



2025/38

15.1.2025

REGULATION (EU) 2025/38 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 19 December 2024

laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 173(3) and Article 322(1), point (a), thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the Court of Auditors ⁽¹⁾,

Having regard to the opinion of the European Economic and Social Committee ⁽²⁾,

Having regard to the opinion of the Committee of the Regions ⁽³⁾,

Acting in accordance with the ordinary legislative procedure ⁽⁴⁾,

Whereas:

- (1) The use of and dependence on information and communication technologies have become fundamental aspects in all sectors of economic activity and society in light of the ever increasing interconnectedness and interdependence of Member State public administrations, businesses and citizens across sectors and borders, simultaneously introducing possible vulnerabilities.
- (2) The magnitude, frequency and impact of cybersecurity incidents, including supply chain attacks for the purposes of cyberespionage, ransomware or disruption, are increasing at Union and global level. They represent a major threat to the functioning of network and information systems. In view of the fast-evolving threat landscape, the threat of possible large-scale cybersecurity incidents causing significant disruption or damage to critical infrastructure demands a heightened preparedness of the Union's cybersecurity framework. That threat goes beyond Russia's war of aggression against Ukraine, and is likely to persist given the multiplicity of actors involved in current geopolitical tensions. Such incidents can impede the provision of public services as cyberattacks are frequently targeted at local, regional or national public services and infrastructure, with local authorities being particularly vulnerable, including due to their limited resources. They can also impede the pursuit of economic activities, including in sectors of high criticality or other critical sectors, generate substantial financial losses, undermine user confidence, cause major damage to the economy and the democratic systems of the Union, and could even have health or life-threatening consequences. Moreover, cybersecurity incidents are unpredictable, as they often emerge and evolve quickly, not contained within any specific geographical area, and occurring simultaneously or spreading instantly across many countries. It is important to have close cooperation between the public sector, the private sector, academia, civil society and the media.
- (3) It is necessary to strengthen the competitive position of industry and services in the Union across the digital economy and support their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market as recommended in three different proposals of the Conference on the Future of Europe. It is necessary to increase the resilience of citizens, businesses, including microenterprises, small and medium-sized enterprises and startups, and entities operating critical infrastructure, against increasing cyber threats, which can have a devastating societal and economic impact. Therefore, investment is needed in infrastructure and services and building

⁽¹⁾ Opinion of 18 April 2023 (not yet published in the Official Journal).

⁽²⁾ OJ C 349, 29.9.2023, p. 167.

⁽³⁾ OJ C, C/2024/1049, 9.2.2024, ELI: <http://data.europa.eu/eli/C/2024/1049/oj>.

⁽⁴⁾ Position of the European Parliament of 24 April 2024 (not yet published in the Official Journal) and decision of the Council of 2 December 2024.

capabilities to develop cybersecurity skills that will support a faster detection of and a faster response to cyber threats and incidents. In addition, Member States need assistance in better preparing for and responding to, as well as assistance in the initial recovery from, significant cybersecurity incidents and large-scale cybersecurity incidents. Building on the existing structures and in close cooperation with them, the Union should also increase its capacities in those areas, in particular as regards the collection and analysis of data on cyber threats and incidents.

- (4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience of critical infrastructure and entities against risks, in particular Regulation (EU) 2019/881 of the European Parliament and of the Council ⁽⁵⁾, Directives 2013/40/EU ⁽⁶⁾ and (EU) 2022/2555 ⁽⁷⁾ of the European Parliament and of the Council and Commission Recommendation (EU) 2017/1584 ⁽⁸⁾. In addition, the Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take measures, and to cooperate with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.
- (5) The growing cybersecurity risks and an overall complex threat landscape, with a clear risk of rapid spillover of incidents from one Member State to others and from a third country to the Union, require the strengthening of solidarity at Union level to better detect, prepare for, respond to, and recover from, cyber threats and incidents, in particular by reinforcing the capabilities of existing structures. Moreover, the Council conclusions of 23 May 2022 on the development of the European Union's cyber posture invited the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity.
- (6) The Joint Communication of the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 10 November 2022 to the European Parliament and the Council on EU Policy on Cyber Defence announced an EU Cyber Solidarity Initiative with the objectives of strengthening of common EU detection, situational awareness and response capabilities by promoting the deployment of an EU infrastructure of Security Operation Centres (SOCs), supporting gradual building of an EU-level cyber reserve with services from trusted private providers and testing of critical entities for potential vulnerabilities based on EU risk assessments.
- (7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to prevent and respond to significant cybersecurity incidents and large-scale cybersecurity incidents. Therefore a pan-European network of cyberhubs (the 'European Cybersecurity Alert System') should be established to build coordinated detection and situational awareness capabilities, reinforcing the Union's threat detection and information-sharing capabilities; a Cybersecurity Emergency Mechanism should be established to support Member States upon their request in preparing for, responding to, mitigating the impact of and initiating recovery from significant cybersecurity incidents and large-scale cybersecurity incidents and to support other users in responding to significant cybersecurity incidents and large-scale-equivalent cybersecurity incidents; and a European Cybersecurity Incident Review Mechanism should be established to review and assess specific significant cybersecurity incidents or large-scale cybersecurity incidents. The actions taken pursuant to this Regulation should be conducted with due respect for Member States' competences and should complement and not duplicate the activities conducted by the CSIRTs network, the European cyber crisis liaison organisation network (EU-CyCLONe) or the Cooperation Group (NIS Cooperation Group), all established pursuant to Directive (EU) 2022/2555. Those actions are without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union (TFEU).

⁽⁵⁾ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

⁽⁶⁾ Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

⁽⁷⁾ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

⁽⁸⁾ Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

- (8) To achieve those objectives, it is necessary to amend Regulation (EU) 2021/694 of the European Parliament and of the Council ⁽⁹⁾ in certain areas. In particular, this Regulation should amend Regulation (EU) 2021/694 as regards the addition of new operational objectives related to the European Cybersecurity Alert System and the Cybersecurity Emergency Mechanism under Specific Objective 3 of the Digital Europe Programme (DEP), which aims to guarantee the resilience, integrity and trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyberattacks and cyber threats and to respond to them, and at reinforcing cross-border cooperation and coordination on cybersecurity. The European Cybersecurity Alert System could play an important role in supporting Member States in anticipating and protecting against cyber threats, and the EU Cybersecurity Reserve could play an important role in supporting Member States, Union institutions, bodies, offices and agencies, and DEP-associated third countries in responding to and mitigating the impact of significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents. That impact could include considerable material or non-material damage and serious public security and safety risks. In light of the specific roles that the European Cybersecurity Alert System and the EU Cybersecurity Reserve could play, this Regulation should amend Regulation (EU) 2021/694 as regards the participation of legal entities that are established in the Union but are controlled from third countries, where there is a real risk that the necessary and sufficient tools, infrastructure and services, or technology, expertise and capacity, are not available in the Union and the benefits of including such entities outweigh the security risk. The specific conditions under which financial support may be granted for actions implementing the European Cybersecurity Alert System and the EU Cybersecurity Reserve should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of those new operational objectives.
- (9) To strengthen the Union's response to cyber threats and incidents, cooperation with international organisations as well as with trusted, like-minded international partners is vital. In that context, trusted, like-minded international partners should be understood to be the countries that share the principles that inspired the Union's creation, namely democracy, the rule of law, the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity, the principles of equality and solidarity, and respect for the principles of the United Nations Charter and international law, and that do not undermine the essential security interests of the Union or its Member States. Such cooperation could also be beneficial with regard to the actions taken pursuant to this Regulation, in particular the European Cybersecurity Alert System and the EU Cybersecurity Reserve. Regulation (EU) 2021/694 should provide, subject to certain availability and security conditions, for tenders for the European Cybersecurity Alert System and the EU Cybersecurity Reserve to be open to legal entities controlled from third countries, subject to security requirements. When assessing the security risk of opening the procurement in this way, it is important to take into account the principles and values which the Union shares with like-minded international partners, where those principles and values are related to essential security interests of the Union. Additionally, where such security requirements are under consideration under Regulation (EU) 2021/694, several elements could be taken into account, such as an entity's corporate structure and decision-making process, the security of data and classified or sensitive information and ensuring that the action's results are not subject to control or restrictions by non-eligible third countries.
- (10) The financing of actions under this Regulation should be provided for in Regulation (EU) 2021/694, which should remain the relevant basic act for the actions enshrined within Specific Objective 3 of the DEP. Specific conditions for participation concerning each action are to be provided for in the relevant work programmes, in accordance with Regulation (EU) 2021/694.
- (11) Horizontal financial rules adopted by the European Parliament and by the Council on the basis of Article 322 TFEU apply to this Regulation. Those rules are laid down in Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council ⁽¹⁰⁾ and determine, in particular, the procedure for establishing and implementing the Union budget, and provide for checks on the responsibility of financial actors. Rules adopted on the basis of

⁽⁹⁾ Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1).

⁽¹⁰⁾ Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (OJ L, 2024/2509, 26.9.2024, ELI: <http://data.europa.eu/eli/reg/2024/2509/oj>).

Article 322 TFEU also include a general regime of conditionality for the protection of the Union budget as established in Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council ⁽¹¹⁾.

- (12) While prevention and preparedness measures are essential to enhance the resilience of the Union in addressing significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents, the occurrence, timing and magnitude of such incidents are, by their nature, unpredictable. The financial resources required to ensure an adequate response can vary significantly from year to year and should be capable of being made available immediately. Reconciling the budgetary principle of predictability with the necessity to react rapidly to new needs therefore requires adaptation of the financial implementation of the work programmes. Consequently, it is appropriate to authorise the carry-over of unused appropriations, but only to the following year and only to the EU Cybersecurity Reserve and the actions supporting mutual assistance, in addition to the carry-over of appropriations authorised pursuant to Article 12(4) of Regulation (EU, Euratom) 2024/2509.
- (13) To more effectively prevent, assess, respond to and recover from cyber threats and incidents, it is necessary to develop more comprehensive knowledge about the threats to critical assets and infrastructure on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyberattacks affecting that infrastructure. A proactive approach to identifying, mitigating and preventing cyber threats includes an increased capacity of advanced detection capabilities. The European Cybersecurity Alert System should consist of several interoperating Cross-Border Cyber Hubs, each grouping together three or more National Cyber Hubs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state-of-the-art technology for advanced collection of relevant data and information, anonymised where appropriate, and analytics tools, enhancing coordinated cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to improve the cyber posture, by increasing detection, aggregation and the analysis of data and information with the aim of preventing cyber threats and incidents and thus complementing and supporting Union entities and networks responsible for cyber crisis management in the Union, in particular EU-CyCLONe.
- (14) Participation in the European Cybersecurity Alert System is voluntary for Member States. Each Member State should designate a single entity at national level tasked with coordinating cyber threat detection activities in that Member State. Those National Cyber Hubs should act as a reference point and gateway at national level for participation in the European Cybersecurity Alert System and should ensure that cyber threat information from public and private entities is shared and collected at national level in an effective and streamlined manner. National Cyber Hubs could strengthen the cooperation and information sharing between public and private entities and could also support the exchange of relevant data and information with relevant sectoral and cross-sectoral communities, including relevant industry Information Sharing and Analysis Centers (ISACs). Close and coordinated cooperation between public and private entities is central to strengthening the Union's cyber resilience. Such cooperation is particularly valuable in the context of sharing cyber threat intelligence to improve active cyber protection. As part of such cooperation and information sharing, National Cyber Hubs could request and receive specific information. Those National Cyber Hubs are neither obliged nor empowered by this Regulation to enforce such requests. Where appropriate and in accordance with Union and national law, the information requested or received could include telemetry, sensor and logging data from entities, such as managed security service providers, that operate in sectors of high criticality or other critical sectors within that Member State, in order to enhance rapid detection of potential cyber threats and incidents at an earlier stage, thereby improving situational awareness. If the National Cyber Hub is not the competent authority designated or established by the relevant Member State pursuant to Article 8(1) of (EU) 2022/2555, it is crucial that it coordinates with that competent authority in respect of requests for and receipt of such data.
- (15) As part of the European Cybersecurity Alert System, a number of Cross-Border Cyber Hubs should be established. Those Cross-Border Cyber Hubs should bring together National Cyber Hubs from at least three Member States to ensure that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-Border Cyber Hubs should be to strengthen capacities to analyse, prevent

⁽¹¹⁾ Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget (OJ L 433 I, 22.12.2020, p. 1, ELI: <http://data.europa.eu/eli/reg/2020/2092/oj>).

and detect cyber threats and to support the production of high-quality cyber threat intelligence, in particular through the sharing of relevant information, anonymised where appropriate, in a trusted and secure environment, from various sources, public or private, as well as through the sharing and joint use of state-of-the-art tools, and the joint development of detection, analysis and prevention capabilities in a trusted and secure environment. Cross-Border Cyber Hubs should provide new additional capacity, building upon and complementing existing SOCs, CSIRTs and other relevant actors, including the CSIRTs network.

