a framework of measures to facilitate the transport of military equipment, goods and personal across the Union].;

deleted

Or. en

Justification

It is sufficient that NIS2 applies to owners, managers and operators of strategic dual-use infrastructure where they are designated as critical entities under the CER Directive, whose provisions are already in force. An open reference to this definition and Regulation could create legal uncertainty regarding the scope of NIS2, particularly for SMEs. Therefore, this paragraph should be removed.

Amendment 61

Christophe Grudler, Morten Løkkegaard

Proposal for a directive

Article 1 – paragraph 1 – point 2 – point a – point ii a (new)

Directive (EU) 2022/2555

Article 3, paragraph 1

Text proposed by the Commission

Amendment

(iia) the following point (i) is added:‘

(i) entities of a type referred to in point (11) of Annex I identified by a Member State as essential because a compromise of their services or operational control could cause a significant disruption of critical societal or economic activities or a severe impact on public safety, regardless of their size.’;

Or. en

Justification

The importance of a space service depends on its role and the consequences of disruption, not only on the operator’s size. This amendment allows Member States to identify space-sector entities as essential where their compromise could seriously disrupt vital activities or threaten public safety.

Amendment 62

Katri Kulmuni, Eero Heinäluoma

Proposal for a directive

Article 1 – paragraph 1 – point 2 – point b

(EU) 2022/2555

Article 1 – Paragraph 2(b)

Text proposed by the Commission

Amendment

(e) the Member States where the entity provides services;

(e) the Member States where the entity provides services **and, where applicable, names of other legal establishments in the Union and the unique identifier of other legal establishments in the Union;**

Or. en

Justification

Where an entity has both its main establishment and other legal establishments in the Union, the entity should, in addition to the address, submit the following information on its other

legal establishments: 1) the names of other legal establishments in the Union; and 2) the unique identifiers of those establishments. This would facilitate cross-border supervision, cross-border crisis management and incident notification.

Amendment 63
Ondřej Krutílek

Proposal for a directive
Article 1 – paragraph 1 – point 2 – point b
Directive (EU) 2022/2555
Article 3

Text proposed by the Commission

(e) the Member States where *the entity provides* services;

Amendment

(e) the Member States where *they provide* services *falling within the scope of this Directive, where applicable*;

Or. en

Amendment 64
Markus Buchheit

Proposal for a directive
Article 1 – paragraph 1 – point 2 – point b
Directive (EU) 2022/2555
Article 1 – Paragraph 1(2)(b)

Text proposed by the Commission

(f) the entity's IP ranges.;

Amendment

(f) *in the case of the entities referred to in Article 26(1)(b), the entity's IP ranges.*

Or. de

Amendment 65
Katri Kulmuni, Eero Heinäluoma

Proposal for a directive
Article 1 – paragraph 1 – point 2 – point b
(EU) 2022/2555
Article 1 – Paragraph 2(b)

Text proposed by the Commission

Amendment

(f) the **entity's** IP ranges.;

(f) the IP ranges ***that the entity continuously uses.***';

Or. en

Justification

The article should explicitly exclude dynamic IP addresses in order to improve legal certainty. The submission and updating of information on dynamic IP ranges or IP ranges used only for short periods is not feasible for the purposes of this list.

Amendment 66

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 3

Directive 2022/2555

Article 5

Text proposed by the Commission

Amendment

Without prejudice to Article 21(5), fifth subparagraph, this Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law.;

This Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law, ***and shall be without prejudice to the Member States' responsibilities pursuant to Article 4(2) of the Treaty on European Union pertaining to national security and the protection of their essential functions, including the protection of their critical infrastructures, essential services, security of supply and essential security interests;***

Or. fr

Amendment 67

Ondřej Krutílek

Proposal for a directive

Article 1 – paragraph 1 – point 3

Directive (EU) 2022/2555

Article 5

Text proposed by the Commission

Without prejudice to Article 21(5), fifth subparagraph, this Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law.;

Amendment

This Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law.;

Or. en

Amendment 68

Morten Løkkegaard, Bart Groothuis

Proposal for a directive

Article 1 – paragraph 1 – point 3

Directive (EU) 2022/2555

Article 5

Text proposed by the Commission

Without prejudice to Article 21(5), fifth subparagraph, this Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law.;

Amendment

Without prejudice to Article ***14a and*** 21(5), fifth subparagraph, this Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law.;

Or. en

Amendment 69

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a directive

Article 1 – paragraph 1 – point 4 – paragraph 2 – introductory part

Text proposed by the Commission

the following points (42) **and (43)** are added:

Amendment

the following points (42), **(43), (44), (45)** are added:

Or. en

Amendment 70

Andrea Wechsler, Christian Ehler

Proposal for a directive

Article 1 – paragraph 1 – point 4 – paragraph 2

Directive (EU) 2022/2555

Article 6, point (42) is inserted:

Text proposed by the Commission

(42) 'small mid-cap enterprise' means a small mid-cap enterprise as defined in the Annex to Commission Recommendation (EU) 2025/1099***;

Amendment

(42) 'small mid-cap enterprise' means a small mid-cap enterprise as defined in the Annex to Commission Recommendation (EU) 2025/1099*** ***For the purposes of this Directive, ownership or control by one or more local or regional authorities shall not prevent an undertaking from qualifying as a small mid-cap enterprise, provided that it carries out an economic activity and meets the applicable size criteria ;***

Or. en

Justification

The introduction of a small mid-cap category should preserve the balance already established by NIS2 for enterprises with public-sector participation. Otherwise, municipal service providers could face different compliance requirements from comparable undertakings solely because of their ownership structure.

Amendment 71

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Article 1 – paragraph 1 – point 4 – paragraph 2

Directive (EU) 2022/2555

Article 6, point 42

Text proposed by the Commission

Amendment

(42) 'small mid-cap enterprise' means a small mid-cap enterprise as defined in *the Annex to Commission Recommendation (EU) 2025/1099****;

(42) 'small mid-cap enterprise' means a small mid-cap enterprise as defined in *Regulation (EU) XXX/XXX* *** [*Proposal for Omnibus IV*];

Or. en

Amendment 72

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Article 1 – paragraph 1 – point 4 – paragraph 2

Directive (EU) 2022/2555

Article 6, point 42

Text proposed by the Commission

Amendment

*** *Commission Recommendation (EU) 2025/1099 of 21 May 2025 on the definition of small mid-cap enterprises (OJ L, 2025/1099, 28.5.2025, ELI: <http://data.europa.eu/eli/reco/2025/1099/oj>).*;

*** *Regulation (EU) XXX/XXX [Proposal for Omnibus IV].;*

Or. en

Amendment 73

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a directive

Article 1 – paragraph 1 – point 4 – paragraph 2

Directive (EU) 2022/2555

Article 6

Text proposed by the Commission

Amendment

(43a) (44) '*agentic AI system*' means an *agentic AI system as defined in Article 2, point (50b), of Regulation (EU) .../...*

[CSA2]; (45) ‘AI high risk security incident’ means an AI high risk security incident as defined in Article 2, point (50c), of Regulation (EU) .../... [CSA2].

Or. en

Amendment 74

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a directive

Article 1 – paragraph 1 – point 4 – paragraph 2

Directive (EU) 2022/2555

Article 6

Text proposed by the Commission

Amendment

(43b) (45) ‘AI high risk security incident’ means an AI high risk security incident as defined in Article 2, point (50c), of Regulation (EU) .../... [CSA2].

Or. en

Amendment 75

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 5

Directive (EU) 2022/2555

Article 7 – paragraph 2 – point k

Text proposed by the Commission

Amendment

(k) for the transition to post-quantum cryptography, taking into account the transition timelines and relevant requirements set out in applicable Union legal acts and policies.;

(k) for the transition to post-quantum cryptography, ***working towards the migration of critical use cases by 31 December 2030 and of all other use cases by 31 December 2035, in line with the Coordinated Implementation Roadmap of the NIS Cooperation Group, taking into account the availability of certified post-quantum cryptographic solutions, the***

operational constraints of legacy systems, and the proportionate costs for the entities concerned, and taking into account the transition timelines and relevant requirements set out in applicable Union legal acts and policies.;

Or. en

Justification

National cybersecurity strategies should promote an ambitious but realistic PQC transition. Mandatory migration language that ignores certified-product availability, legacy-system constraints and proportionate costs risks paper compliance. Working-towards targets preserve the 2030/2035 ambition while allowing operationally grounded planning.

Amendment 76

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Article 1 – paragraph 1 – point 5

Directive (EU) 2022/2555

Article 7, point 2(k)

Text proposed by the Commission

(k) for the transition to post-quantum cryptography, taking into account the transition timelines and relevant requirements set out in applicable Union legal acts and policies.;

Amendment

(k) for the transition to post-quantum cryptography, taking into account the transition timelines and relevant requirements set out in applicable Union legal acts and policies, *including the identification and prioritisation of critical use cases, the inventory of relevant cryptographic assets, the establishment of migration plans, and appropriate risk assessment and mitigation measures where timely migration cannot be achieved.*;

Or. en

Amendment 77

Morten Løkkegaard, Bart Groothuis

Proposal for a directive

Article 1 – paragraph 1 – point 5

Directive (EU) 2022/2555

Article 7(2), point (k)

Text proposed by the Commission

(k) for the transition to post-quantum cryptography, ***taking into account*** the transition timelines and relevant requirements set out in applicable Union legal acts and policies.;

Amendment

(k) for the transition to post-quantum cryptography, ***including policies to identify critical, medium and low level use cases, establishing risk-based plans for migration to post-quantum cryptography and addressing residual risks where migration is not completed according to those plans, according to*** the transition timelines and relevant requirements set out in applicable Union legal acts and policies.;

Or. en

Amendment 78

Morten Løkkegaard, Bart Groothuis, Barry Andrews

Proposal for a directive

Article 1 – paragraph 1 – point 5 a (new)

Directive (EU) 2022/2555

Article 14a (new)

Text proposed by the Commission

Amendment

(5a) the following Article is inserted:

‘Article 14a

Harmonised application of this Directive

1. To ensure a consistent and proportionate application of this Directive across the Union, the Commission shall, in cooperation with the Cooperation Group and ENISA, adopt a delegated act in accordance with Article 38 on the harmonised interpretation and application of key obligations under this Directive. This act shall, in particular, address:

(a) the classification of entities as essential or important entities, including the avoidance of additional or diverging national categorisations beyond those provided for in this Directive;

(b) the conditions under which cybersecurity audits, assessments or equivalent supervisory measures may be required, including their frequency and scope;

(c) registration, notification, and reporting obligations applicable to entities operating in more than one Member State and;

(d) common criteria for the application of proportionality in supervisory and enforcement practices.'

Or. en

Justification

The targeted revision of the NIS2 directive must ensure a greater level of harmonised implementation across the Union. This amendment is tabled with reference to parallel negotiations on the NIS2 directive as part of the Digital Omnibus.