- (16) A Member State selected by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) established by Regulation (EU) 2021/887 of the European Parliament and of the Council ⁽¹²⁾ following a call for expressions of interest to set up, or enhance the capabilities of, a National Cyber Hub, should, jointly with the ECCC, purchase relevant tools, infrastructure or services. Such a Member State should be eligible to receive a grant to operate the tools, infrastructure or services. A Hosting Consortium, consisting of at least three Member States, which has been selected by the ECCC following a call for expressions of interest to set up or enhance the capabilities of a Cross-Border Cyber Hub should purchase relevant tools, infrastructure or services jointly with the ECCC. The Hosting Consortium should be eligible to receive a grant to operate the tools, infrastructure or services. The procurement procedure to purchase the relevant tools, infrastructure or services should be carried out jointly by the ECCC and relevant contracting authorities of the Member States selected, following such calls for expressions of interest. Such procurement should comply with Article 168(2) of Regulation (EU, Euratom) 2024/2509, and the ECCC's Financial Rules. Private entities should not therefore be eligible to participate in the calls for expressions of interest to purchase tools, infrastructure or services jointly with the ECCC, or to receive grants to operate those tools, infrastructure or services. However, the Member States should be able to involve private entities in the setting up, enhancement and operation of their National Cyber Hubs and Cross-Border Cyber Hubs in other ways which they deem appropriate, in accordance with Union and national law. Private entities could also be eligible to receive Union funding pursuant to Regulation (EU) 2021/887 for the purpose of providing support to National Cyber Hubs.
- (17) In order to enhance the detection of cyber threats and situational awareness in the Union, a Member State which, following a call for expressions of interest, is selected to set up, or enhance the capabilities of, a National Cyber Hub should commit to applying to participate in a Cross-Border Cyber Hub. If a Member State is not a participant in a Cross-Border Cyber Hub within two years of the date on which the tools, infrastructure or services are acquired or on which it receives grant funding, whichever occurs sooner, it should not be eligible to participate in further Union support actions within the framework of the European Cybersecurity Alert System to enhance the capabilities of its National Cyber Hub. In such cases, entities from Member States could still participate in calls for proposals on other topics under the DEP or other Union funding programmes, including calls on capacities for cyber detection and information sharing, provided that those entities meet the eligibility criteria established in those programmes.
- (18) CSIRTs exchange information within the CSIRTs network in accordance with Directive (EU) 2022/2555. The European Cybersecurity Alert System should constitute a new capability that is complementary to the CSIRTs network by contributing to building a Union situational awareness allowing the reinforcement of the capabilities of the CSIRTs network. Cross-Border Cyber Hubs should coordinate and cooperate closely with the CSIRTs network. They should act by pooling data and sharing relevant information, anonymised where appropriate, on cyber threats from public and private entities, enhancing the value of such data and information through expert analysis and jointly acquired infrastructure and state-of-the-art tools, and contributing to the Union's technological sovereignty, its open strategic autonomy, competitiveness and resilience and to the development of Union capabilities.
- (19) Cross-Border Cyber Hubs should act as central points allowing for a broad pooling of relevant data and cyber threat intelligence, and enable the spreading of threat information among a large and diverse set of stakeholders, such as Computer Emergency Response Teams (CERTs), CSIRTs, ISACs and operators of critical infrastructure. The members of a Hosting Consortium should specify in the consortium agreement the relevant information to be shared among the participants of the Cross-Border Cyber Hub concerned. The information exchanged among participants in a Cross-Border Cyber Hub could include, for instance, data from networks and sensors, threat intelligence feeds, indicators of compromise, and contextualised information about incidents, cyber threats, near misses, vulnerabilities,

⁽¹²⁾ Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202, 8.6.2021, p. 1, ELI: <http://data.europa.eu/eli/reg/2021/887/oj>).

techniques and procedures, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyberattacks. In addition, Cross-Border Cyber Hubs should also enter into cooperation agreements with each other. Such cooperation agreements should, in particular, specify information-sharing principles and interoperability. Their clauses concerning interoperability, in particular information-sharing formats and protocols, should be guided by and therefore take as their starting point interoperability guidelines issued by the European Union Agency for Cybersecurity established by Regulation (EU) 2019/881 (ENISA). Those guidelines should be issued swiftly to ensure that they can be taken into account by Cross-Border Cyber Hubs at an early stage. They should take into account international standards and best practices, and the functioning of any established Cross-Border Cyber Hubs.

- (20) Cross-Border Cyber Hubs and the CSIRTs network should cooperate closely to ensure synergies and complementarity of activities. For that purpose, they should agree on procedural arrangements on cooperation and the sharing of relevant information. This could include the sharing of relevant information on cyber threats and significant cybersecurity incidents and ensuring that experience with state-of-the-art tools, in particular artificial intelligence and data analytics technology, used within the Cross-Border Cyber Hubs, is shared with the CSIRTs network.
- (21) Shared situational awareness among relevant authorities is an indispensable prerequisite for Union-wide preparedness and coordination with regards to significant cybersecurity incidents and large-scale cybersecurity incidents. Directive (EU) 2022/2555 established EU-CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies. Directive (EU) 2022/2555 also established the CSIRTs network to promote swift and effective operational cooperation among all Member States. To ensure situational awareness and strengthen solidarity, in situations where Cross-Border Cyber Hubs obtain information related to a potential or ongoing large-scale cybersecurity incident, they should provide relevant information to the CSIRTs network and inform, as an early warning, EU-CyCLONe. In particular, depending on the situation, information to be shared could include technical information, information about the nature and motives of the attacker or potential attacker, and higher-level, non-technical information about a potential or ongoing large-scale cybersecurity incident. In that context, due regard should be paid to the need-to-know principle and to the potentially sensitive nature of the information shared. Directive (EU) 2022/2555 also reiterates the Commission's responsibilities in the Union Civil Protection Mechanism (UCPM) established by Decision 1313/2013/EU of the European Parliament and of the Council⁽¹³⁾, and its responsibility for providing the analytical reports for the EU Integrated Political Crisis Response Arrangements (IPCR Arrangements) pursuant to Council Implementing Decision (EU) 2018/1993⁽¹⁴⁾. Where Cross-Border Cyber Hubs share relevant information and early warnings related to a potential or ongoing large-scale cybersecurity incident with EU-CyCLONe and the CSIRTs network, it is imperative that that information be shared through those networks with Member States' authorities as well as with the Commission. In that respect, Directive (EU) 2022/2555 provides that EU-CyCLONe's purpose is to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies. EU-CyCLONe's tasks include developing a shared situational awareness of such incidents and crises. It is of paramount importance that EU-CyCLONe ensure, in line with that purpose and its tasks, that such information is provided immediately to the relevant Member State representatives and to the Commission. To that end, it is crucial that EU-CyCLONe's rules of procedure include appropriate provisions.
- (22) Entities participating in the European Cybersecurity Alert System should ensure a high level of interoperability among themselves including, as appropriate, as regards data formats, taxonomy, data handling and data analytics tools. They should also ensure secure communications channels, a minimum level of application layer security, a situational awareness dashboard, and indicators. The adoption of a common taxonomy and the development of a template for situational reports to describe the causes of detected cyber threats and risks, should take into account existing work done in the context of the implementation of Directive (EU) 2022/2555.

⁽¹³⁾ Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924, ELI: <http://data.europa.eu/eli/dec/2013/1313/oj>).

⁽¹⁴⁾ Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements (OJ L 320, 17.12.2018, p. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

- (23) In order to enable the exchange of relevant data and information on cyber threats from various sources, on a large-scale basis, in a trusted and secure environment, entities participating in the European Cybersecurity Alert System should be equipped with state-of-the-art, highly secure tools, equipment and infrastructure, as well as skilled personnel. This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, in particular by using the latest artificial intelligence and data analytics technologies.
- (24) By collecting, analysing, sharing and exchanging relevant data and information, the European Cybersecurity Alert System should enhance the Union's technological sovereignty and open strategic autonomy in the area of cybersecurity, competitiveness and resilience. The pooling of high-quality, curated data could also contribute to the development of advanced artificial intelligence and data analytics technologies. Human oversight and, to that end, a skilled labour force remains essential for the effective pooling of high-quality data.
- (25) While the European Cybersecurity Alert System is a civilian project, the cyber defence community could benefit from stronger civilian detection and situational awareness capabilities developed for the protection of critical infrastructure.
- (26) Information sharing among participants of the European Cybersecurity Alert System should comply with existing legal requirements and in particular Union and national data protection law, as well as the Union rules on competition governing the exchange of information. The recipient of the information should implement, insofar as the processing of personal data is necessary, technical and organisational measures that safeguard the rights and freedoms of data subjects, and destroy the data as soon as they are no longer necessary for the stated purpose and inform the entity making the data available that the data have been destroyed.
- (27) Preserving confidentiality and information security are of paramount importance for all three pillars of this Regulation, whether for encouraging the sharing or exchange of information in the context of the European Cybersecurity Alert System, preserving the interests of the entities applying for support under the Cybersecurity Emergency Mechanism, or ensuring that reports under the European Cybersecurity Incident Review Mechanism can yield useful lessons learned without having a negative impact on the entities affected by the incidents. The participation of Member States and entities in those mechanisms depend on relationships of trust between their components. Where information is confidential pursuant to Union or national rules, its sharing or exchange under this Regulation should be limited to that which is relevant and proportionate to the purpose of the sharing or exchange. That sharing or exchange should also preserve the confidentiality of that information, including protecting the security and commercial interests of any entities concerned. Information sharing or exchange pursuant to this Regulation could take place using non-disclosure agreements, or guidance on information distribution such as the traffic light protocol (TLP). The TLP is to be understood as a means to provide information about any limitations with regard to the further spreading of information. It is used in almost all CSIRTs and in some ISACs. In addition to those general requirements, when it comes to the European Cybersecurity Alert System, Hosting Consortia agreements should lay down specific rules regarding the conditions for information sharing within the Cross-Border Cyber Hub concerned. Those agreements could, in particular, require that information be shared only in accordance with Union and national law.
- (28) In respect of the deployment of the EU Cybersecurity Reserve, specific confidentiality rules are necessary. Support will be requested, assessed and provided in a crisis context and in respect of entities operating in sensitive sectors. For the EU Cybersecurity Reserve to function effectively, it is essential that users and entities are able to share, and provide access, without delay, to all information that is necessary for each entity to play its part in the assessment of requests and the deployment of support. Accordingly, this Regulation should provide that all such information is to be used or shared only where necessary for the operation of the EU Cybersecurity Reserve, and that information that is confidential or classified pursuant to Union and national law is to be used and shared only in accordance with that law. Additionally, users should be able, where appropriate, to use information-sharing protocols such as the TLP to further specify limitations. Whilst users have discretion in this regard, it is important that when applying such limitations, they take into account the possible consequences, in particular with regard to delayed assessment or delivery of the requested services. In order to have an efficient EU Cybersecurity Reserve, it is important that the

contracting authority clarify those consequences to the user before it submits a request. Those safeguards are limited to the request and provision of EU Cybersecurity Reserve services and do not affect information exchange in other contexts, such as in the procurement of the EU Cybersecurity Reserve.

- (29) In view of the increasing risks and number of incidents affecting Member States, it is necessary to set up a crisis support instrument, namely the Cybersecurity Emergency Mechanism, to improve the Union's resilience to significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, incident response and initial recovery of essential services. As the full recovery from an incident is a comprehensive process of restoring the functioning of the entity affected by the incident to the state from before the incident and could be a long process that entails significant costs, the support from the EU Cybersecurity Reserve should be limited to the initial stage of the recovery process, leading to the restoration of basic functionalities of the systems. The Cybersecurity Emergency Mechanism should enable the rapid and effective deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the primary responsibility for preventing, preparing for and responding to incidents and crises lies with the Member States, the Cybersecurity Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union (TEU).
- (30) The Cybersecurity Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in the case of response to, and initial recovery from, significant cybersecurity incidents and large-scale cybersecurity incidents, such as the services provided by ENISA in accordance with its mandate, the coordinated response and the assistance from the CSIRTs network, the mitigation support from EU-CyCLONe, as well as mutual assistance between Member States including in the context of Article 42(7) TEU and the permanent structured cooperation (PESCO) Cyber Rapid Response Teams established pursuant to Council Decision (CFSP) 2017/2315 ⁽¹⁵⁾. It should address the need to ensure that specialised means are available to support preparedness for, response to and recovery from such incidents across the Union and in DEP-associated third countries.
- (31) This Regulation is without prejudice to procedures and frameworks to coordinate crisis responses at Union level, in particular Directive (EU) 2022/2555, the Union Civil Protection Mechanism established by Decision No 1313/2013/EU of the European Parliament and of the Council ⁽¹⁶⁾, the IPCR Arrangements and Commission Recommendation (EU) 2017/1584 ⁽¹⁷⁾. Support provided under the Cybersecurity Emergency Mechanism can complement assistance provided in the context of the common foreign and security policy and the common security and defence policy, including through the Cyber Rapid Response Teams, taking into account the civilian nature of the Cybersecurity Emergency Mechanism. Support provided under the Cybersecurity Emergency Mechanism can complement actions implemented in the context of Article 42(7) TEU, including assistance provided by one Member State to another Member State, or form part of the joint response between the Union and Member States or in situations referred to in Article 222 TFEU. The implementation of this Regulation should also be coordinated with the implementation of measures under the Cyber Diplomacy Toolbox, where appropriate.
- (32) Assistance provided under this Regulation should be in support of, and complementary to, the actions taken by Member States at national level. To that end, close cooperation and consultation between the Commission, ENISA, the Member States and, where relevant, the ECCC should be ensured. When requesting support under the Cybersecurity Emergency Mechanism, Member States should provide relevant information justifying the need for support.
- (33) Directive (EU) 2022/2555 requires Member States to designate or establish one or more cyber crisis management authorities and ensure that they have adequate resources to carry out their tasks in an effective and efficient manner. It also requires Member States to identify capabilities, assets and procedures that can be deployed in the case of a crisis as well as to adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. Member States are also required to establish one or more CSIRTs tasked with incident-handling responsibilities in accordance with

⁽¹⁵⁾ Council Decision (CFSP) 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States (OJ L 331, 14.12.2017, p. 57, ELI: <http://data.europa.eu/eli/dec/2017/2315/oj>).

⁽¹⁶⁾ Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

⁽¹⁷⁾ Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

a well-defined process and covering at least the sectors, subsectors and types of entity under the scope of that Directive, and to ensure that they have adequate resources to carry out effectively their tasks. This Regulation is without prejudice to the Commission's role in ensuring the compliance by Member States with the obligations of Directive (EU) 2022/2555. The Cybersecurity Emergency Mechanism should provide assistance for actions aiming to reinforce preparedness as well as incident response actions to mitigate the impact of significant cybersecurity incidents and large-scale cybersecurity incidents, to support initial recovery or to restore the basic functionalities of the services provided by entities operating in sectors of high criticality or entities operating in other critical sectors.

- (34) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in sectors of high criticality identified pursuant to Directive (EU) 2022/2555 in a coordinated manner, including through exercise and training. For that purpose, the Commission, after consulting ENISA, the NIS Cooperation Group and EU-CyCLONe, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated preparedness testing at Union level. The sectors or subsectors should be selected from the sectors of high criticality listed in Annex I to Directive (EU) 2022/2555. The coordinated preparedness testing should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture conducted by the Commission, the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative') and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including EU-CyCLONe, as well as the risk assessment of communications networks and infrastructure requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications established by Regulation (EU) 2018/1971 of the European Parliament and of the Council⁽¹⁸⁾, the Union level coordinated security risk assessments of critical supply chains to be conducted pursuant to Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council⁽¹⁹⁾. The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.
- (35) In addition, the Cybersecurity Emergency Mechanism should provide support for other preparedness actions and support preparedness in other sectors, not covered by the coordinated preparedness testing of entities operating in sectors of high criticality or entities operating in other critical sectors. Those actions could include various types of national preparedness activity.
- (36) When Member States receive grants to support preparedness actions, entities in sectors of high criticality can participate in those actions on a voluntary basis. It is good practice that following such actions, participating entities draw up a remediation plan to implement any resulting recommendations of specific measures to benefit to the fullest extent from the preparedness action. While it is important that Member States request as part of the actions, that participating entities draw up and implement such remediation plans, Member States are neither obliged nor empowered by this Regulation to enforce such requests. Such requests are without prejudice to requirements for entities and supervisory powers for competent authorities in accordance with Directive (EU) 2022/2555.
- (37) The Cybersecurity Emergency Mechanism should also provide support for incident response actions to mitigate the impact of significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents, to support initial recovery or restore the functioning of essential services. Where appropriate, it should complement the UCPM to ensure a comprehensive approach to respond to the impact of incidents on citizens.

⁽¹⁸⁾ Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Agency for Support for BEREC (BEREC Office), amending Regulation (EU) 2015/2120 and repealing Regulation (EC) No 1211/2009 (OJ L 321, 17.12.2018, p. 1).

⁽¹⁹⁾ Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).

- (38) The Cybersecurity Emergency Mechanism should support technical assistance provided by one Member State to another Member State that is affected by a significant cybersecurity incident or large-scale cybersecurity incident, including by CSIRTs as referred to in Article 11(3), point (f), of Directive (EU) 2022/2555. Member States providing such assistance should be allowed to submit requests to cover costs related to dispatching of expert teams in the framework of mutual assistance. The eligible costs could include travel, accommodation and daily allowance expenses of cybersecurity experts.
- (39) Given the essential role that private undertakings play in the detection of, preparedness for and response to large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents, it is important to recognise the value of voluntary pro bono cooperation with such undertakings, whereby they offer services without remuneration in the case of large-scale cybersecurity incidents and crises and large-scale-equivalent cybersecurity incidents and crises. ENISA, in cooperation with EU-CyCLONe could monitor the evolution of such pro bono initiatives and promote their compliance with the criteria applicable to trusted managed security service providers under this Regulation, including in relation to the trustworthiness of private undertakings, their experience as well as the ability to handle sensitive information in a secure manner.
- (40) As part of the Cybersecurity Emergency Mechanism, an EU Cybersecurity Reserve should gradually be set up, consisting of services from trusted managed security service providers to support response and initiate recovery actions in the case of significant cybersecurity incidents, large-scale cybersecurity incidents or large-scale-equivalent cybersecurity incidents affecting Member States, Union institutions, bodies, offices or agencies, or DEP-associated third countries. The EU Cybersecurity Reserve should ensure the availability and readiness of services. It should therefore include services that are committed in advance, including for instance capacities that are on stand-by and deployable at short notice. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in sectors of high criticality or to affected entities operating in other critical sectors as a complement to their own actions at national level. The services from the EU Cybersecurity Reserve should also be able to serve to support Union institutions, bodies, offices and agencies, under similar conditions. The EU Cybersecurity Reserve could also contribute to strengthening the competitive position of industry and services in the Union across the digital economy, including microenterprises and small and medium-sized enterprises as well as start-ups, including by providing incentives for investment in research and innovation. It is important to take into account ENISA's European cybersecurity skills framework when procuring the services for the EU Cybersecurity Reserve. When requesting support from the EU Cybersecurity Reserve, users should include in their application appropriate information regarding the affected entity and potential impact, information about the requested service from the EU Cybersecurity Reserve, and the support provided to the affected entity at the national level, which should be taken into account when assessing the request from the applicant. To ensure complementarity with other forms of support available to the affected entity, the request should also include, where available, information on contractual arrangements in place for incident response and initial recovery services, as well as insurance contracts potentially covering such a type of incident.
- (41) In order to ensure the effective use of Union funding, pre-committed services under the EU Cybersecurity Reserve should be convertible, in accordance with the relevant contract, into preparedness services related to incident prevention and response in the event that those pre-committed services are not used for incident response during the time for which they are pre-committed. Those services should be complementary to and should not duplicate the preparedness actions to be managed by the ECCC.
- (42) Requests for support from the EU Cybersecurity Reserve from Member States' cyber crisis management authorities and CSIRTs, or CERT-EU on behalf of Union institutions, bodies, offices and agencies, should be assessed by the contracting authority. Where ENISA has been entrusted with the administration and operation of the EU Cybersecurity Reserve, that contracting authority is ENISA. Requests for support from DEP-associated third countries should be assessed by the Commission. To facilitate the submission and assessment of requests for support, ENISA could set up a secure platform.
- (43) Where multiple concurrent requests are received, those requests should be prioritised in accordance with criteria laid down in this Regulation. In light of the general objectives of this Regulation, those criteria should include the scale and severity of the incident, the type of entity affected, the potential impact of the incident on the Member States and users affected, the potential cross-border nature of the incident and risk of spillover, and the measures already taken by the user to assist the response and initial recovery. In light of those objectives and given that requests from

Member State users are exclusively intended to support, across the Union, entities operating in sectors of high criticality or entities operating in other critical sectors, it is appropriate to give higher priority to requests from Member State users where those criteria lead to two or more requests being assessed as equal. This is without prejudice to any obligations that Member States may have under relevant hosting agreements to take measures to protect and assist Union institutions, bodies, offices and agencies.