Amendment 79 **Diego Solier**

Proposal for a directive

Article 1 – paragraph 1 – point 5 a (new)

Directive (EU) 2022/2555

Article 12 – paragraph 2 – subparagraph 1a (new)

Text proposed by the Commission

Amendment

(5a) The following is added as Article 12 – paragraph 2 – subparagraph 1a (new)

ENISA shall establish and maintain the European Union Vulnerability Database (EUVDB) to collect and publish information on vulnerabilities affecting ICT products and services used by essential and important entities. ENISA shall accept voluntary vulnerability registrations from entities not subject to this Directive and from security researchers acting in good faith under a responsible disclosure policy. ENISA shall publish aggregate statistics on vulnerability categories and remediation

timelines in its annual threat landscape report.

Or. en

Justification

A closed, mandatory-only vulnerability database provides less complete threat intelligence than one that allows voluntary contributions. Open-source community and private-sector actors who discover vulnerabilities outside regulated sectors should have a clear, trusted channel for responsible disclosure. Voluntary participation enriches the database without imposing new obligations.

Amendment 80

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a directive

Article 1 – paragraph 1 – point 5 a (new)

Directive (EU) 2022/2555

Article 14(4)

Text proposed by the Commission

Amendment

(5a) *(5a) in Article 14(4), the following point is added:*

‘ (s) exchanging, with the AI Office established by Commission Decision C(2024) 390 and with the scientific panel of independent experts established pursuant to Article 68 of Regulation (EU) 2024/1689, information on systemic cybersecurity risks arising from general-purpose AI models, and agreeing with ENISA the methodology for the coordinated security risk assessment referred to in Article 99(1a) of Regulation (EU) .../... [CSA2]. ’

Or. en

Amendment 81

Ondřej Krutílek

Proposal for a directive
Article 1 – paragraph 1 – point 5 a (new)
Directive (EU) 2022/2555
in Article 14 – paragraph 4

Present text

to carry out coordinated security risk assessments of critical supply chains in accordance with Article 22(1);

Amendment

(5 a) in Article 14(4), point (i) is replaced by the following:

"to carry out coordinated security risk assessments of critical supply chains in accordance with Article 22(1) **on the basis of a roadmap setting their order and priority**;"

Or. en

(Directive (EU) 2022/2555)

Amendment 82

Bart Groothuis, Morten Løkkegaard, Barry Andrews, Ivars Ijabs

Proposal for a directive
Article 1 – paragraph 1 – point 5 a (new)

Text proposed by the Commission

Amendment

(5a) Article 7, Paragraph 2, point (j) is amended as follows:

promoting active cyber protection, including protective DNS measures

Or. en

Amendment 83

Bart Groothuis, Morten Løkkegaard, Barry Andrews, Ivars Ijabs

Proposal for a directive
Article 1 – paragraph 1 – point 5 b (new)

Text proposed by the Commission

Amendment

(5b) Article 11, Paragraph 4 is amended as follows:

4. The CSIRTs shall establish cooperation

relationships with relevant stakeholders in the private sector, with a view to achieving the objectives of this Directive. This includes the exchange, where possible in real-time, of relevant data for the purpose of detecting and preventing cyber threats and incidents affecting essential and important entities.

Member States shall ensure that, where necessary and proportionate for the performance of the tasks referred to in paragraph 3, points (a) and (b), the CSIRT or the competent authority may, by means of a duly reasoned request, require a managed security service provider, which provides services to essential or important entities, to provide it with telemetry, sensor or logging data relating to those entities.

The request shall specify:

- (a) the categories of data requested, which shall be limited to what is strictly necessary for the tasks described in the previous subparagraph;*
- (b) the duration and, where applicable, the frequency of the data provision, as well as the data retention period;*
- (c) the technical modalities for the provision of the data, including format and means of secure transmission, taking into account the technical capabilities of the managed security service provider.*

Data obtained under this Paragraph shall:

- (a) not include the content of communications;*
- (b) not disclose proprietary information or trade secret from the managed security service provider;*
- (c) be used only for the tasks referred to in paragraph 3, points (a) and (b), and shall not be used as evidence in supervisory or enforcement proceedings against the entity concerned or the managed security service provider;*
- (d) be protected by appropriate technical and organisational measures, with access restricted to authorised CSIRT staff, and*

deleted once no longer necessary for the stated purpose.

The Commission may adopt implementing acts laying down the technical and the methodological requirements and modalities of the request.

Or. en

Justification

Advanced persistent threat actors increasingly exploit vulnerabilities in critical networks, in particular legacy systems, and can stay undetected for long periods. MSSPs see this activity across many clients that are critical or important entities. As a matter of sovereignty and for the purpose and to enhance situational awareness, the national CSIRT responsible for protecting those entities should have access to the relevant telemetry, logging and and sensor data. A CSIRT that can combine this with its own cyber threat intelligence, allowing it to be better positioned to spot campaigns or to respond more quickly in case of an incident. This amendment builds on the voluntary sharing of such data that is already established in the Cyber Solidarity Act.

Amendment 84

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 5 b (new)

Directive (EU) 2022/2555

Article 14a (new)

Text proposed by the Commission

Amendment

(5b) Article 14a (new)

Harmonised application

1. To ensure a consistent and proportionate application of this Directive across the Union, the Commission shall, by ... [12 months after the date of entry into force of this amending Directive], in cooperation with the NIS Cooperation Group and ENISA, issue guidance on the harmonised interpretation and application of key obligations under this Directive. Such guidance shall address in particular: (a) the classification of entities as essential or important entities, including the avoidance of additional or diverging national categorisations beyond

those provided for in this Directive; (b) the conditions under which cybersecurity audits, assessments or equivalent supervisory measures may be required, including their frequency and scope; (c) registration, notification and reporting obligations applicable to entities operating in more than one Member State; (d) the application of proportionality in supervisory and enforcement practices, including avoiding the imposition of disproportionate administrative burden on micro and small enterprises; (e) the avoidance of gold-plating and of additional national requirements beyond those provided for in this Directive that have not been justified by specific national threat assessments.

2. Member States shall have regard to that guidance when implementing and applying this Directive. The guidance shall be without prejudice to the competence of Member States to adopt measures providing for a higher level of cybersecurity proportionate to the specific threat environment of their critical infrastructure, provided such measures are compatible with Union law and are notified to the Commission. The Commission shall assess notified measures and may issue a reasoned opinion where it considers the measure incompatible with Union law.

Or. en

Justification

Harmonised application guidance reduces internal-market fragmentation, but a rigid obligation to refrain from additional national measures would prevent Member States from responding to specific threat environments. Replacing that lock with a notification mechanism preserves national security prerogatives while ensuring transparency. Adding gold-plating avoidance and SME proportionality to the guidance scope addresses implementation burden.

Amendment 85
Diego Solier

Proposal for a directive
Article 1 – paragraph 1 – point 6 a (new)
Directive (EU) 2022/2555
Article 19 – paragraph 1

Present text

Member States *shall ensure that* essential entities *are subject to regular peer reviews of* their cybersecurity risk management measures *at intervals not exceeding three years*.

Amendment

(6 a) Article 19 is amended as follows:

"Member States *may establish voluntary peer review mechanisms for* essential entities *to improve* their cybersecurity risk management measures. *Member States may require peer reviews where a significant incident has occurred or where there is documented evidence of serious inadequacy in an entity's risk management measures.*"

Or. en

(2022/2555)

Justification

Mandatory peer reviews at fixed intervals create a compliance-driven culture rather than a genuine security-improvement culture. Voluntary peer reviews with targeted mandatory triggers for high-risk situations achieve the security objective while respecting Member State autonomy and reducing administrative burden.

Amendment 86
Ondřej Krutílek

Proposal for a directive
Article 1 – paragraph 1 – point 7 – point a
Directive (EU) 2022/2555
Article 21(5)

Text proposed by the Commission

The Commission may adopt implementing acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph. The Commission shall **regularly assess**

Amendment

The Commission may adopt implementing acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph. The Commission shall **carry out an open,**

whether implementing acts *referred to in this subparagraph shall be adopted for specific sectors or types of entities to improve the functioning of the internal market*. When preparing *such assessments*, the Commission shall focus in particular on the cross-border nature of sectors or types of entities *and shall carry out an open, transparent and inclusive consultation process with relevant stakeholders and Member States*.;

transparent and inclusive consultation process with relevant Member States and stakeholders in order to determine the relevance and the need for implementing acts. When preparing *the implementing acts*, the Commission shall focus in particular on the cross-border nature of sectors or types of entities.;

Or. en

Amendment 87
Markus Buchheit

Proposal for a directive
Article 1 – paragraph 1 – point 7 – point a
Directive (EU) 2022/2555
Article 1 – Paragraph 1(7)(a)

Text proposed by the Commission

The Commission may adopt implementing acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph. *The Commission shall regularly assess whether implementing acts referred to in this subparagraph shall be adopted for specific sectors or types of entities to improve the functioning of the internal market*. When preparing such *assessments*, the Commission shall focus in particular on the cross-border nature of sectors or types of entities and shall carry out an open, transparent and inclusive consultation process with relevant stakeholders and Member States.;

Amendment

The Commission may, *at the request of the Cooperation Group*, adopt implementing acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph. When preparing such *implementing acts*, the Commission shall focus in particular on the cross-border nature of sectors or types of entities and shall carry out an open, transparent and inclusive consultation process with relevant stakeholders and Member States. *Prior to adoption, the Commission shall carry out an impact assessment setting out the compliance costs, in particular for SMEs and small mid-cap enterprises*.

Or. de

Amendment 88

Morten Løkkegaard, Bart Groothuis, Barry Andrews

Proposal for a directive

Article 1 – paragraph 1 – point 7 – point a

Directive (EU) 2022/2555

Article 21(5)

Text proposed by the Commission

The Commission may adopt **implementing** acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph. The Commission shall regularly assess whether implementing acts referred to in this subparagraph shall be adopted for specific sectors or types of entities to improve the functioning of the internal market. When preparing such assessments, the Commission shall focus in particular on the cross-border nature of sectors or types of entities and shall carry out an open, transparent and inclusive consultation process with relevant stakeholders and Member States.;

Amendment

The Commission may adopt **delegated** acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph. The Commission shall regularly assess whether implementing acts referred to in this subparagraph shall be adopted for specific sectors or types of entities to improve the functioning of the internal market. When preparing such assessments, the Commission shall focus in particular on the cross-border nature of sectors or types of entities and shall carry out an open, transparent and inclusive consultation process with relevant stakeholders and Member States.;

Or. en

Justification

Linked to Article 5 and 14a (new).

Amendment 89

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 7 – point a a (new)

Directive (EU) 2022/2555

Article 21 – paragraph 5 – subparagraph 2

Text proposed by the Commission

Amendment

(aa) Article 21 – paragraph 5 –

subparagraph 2 is amended as follows

The Commission may adopt delegated acts in accordance with Article 38 laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph. Implementing acts shall be used only for purely technical or procedural matters that do not involve policy choices. Any measure that determines the scope of obligations, the categories of entities subject to this Directive, or the criteria for risk assessment shall be adopted by delegated act.