- (44) The Commission should have overall responsibility for the implementation of the EU Cybersecurity Reserve. Given the extensive experience gained by ENISA with cybersecurity support action, ENISA is the most suitable agency to implement the EU Cybersecurity Reserve. Therefore, the Commission should entrust ENISA, partially or, where the Commission considers it to be appropriate, entirely with the operation and administration of the EU Cybersecurity Reserve. The entrustment should be carried out in accordance with the applicable rules under Regulation (EU, Euratom) 2024/2509 and in particular should be subject to the relevant conditions for signing a contribution agreement being fulfilled. Any aspects of the operation and administration of the EU Cybersecurity Reserve not entrusted to ENISA should be subject to direct management by the Commission, including prior to the signing of the contribution agreement.
- (45) Member States should have a key role in the constitution, deployment and post-deployment of the EU Cybersecurity Reserve. As Regulation (EU) 2021/694 is the relevant basic act for actions implementing the EU Cybersecurity Reserve, the actions under the EU Cybersecurity Reserve should be provided for in the work programmes referred to in Article 24 of Regulation (EU) 2021/694. Pursuant to paragraph 6 of that Article, those work programmes are to be adopted by the Commission by means of implementing acts in accordance with the examination procedure. Furthermore, the Commission, in coordination with the NIS Cooperation Group, should determine the priorities and the evolution of the EU Cybersecurity Reserve.
- (46) The contracts established within the framework of the EU Cybersecurity Reserve should not affect the business-to-business relationship and existing obligations between the affected entity or users and the service provider.
- (47) For the purpose of selecting private service providers to provide services in the context of the EU Cybersecurity Reserve, it is necessary to establish a set of minimum criteria and requirements that should be included in the call for tenders to select those providers, so as to ensure that the needs of Member States' authorities, entities operating in sectors of high criticality and entities operating in other critical sectors are met. In order to address the specific needs of Member States, when procuring services for the EU Cybersecurity Reserve, the contracting authority should, where appropriate, develop selection criteria and requirements additional to those laid down in this Regulation. It is important to encourage the participation of smaller providers, active at regional and local level.
- (48) When selecting providers for inclusion in the EU Cybersecurity Reserve, the contracting authority should aim to ensure that the EU Cybersecurity Reserve, when taken as a whole, contains providers that are able to accommodate users' language requirements. To that end, the contracting authority should, before preparing tender specifications, inquire whether the potential users of the EU Cybersecurity Reserve have specific language requirements, so that EU Cybersecurity Reserve support services can be provided in a language from among the official languages of the Union institutions or of the Member States, likely to be understood by the user or affected entity. In the case that more than one language is required by a user for the provision of EU Cybersecurity Reserve support services and those services have been procured in those languages for that user, the user should be able to specify, in the request for EU Cybersecurity Reserve support, in which of those languages the services should be provided in relation to the specific incident giving rise to the request.
- (49) To support the establishment of the EU Cybersecurity Reserve, it is important that the Commission requests ENISA to prepare a candidate cybersecurity certification scheme for managed security services pursuant to Regulation (EU) 2019/881, in the areas covered by the Cybersecurity Emergency Mechanism.
- (50) In order to support the objectives of this Regulation of promoting shared situational awareness, enhancing the Union's resilience and enabling effective response to significant cybersecurity incidents and large-scale cybersecurity incidents, the Commission or EU-CyCLONe should be able to request ENISA, with the support of the CSIRTs network and with the approval of the Member States concerned, to review and assess cyber threats, known exploitable vulnerabilities and mitigation actions with respect to a specific significant cybersecurity incident or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA should prepare an incident review report, in collaboration with the Member State concerned, relevant stakeholders,

including representatives from the private sector, the Commission and other relevant Union institutions, bodies, offices and agencies. Building on the collaboration with stakeholders, including from the private sector, the review report on specific incidents should aim to assess the causes, impact and mitigation of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered to EU-CyCLONe, the CSIRTs network and the Commission and should be used to inform their work as well as that of ENISA. Where the incident relates to a DEP-associated third country, the Commission should also provide the report to the High Representative.

- (51) Taking into account the unpredictable nature of cyberattacks and the fact that they are often not contained in a specific geographical area and pose a high risk of spillover, the strengthening of resilience of neighbouring countries and their capacity to respond effectively to significant cybersecurity incidents and large-scale-equivalent cybersecurity incidents contributes to the protection of the Union, and in particular its internal market and industry, as a whole. Such activities could further contribute to the Union's cyber diplomacy. Therefore, DEP-associated third countries should be able to request support from the EU Cybersecurity Reserve, in all or part of their territories, where this is provided for in the agreement through which the third country is associated to the DEP. The funding for DEP-associated third countries should be supported by the Union in the framework of relevant partnerships and funding instruments for those countries. The support should cover services in the area of response to and initial recovery from significant cybersecurity incidents or large-scale-equivalent cybersecurity incidents.
- (52) The conditions set for the EU Cybersecurity Reserve and trusted managed security service providers in this Regulation should apply when providing support to DEP-associated third countries. DEP-associated third countries should be able to request support from the EU Cybersecurity Reserve where the entities targeted and for which they request support from the EU Cybersecurity Reserve are entities operating in sectors of high criticality or entities operating in other critical sectors and where the incidents detected lead to significant operational disruptions or might have spillover effects in the Union. DEP-associated third countries should only be eligible to receive support where the agreement through which they are associated to the DEP specifically provides for such support. In addition, such third countries should remain eligible only so long as three criteria are fulfilled. First, the third country should be complying in full with the relevant terms of that agreement. Second, given the complementary nature of the EU Cybersecurity Reserve, the third country should have taken adequate steps to prepare for significant cybersecurity incidents or large-scale-equivalent cybersecurity incidents. Third, the provision of support from the EU Cybersecurity Reserve should be consistent with the Union's policy towards and overall relations with that country and with other Union policies in the field of security. In the context of its assessment of the compliance with that third criterion, the Commission should consult the High Representative for the alignment of the granting of such support with the common foreign and security policy.
- (53) The provision of support to DEP-associated third countries may affect relations with third countries and the Union's security policy, including in the context of the common foreign and security policy and the common security and defence policy. Accordingly, it is appropriate for the Council to be granted implementing powers to authorise and specify the period during which such support can be provided. The Council should act on the basis of a Commission proposal, taking due account of the Commission's assessment of the three criteria. The same should apply to renewals and to proposals to amend or repeal such acts. Where, in exceptional circumstances, the Council considers there to have been a significant change of circumstances in respect of the third criterion, the Council should be able to act on its own initiative to amend or repeal an implementing act, without awaiting a Commission proposal. Such significant changes are likely to require urgent action, to have particularly important implications for relations with third countries, and not to require detailed assessment in advance by the Commission. Moreover, the Commission should cooperate with the High Representative in respect of requests for support from DEP-associated third countries and the implementation of support granted to such third countries. The Commission should also take into account any views provided by ENISA in respect of such requests and support. The Commission should inform the Council about the outcome of the assessment of the requests, including relevant considerations made in that regard, and the services that are deployed.

- (54) The Commission communication of 18 April 2023 on the Cyber Skills Academy acknowledged the shortage of skilled professionals. Such skills are needed to pursue the objectives of this Regulation. The Union urgently needs professionals with the skills and competences to prevent, detect and deter cyberattacks and defend the Union, including its most critical infrastructure, against such attacks and ensure its resilience. To that end, it is important to encourage cooperation among stakeholders, including from the private sector, academia and public sector. It is equally important to create synergies, in all territories of the Union, for investment in education and training to promote the creation of safeguards to avoid a brain drain or the widening of the skills gap in some regions more than in others. It is urgent that the cybersecurity skills gap, with a particular focus on reducing the gender gap in the cybersecurity workforce to promote women's presence and participation in the design of digital governance, be closed.
- (55) In order to boost the innovation in the Digital Single Market, strengthening research and innovation in cybersecurity is important, with a view to contributing to increasing the resilience of Member States and the open strategic autonomy of the Union, both of which are objectives of this Regulation. Synergies are essential to strengthen cooperation and coordination among the different stakeholders, including from the private sector, civil society and academia.
- (56) This Regulation should take into account the commitment set out in the Joint Declaration of 26 January 2022 of the European Parliament, the Council and the Commission entitled 'European Declaration on Digital Rights and Principles for the Digital Decade' to protect the interests of the Union's democracies, people, businesses and public institutions against cybersecurity risks and cybercrime including data breaches and identity theft or manipulation.
- (57) In order to supplement certain non-essential elements of this Regulation, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to specify the types and number of response services required for the EU Cybersecurity Reserve. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making⁽²⁰⁾. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.
- (58) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to specify further the detailed procedural arrangements for allocating the EU Cybersecurity Reserve support services. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council⁽²¹⁾.
- (59) Without prejudice to the rules relating to the Union's annual budget under the Treaties, the Commission should take into account the obligations arising from this Regulation when assessing the budgeting and staffing needs of ENISA.
- (60) The Commission should carry out an evaluation of the measures laid down in this Regulation on a regular basis. The first such evaluation should take place in the first 2 years after the date of entry into force of this Regulation and at least every 4 years thereafter, taking into account the timing of the revision of the multiannual financial framework established pursuant to Article 312 TFEU. The Commission should submit a report on progress made to the European Parliament and to the Council. In order to assess the different elements required, including the extent of information shared within the European Cybersecurity Alert System, the Commission should base itself exclusively on information that is readily available or voluntarily provided. Taking into consideration geopolitical developments and in order to ensure continuity and further development of the measures laid down in this Regulation beyond 2027, it is important that the Commission assess the necessity to allocate an appropriate budget in the multiannual financial framework for 2028 to 2034.

⁽²⁰⁾ OJ L 123, 12.5.2016, p. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

⁽²¹⁾ Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13, ELI: <http://data.europa.eu/eli/reg/2011/182/oj>).

- (61) Since the objectives of this Regulation, namely to reinforce the competitive position of industry and services in the Union across the digital economy and to contribute to the Union's technological sovereignty and open strategic autonomy in the area of cybersecurity, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject-matter and objectives

1. This Regulation lays down measures to strengthen capacities in the Union to detect, prepare for and respond to cyber threats and incidents, in particular by establishing:
 - (a) a pan-European network of cyber hubs (European Cybersecurity Alert System) to build and enhance coordinated detection and common situational awareness capabilities;
 - (b) a Cybersecurity Emergency Mechanism to support Member States in preparing for, responding to, mitigating the impact of and initiating recovery from significant cybersecurity incidents and large-scale cybersecurity incidents and to support other users in responding to significant cybersecurity incidents and large-scale-equivalent cybersecurity incidents;
 - (c) a European Cybersecurity Incident Review Mechanism to review and assess significant cybersecurity incidents or large-scale cybersecurity incidents.
2. This Regulation pursues the general objectives of reinforcing the competitive position of industry and services in the Union across the digital economy, including microenterprises and small and medium-sized enterprises as well as start-ups, and of contributing to the Union's technological sovereignty and open strategic autonomy in the area of cybersecurity, including by boosting innovation in the Digital Single Market. It pursues those objectives by strengthening solidarity at Union level, reinforcing the cybersecurity ecosystem, enhancing Member States' cyber resilience and developing the skills, knowhow, abilities and competencies of the workforce in relation to cybersecurity.
3. The achievement of the general objectives referred to in paragraph 2 shall be pursued through the following specific objectives:
 - (a) to strengthen common coordinated Union detection capacities and common situational awareness of cyber threats and incidents;
 - (b) to reinforce preparedness of entities operating in sectors of high criticality or entities operating in other critical sectors across the Union and strengthen solidarity by developing coordinated preparedness testing and enhanced response and recovery capacities to handle significant cybersecurity incidents, large-scale cybersecurity incidents or large-scale-equivalent cybersecurity incidents, including the possibility of making Union cybersecurity incident response support available for DEP-associated third countries;
 - (c) to enhance the Union's resilience and contribute to effective incident response by reviewing and assessing significant cybersecurity incidents or large-scale cybersecurity incidents, including drawing lessons learned and, where appropriate, recommendations.
4. The actions under this Regulation shall be conducted with due respect to the Member States' competences and shall be complementary to the activities carried out by the CSIRTs network, EU-CyCLONe and the NIS Cooperation Group.

5. This Regulation is without prejudice to the Member States' essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

6. The sharing or exchange of information under this Regulation that is confidential pursuant to Union or national rules shall be limited to that which is relevant and proportionate to the purpose of that sharing or exchange. Such sharing or exchange of information shall preserve the confidentiality of the information, and protect the security and commercial interests of the entities concerned. It shall not entail the supply of information the disclosure of which would be contrary to the Member States' essential interests of national security, public security or defence.

Article 2

Definitions

For the purposes of this Regulation, the following definitions apply:

- (1) 'Cross-Border Cyber Hub' means a multi-country platform, established by a written consortium agreement that brings together in a coordinated network structure National Cyber Hubs from at least three Member States, and that is designed to enhance the monitoring, detection and analysis of cyber threats to prevent incidents and to support the production of cyber threat intelligence, in particular through the exchange of relevant data and information, anonymised where appropriate, as well as through the sharing of state-of-the-art tools and the joint development of cyber detection, analysis, and prevention and protection capabilities in a trusted environment;
- (2) 'Hosting Consortium' means a consortium composed of participating Member States, that have agreed to establish and to contribute to the acquisition of tools, infrastructure or services for, and the operation of, a Cross-Border Cyber Hub;
- (3) 'CSIRT' means a CSIRT designated or established pursuant to Article 10 of Directive (EU) 2022/2555;
- (4) 'entity' means an entity as defined in Article 6, point (38), of Directive (EU) 2022/2555;
- (5) 'entities operating in sectors of high criticality' means the types of entity listed in Annex I to Directive (EU) 2022/2555;
- (6) 'entities operating in other critical sectors' means the types of entity listed in Annex II to Directive (EU) 2022/2555;
- (7) 'risk' means risk as defined in Article 6, point (9), of Directive (EU) 2022/2555;
- (8) 'cyber threat' means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;
- (9) 'incident' means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;
- (10) 'significant cybersecurity incident' means an incident fulfilling the criteria set out in Article 23(3) of Directive (EU) 2022/2555;
- (11) 'major incident' means a major incident as defined in Article 3, point (8), of Regulation (EU, Euratom) 2023/2841 of the European Parliament and the Council⁽²²⁾;
- (12) 'large-scale cybersecurity incident' means a large-scale cybersecurity incident as defined in Article 6, point (7), of Directive (EU) 2022/2555;

⁽²²⁾ Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (OJ L, 2023/2841, 18.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2841/oj>).

- (13) 'large-scale-equivalent cybersecurity incident' means, in the case of Union institutions, bodies, offices and agencies, a major incident and, in the case of DEP-associated third countries, an incident which causes a level of disruption that exceeds the capacity of the DEP-associated third country concerned to respond to it;
- (14) 'DEP-associated third country' means a third country which is party to an agreement with the Union allowing for its participation in the Digital Europe Programme pursuant to Article 10 of Regulation (EU) 2021/694;
- (15) 'contracting authority' means the Commission or, to the extent that the operation and administration of the EU Cybersecurity Reserve has been entrusted to ENISA pursuant to Article 14(5), ENISA;
- (16) 'managed security service provider' means a managed security service provider as defined in Article 6, point (40), of Directive (EU) 2022/2555;
- (17) 'trusted managed security service providers' means managed security service providers selected to be included in the EU Cybersecurity Reserve in accordance with Article 17.

CHAPTER II

THE EUROPEAN CYBERSECURITY ALERT SYSTEM

Article 3

Establishment of the European Cybersecurity Alert System

1. A pan-European network of infrastructure that consists of National Cyber Hubs and Cross-Border Cyber Hubs joining on a voluntary basis, the European Cybersecurity Alert System, shall be established to support the development of advanced capabilities for the Union to enhance detection, analysis and data processing capabilities in relation to cyber threats and the prevention of incidents in the Union.
2. The European Cybersecurity Alert System shall:
 - (a) contribute to better protection from and responses to cyber threats by supporting and cooperating with, and reinforcing the capabilities of, relevant entities, in particular CSIRTs, the CSIRTs network, EU-CyCLONe and competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555;
 - (b) pool relevant data and information on cyber threats and incidents from various sources within the Cross-Border Cyber Hubs and share analysed or aggregated information through Cross-Border Cyber Hubs, where relevant with the CSIRTs network;
 - (c) collect and support the production of high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools and advanced technologies, and share that information and cyber threat intelligence;
 - (d) contribute to enhancing the coordinated detection of cyber threats and common situational awareness across the Union, and to the issuing of alerts, including, where relevant, by providing concrete recommendations to entities;
 - (e) provide services and activities for the cybersecurity community in the Union, including contributing to the development of advanced tools and technologies, such as artificial intelligence and data analytics tools.
3. Actions implementing the European Cybersecurity Alert System shall be supported by funding from the Digital Europe Programme (DEP) and implemented in accordance with Regulation (EU) 2021/694, in particular Specific Objective 3 thereof.

*Article 4***National Cyber Hubs**

1. Where a Member State decides to participate in the European Cybersecurity Alert System, it shall designate or, where applicable, establish a National Cyber Hub for the purposes of this Regulation.
2. A National Cyber Hub shall be a single entity acting under the authority of a Member State. It may be a CSIRT or, where applicable, a national cyber crisis management authority or other competent authority designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555, or another entity. The National Cyber Hub shall:
 - (a) have the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cyber threats and incidents and to contribute to a Cross-Border Cyber Hub as referred to in Article 5; and
 - (b) be capable of detecting, aggregating, and analysing data and information relevant to cyber threats and incidents, such as cyber threat intelligence, by using in particular state-of-the-art technologies, with the aim of preventing incidents.
3. As part of the functions referred to in paragraph 2 of this Article, National Cyber Hubs may cooperate with private sector entities to exchange relevant data and information for the purpose of detecting and preventing cyber threats and incidents, including with sectoral and cross-sectoral communities of essential and important entities as referred to in Article 3 of Directive (EU) 2022/2555. Where appropriate and in accordance with Union and national law, the information requested or received by National Cyber Hubs may include telemetry, sensor and logging data.
4. A Member State selected pursuant to Article 9(1) shall commit to applying for its National Cyber Hub to participate in a Cross-Border Cyber Hub.

*Article 5***Cross-Border Cyber Hubs**

1. Where at least three Member States are committed to ensuring that their National Cyber Hubs work together to coordinate their cyber-detection and threat monitoring activities, those Member States may establish a Hosting Consortium for the purposes of this Regulation.
2. A Hosting Consortium shall be composed of at least three participating Member States that have agreed to establish and contribute to the acquisition of tools, infrastructure or services for, and the operation of, a Cross-Border Cyber Hub, in accordance with paragraph 4.
3. Where a Hosting Consortium is selected in accordance with Article 9(3), its members shall conclude a written consortium agreement which:
 - (a) sets out the internal arrangements for implementing the hosting and usage agreement referred to in Article 9(3);
 - (b) establishes the Hosting Consortium's Cross-Border Cyber Hub; and
 - (c) includes the specific clauses required pursuant to Article 6(1) and (2).
4. A Cross-Border Cyber Hub shall be a multi-country platform established by a written consortium agreement as referred to in paragraph 3. It shall bring together in a coordinated network structure the National Cyber Hubs of the Hosting Consortium's Member States. It shall be designed to enhance the monitoring, detection and analysis of cyber threats, to prevent incidents and to support the production of cyber threat intelligence, in particular through the exchange of relevant data and information, anonymised where appropriate, as well as through the sharing of state-of-the-art tools and the joint development of cyber detection, analysis, and prevention and protection capabilities in a trusted environment.
5. A Cross-Border Cyber Hub shall be represented for legal purposes by a member of the corresponding Hosting Consortium acting as a coordinator, or by the Hosting Consortium if it has legal personality. Responsibility for compliance by the Cross-Border Cyber Hub with this Regulation and the hosting and usage agreement shall be allocated in the written consortium agreement referred to in paragraph 3.

6. A Member State may join an existing Hosting Consortium with the agreement of the Hosting Consortium members. The written consortium agreement referred to in paragraph 3 and the hosting and usage agreement shall be modified accordingly. This shall not affect the ownership rights of the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) over the tools, infrastructure or services already jointly procured with that Hosting Consortium.

Article 6

Cooperation and information sharing within and between Cross-Border Cyber Hubs

1. Members of a Hosting Consortium shall ensure that their National Cyber Hubs share, in accordance with the written consortium agreement referred to in Article 5(3), relevant information, anonymised where appropriate, such as information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyberattacks, among themselves within the Cross-Border Cyber Hub where such information sharing:

- (a) fosters and enhances the detection of cyber threats and reinforces the capabilities of the CSIRTs network to prevent and respond to incidents or to mitigate their impact;
- (b) enhances the level of cybersecurity, for example through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, response and recovery stages or promoting collaborative threat research between public and private entities.

2. The written consortium agreement referred to in Article 5(3) shall establish:

- (a) a commitment to share among the members of the Hosting Consortium information as referred to in paragraph 1 and the conditions under which that information is to be shared;
- (b) a governance framework clarifying and incentivising the sharing by all participants of relevant information, anonymised where appropriate, as referred to in paragraph 1;
- (c) targets for contribution to the development of advanced tools and technologies, such as artificial intelligence and data analytics tools.

The written consortium agreement may specify that the information referred to in paragraph 1 is to be shared in accordance with Union and national law.

3. Cross-Border Cyber Hubs shall conclude cooperation agreements with one another, specifying interoperability and information-sharing principles among the Cross-Border Cyber Hubs. Cross-Border Cyber Hubs shall inform the Commission about the cooperation agreements concluded.

4. Information sharing as referred to in paragraph 1 between Cross-Border Cyber Hubs shall be ensured by a high level of interoperability. To support such interoperability, ENISA shall, in close consultation with the Commission, without undue delay and in any event by 5 February 2026, issue interoperability guidelines specifying in particular information-sharing formats and protocols, taking into account international standards and best practices, as well as the functioning of any established Cross-Border Cyber Hubs. Interoperability requirements provided for in the cooperation agreements of Cross-Border Cyber Hubs shall be based on the guidelines issued by ENISA.

Article 7

Cooperation and information sharing with Union-level networks

1. Cross-Border Cyber Hubs and the CSIRTs network shall cooperate closely, in particular for the purpose of sharing information. To that end, they shall agree on procedural arrangements on cooperation and sharing of relevant information and, without prejudice to paragraph 2, on the types of information to be shared.

2. Where the Cross-Border Cyber Hubs obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall ensure, for the purposes of common situational awareness, that relevant information as well as early warnings are provided to Member States' authorities and the Commission through EU-CyCLONe and the CSIRTs network without undue delay.