Or. en

Justification

Delegated acts preserve the European Parliament's right of scrutiny and revocation; implementing acts bypass that scrutiny. Article 21(5) technical requirements effectively determine cybersecurity compliance obligations for thousands of entities and must therefore remain under full co-legislator oversight. The standard delegation clause is required as a matter of legislative practice and Interinstitutional Agreement compliance. This is aligned with the ECR CSA2 preference for delegated acts on substantive policy choices.

Amendment 90
Ondřej Krutílek

Proposal for a directive
Article 1 – paragraph 1 – point 7 – point b
Directive (EU) 2022/2555
Article 21(5)

Text proposed by the Commission

Amendment

Where the Commission adopts implementing acts referred to in the first and second subparagraphs of this paragraph, Member States shall not impose any further technical, methodological or sectoral requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555 on the

deleted

entities in scope of those implementing acts.;

Or. en

Amendment 91

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 7 – point b

Directive 2022/2555

Article 21, paragraph 5, fifth subparagraph

Text proposed by the Commission

Where the Commission adopts implementing acts referred to in the first and second subparagraphs of this paragraph, Member States ***shall not impose any*** further technical, methodological or sectoral requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555 on the entities in scope of those implementing acts.;

Amendment

Where the Commission adopts implementing acts referred to in the first and second subparagraphs of this paragraph, Member States ***may maintain or adopt*** further technical, methodological or sectoral requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555 on the entities in scope of those implementing acts, ***where these requirements are necessary for the protection of the Member States' national security, critical infrastructures, essential services, security of supply or essential security interests;***

Or. fr

Amendment 92

Markus Buchheit

Proposal for a directive

Article 1 – paragraph 1 – point 7 – point b

Directive (EU) 2022/2555

Article 1 – Paragraph 1(7)(b)

Text proposed by the Commission

Where the Commission adopts implementing acts referred to in the first and second subparagraphs of this paragraph, Member States shall not impose

Amendment

Where the Commission adopts implementing acts referred to in the first and second subparagraphs of this paragraph, Member States shall not impose

any further technical, methodological or sectoral requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555 on the entities in scope of those implementing acts.;

any further technical, methodological or sectoral requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555 on the entities in scope of those implementing acts. ***This shall not affect any requirements laid down by Member States for public administration entities or for the protection of national security.***

Or. de

Amendment 93

Morten Løkkegaard, Bart Groothuis, Barry Andrews

Proposal for a directive

Article 1 – paragraph 1 – point 7 – point b

Directive (EU) 2022/2555

Article 21(5)

Text proposed by the Commission

Where the Commission adopts ***implementing*** acts referred to in the first and second subparagraphs of this paragraph, Member States shall not impose any further technical, methodological or sectoral requirements of the measures referred to in Article 21(2) ***of Directive (EU) 2022/2555*** on the entities in scope of those implementing acts.;

Amendment

Where the Commission adopts ***delegated*** acts referred to in the first and second subparagraphs of this paragraph, Member States shall not impose any further technical, methodological or sectoral requirements of the measures referred to in Article 21(2) on the entities in scope of those implementing acts.;

Or. en

Justification

Linked to Article 5 and 14a (new).

Amendment 94

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 7 – point b a (new)

Directive (EU) 2022/2555

Article 21 – paragraph 5a (new)

(ba) In Article 21, the following paragraph is added:

5a . By ... [12 months after the date of entry into force of this amending Directive], the Commission shall, after consulting ENISA, the NIS Cooperation Group and the relevant stakeholders, including representatives of free and open-source software developers, adopt guidelines on the cybersecurity-related requirements that essential and important entities pass on to their suppliers and service providers as referred to in paragraph 2, point (d). The guidelines shall:

(a) establish a common, machine-readable format for supplier information requests;

(b) ensure that obligations under this Directive are not unduly passed on to entities outside its scope, in particular to micro and small enterprises and to developers, maintainers and foundations of free and open-source software;

(c) address the proliferation of divergent supplier questionnaires. Where an essential or important entity uses, in the context of supply-chain security requirements under Article 21(2), point (d), a questionnaire or information-request format other than the format established in the guidelines referred to in this paragraph, or requires its suppliers or service providers to provide information beyond what is provided for in those guidelines, that entity shall: (a) document and retain for a period of three years the justification for the additional requirements; (b) bear the full cost of the additional compliance burden imposed on the supplier or service provider, and shall not make the commercial relationship contingent on the supplier or service provider providing additional information; (c) not transmit additional information received to third parties

without the express consent of the supplier or service provider. ENISA shall maintain and publish a registry of questionnaire formats used by essential and important entities, to facilitate convergence towards the standard format. ENISA shall report annually to the Commission on the uptake of the standard format. The Commission shall review the guidelines every two years.

Or. en

Justification

Divergent supplier questionnaires are one of the most significant practical compliance burdens on SMEs in the NIS2 ecosystem. Commission guidelines will only be effective if entities that deviate from them face tangible consequences. Documentation, cost-bearing and transmission-restriction obligations align incentives and protect suppliers, while an ENISA format registry facilitates convergence over time.

Amendment 95

Bart Groothuis, Morten Løkkegaard, Barry Andrews, Ivars Ijabs

Proposal for a directive

Article 1 – paragraph 1 – point 7 a (new)

Text proposed by the Commission

Amendment

(7a) In Article 21, Paragraph 2, Point (ja) is added:

(ja) traffic management measures taken by providers of publicly available electronic communications services, when acting as providers of internet access services, to prevent and mitigate cybersecurity incidents and malicious use of the network, including protective and security measures at the level of the domain name system (DNS) and, where relevant, mitigation measures to preserve the availability, integrity and security of the connected networks of essential and important entities.

In article 21, Paragraph 5, the following is added to the second subparagraph:

The Commission may also adopt implementing acts laying down the technical and the methodological requirements of traffic management measures referred to in paragraph 2 that are consistent with Article 93 Regulation (EU) XXXX/XXXX [Digital Networks Act].

Or. en

Justification

DDoS attacks and other large-scale malicious traffic keep growing in intensity and sophistication, and AI tools will speed this up. Despite BEREC and ENISA guidance on the traffic management measures that ISPs should take to enhance cybersecurity, Member States still interpret this intersection of the NIS2 and the Open Internet Regulation differently: Phishing shields are active by default in some Member States and opt-in only in others, because of perceived net neutrality limits. Blocking port 25 (SMTP) is allowed in some Member States and not in others. As a result, there is no coherent policy across the Union. This amendment requires ISPs to go after the low-hanging fruit of DDoS mitigation based on metadata at the network and transport layers, and protective DNS-level phishing protection. More advanced, content-based mitigation (deep packet inspection) stays outside its scope, because it goes beyond what a general-purpose ISP can be expected to do. Safeguards keep the measures proportionate and consistent with the DNA.

Amendment 96 **Markus Buchheit**

Proposal for a directive
Article 1 – paragraph 1 – point 7 a (new)
Directive (EU) 2022/2555
Article 1 – paragraph 1 – point 7 a (new)

Text proposed by the Commission

Amendment

7a. In Article 21 the following paragraph 6 is added: (6) By ... [twelve months after the entry into force of this amending Directive], the Commission shall, after consulting the Cooperation Group and stakeholders, adopt guidelines setting out a standard template for requests for information from essential and important entities to their suppliers and service providers within the framework of paragraph 2(d). Member States shall ensure that suppliers and

service providers which are micro-enterprises or small or medium-sized enterprises can fulfil their information obligations by using this template or by submitting a valid European cybersecurity certificate, and shall not be required to complete questionnaires that differ from or go beyond this.

Or. de

Amendment 97

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 7 a (new)

Directive (EU) 2022/2555

Article 21 – paragraph 3 – subparagraph 1a (new)

Text proposed by the Commission

Amendment

(7a) The following part is added to Article 21 – paragraph 3 – subparagraph 1a (new)

Essential and important entities shall take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems, including measures addressing the security of the supply chain. ENISA shall, in cooperation with Member States, develop specific guidelines for small and medium-sized enterprises on implementing supply chain security measures proportionate to their risk profile and capabilities, within 18 months of entry into force of this amending Directive.

Or. en

Justification

Supply-chain security is a legitimate objective. Without proportionate implementation guidance, identical requirements applied to large enterprises and SMEs create an uneven

playing field and risk market exit by smaller entities from critical sectors. SME-specific guidance is essential to achieve security objectives without disproportionate costs.

Amendment 98

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a directive

Article 1 – paragraph 1 – point 7 a (new)

Directive (EU) 2022/2555

Article 21(2)

Text proposed by the Commission

Amendment

(7a) (7a) in Article 21(2), the following point is added:

‘(k) the secure integration and use of AI systems, including agentic AI systems, comprising the protection of model parameters, training data and credentials for access to AI services, least privilege for autonomous actions, per agent identity and logging, and the ability to stop an autonomous system promptly.’

Or. en

Amendment 99

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Article 1 – paragraph 1 – point 7 a (new)

Directive (EU) 2022/2555

Article 21, paragraph 5, subparagraph 2

Text proposed by the Commission

Amendment

(7a) When preparing such assessments, the Commission shall consult the NIS Cooperation Group and relevant stakeholders, in an open and transparent manner. This shall be without prejudice to the consultation of the Cooperation

Group and ENISA on draft implementing acts in accordance with this paragraph.

Or. en

Amendment 100
Diego Solier

Proposal for a directive
Article 1 – paragraph 1 – point 7 b (new)
Directive (EU) 2022/2555
Article 21 – paragraph 3a (new)

Text proposed by the Commission

Amendment

(7b) The following part is added to Article 21 – paragraph 3a (new)

Essential and important entities shall take measures to address cybersecurity risks in their supply chain, including risks arising from supplier relationships and dependencies on ICT products and services. The obligations of this Article shall not apply to natural persons or non-profit entities that develop, maintain, or distribute open-source software outside the course of commercial activity. This exemption shall not apply where open-source software is deployed as a critical dependency in essential or important entities' core services and the developer receives commercial compensation for that specific deployment.

Or. en

Justification

Open-source software underpins the internet's security infrastructure. Imposing NIS2 security-management obligations on volunteer developers and non-commercial foundations would chill open-source development without a corresponding security benefit. Commercial deployments in critical infrastructure remain covered through the essential and important entity classification. This wording is coherent with the open-source carve-out in the ECR CSA2 package.