Article 8

Security

1. Member States participating in the European Cybersecurity Alert System shall ensure a high level of cybersecurity, including confidentiality and data security, as well as physical security of the European Cybersecurity Alert System network, and shall ensure that the network is adequately managed and controlled in such a way as to protect it from threats and to ensure its security and that of the systems, including that of data and information shared through the network.

2. Member States participating in the European Cybersecurity Alert System shall ensure that the sharing of information referred to in Article 6(1) within the European Cybersecurity Alert System with any entity other than a public authority or body of a Member State does not negatively affect the security interests of the Union or of the Member States.

Article 9

Funding of the European Cybersecurity Alert System

1. Following a call for expressions of interest for Member States intending to participate in the European Cybersecurity Alert System, the ECCC shall select Member States to take part with the ECCC in the joint procurement of tools, infrastructure or services in order to set up, or enhance the capabilities of, National Cyber Hubs designated or established pursuant to Article 4(1). The ECCC may award to the selected Member States grants to fund the operation of such tools, infrastructure or services. The Union financial contribution shall cover up to 50 % of the acquisition costs of the tools, infrastructure or services and up to 50 % of the operational costs. The selected Member States shall cover the remaining costs. Before launching the procedure for the acquisition of tools, infrastructure or services, the ECCC and the selected Member States shall conclude a hosting and usage agreement regulating the usage of the tools, infrastructure or services.

2. Where a Member State's National Cyber Hub is not a participant in a Cross-Border Cyber Hub within 2 years of the date on which the tools, infrastructure or services were acquired, or on which it received grant funding, whichever occurred sooner, the Member State shall not be eligible for additional Union support under this Chapter until it has joined a Cross-Border Cyber Hub.

3. Following a call for expressions of interest, a Hosting Consortium shall be selected by the ECCC to participate in a joint procurement of tools, infrastructure or services with the ECCC. The ECCC may award a grant to the Hosting Consortium to fund the operation of the tools, infrastructure or services. The Union financial contribution shall cover up to 75 % of the acquisition costs of the tools, infrastructure or services, and up to 50 % of the operational costs. The Hosting Consortium shall cover the remaining costs. Before launching the procedure for the acquisition of tools, infrastructure or services, the ECCC and the Hosting Consortium shall conclude a hosting and usage agreement regulating the usage of the tools, infrastructure or services.

4. The ECCC shall prepare, at least every 2 years, a mapping of the tools, infrastructure or services necessary and of adequate quality to establish, or enhance the capabilities of, National Cyber Hubs and Cross-Border Cyber Hubs, and their availability, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. When preparing the mapping, the ECCC shall consult the CSIRTs network, any existing Cross-Border Cyber Hubs, ENISA and the Commission.

CHAPTER III
CYBERSECURITY EMERGENCY MECHANISM

Article 10

Establishment of the Cybersecurity Emergency Mechanism

1. A Cybersecurity Emergency Mechanism is established to support the improvement of the Union's resilience to cyber threats and the preparation for and mitigation of, in a spirit of solidarity, the short-term impact of significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents.
2. In the case of the Member States, actions under the Cybersecurity Emergency Mechanism shall be provided upon request and shall be complementary to Member States' efforts and actions to prepare for, respond to and recover from incidents.
3. The actions implementing the Cybersecurity Emergency Mechanism shall be supported by funding from the DEP and shall be implemented in accordance with Regulation (EU) 2021/694, in particular Specific Objective 3 thereof.
4. The actions under the Cybersecurity Emergency Mechanism shall be implemented primarily through the ECCC in accordance with Regulation (EU) 2021/887. However, actions implementing the EU Cybersecurity Reserve as referred to in Article 11, point (b), of this Regulation shall be implemented by the Commission and ENISA.

Article 11

Types of action

The Cybersecurity Emergency Mechanism shall support the following types of action:

- (a) preparedness actions, namely:
 - (i) the coordinated preparedness testing of entities operating in sectors of high criticality across the Union as specified in Article 12;
 - (ii) other preparedness actions for entities operating in sectors of high criticality or entities operating in other critical sectors, as specified in Article 13;
- (b) actions supporting response to and initiating recovery from significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents, to be provided by trusted managed security service providers participating in the EU Cybersecurity Reserve established under Article 14;
- (c) actions supporting mutual assistance as referred to in Article 18.

Article 12

Coordinated preparedness testing of entities

1. The Cybersecurity Emergency Mechanism shall support the voluntary coordinated preparedness testing of entities operating in sectors of high criticality.
2. The coordinated preparedness testing may consist of preparedness activities, such as penetration testing, and threat assessment.
3. Support for preparedness actions under this Article shall be provided to Member States primarily in the form of grants and subject to the conditions provided for in the relevant work programmes as referred to in Article 24 of Regulation (EU) 2021/694.
4. For the purpose of supporting the coordinated preparedness testing of entities referred to in Article 11, point (a)(i), of this Regulation across the Union, the Commission shall, after consulting the NIS Cooperation Group, EU-CyCLONe and ENISA, identify the sectors or sub-sectors concerned from the sectors of high criticality listed in Annex I to Directive (EU)

2022/2555 for which a call for proposals to award grants may be issued. The participation of Member States in those calls for proposals is voluntary.

5. When identifying the sectors or sub-sectors referred to in paragraph 4, the Commission shall take into account coordinated risk assessments and resilience testing at Union level and the results thereof.

6. The NIS Cooperation Group in cooperation with the Commission, the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative') and ENISA, and, within the remit of its mandate, EU-CyCLONe, shall develop common risk scenarios and methodologies for the coordinated preparedness testing referred to in Article 11, point (a)(i), and, where appropriate, for other preparedness actions referred to in point (a)(ii) of that Article.

7. Where an entity operating in a sector of high criticality participates voluntarily in coordinated preparedness testing and that testing results in recommendations for specific measures, which the participating entity could integrate into a remediation plan, the Member State authority responsible for the coordinated preparedness testing shall, where appropriate, review the follow-up of those measures by the participating entities with a view to reinforcing preparedness.

Article 13

Other preparedness actions

1. The Cybersecurity Emergency Mechanism shall support preparedness actions not covered by Article 12. Such actions shall include preparedness actions for entities in sectors not identified for coordinated preparedness testing pursuant to Article 12. Such actions may support vulnerability monitoring, risk monitoring, exercises and training.

2. Support for preparedness actions under this Article shall be provided to Member States upon request and primarily in the form of grants and subject to the conditions provided for in the relevant work programmes as referred to in Article 24 of Regulation (EU) 2021/694.

Article 14

Establishment of the EU Cybersecurity Reserve

1. An EU Cybersecurity Reserve is established in order to assist, upon request, users as referred to in paragraph 3, in responding to, or providing support for a response to, significant cybersecurity incidents, large-scale cybersecurity incidents or large-scale-equivalent cybersecurity incidents, and initiating recovery from such incidents.

2. The EU Cybersecurity Reserve shall consist of response services from trusted managed security service providers selected in accordance with the criteria laid down in Article 17(2). The EU Cybersecurity Reserve may include pre-committed services. The pre-committed services of a trusted managed security service provider shall be convertible into preparedness services related to incident prevention and response where those pre-committed services are not used for incident response during the time for which those services are pre-committed. The EU Cybersecurity Reserve shall be deployable, upon request, in all Member States, in Union institutions, bodies, offices and agencies, and in DEP-associated third countries as referred to in Article 19(1).

3. The users of the services provided by the EU Cybersecurity Reserve shall consist of the following:

(a) Member States' cyber crisis management authorities and CSIRTs as referred to, respectively, in Article 9(1) and (2) and Article 10 of Directive (EU) 2022/2555;

(b) CERT-EU in accordance with Article 13 of Regulation (EU, Euratom) 2023/2841;

(c) competent authorities such as computer security incident response teams and cyber crisis management authorities of DEP-associated third countries in accordance with Article 19(8).

4. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission shall determine the priorities and the evolution of the EU Cybersecurity Reserve in coordination with the NIS Cooperation Group and, in line with the requirements of the users referred to in paragraph 3, shall supervise its implementation and shall ensure complementarity, consistency, synergies and links with other support actions under this

Regulation as well as with other Union actions and programmes. Those priorities shall be reviewed and, if appropriate, revised every 2 years. The Commission shall inform the European Parliament and the Council of those priorities and any revisions thereof.

5. Without prejudice to the Commission's overall responsibility for the implementation of the EU Cybersecurity Reserve referred to in paragraph 4 of this Article and subject to a contribution agreement as defined in Article 2, point (19), of Regulation (EU, Euratom) 2024/2509, the Commission shall entrust the operation and administration of the EU Cybersecurity Reserve, in full or in part, to ENISA. Aspects not entrusted to ENISA shall remain subject to direct management by the Commission.

6. ENISA shall prepare, at least every 2 years, a mapping of the services needed by the users referred to in paragraph 3, points (a) and (b), of this Article. The mapping shall also include the availability of such services, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. In mapping that availability, ENISA shall assess the skills and capacity of the Union cybersecurity workforce relevant to the objectives of the EU Cybersecurity Reserve. When preparing the mapping, ENISA shall consult the NIS Cooperation Group, EU-CyCLONe, the Commission and, where applicable, the Interinstitutional Cybersecurity Board established pursuant to Article 10 of Regulation (EU, Euratom) 2023/2841 (IICB). In mapping the availability of services, ENISA shall also consult relevant cybersecurity industry stakeholders, including managed security service providers. ENISA shall prepare a similar mapping, after informing the Council and after consulting EU-CyCLONe, the Commission and, where relevant, the High Representative, to identify the needs of users referred to in paragraph 3, point (c), of this Article.

7. The Commission is empowered to adopt delegated acts in accordance with Article 23 to supplement this Regulation by specifying the types and the number of response services required for the EU Cybersecurity Reserve. When preparing those delegated acts, the Commission shall take into account the mapping referred to in paragraph 6 of this Article and may exchange advice and cooperate with the NIS Cooperation Group and ENISA.

Article 15

Requests for support from the EU Cybersecurity Reserve

1. The users referred to in Article 14(3) may request services from the EU Cybersecurity Reserve to support response to and initiate recovery from significant cybersecurity incidents, large-scale cybersecurity incidents or large-scale-equivalent cybersecurity incidents.

2. To receive support from the EU Cybersecurity Reserve, the users referred to in Article 14(3) shall take all appropriate measures to mitigate the effects of the incident for which the support is requested, including, where relevant, the provision of direct technical assistance, and other resources to assist the response to the incident, and recovery efforts.

3. Requests for support shall be transmitted to the contracting authority as follows:

(a) in the case of the users referred to in Article 14(3), point (a), of this Regulation, via the single point of contact designated or established pursuant to Article 8(3) of Directive (EU) 2022/2555;

(b) in the case of the user referred to in Article 14(3), point (b), by that user;

(c) in the case of the users referred to in Article 14(3), point (c), via the single point of contact referred to in Article 19(9).

4. In the case of requests from the users referred to in Article 14(3), point (a), Member States shall inform the CSIRTs network, and, where appropriate, EU-CyCLONe, about their users' requests for incident response and initial recovery support pursuant to this Article.

5. Requests for incident response and initial recovery support shall include:

(a) appropriate information regarding the entity affected and the potential impact of the incident on:

(i) in the case of users referred to in Article 14(3), point (a), the Member States and users affected, including the risk of spillover to another Member State;

- (ii) in the case of the user referred to in Article 14(3), point (b), the Union institutions, bodies, offices or agencies affected,
 - (iii) in the case of users referred to in Article 14(3), point (c), the DEP-associated countries affected;
 - (b) information regarding the requested service, together with the planned use of the requested support, including an indication of the estimated needs;
 - (c) appropriate information about measures taken to mitigate the incident for which the support is requested, as referred to in paragraph 2;
 - (d) where relevant, available information about other forms of support available to the entity affected.
6. ENISA, in cooperation with the Commission and EU-CyCLONe, shall develop a template to facilitate the submission of requests for support from the EU Cybersecurity Reserve.
7. The Commission may, by means of implementing acts, specify further the detailed procedural arrangements for the way in which the EU Cybersecurity Reserve support services are to be requested and the way in which those requests are to be responded to pursuant to this Article, to Article 16(1) and to Article 19(10), including arrangements for submitting such requests and delivering the responses and templates for the reports referred to in Article 16(9). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 24(2).

Article 16

Implementation of the support from the EU Cybersecurity Reserve

1. In the case of requests from users referred to in Article 14(3), points (a) and (b), requests for support from the EU Cybersecurity Reserve shall be assessed by the contracting authority. A response shall be transmitted to the users referred to in Article 14(3), points (a) and (b), without delay and in any event no later than 48 hours from the submission of the request to ensure effectiveness of the support. The contracting authority shall inform the Council and the Commission of the results of the process.
2. As regards information shared in the course of requesting and providing the services of the EU Cybersecurity Reserve, all parties involved in the application of this Regulation shall:
- (a) limit the use and sharing of that information to what is necessary to discharge their obligations or functions under this Regulation;
 - (b) use and share any information that is confidential or classified pursuant to Union and national law only in accordance with that law; and
 - (c) ensure effective, efficient and secure information exchange, where appropriate by using and respecting relevant information-sharing protocols including the traffic light protocol.
3. In assessing individual requests under Article 16(1) and Article 19(10), the contracting authority or the Commission, as applicable, shall first assess whether the criteria referred to in Article 15(1) and (2) are fulfilled. If that is the case, it shall assess the duration and nature of support that is appropriate, having regard to the objective referred to in Article 1(3), point (b), and the following criteria, where relevant:
- (a) the scale and severity of the incident;
 - (b) the type of entity affected, with higher priority given to incidents affecting essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555;
 - (c) the potential impact of the incident on the affected Member States, Union institutions, bodies, offices or agencies, or DEP-associated third countries;
 - (d) the potential cross-border nature of the incident and the risk of spillover to other Member States, Union institutions, bodies, offices or agencies, or DEP-associated third countries;
 - (e) the measures taken by the user to assist the response, and initial recovery efforts, as referred in Article 15(2).

4. To prioritise requests, in the case of concurrent requests from users referred to in Article 14(3), the criteria referred to in paragraph 3 of this Article shall be taken into account, where relevant, without prejudice to the principle of sincere cooperation between Member States and Union institutions, bodies, offices and agencies. Where two or more requests are assessed as equal under those criteria, higher priority shall be given to requests from Member State users. Where the operation and administration of the EU Cybersecurity Reserve has been entrusted, in full or in part, to ENISA pursuant to Article 14(5), ENISA and the Commission shall closely cooperate to prioritise requests in accordance with this paragraph.

5. The EU Cybersecurity Reserve services shall be provided in accordance with specific agreements between the trusted managed security service provider and the user to which the support under the EU Cybersecurity Reserve is provided. Those services may be provided in accordance with specific agreements between the trusted managed security service provider, the user and the entity affected. All agreements referred to in this paragraph shall include, inter alia, liability conditions.

6. The agreements referred to in paragraph 5 shall be based on templates prepared by ENISA, after consulting Member States and, where appropriate, other users of the EU Cybersecurity Reserve.

7. The Commission, ENISA and the users of the EU Cybersecurity Reserve shall bear no contractual liability for damage caused to third parties by the services provided in the framework of the implementation of the EU Cybersecurity Reserve.

8. Users may use the EU Cybersecurity Reserve services provided in response to a request under Article 15(1) only in order to support response to and initiate recovery from significant cybersecurity incidents, large-scale cybersecurity incidents or large-scale-equivalent cybersecurity incidents. They may use those services only in respect of:

(a) entities operating in sectors of high criticality or entities operating in other critical sectors, in the case of users referred to in Article 14(3), point (a), and equivalent entities in the case of users referred to in Article 14(3), point (c); and

(b) Union institutions, bodies, offices and agencies, in the case of the user referred to in Article 14(3), point (b).

9. Within 2 months of the end of a support, users that have received support shall provide a summary report about the service provided, the results achieved and the lessons learned, to:

(a) the Commission, ENISA, the CSIRTs network and EU-CyCLONe in the case of users referred to in Article 14(3), point (a);

(b) the Commission, ENISA and the IICB in the case of the user referred to in Article 14(3), point (b);

(c) the Commission in the case of users referred to in Article 14(3), point (c).

The Commission shall transmit any summary report received from users referred to in Article 14(3) pursuant to the first subparagraph, point (c), of this paragraph, to the Council and the High Representative.

10. Where the operation and administration of the EU Cybersecurity Reserve has been entrusted, in full or in part, to ENISA pursuant to Article 14(5) of this Regulation, ENISA shall report to and consult the Commission on a regular basis in that respect. In that context, ENISA shall immediately send to the Commission any requests it receives from users referred to in Article 14(3), point (c), of this Regulation and, where required for the purposes of prioritisation under this Article, any requests it has received from users referred to in Article 14(3), point (a) or (b), of this Regulation. The obligations in this paragraph shall be without prejudice to Article 14 of Regulation (EU) 2019/881.

11. In the case of users referred in Article 14(3), points (a) and (b), the contracting authority shall report to the NIS Cooperation Group, on a regular basis and at least twice per year, about the use and the results of the support.

12. In the case of users referred to in Article 14(3), point (c), the Commission shall report to the Council and inform the High Representative on a regular basis and at least twice per year, about the use and the results of the support.

Article 17

Trusted managed security service providers

1. In procurement procedures for the purpose of establishing the EU Cybersecurity Reserve, the contracting authority shall act in accordance with the principles laid down in Regulation (EU, Euratom) 2024/2509 and in accordance with the following principles:

- (a) ensure that the services included in the EU Cybersecurity Reserve, when taken as a whole, are such that the EU Cybersecurity Reserve includes services that may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including on languages, certification or accreditation;
- (b) ensure the protection of the essential security interests of the Union and its Member States;
- (c) ensure that the EU Cybersecurity Reserve brings Union added value, by contributing to the objectives set out in Article 3 of Regulation (EU) 2021/694, including promoting the development of cybersecurity skills in the Union.

2. When procuring services for the EU Cybersecurity Reserve, the contracting authority shall include in the procurement documents the following criteria and requirements:

- (a) the provider shall demonstrate that its personnel has the highest degree of professional integrity, independence, responsibility, and the requisite technical competence to perform the activities in their specific field, and ensures the permanence and continuity of expertise as well as the required technical resources;
- (b) the provider, and any relevant subsidiaries and subcontractors, shall comply with applicable rules on the protection of classified information and shall have in place appropriate measures, including, where relevant, agreements between one another, to protect confidential information relating to the service, and in particular evidence, findings and reports;
- (c) the provider shall provide sufficient proof that its governing structure is transparent, not likely to compromise its impartiality and the quality of its services or to cause conflicts of interest;
- (d) the provider shall have appropriate security clearance, at least for personnel intended for service deployment, where required by a Member State;
- (e) the provider shall have the relevant level of security for its IT systems;
- (f) the provider shall be equipped with the hardware and software necessary to support the requested service, which shall not contain known exploitable vulnerabilities, shall include the latest security updates and shall in any case comply with any applicable provision of Regulation (EU) 2024/2847 of the European Parliament and of the Council ⁽²³⁾;
- (g) the provider shall be able to demonstrate that it has experience in delivering similar services to relevant national authorities, entities operating in sectors of high criticality or entities operating in other critical sectors;
- (h) the provider shall be able to provide the service within a short timeframe in the Member States where it can deliver the service;
- (i) the provider shall be able to provide the service in one or more official languages of the Union institutions or of a Member State as required, if any, by the Member States or users referred to in Articles 14(3), points (b) and (c), where the provider can deliver the service;
- (j) once an European cybersecurity certification scheme for managed security services pursuant to Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme within 2 years from the date of application of the scheme;

⁽²³⁾ Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>).

- (k) the provider shall include in the tender the conversion conditions for any unused incident response service that could be converted into preparedness services closely related to incident response, such as exercises or training.

3. For the purpose of procuring services for the EU Cybersecurity Reserve, the contracting authority may, where appropriate, develop criteria and requirements in addition to those referred to in paragraph 2, in close cooperation with Member States.

Article 18

Actions supporting mutual assistance

1. The Cybersecurity Emergency Mechanism shall provide support for technical assistance from one Member State to another Member State affected by a significant cybersecurity incident or a large-scale cybersecurity incident, including in cases referred to in Article 11(3), point (f), of Directive (EU) 2022/2555.

2. The support for the technical mutual assistance referred to in paragraph 1 of this Article shall be provided in the form of grants and subject to the conditions provided for in the relevant work programmes as referred to in Article 24 of Regulation (EU) 2021/694.

Article 19

Support to DEP-associated third countries

1. A DEP-associated third country may request support from the EU Cybersecurity Reserve where the agreement through which it is associated to the DEP provides for participation in the EU Cybersecurity Reserve. That agreement shall include provisions requiring the DEP-associated third country concerned to comply with the obligations set out in paragraphs 2 and 9 of this Article. For the purposes of the participation of a third country in the EU Cybersecurity Reserve, the partial association of a third country to the DEP may include an association limited to the operational objective referred to in Article 6(1), point (g), of Regulation (EU) 2021/694.

2. Within 3 months of the conclusion of the agreement referred to in paragraph 1 and in any event prior to receiving any support from the EU Cybersecurity Reserve, the DEP-associated third country shall provide to the Commission information about its cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant cybersecurity incidents or large-scale-equivalent cybersecurity incidents, as well as information on responsible national entities, including computer security incident response teams or equivalent entities, their capabilities and the resources allocated to them. The DEP-associated third country shall provide updates of that information on a regular basis and at least once a year. The Commission shall provide the High Representative and ENISA with that information for the purposes of facilitating the application of paragraph 11.

3. The Commission shall assess regularly, and at least once a year, the following criteria in respect of each DEP-associated third country referred to in paragraph 1:

- (a) whether that country is complying with the terms of the agreement referred to in paragraph 1, insofar as those terms relate to participation in the EU Cybersecurity Reserve;
- (b) whether that country has taken adequate steps to prepare for significant cybersecurity incidents or large-scale-equivalent cybersecurity incidents, based on the information referred to in paragraph 2; and
- (c) whether the provision of support is consistent with the Union's policy towards and overall relations with that country and whether it is consistent with other Union policies in the field of security.

The Commission shall consult the High Representative when conducting the assessment referred to in the first subparagraph, with regard to the criterion referred to in point (c) of that subparagraph.

Where the Commission concludes that a DEP-associated third country meets all of the conditions referred to in the first subparagraph, the Commission shall submit a proposal to the Council to adopt an implementing act in accordance with paragraph 4 authorising the provision of support from the EU Cybersecurity Reserve to that country.