Amendment 101

Morten Løkkegaard, Bart Groothuis

Proposal for a directive

Article 1 – paragraph 1 – point 8 – introductory part

Directive (EU) 2022/2555

Article 23

Text proposed by the Commission

Amendment

(8) in Article 23, the following paragraphs **12 and 13** are added:

(8) in Article 23, the following paragraphs **11a, 11b, 12, 13 and 13a** are added:

Or. en

Amendment 102

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a directive

Article 1 – paragraph 1 – point 8 – introductory part

Text proposed by the Commission

Amendment

(8) in Article 23, the following paragraphs 12 **and 13** are added:

(8) in Article 23, the following paragraphs 12, **13 and 14** are added:

Or. en

Amendment 103

Ondřej Krutílek

Proposal for a directive

Article 1 – paragraph 1 – point 8

Directive (EU) 2022/2555

Article 23(12)

Text proposed by the Commission

Amendment

12. When adopting an implementing act pursuant to paragraph 11, first subparagraph, the Commission shall include requirements that the following information as regards ransomware

deleted

attacks is submitted pursuant to paragraph 1:

(a) whether the entity detected a ransomware attack;

(b) the attack vector of the ransomware attack;

(c) whether mitigation measures have been implemented.

Or. en

Amendment 104

Katri Kulmuni, Eero Heinäluoma

Proposal for a directive

Article 1 – paragraph 1 – point 8

(EU) 2022/2555

Article 1, Paragraph (8)

Text proposed by the Commission

Amendment

(b) the attack vector of the ransomware attack;

(b) the attack vector of the ransomware attack, ***if known***;

Or. en

Justification

In line with Amendment 3 (Proposal for a directive, Recital 10a (new)), ransomware information that is not necessary for prevention, situational awareness or support should not be reported. Detailed payment information is not necessary for the tasks of CSIRTs or NIS2 competent authorities and should therefore not be collected for all incidents, also considering the proposal's objective of simplification. In addition, attack vectors may not always be known within the timelines for incident reporting.

Amendment 105

Ondřej Krutílek

Proposal for a directive

Article 1 – paragraph 1 – point 8

Directive (EU) 2022/2555

Article 23(13)

Text proposed by the Commission

Amendment

13. Member States shall ensure that in case of a significant incident caused by a ransomware attack, the entities concerned inform, upon request of the CSIRT or, where applicable, the competent authority via a communication channel provided by the CSIRT or, where applicable, the competent authority:

(a) if the entity has received a ransom demand and, where applicable, by whom;

(b) if a ransom was paid and if yes, what amount in what means of payment and to which recipient or receiving end, including the crypto-asset and crypto-asset service provider, where applicable.;

Or. en

Amendment 106
Katri Kulmuni, Eero Heinäluoma

Proposal for a directive
Article 1 – paragraph 1 – point 8
(EU) 2022/2555
Article 1, Paragraph (8)

Text proposed by the Commission

Amendment

(b) if a ransom was paid and if yes, what amount ***in what means of payment and to which recipient or receiving end, including the crypto-asset and crypto-asset service provider, where applicable.;***

(b) if a ransom was paid and if yes, what amount. ';

Or. en

Justification

In line with Amendment 3 (Proposal for a directive, Recital 10a (new)), ransomware information that is not necessary for prevention, situational awareness or support should not be reported. Detailed payment information is not necessary for the tasks of CSIRTs or NIS2 competent authorities and should therefore not be collected for all incidents, also considering the proposal's objective of simplification. In addition, attack vectors may not always be known within the timelines for incident reporting.

Amendment 107

Morten Løkkegaard, Bart Groothuis, Elisabetta Gualmini

Proposal for a directive

Article 1 – paragraph 1 – point 8

Directive 2022/2555

Article 23(13)

Text proposed by the Commission

(b) if a ransom was paid and if yes, what amount in what means of payment and to which recipient or receiving end, including the crypto-asset and crypto-asset service provider, where applicable.;

Amendment

(b) if a ransom was paid and if yes, what amount in what means of payment and to which recipient or receiving end, including the crypto-asset and crypto-asset service provider, where applicable ***and where this information is available to the entities concerned.***;

Or. en

Amendment 108

Morten Løkkegaard, Bart Groothuis, Elisabetta Gualmini

Proposal for a directive

Article 1 – paragraph 1 – point 8

Directive 2022/2555

Article 23(13)

Text proposed by the Commission

Amendment

(ba) Information submitted pursuant to paragraph 13 shall be treated as confidential. It shall be used exclusively for the purposes of incident response, threat analysis, support to affected entities or cross-border coordination. Such information shall be retained only for as long as necessary for those purposes and shall not be made publicly available in a form that enables the reporting entity or other affected persons to be identified.

Or. en

Amendment 109

Markéta Gregorová

on behalf of the Verts/ALE Group
Jens Geier
on behalf of the S&D Group

Proposal for a directive
Article 1 – paragraph 1 – point 8
Directive (EU) 2022/2555
Article 23

Text proposed by the Commission

Amendment

13a. 14. An AI high risk security incident, or an event in which any other AI system within the meaning of Article 3, point (1), of Regulation (EU) 2024/1689, irrespective of the AI model on which it is built, carries out any of the acts referred to in Article 2, point (50c), points (a) to (d), of Regulation (EU) .../... [CSA2], affecting the network and information systems of an essential or important entity, or caused by an AI system, including an agentic AI system, operated by such an entity, shall be deemed to be a significant incident for the purposes of paragraph 3. The CSIRT or, where applicable, the competent authority shall forward the notification without undue delay to ENISA, which shall forward it to the AI Office established by Commission Decision C(2024) 390.

Or. en

Amendment 110
Markus Buchheit

Proposal for a directive
Article 1 – paragraph 1 – point 8
Directive (EU) 2022/2555
Article 1 – paragraph 1 – point 8

Text proposed by the Commission

Amendment

(13a) The information provided in accordance with paragraph 13 shall be treated as confidential and used solely for the purposes of responding to security

incidents, assessing the situation and law enforcement. It shall not be used as a basis for supervisory or enforcement measures against the reporting organisation, nor shall it be disclosed to third parties for any purpose other than those specified. The payment of a ransom shall not, in itself, constitute a breach of this Directive.

Or. de

Amendment 111

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Article 1 – paragraph 1 – point 8 a (new)

2022/2555

Article 23, paragraph 11, new subparagraph

Text proposed by the Commission

Amendment

(8a) in Article 23, paragraph 11, the following subparagraph is added:

When adopting implementing acts pursuant to this paragraph, the Commission shall, where appropriate, ensure consistency with reporting requirements under other relevant Union legal acts, including Regulation (EU) 2016/679, Regulation (EU) 2022/2554 and Regulation (EU) 2024/2847. Those implementing acts shall, to the extent possible, provide for common reporting templates, harmonised information requirements and the reuse of information already submitted under Union law, in order to avoid duplicate reporting.

Or. en

Amendment 112

Morten Løkkegaard, Bart Groothuis, Barry Andrews, Elisabetta Gualmini

Proposal for a directive

Article 1 – paragraph 1 – point 8 a (new)

Directive 2022/2555

Article 23(11a)

Text proposed by the Commission

Amendment

(8a) 11a. When adopting implementing acts pursuant to paragraph 11 of this Article, the Commission shall ensure consistency with reporting obligations established under other relevant Union legal acts. To the extent possible, those implementing acts shall provide for the alignment of relevant definitions, timelines, procedures and formats, and facilitate the secure exchange and reuse of information already submitted under Union law.

Or. en

Amendment 113

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 8 a (new)

Directive (EU) 2022/2555

Article 23 – paragraph 4 – subparagraph 1 – point a

Present text

Amendment

(a) without undue delay and in any event within **24** hours of becoming aware of **the** significant incident, an early warning, **which, where applicable,** shall **indicate** whether the **significant** incident is **suspected of being caused by unlawful or malicious acts or could have a cross-border impact**

"(a) without undue delay and in any event within **72** hours of becoming aware of **a** significant incident, **the entity shall submit** an early warning **to the competent authority or the CSIRT. The early warning requirement shall not apply where the entity has insufficient information to determine** whether the incident is **significant**;"

Or. en

(2022/2555)

Justification

The 24-hour early-warning timeline is too short for accurate initial assessment. The 72-hour standard already adopted in the original NIS2 Directive strikes the right balance between timely reporting and accuracy. Forcing incomplete reports within 24 hours risks overloading national CSIRTs with low-quality information that impedes rather than aids response coordination.

Amendment 114

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 8 b (new)

Directive (EU) 2022/2555

Article 23 – paragraph 5

Present text

Where the significant incident is suspected to be of criminal nature, the CSIRT or the competent authority shall also provide guidance on reporting the significant incident to law enforcement authorities.

Amendment

(8 b) Article 23 (5) is replaced by the following;

"Where the significant incident is suspected to be of criminal nature, the CSIRT or the competent authority shall also provide guidance on reporting the significant incident to law enforcement authorities. **Where the significant incident is supported by reasonable evidence that it results from unlawful or malicious acts or constitutes a criminal offence, the CSIRT or the competent authority may, after informing the entity concerned, notify the relevant law enforcement authority. The entity concerned may voluntarily notify law enforcement authorities where it has reasonable grounds to believe that the incident involves criminal activity. Information notified pursuant to this Article shall not be transmitted to law enforcement authorities solely on the ground that the incident is significant.**"

Or. en

(2022/2555)

Justification

Directive (EU) 2022/2555 currently only requires CSIRTs and competent authorities to provide guidance on reporting suspected criminal incidents to law enforcement. This amendment clarifies the conditions under which authorities may themselves refer an incident to law enforcement, introducing an evidence-based threshold and prior information of the entity, and confirms the entity's right to notify voluntarily. Excluding automatic referral based solely on the significance of an incident keeps cybersecurity reporting separate from criminal investigation and preserves the trust on which effective incident reporting depends.

Amendment 115

Morten Løkkegaard, Bart Groothuis, Barry Andrews, Elisabetta Gualmini

Proposal for a directive

Article 1 – paragraph 1 – point 8 b (new)

Directive/2022/2555

Article 23(11b)

Text proposed by the Commission

Amendment

(8b) 11b. Where reporting obligations according to this Article have been fulfilled through the single-entry point, according to Article 23a, Member States shall not require the entity to submit the same information through a separate national reporting channel.

Or. en

Amendment 116

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 8 c (new)

Directive (EU) 2022/2555

Article 23 – paragraph 13 – subparagraph 1 – introductory wording

Present text

Amendment

(8 c) Article 23 (13) – subparagraph 1 – introductory wording is amended as follows;

13. Member States shall ensure that in case of a significant incident caused by a ransomware attack, the entities concerned

"13. Member States shall ensure that in case of a significant incident caused by a ransomware attack, the entities concerned

inform, upon request of the CSIRT or, where applicable, the competent authority via a communication channel provided by the CSIRT or, where applicable, the competent authority:

inform, upon request of the CSIRT or, where applicable, the competent authority, ***exclusively for the purposes of prevention, situational awareness and support***, via a communication channel provided by the CSIRT or, where applicable, the competent authority: ***The provision of information pursuant to this paragraph shall not of itself subject the entity concerned to increased liability. That information shall be treated confidentially, shall not be used in supervisory or enforcement proceedings against the reporting entity and shall be transmitted to other authorities only where Union or national law expressly so provides. The prohibition on use in supervisory or enforcement proceedings shall apply equally to the reporting entity's directors, officers and employees, as well as to entities affiliated with the reporting entity. National competent authorities and CSIRTs shall implement technical access controls ensuring that information collected pursuant to this paragraph is accessible only to personnel directly and specifically responsible for incident response or situational awareness, and is not accessible in any supervisory, enforcement or audit file concerning the reporting entity. Information collected pursuant to this paragraph shall not be shared with law enforcement authorities except where a Union legal act expressly so provides, and with prior notice to the reporting entity where operationally possible. The communication channel referred to in the first subparagraph shall ensure end-to-end encryption by default.***"

Or. en

(2022/2555)

Justification

Using ransomware payment and negotiation data in enforcement actions chills voluntary reporting, which is the primary source of situational awareness. Extending the shield to directors and employees addresses personal-liability risks that may otherwise deter reporting.

Mandatory national access controls prevent supervisory spillover, and restricted law-enforcement sharing preserves the exclusive prevention and support purpose of the channel.

Amendment 117

Morten Løkkegaard, Bart Groothuis, Elisabetta Gualmini

Proposal for a directive

Article 1 – paragraph 1 – point 8 c (new)

Directive 2022/2555

Article 23(13a)

Text proposed by the Commission

Amendment

(8c) 13a. Where the same incident is subject to notification obligations under this Directive and under another Union legal act, a notification submitted in accordance with that other Union legal act shall satisfy the notification obligation under paragraph 4 of this Article, provided that it contains the information required for that obligation and is made available to the CSIRT or, where applicable, the competent authority within the time limit applicable under paragraph 4. The entity concerned may be required to submit only information required under paragraph 4 that has not already been provided.

Or. en

Amendment 118

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 8 d (new)

Directive (EU) 2022/2555

Article 23 – paragraph 9a (new)

Text proposed by the Commission

Amendment

(8d) In Article 23, the following paragraph is inserted:

9a. Where a Member State has established a national incident reporting system that

meets the technical, security and interoperability requirements established for the single entry point pursuant to this Article, and that system has been successfully audited in accordance with the applicable security requirements, the Commission shall, upon application by that Member State, certify that national system as a certified equivalent national entry point. A notification submitted through a certified equivalent national entry point shall constitute a notification through the single entry point for all purposes of Union law. A notification submitted through the single entry point shall be automatically transmitted as metadata only to the certified equivalent national entry point of the Member State of the addressee authority. ENISA shall maintain and publish a register of certified equivalent national entry points and the date of their most recent audit. Member States shall not be required to migrate entities from their certified equivalent national entry point to the Union-level single entry point during the period of validity of the certification.

Or. en

Justification

Several Member States have made significant investments in national incident-reporting systems. Subsidiarity and proportionality require that the Union-level system build on, not replace, those systems. A certification mechanism ensures equivalent security standards while respecting operational and financial investments. Metadata-only transmission preserves a federated architecture and ENISA's limited data-access role, consistent with the ECR single-entry-point architecture in the CSA2 package.

Amendment 119

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Article 1 – paragraph 1 – point 9 – introductory part

Text proposed by the Commission

Amendment

(9) in Article 24, the following paragraphs 4, 5 **and 6** are added:

(9) in Article 24, the following paragraphs 4, 5, **6, 7 and 8** are added:

Or. en

Amendment 120

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 9

Directive 2022/2555

Article 24

Text proposed by the Commission

Amendment

4. In order to demonstrate compliance with Article 21, Member States may require essential and important entities to obtain a certificate on the cyber posture under a European cybersecurity certification scheme adopted pursuant to Article 75 of Regulation (EU) XXX/XXX ** [Proposal for CSA2].**

deleted

Or. fr

Amendment 121

Jens Geier

Proposal for a directive

Article 1 – paragraph 1 – point 9

Directive (EU) 2022/2555

Article 24

Text proposed by the Commission

Amendment

4. In order to demonstrate compliance with Article 21, Member States *may* require essential and important entities to obtain a certificate on the cyber posture under a European cybersecurity certification scheme adopted pursuant to Article 75 of Regulation (EU) XXX/XXX ** [Proposal for CSA2].**

4. In order to demonstrate compliance with Article 21, Member States *shall* require essential and important entities to obtain a certificate on the cyber posture under a European cybersecurity certification scheme adopted pursuant to Article 75 of Regulation (EU) XXX/XXX ** [Proposal for CSA2]. *This obligation shall apply twelve months after an applicable scheme enters into application.***

Essential and important entities shall thereafter maintain valid certification.

Or. en

Amendment 122

Morten Løkkegaard, Bart Groothuis, Barry Andrews

Proposal for a directive

Article 1 – paragraph 1 – point 9

Directive 2022/2555

Article 24(4)

Text proposed by the Commission

4. In order to demonstrate compliance with Article 21, Member States may ***require essential and important entities to obtain*** a certificate on the cyber posture under a European cybersecurity certification scheme adopted pursuant to Article 75 of Regulation (EU) XXX/XXX **** [Proposal for CSA2].

Amendment

4. In order to demonstrate compliance with Article 21, Member States may ***recognise*** a certificate on the cyber posture under a European cybersecurity certification scheme adopted pursuant to Article 75 of Regulation (EU) XXX/XXX **** [Proposal for CSA2] ***which has been voluntarily obtained by essential and important entities.***

Or. en

Amendment 123

Markus Buchheit

Proposal for a directive

Article 1 – paragraph 1 – point 9

Directive (EU) 2022/2555

Article 1 – paragraph 1 – point 9

Text proposed by the Commission

4. In order to demonstrate compliance with Article 21, ***Member States may require*** essential and important entities ***to obtain*** a certificate on the cyber posture under a European cybersecurity certification scheme adopted pursuant to Article 75 of Regulation (EU) XXX/XXX **** [Proposal for CSA2].

Amendment

4. In order to demonstrate compliance with Article 21, essential and important entities ***may, on a voluntary basis, submit*** a certificate on the cyber posture under a European cybersecurity certification scheme adopted pursuant to Article 74 of Regulation (EU) XXX/XXX **** [Proposal for CSA2].

Amendment 124

Ondřej Krutílek

Proposal for a directive

Article 1 – paragraph 1 – point 9

Directive (EU) 2022/2555

Article 24(4)

Text proposed by the Commission

4. In order to demonstrate compliance with Article 21, Member States may require essential and important entities to obtain a certificate on the cyber posture under a European cybersecurity certification scheme adopted pursuant to Article 75 of Regulation (EU) XXX/XXX **** [Proposal for CSA2].

Amendment

4. In order to demonstrate compliance with Article 21, Member States may require essential and important entities to obtain a certificate on the cyber posture under a European cybersecurity certification scheme adopted pursuant to Article 74 of Regulation (EU) XXX/XXX **** [Proposal for CSA2].

Or. en

Amendment 125

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 9

Directive 2022/2555

Article 24

Text proposed by the Commission

Amendment

4a. Where an essential or important entity has already forwarded to a competent authority information, reports, evidence, audit results, certificates or statements of conformity pursuant to this Directive, Regulation (EU) 2022/2554 on digital operational resilience for the financial sector, Regulation (EU) 2024/2847 on cyber resilience, or a sectoral cybersecurity framework that is applicable at Union level, the competent authorities shall ensure, where possible, that these items of information are

reusable for the purposes of this Directive.

The competent authorities may not request that essential or important entities re-submit equivalent information or evidence, unless this is strictly necessary for carrying out of their supervisory duties and the protection of a Member State's national security, critical infrastructures, essential services, security of supply or essential security interests.

Or. fr

Amendment 126

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 9

Directive 2022/2555

Article 24

Text proposed by the Commission

Amendment

5. Where the cyber posture of an essential or important entity is certified under a European cybersecurity certification scheme adopted pursuant to Article 74 of Regulation (EU) XXX/XXX** [Proposal for CSA2] and where the certificate demonstrates compliance with the requirements laid down in an implementing act adopted pursuant to Article 21(5) of this Directive or national law transposing Article 21(1) and (2) of this Directive, competent authorities shall not subject the entity to additional measures pursuant to Article 32(2), point (b), or Article 33(2), point (b), as applicable with regard to the requirements covered by the certificate.**

deleted

Or. fr

Amendment 127

Morten Løkkegaard, Bart Groothuis, Barry Andrews

Proposal for a directive

Article 1 – paragraph 1 – point 9

Directive 2022/2555

Article 24(5)

Text proposed by the Commission

5. Where the cyber posture of an essential or important entity is certified under a European cybersecurity certification scheme adopted pursuant to Article 74 of Regulation (EU) XXX/XXX**** [Proposal for CSA2] and where the certificate demonstrates compliance with the requirements laid down in an implementing act adopted pursuant to Article 21(5) of this Directive or national law transposing Article 21(1) and (2) of this Directive, competent authorities shall not subject the entity to additional measures pursuant to Article 32(2), point (b), or Article 33(2), point (b), as applicable with regard to the requirements covered by the certificate.

Amendment

5. Where the cyber posture of an essential or important entity is certified under a European cybersecurity certification scheme adopted pursuant to Article 74 of Regulation (EU) XXX/XXX**** [Proposal for CSA2] and where the certificate demonstrates compliance with the requirements laid down in an implementing act adopted pursuant to Article 21(5) of this Directive or national law transposing Article 21(1) and (2) of this Directive, competent authorities ***in all Member States shall recognise that certificate as evidence of compliance and*** not subject the entity to additional measures pursuant to Article 32(2), point (b), or Article 33(2), point (b), as applicable with regard to the requirements covered by the certificate.

Or. en

Amendment 128

Ondřej Krutílek

Proposal for a directive

Article 1 – paragraph 1 – point 9

Directive (EU) 2022/2555

Article 24(5)

Text proposed by the Commission

5. Where the cyber posture of an essential or important entity is certified under a European cybersecurity certification scheme adopted pursuant to Article 74 of Regulation (EU) XXX/XXX**** [Proposal for CSA2] and where the certificate demonstrates compliance with the requirements laid

Amendment

5. Where the cyber posture of an essential or important entity is certified under a European cybersecurity certification scheme adopted pursuant to Article 74 of Regulation (EU) XXX/XXX**** [Proposal for CSA2] and where the certificate demonstrates compliance with the requirements laid

down in an implementing act adopted pursuant to Article 21(5) of this Directive ***or national law transposing Article 21(1) and (2) of this Directive***, competent authorities shall not subject the entity to additional measures pursuant to Article 32(2), point (b), or Article 33(2), point (b), as applicable with regard to the requirements covered by the certificate.

down in an implementing act adopted pursuant to Article 21(5) of this Directive, competent authorities shall not subject the entity to additional measures pursuant to Article 32(2), point (b), or Article 33(2), point (b), as applicable with regard to the requirements covered by the certificate.

Or. en

Amendment 129

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 9

Directive 2022/2555

Article 24

Text proposed by the Commission

Amendment

6. A certification pursuant to paragraph 4 shall not affect the responsibility of the essential or important entity to comply with this Directive.

deleted

****** Regulation (EU) XXX/XXX
[Proposal for CSA2];**

Or. fr

Amendment 130

Ondřej Krutílek

Proposal for a directive

Article 1 – paragraph 1 – point 9

Directive (EU) 2022/2555

Article 24(6)

Text proposed by the Commission

Amendment

A certification pursuant to paragraph 4 shall not affect the responsibility of the essential or important entity to comply

deleted

with this Directive.

Or. en

Amendment 131

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 9 a (new)

Directive (EU) 2022/2555

Article 25a (new)

Text proposed by the Commission

Amendment

(9a) The following Article is inserted:

Article 25a (new)

***Union register of implementation
divergences***

***1. By [12 months after the entry into force
of this amending Directive], ENISA shall
establish and maintain a publicly
accessible register identifying significant
divergences in the national
implementation of this Directive that
create barriers to cross-border service
provision or result in materially different
levels of cybersecurity protection across
Member States.***

***2. ENISA shall update that register at
least annually, on the basis of information
provided by Member States, publicly
available national measures and its own
technical analysis.***

***3. ENISA shall submit to the Commission,
on an annual basis, recommendations on
priority areas for further harmonisation.***

***4. The Commission shall inform the
European Parliament and the Council of
the actions taken in response to the
recommendations referred to in
paragraph 3.***

Or. en

Justification

Fragmented national implementation undermines the effectiveness of Directive (EU) 2022/2555 and increases compliance costs for cross-border operators. A transparency register is a proportionate mechanism to identify implementation divergences and support convergence, while fully respecting Member State competences.

Amendment 132

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Article 1 – paragraph 1 – point 9 a (new)

Directive (EU) 2022/2555

Article 24, new paragraph 7

Text proposed by the Commission

Amendment

(9a) 7. Where the Commission requests the preparation of a European cybersecurity certification scheme on the cyber posture of entities for the purposes of paragraph 4, it shall ensure that the NIS Cooperation Group, competent authorities and relevant stakeholders, including industry representatives and the entities concerned, are consulted in an open and transparent manner.

Or. en

Amendment 133

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 9 b (new)

Directive (EU) 2022/2555

Article 25 – paragraph 2

Present text

Amendment

2. ENISA, in cooperation with Member States, and, where appropriate, after consulting relevant stakeholders, shall

(9 b) Article 25 (2) is amended as follow;

"2. ENISA, in cooperation with Member States, and, where appropriate, after consulting relevant stakeholders, shall

draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including national standards, which would allow for those areas to be covered.

draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including national standards, which would allow for those areas to be covered. ***Advice and guidelines issued by ENISA pursuant to this Directive shall be non-binding and shall not create legal obligations for Member States or entities. Where binding technical requirements are necessary, they shall be adopted by means of delegated or implementing acts in accordance with this Directive. Competent authorities shall not treat compliance with ENISA advice or guidelines as a mandatory condition for compliance with this Directive.***

Or. en

(2022/2555)

Justification

ENISA was established as an expert advisory body. Its guidance is valuable, but it must not become de facto binding through supervisory practice, as this would bypass the legislative process and the principle of conferred powers. Where binding technical requirements are needed, they must be adopted through the procedures laid down in this Directive, ensuring democratic accountability. This is coherent with the advisory role of ENISA defended in the ECR position on the Cybersecurity Act revision.

Amendment 134

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Article 1 – paragraph 1 – point 9 b (new)

Directive (EU) 2022/2555

Article 24, new paragraph 8

Text proposed by the Commission

Amendment

(9b) 8. Where a European cybersecurity certification scheme on the cyber posture of entities is used for the purposes of paragraph 4, the scheme shall, where appropriate, take into

account existing European and international standards and allow for the reuse of relevant assessments, certificates and documentation, in order to avoid unnecessary duplication of audits or conformity assessment activities. This paragraph shall not affect the requirements applicable under Regulation (EU) XXX/XXX [Proposal for CSA2].

Or. en

Amendment 135

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 10 – point b

Directive 2022/2555

Article 26, paragraph 3

Text proposed by the Commission

3. If an essential or important entity is not established in the Union but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established. Where such an entity is an entity as referred to in paragraph 1, point (a), it shall be considered to fall under the jurisdiction of the Member State in which it provides its services. In the absence of a representative in the Union designated under this paragraph, any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Directive.;

Amendment

3. If an essential or important entity is not established in the Union but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established. Where such an entity is an entity as referred to in paragraph 1, point (a), it shall be considered to fall under the jurisdiction of the Member State in which it provides its services. In the absence of a representative in the Union designated under this paragraph, any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Directive. ***The designation of a representative in the Union shall not prevent the adoption, by the competent authority of a Member State in which the entity provides services, of the necessary provisional emergency measures in cases where these services affect or may affect that Member State's***

national security, critical infrastructures, essential services, security of supply or essential security interests. The competent authority of the Member State concerned shall inform without delay the competent authority of the Member State in which the representative is established as well as the competent single point of contact.

Or. fr

Amendment 136

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 10 – point b a (new)

Text proposed by the Commission

Amendment

(ba) The following paragraph 2a is inserted:

2a. Notwithstanding paragraphs 1 and 2, where an entity under the jurisdiction of a Member State provides services in another Member State, the competent authority of the latter Member State may adopt the necessary provisional emergency measures in cases where these services affect or may affect its national security, critical infrastructures, essential services, security of supply or essential security interests. The competent authority of the Member State concerned shall inform without delay the competent authority of the Member State that has jurisdiction over the entity in question.

Or. fr

Amendment 137

Ondřej Krutílek

Proposal for a directive

Article 1 – paragraph 1 – point 11

Directive (EU) 2022/2555

(11) Article 27 is amended as follows: deleted

(a) paragraph 1 is replaced by the following:

‘1. ENISA shall create and maintain a registry of essential and important entities as well as entities providing domain name registration services, on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to information concerning DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms and air carriers stored in that registry, while ensuring that the confidentiality of information is protected where applicable.;’

(c) paragraphs 3, 4 and 5 are replaced by the following:

‘3. Member States shall ensure that the essential and important entities notify the competent authority about any changes to the information they submitted under Article 3(4) without delay and in any event within two weeks of the date of the change.

4. Upon receipt of the information referred to in Article 3(4), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.

5. Where applicable, the information referred to in Article 3(4), first subparagraph, shall be submitted through

the national mechanism referred to in Article 3(4), fourth subparagraph.;

Or. en

Amendment 138

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 11 – point a

Directive 2022/2555

Article 27, paragraph 1

Text proposed by the Commission

1. ENISA shall create and maintain a registry of essential and important entities as well as entities providing domain name registration services, on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to information concerning DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms and air carriers stored in that registry, while ensuring **that** the confidentiality **of** information **is protected where applicable.;**

Amendment

1. ENISA shall create and maintain a registry of essential and important entities as well as entities providing domain name registration services, on the basis of the information received from the single points of contact in accordance with paragraph 4. ***This registry shall only contain the information that is strictly necessary for the identification of the entities concerned and for cooperation among competent authorities. It shall not include IP ranges, classified information, sensitive information, information pertaining to unpatched vulnerabilities or information whose disclosure could be detrimental to the Member States' national security, critical infrastructures, essential services or essential security interests.*** Upon request, ENISA shall allow the competent authorities **concerned** access to information concerning DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms and air carriers stored in that registry, while ensuring **at all times** the confidentiality, **integrity and security of**

the information that is recorded and accessed. This access is restricted to the competent authorities concerned on a need-to-know basis. This access shall not result in the disclosure of sensitive information, information pertaining to national security or information enabling the mapping of the critical infrastructures, essential services, or information networks and systems of the entities concerned.

Or. fr

Amendment 139

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Article 1 – paragraph 1 – point 11 – point a

Directive (EU) 2022/2555

Article 27, paragraph 1

Text proposed by the Commission

1. ENISA shall create and maintain a registry of essential and important entities as well as entities providing domain name registration services, on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to information concerning DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms and air carriers stored in that registry, while ensuring that the confidentiality of information is protected where applicable.;

Amendment

1. ENISA shall create and maintain a registry of essential and important entities as well as entities providing domain name registration services, on the basis of the information received from the single points of contact in accordance with paragraph 4. ***The information contained in the registry shall be limited to what is necessary for the performance of ENISA's tasks under this Directive, in particular for the purposes of Article 37a, and shall avoid unnecessary duplication of information already maintained by competent authorities.*** Upon request, ENISA shall allow the competent authorities access to information concerning DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as

providers of online marketplaces, of online search engines and of social networking services platforms and air carriers stored in that registry, while ensuring that the confidentiality of information is protected where applicable.;

Or. en

Amendment 140

Markus Buchheit

Proposal for a directive

Article 1 – paragraph 1 – point 11 – point a

Directive (EU) 2022/2555

Article 1 – paragraph 1 – point 11 – point a

Text proposed by the Commission

1. ENISA shall create and maintain a registry of ***essential and important entities as well as entities providing domain name registration services, on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to information concerning*** DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms and air carriers stored in that registry, while ensuring that the confidentiality of information is protected where applicable.;

Amendment

1. ENISA shall create and maintain a registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms and air carriers ***on the basis of the information received from the single entry points in accordance with Article 4. Upon request, ENISA shall allow the competent authorities access to the information*** stored in that registry, while ensuring that the confidentiality of information is protected where applicable. ***The lists of the other essential and important entities shall be maintained exclusively by the Member States in accordance with Article 3(3).***

Or. de

Amendment 141

Morten Løkkegaard, Bart Groothuis

Proposal for a directive

Article 1 – paragraph 1 – point 11 – point c

Directive 2022/2555

Article 27(4)

Text proposed by the Commission

4. Upon receipt of the information referred to in Article 3(4), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.

Amendment

4. Upon receipt of the information referred to in Article 3(4), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA. ***Information concerning IP ranges referred to in Article 3(4), first subparagraph, point (f), shall only be forwarded in duly justified cases where a specific task under Article 37a cannot be performed without this information.***

Or. en

Amendment 142

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 11 – point c

Directive 2022/2555

Article 27, paragraph 4

Text proposed by the Commission

4. Upon receipt of the information referred to in Article 3(4), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.

Amendment

4. Upon receipt of the information referred to in Article 3(4), ***except for the information referred to in Article 3(4), first subparagraph, point (f)***, the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.

Or. fr

Amendment 143

Markus Buchheit

Proposal for a directive

Article 1 – paragraph 1 – point 11 – point c
Directive (EU) 2022/2555
Article 1 – paragraph 1 – point 11 – point c

Text proposed by the Commission

4. Upon receipt of the information referred to in Article 3(4), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.

Amendment

4. Upon receipt of the information referred to in Article 3(4) ***on the entities referred to in paragraph 1***, the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.

Or. de

Amendment 144
Diego Solier

Proposal for a directive
Article 1 – paragraph 1 – point 11 – point c a (new)
Directive (EU) 2022/2555
Article 27 – paragraph 4

Present text

4. Upon receipt of the information referred to in Article 3(4), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.

Amendment

"4. Upon receipt of the information referred to in Article 3(4), ***except for the information referred to in Article 3(4), first subparagraph, point (f)***, the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA. ***5a. ENISA shall, on an ongoing basis, monitor and assess whether third-country laws or regulations applicable to ENISA or to its hosting and infrastructure providers may require the disclosure of information contained in the registry to third-country authorities. Where such a risk is identified, ENISA shall notify the Commission, the Management Board, and the Member States concerned without delay, and shall take all technically feasible measures to mitigate the risk of disclosure, including data minimisation, geographic restrictions on data storage, and enhanced access controls. The Commission shall report annually to the European Parliament and***

to the Council on this monitoring."

Or. en

(2022/2555)

Justification

Centralising IP-range data at Union level creates a high-value target for adversaries. IP ranges should remain with national competent authorities. The additional third-country legal-risk notification obligation addresses the related risk of foreign legal-access obligations on ENISA or its hosting providers, which is particularly relevant for an agency holding security-sensitive data on critical-infrastructure entities.

Amendment 145

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 11 a (new)

Directive (EU) 2022/2555

Article 32 – paragraph 1

Text proposed by the Commission

Amendment

(11a) Article 32(1) is amended as follows:

Competent authorities shall have the power to issue binding instructions, conduct on-site inspections, require audits, and impose administrative sanctions on essential and important entities that fail to comply with the obligations under this Directive. Competent authorities shall apply supervisory measures in a graduated manner proportionate to the severity and persistence of the non-compliance, starting with the least intrusive measure capable of achieving compliance before proceeding to more stringent measures, except where there is an imminent threat to public safety or national security.

Or. en

Justification

Proportionality is a fundamental principle of Union law. Supervisory powers that allow authorities to jump directly to the most severe measures without prior remediation steps risk disproportionate harm to entities and to the continuity of essential services. A graduated enforcement ladder ensures a fair opportunity to remedy non-compliance before the most intrusive measures are applied.

Amendment 146

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 11 b (new)

Directive (EU) 2022/255

Article 34 – paragraph 4

Present text

4. Member States shall ensure that ***where they infringe Article 21 or 23, essential entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.*** ***Δ*** *The current left column (“may amount to at least 2%”) does not exist in the Directive. Redraft the right column on top of the verbatim text: “maximum of at least” → “maximum of”, plus the SME cap. Important entities are covered by Art. 34(5), which would need a parallel amendment.*

Amendment

(11 b) Article 34 (4) is amended as follows;

“4. Member States shall ensure that administrative fines applicable to essential entities for infringements of the obligations under this Directive are effective, proportionate and dissuasive. In determining the amount of administrative fines, competent authorities shall give full consideration to: (a) the size and economic capacity of the entity; (b) the degree of responsibility and the measures taken to mitigate damage; (c) whether the entity proactively disclosed the violation; (d) any action taken by the entity to remedy the non-compliance. For entities with fewer than 250 employees, administrative fines shall not exceed EUR 500 000.”

Or. en

(2022/2555)

Justification

Minimum penalty floors undermine administrative and judicial discretion and risk bankrupting SME operators of critical services. Maximum-based deterrence already exists; proportionality requires full discretion to calibrate penalties to the circumstances of each

case. An SME cap prevents disproportionate penalties that could force critical service providers out of the market. This position is consistent with the ECR rejection of minimum penalty floors in the CSA2 package.

Amendment 147

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 12

Directive 2022/2555

Article 37a

Text proposed by the Commission

Amendment

(12) the following Article 37a is inserted:

deleted

Or. fr

Amendment 148

Ondřej Krutílek

Proposal for a directive

Article 1 – paragraph 1 – point 12

Directive (EU) 2022/2555

Article 37a

Text proposed by the Commission

Amendment

[...]

deleted

Or. en

Amendment 149

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 12

Directive 2022/2555

Article 37a

Text proposed by the Commission

Amendment

1. ENISA shall assist Member States in carrying out mutual assistance within the meaning of Article 37 and help facilitate

1. ***At the request of the competent authorities of the Member States concerned and without prejudice to their***

such cooperation processes for essential and important entities that provide services in more than one Member State or that provide services in one or more Member States and have their network and information systems located in one or more other Member States.

national supervisory, monitoring and enforcement competences, ENISA shall assist Member States in carrying out mutual assistance within the meaning of Article 37 and help facilitate such cooperation processes for essential and important entities that provide services in more than one Member State or that provide services in one or more Member States and have their network and information systems located in one or more other Member States.

Or. fr

Amendment 150

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 12

Directive 2022/2555

Article 37a

Text proposed by the Commission

2. For the purposes set out in paragraph 1, by ... [15 months after the entry into force of this Regulation], ENISA shall conduct a comprehensive analysis of cross-border cybersecurity risks relating to essential and important entities that provide services in more than one Member State or that provide services in one or more Member States and have their network and information systems located in one or more other Member States. The analysis shall evaluate the extent of possible cross-border and internal market consequences of incidents affecting such essential and important entities. For the purpose of this analysis, ENISA shall, in cooperation with the Commission and the Cooperation Group, develop a methodology. Based on the analysis, ENISA shall draw up a comprehensive cross-border cybersecurity risk assessment report, which shall be updated annually.

Amendment

2. For the purposes set out in paragraph 1, by ... [15 months after the entry into force of this Regulation], ENISA shall conduct a comprehensive analysis of cross-border cybersecurity risks relating to essential and important entities that provide services in more than one Member State or that provide services in one or more Member States and have their network and information systems located in one or more other Member States. The analysis shall evaluate the extent of possible cross-border and internal market consequences of incidents affecting such essential and important entities. For the purpose of this analysis, ENISA shall, in cooperation with the Commission and the Cooperation Group ***and after consulting the competent authorities of the Member States concerned***, develop a methodology. Based on the analysis, ENISA shall draw up a comprehensive cross-border cybersecurity risk assessment report, which shall be

updated annually. *The analysis and report in question shall not include classified information, sensitive information, information pertaining to unpatched vulnerabilities, the results of confidential audits, or information pertaining to the national security, critical infrastructures, essential services, or essential security interests of a Member State, unless the Member State concerned explicitly agrees otherwise.*

Or. fr

Amendment 151
Markus Buchheit

Proposal for a directive
Article 1 – paragraph 1 – point 12
Directive (EU) 2022/2555
Article 1 – paragraph 1 – point 12

Text proposed by the Commission

2. For the purposes set out in paragraph 1, by ... [15 months after the entry into force of this Regulation], ENISA shall conduct a comprehensive analysis of cross-border cybersecurity risks *relating to essential and important entities that provide services in more than one Member State or that provide services in one or more Member States and have their network and information systems located in one or more other Member States. The analysis shall evaluate the extent of possible cross-border and internal market consequences of incidents affecting such essential and important entities.* For the purpose of this analysis, ENISA shall, in cooperation with the Commission *and the Cooperation Group*, develop a methodology. Based on the analysis, ENISA shall draw up a comprehensive cross-border cybersecurity risk assessment report, which shall be updated *annually*.

Amendment

2. For the purposes set out in paragraph 1, by ... [15 months after the entry into force of this **amending** Regulation], ENISA shall conduct a comprehensive analysis of cross-border cybersecurity risks [...]. [...] For the purpose of this analysis, ENISA shall, in *consultation with the Cooperation Group and in* cooperation with the Commission, develop a methodology. Based on the analysis, ENISA shall draw up a comprehensive cross-border cybersecurity risk assessment report, which shall be updated *every two years. ENISA shall base its assessment on the information already available and shall not request any further details from the entities.*

Amendment 152

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Angelika Winzig, Pilar del Castillo Vera

Proposal for a directive

Article 1 – paragraph 1 – point 12

Directive (EU) 2022/2555

Article 37a, paragraph 2

Text proposed by the Commission

2. For the purposes set out in paragraph 1, by ... [15 months after the entry into force of this **Regulation**], ENISA shall conduct a comprehensive analysis of cross-border cybersecurity risks relating to essential and important entities that provide services in more than one Member State or that provide services in one or more Member States and have their network and information systems located in one or more other Member States. The analysis shall evaluate the extent of possible cross-border and internal market consequences of incidents affecting such essential and important entities. For the purpose of this analysis, ENISA shall, in cooperation with the Commission and the Cooperation Group, develop a methodology. Based on the analysis, ENISA shall draw up a comprehensive cross-border cybersecurity risk assessment report, which shall be updated annually.

Amendment

2. For the purposes set out in paragraph 1, by ... [15 months after the entry into force of this **amending Directive**], ENISA shall conduct a comprehensive analysis of cross-border cybersecurity risks relating to essential and important entities that provide services in more than one Member State or that provide services in one or more Member States and have their network and information systems located in one or more other Member States. The analysis shall evaluate the extent of possible cross-border and internal market consequences of incidents affecting such essential and important entities. For the purpose of this analysis, ENISA shall, in cooperation with the Commission and the Cooperation Group, develop a methodology. Based on the analysis, ENISA shall draw up a comprehensive cross-border cybersecurity risk assessment report, which shall be updated annually.

Amendment 153

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 12

Directive 2022/2555

Article 37a

Text proposed by the Commission

Amendment

(a) where appropriate, recommend the relevant competent authorities to set up joint examination teams to support the supervision of specific entities;

(a) ***upon the request or with the agreement of the competent authorities of the Member States concerned, and*** where appropriate, recommend the relevant competent authorities to set up joint examination teams to support the supervision of specific entities;

Or. fr

Amendment 154
Markus Buchheit

Proposal for a directive
Article 1 – paragraph 1 – point 12
Directive (EU) 2022/2555
Article 1 – paragraph 1 – point 12

Text proposed by the Commission

Amendment

(a) ***where appropriate***, recommend the relevant competent authorities to set up joint examination teams to support the supervision of specific entities;

(a) ***at the request of the competent authorities of the relevant Member States:*** recommend the relevant competent authorities to set up joint examination teams to support the supervision of specific entities;

Or. de

Amendment 155
Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive
Article premier – paragraph 1 – point 12
Directive 2022/2555
Article 37a

Text proposed by the Commission

Amendment

(b) develop guidelines for joint supervisory actions;

(b) develop guidelines for joint supervisory actions, ***without prejudice to the national competences of the competent authorities and without***

harmonising national supervisory powers;

Or. fr

Amendment 156

Morten Løkkegaard, Bart Groothuis, Elisabetta Gualmini

Proposal for a directive

Article 1 – paragraph 1 – point 12

Directive 2022/2555

Article 37a(3) – point (d)

Text proposed by the Commission

(d) at the request of the competent authorities of the Member States concerned and subject and proportionate to its own resources, participate in joint supervisory actions;

Amendment

(d) at the request of the competent authorities of the Member States concerned and subject and proportionate to its own resources, participate in joint supervisory actions *in an advisory role*;

Or. en

Amendment 157

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 12

Directive 2022/2555

Article 37a

Text proposed by the Commission

(e) at the request of the competent authorities of the Member States concerned, assist in the assessment of an essential or an important entity's level of implementation of the cybersecurity risk-management measures laid down in Article 21.

Amendment

(e) at the request of the competent authorities of the Member States concerned, assist in the assessment of an essential or an important entity's level of implementation of the cybersecurity risk-management measures laid down in Article 21, *without substituting the assessment and decisions of the competent national authorities*.

Or. fr

Amendment 158
Markus Buchheit

Proposal for a directive
Article 1 – paragraph 1 – point 12
Directive (EU) 2022/2555
Article 1 – paragraph 1 – point 12

Text proposed by the Commission

4. For the purpose of paragraph 3, point (e), of this Article the competent authorities of the Member States concerned shall, where available, provide to ENISA a list of cybersecurity-risk management measures taken by the essential or important entity in accordance with Article 21, a list of supervisory or enforcement actions carried out, as well as the relevant documentation including evidence of implementation of cybersecurity policies, such as the results of security audits, that the competent authorities have undertaken pursuant to Articles 32 and 33 in respect of that entity.

Amendment

4. For the purpose of paragraph 3, point (e), of this Article the competent authorities of the Member States concerned shall, where available **and necessary**, provide to ENISA a list of cybersecurity-risk management measures taken by the essential or important entity in accordance with Article 21, a list of supervisory or enforcement actions carried out, as well as the relevant documentation including evidence of implementation of cybersecurity policies, such as the results of security audits, that the competent authorities have undertaken pursuant to Articles 32 and 33 in respect of that entity. ***The entity concerned shall be informed about the transmission. ENISA shall use the information solely for the purpose of the request in question, safeguard trade secrets and delete the documents once the assistance has been completed.***

Or. de

Amendment 159
Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive
Article premier – paragraph 1 – point 12
Directive 2022/2555
Article 37a

Text proposed by the Commission

4. For the purpose of paragraph 3, point (e), of this Article the competent authorities of the Member States concerned shall, where available, provide to ENISA **a**

Amendment

4. For the purpose of paragraph 3, point (e), of this Article the competent authorities of the Member States concerned shall, where available, provide to ENISA

list of cybersecurity-risk management measures taken by the essential or important entity in accordance with Article 21, a list of supervisory or enforcement actions carried out, as well as the relevant documentation including evidence of implementation of cybersecurity policies, such as the results of security audits, that the competent authorities have undertaken pursuant to Articles 32 and 33 in respect of that entity.

the information strictly necessary for providing the assistance requested, under conditions which ensure its confidentiality. This information shall not include classified information, sensitive information, information pertaining to unpatched vulnerabilities, the results of confidential audits, information pertaining to ongoing supervisory or enforcement measures, or information pertaining to the national security, critical infrastructures, essential services, or essential security interests of a Member State, unless the Member State concerned explicitly agrees otherwise.

Or. fr

Amendment 160

Aleksandar Nikolic, Pierre-Romain Thionnet, Mélanie Disdier, Julie Rechagneux

Proposal for a directive

Article premier – paragraph 1 – point 12

Directive 2022/2555

Article 37a

Text proposed by the Commission

5. Where a Member State receives mutual assistance as referred to in Article 37(1), first subparagraph, point (c), the single point of contact **shall** inform ENISA that mutual assistance took place. Where applicable, the single point of contact shall state which cross-border incident as referred to in Article 23(6) was connected to the case of mutual assistance.

Amendment

5. Where a Member State receives mutual assistance as referred to in Article 37(1), first subparagraph, point (c), the single point of contact **may** inform ENISA that mutual assistance took place **where this is strictly necessary for carrying out the Agency's technical support duties and without prejudice to the protection of sensitive information or information pertaining to the national security of Member States**. Where applicable, the single point of contact shall state which cross-border incident as referred to in Article 23(6) was connected to the case of mutual assistance.

Or. fr

Amendment 161

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 12 a (new)

Directive (EU) 2022/2555

Article 38

Text proposed by the Commission

Amendment

(12a) In Article 38, paragraphs 2, 3 and 6, the words ‘Article 24(2)’ are replaced by ‘Article 21(5), second subparagraph, and Article 24(2)’. The power to adopt delegated acts referred to in Article 21(5), second subparagraph, shall be conferred on the Commission for a period of five years from [the date of entry into force of this amending Directive]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period. The delegation of power referred to in Article 21(5), second subparagraph, may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council. A delegated act adopted pursuant to Article 21(5), second subparagraph, shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act, or if, before the

expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object.

Or. en

Justification

Delegated acts preserve the European Parliament's right of scrutiny and revocation; implementing acts bypass that scrutiny. Article 21(5) technical requirements effectively determine cybersecurity compliance obligations for thousands of entities and must therefore remain under full co-legislator oversight. The standard delegation clause is required as a matter of legislative practice and Interinstitutional Agreement compliance. This is aligned with the ECR CSA2 preference for delegated acts on substantive policy choices.

Amendment 162

Diego Solier

Proposal for a directive

Article 1 – paragraph 1 – point 12 b (new)

Directive (EU) 2022/2555

Article 37a – paragraph 2

Text proposed by the Commission

Amendment

(12b) Article 37a is amended as follows:

2. For the purposes set out in paragraph 1, by ... [15 months after the entry into force of this amending Directive], ENISA shall conduct a comprehensive analysis of cross-border cybersecurity risks relating to essential and important entities that provide services in more than one Member State or that provide services in one or more Member States and have their network and information systems located in one or more other Member States. The cross-border cybersecurity risk assessment report and its annual updates shall be transmitted simultaneously to the European Parliament, to the Council and to the Commission.

3a. The methodology developed pursuant to paragraph 2 shall be subject to a public consultation of not less than eight weeks before its adoption. ENISA shall publish

the draft methodology and all responses received. The European Parliament may issue a non-binding opinion on the draft methodology within three months of its publication; ENISA shall take utmost account of any such opinion.

3b. The cross-border cybersecurity risk assessment report and its annual updates shall indicate, for each finding, the methodology used, the data sources relied upon and any significant uncertainties or gaps in the underlying data. Findings classified for national security reasons shall be transmitted separately to the European Parliament, the Council and the Commission in a classified format.

Or. en

Justification

Simultaneous transmission of the cross-border risk assessment to the co-legislators is essential for democratic oversight. Methodology determines conclusions, so parliamentary input on the methodology is as important as scrutiny of the report. Transparency about data sources and uncertainties prevents disproportionate or misdirected policy responses based on incomplete evidence.

Amendment 163

Ondřej Krutílek

Proposal for a directive

Article 2 – paragraph 1 – subparagraph 1

Text proposed by the Commission

By ... [12 months after entry into force of this Directive], Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

Amendment

By ... [24 months after entry into force of this Directive], Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

Or. en

Amendment 164

Markus Buchheit

Proposal for a directive

Article 2 – paragraph 1 – subparagraph 1

Text proposed by the Commission

By ... [**12** months after entry into force of this Directive], Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

Amendment

By ... [**18** months after entry into force of this Directive], Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

Or. de

Amendment 165

Katri Kulmuni, Eero Heinäluoma

Proposal for a directive

Article 2 – paragraph 1 – subparagraph 1

Text proposed by the Commission

By ... [**12** months after entry into force of this Directive], Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

Amendment

By ... [**24** months after entry into force of this Directive], Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

Or. en

Justification

A sufficient transition period is needed to allow Member States to align national legislation with the changes. The transition period should be at least 24 months after the entry into force of the Directive. In light of the difficulties experienced by Member States in transposing NIS2 and completing national legislative procedures, a 12-month transposition period does not appear feasible.

Amendment 166

Diego Solier

Proposal for a directive

Annex I – point 1 – point a a (new)

Directive (EU) 2022/2555

Text proposed by the Commission

Amendment

(aa) Annex I, point 1, point (d), of the Commission proposal is retained:

(d) in point 5, the first indent in the third column is replaced by the following: ‘- Healthcare providers as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council, excluding providers of services to which Directive 2011/24/EU does not apply pursuant to its Article 1(3), point (a)’

Or. en

Justification

The Rapporteur's deletion of the Commission's healthcare-provider clarification removes legal certainty without substantive justification. Aligning Annex I with the Patients' Rights Directive reduces operational and legal ambiguity for a highly critical sector and should be retained.

Amendment 167

Diego Solier

Proposal for a directive

Annex I – point 1 – point c a (new)

Directive (EU) 2022/2555

Annex I – point 2

Text proposed by the Commission

Amendment

(ca) Annex I, point 2, of the Commission proposal is retained:

2. in Annex II, point 3 is amended as follows: (a) the text in the first column is replaced by the following: ‘3. Manufacture and production of chemicals;’ (b) the text in the third column is replaced by the following: ‘- Undertakings carrying out the manufacture of substances, as referred to in Article 3, point (9), of Regulation (EC) No 1907/2006 of the European Parliament and of the Council, where the

undertaking is subject to the general obligation to register substances on their own or in mixtures pursuant to Article 6 of Regulation (EC) No 1907/2006 - Undertakings carrying out the production of articles, as defined in Article 3, point (3), of Regulation (EC) No 1907/2006, from substances or mixtures, where the undertaking is subject to the obligation to notify substances in articles pursuant to Article 7(2) of Regulation (EC) No 1907/2006'

Or. en

Justification

The Rapporteur's deletion of the Commission's chemicals-sector amendment restores ambiguity contrary to the proposal's simplification objective. REACH-based registration and notification thresholds provide an objective, well-understood legal benchmark for which undertakings fall within NIS2 scope and should be retained.

Amendment 168

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a directive

Annex I – point 1 – point e

Directive (EU) 2022/2555

Annex I, point 8

Text proposed by the Commission

Amendment

– ***Providers of general-purpose AI models with systemic risk***

Or. en

Amendment 169

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a directive
Annex I – point 1 – point e
Directive (EU) 2022/2555
Annex I, point 8

Text proposed by the Commission

Amendment

- ***Operators of AI compute infrastructure, including AI Factories and AI gigafactories established pursuant to Council Regulation (EU) 2021/1173, and providers of hosted inference services***

Or. en

Amendment 170
Christophe Grudler, Morten Løkkegaard

Proposal for a directive
Annex I – point 1 – point e a (new)

Text proposed by the Commission

Amendment

(ea) In point 11, the third column, the following indent is added:

— Space operators, including those operating Union-owned assets, collision avoidance space services providers and primary providers of space-based data, as referred to respectively in Article 2(1), points (a), (b) and (c), of Regulation (EU) [...] ^{1a}

^{1a} Regulation (EU) [...] [Proposal for a Regulation on the safety, resilience and sustainability of Space activities in the Union].;

Or. en

Justification

The current space-sector entry focuses on ground infrastructure. This amendment adds space operators, such as satellite and launch operators, providers helping prevent collisions in orbit, and providers making space-based data first available. It uses the categories identified in the Space Act and expressly includes operators of Union-owned assets.