4. The Council may adopt the implementing acts referred to in paragraph 3. Those implementing acts shall apply for a maximum of one year. They may be renewed. They may include a limit of no less than 75 days on the number of days for which support can be provided in response to a single request.

For the purposes of this Article, the Council shall act expeditiously and shall, as a rule, adopt the implementing acts referred to in this paragraph within eight weeks of the adoption of the relevant Commission proposal pursuant to paragraph 3, third subparagraph.

5. The Council may amend or repeal an implementing act adopted pursuant to paragraph 4 at any time, acting on a proposal of the Commission.

Where the Council considers there to have been a significant change concerning the criterion referred to in paragraph 3, first subparagraph, point (c), the Council may amend or repeal an implementing act adopted pursuant to paragraph 4 acting on the duly reasoned initiative of one or more Member States.

6. In the exercise of its implementing powers under this Article, the Council shall apply the criteria referred to in paragraph 3, first subparagraph, and shall explain its assessment of those criteria. In particular, where it acts on its own initiative pursuant to paragraph 5, second subparagraph, the Council shall explain the significant change referred to in that subparagraph.

7. Support from the EU Cybersecurity Reserve to a DEP-associated third country shall comply with any specific conditions laid down in the agreement referred to in paragraph 1.

8. Users from DEP-associated third countries eligible to receive services from the EU Cybersecurity Reserve shall include competent authorities such as computer security incident and response teams or equivalent entities and cyber crisis management authorities.

9. Each DEP-associated third country eligible for support from the EU Cybersecurity Reserve shall designate an authority to act as a single point of contact for the purposes of this Regulation.

10. Requests for support from the EU Cybersecurity Reserve under this Article shall be assessed by the Commission. The contracting authority may provide support to a third country only where, and for so long as, a Council implementing act authorising such support in respect of that country adopted pursuant to paragraph 4 of this Article is in force. A response shall be transmitted to the users referred to in Article 14(3), point (c), without undue delay.

11. Upon receipt of a request for support under this Article, the Commission shall immediately inform the Council. The Commission shall keep the Council informed of the assessment of the request. The Commission shall also cooperate with the High Representative about the requests received and the implementation of the support granted to DEP-associated third countries from the EU Cybersecurity Reserve. Additionally, the Commission shall also take into account any views provided by ENISA in respect of those requests.

Article 20

Coordination with Union crisis management mechanisms

1. Where a significant cybersecurity incident, a large-scale cybersecurity incident or a large-scale-equivalent cybersecurity incident originates from or results in a disaster as defined in Article 4, point (1), of Decision No 1313/2013/EU, the support provided under this Regulation for responding to such incident shall complement actions under, and be without prejudice to, that Decision.

2. In the event of a large-scale cybersecurity incident or a large-scale-equivalent cybersecurity incident where the EU Integrated Political Crisis Response Arrangements under Implementing Decision (EU) 2018/1993 (IPCR Arrangements) are activated, support provided under this Regulation for responding to such incident shall be handled in accordance with the relevant procedures under the IPCR Arrangements.

CHAPTER IV

EUROPEAN CYBERSECURITY INCIDENT REVIEW MECHANISM

Article 21

European Cybersecurity Incident Review Mechanism

1. At the request of the Commission or EU-CyCLONe, ENISA shall, with the support of the CSIRTs network and with the approval of the Member States concerned, review and assess cyber threats, known exploitable vulnerabilities and mitigation actions with respect to a specific significant cybersecurity incident or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident and with the aim of drawing lessons learned to avoid or mitigate future incidents, ENISA shall deliver an incident review report to EU-CyCLONe, the CSIRTs network, the Member States concerned and the Commission to support them in carrying out their tasks, in particular the tasks set out in Articles 15 and 16 of Directive (EU) 2022/2555. Where an incident has an impact on a DEP-associated third country, ENISA shall provide the report to the Council. In such cases, the Commission shall provide the report to the High Representative.
2. To prepare the incident review report referred to in paragraph 1 of this Article, ENISA shall cooperate with and gather feedback from all relevant stakeholders, including representatives of Member States, the Commission, other relevant Union institutions, bodies, offices and agencies, industry, including managed security services providers, and users of cybersecurity services. Where appropriate, ENISA shall, in cooperation with CSIRTs and, where relevant, the competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555, also cooperate with entities affected by significant cybersecurity incidents or large-scale cybersecurity incidents. Consulted representatives shall disclose any potential conflict of interest.
3. The incident review report referred to in paragraph 1 of this Article shall cover a review and analysis of the specific significant cybersecurity incident or large-scale cybersecurity incident, including the main causes, known exploitable vulnerabilities and lessons learned. ENISA shall ensure that the report complies with Union or national law concerning the protection of sensitive or classified information. If the relevant Member States or other users referred to in Article 14(3) that are affected by the incident so request, the data and information contained in the report shall be anonymised. It shall not include any details about actively exploited vulnerabilities that remain unpatched.
4. Where appropriate, the incident review report shall draw recommendations to improve the Union's cyber posture and may include best practices and lessons learned from relevant stakeholders.
5. ENISA may issue a publicly available version of the incident review report. That version of the report shall include only reliable public information, or other reliable information with the consent of the Member States concerned and, as regards information relating to a user as referred to in Article 14(3), point (b) or (c), with the consent of that user.

CHAPTER V

FINAL PROVISIONS

Article 22

Amendments to Regulation (EU) 2021/694

Regulation (EU) 2021/694 is amended as follows:

(1) Article 6 is amended as follows:

(a) paragraph 1 is amended as follows:

(i) the following point is inserted:

‘(aa) support the development of the European Cybersecurity Alert System established by Article 3 of Regulation (EU) 2025/38 of the European Parliament and of the Council (*) (the “European Cybersecurity Alert System”), including the development, deployment and operation of National Cyber Hubs and Cross-Border Cyber Hubs that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union;

(*) Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) (OJ L, 2025/38, 15.1.2025, ELI: <http://data.europa.eu/eli/reg/2025/38/oj>);

(ii) the following point is added:

‘(g) establish and operate the Cybersecurity Emergency Mechanism established by Article 10 of Regulation (EU) 2025/38, including the EU Cybersecurity Reserve established by Article 14 of that Regulation (the “EU Cybersecurity Reserve”), to support Member States in preparing for and responding to significant cybersecurity incidents and large-scale cybersecurity incidents that is complementary to national resources and capabilities and other forms of support available at Union level, and to support other users in responding to significant cybersecurity incidents and large-scale-equivalent cybersecurity incidents;’

(b) paragraph 2 is replaced by the following:

‘2. The actions under Specific Objective 3 shall be implemented primarily through the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council (*). However, the EU Cybersecurity Reserve shall be implemented by the Commission and, in accordance with Article 14(6) of Regulation (EU) 2025/38, by ENISA.

(*) Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202, 8.6.2021, p. 1).’

(2) Article 9 is amended as follows:

(a) in paragraph 2, points (b), (c) and (d) are replaced by the following:

‘(b) EUR 1 760 806 000 for Specific Objective 2 – Artificial Intelligence;

(c) EUR 1 372 020 000 for Specific Objective 3 – Cybersecurity and Trust;

(d) EUR 482 640 000 for Specific Objective 4 – Advanced Digital Skills;’

(b) the following paragraph is added:

‘8. By way of derogation from Article 12(1) of the Financial Regulation, unused commitment and payment appropriations for actions in the context of the implementation of the EU Cybersecurity Reserve and the actions supporting mutual assistance pursuant to Regulation 2025/38, pursuing the objectives set out in Article 6(1), point (g), of this Regulation shall be automatically carried over and may be committed and paid up to 31 December of the following financial year. The European Parliament and the Council shall be informed of appropriations carried over pursuant to Article 12(6) of the Financial Regulation.’;

(3) Article 12 is amended as follows:

(a) the following paragraphs are inserted:

‘5a. Paragraph 5 shall not apply, insofar as concerns legal entities that are established in the Union but are controlled from third countries, to any action implementing the European Cybersecurity Alert System where both of the following conditions are fulfilled in respect of the action concerned:

- (a) there is a real risk, taking into account the results of the mapping carried out pursuant to Article 9(4) of Regulation (EU) 2025/38, that the tools, infrastructure or services necessary and sufficient for that action to adequately contribute to the objective of the European Cybersecurity Alert System will not be available from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States;
- (b) the security risk of procuring from such legal entities within the European Cybersecurity Alert System is proportionate to the benefits and does not undermine the essential security interests of the Union and its Member States.

5b. Paragraph 5 shall not apply, insofar as concerns legal entities that are established in the Union but are controlled from third countries, to any action implementing the EU Cybersecurity Reserve where both of the following conditions are fulfilled in respect of the action concerned:

- (a) there is a real risk, taking into account the results of the mapping carried out pursuant to Article 14(6) of Regulation (EU) 2025/38, that the technology, expertise or capacity necessary and sufficient for the EU Cybersecurity Reserve to adequately perform its functions will not be available from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States;
- (b) the security risk of including such legal entities within the EU Cybersecurity Reserve is proportionate to the benefits and does not undermine the essential security interests of the Union and its Member States.’;

(b) paragraph 6 is replaced by the following:

‘6. If duly justified for security reasons, the work programme may also provide that legal entities established in associated countries and legal entities that are established in the Union but are controlled from third countries may be eligible to participate in all or some actions under Specific Objectives 1 and 2 only if they comply with the requirements to be fulfilled by those legal entities to guarantee the protection of the essential security interests of the Union and the Member States and to ensure the protection of classified documents information. Those requirements shall be set out in the work programme.

The first subparagraph shall also apply, insofar as concerns legal entities that are established in the Union but are controlled from third countries, to actions under Specific Objective 3:

- (a) to implement the European Cybersecurity Alert System where paragraph 5a applies; and
- (b) to implement the EU Cybersecurity Reserve where paragraph 5b applies.’;

(4) in Article 14, paragraph 2 is replaced by the following:

‘2. The Programme may provide funding in any of the forms laid down in the Financial Regulation, including in particular through procurement as a primary form, or grants and prizes.

Where the achievement of the objective of an action requires the procurement of innovative goods and services, grants may be awarded only to beneficiaries that are contracting authorities or contracting entities as defined in Directives 2014/24/EU (*) and 2014/25/EU (**) of the European Parliament and of the Council.

Where the supply of innovative goods or services that are not yet available on a large-scale commercial basis is necessary to achieve the objectives of an action, the contracting authority or the contracting entity may authorise the award of multiple contracts within the same procurement procedure.

For duly justified reasons of public security, the contracting authority or the contracting entity may require that the place of performance of the contract be situated within the territory of the Union.

When implementing procurement procedures for the EU Cybersecurity Reserve, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of third countries associated to the Programme in accordance with Article 10 of this Regulation. The Commission and ENISA may also act as wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to those third countries. By way of

derogation from Article 168(3) of Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council (**), the request from a single third country shall be sufficient to mandate the Commission or ENISA to act.

When implementing procurement procedures for the EU Cybersecurity Reserve, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of Union institutions, bodies, offices or agencies. The Commission and ENISA may also act as a wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to Union institutions, bodies, offices or agencies. By way of derogation from Article 168(3) of Regulation (EU, Euratom) 2024/2509, a request from a single Union institution, body, office or agency shall be sufficient to mandate the Commission or ENISA to act.

The Programme may also provide financing in the form of financial instruments within blending operations.

-
- (*) Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).
 - (**) Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94, 28.3.2014, p. 243).
 - (***) Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (OJ L, 2024/2509, 26.9.2024, ELI: <http://data.europa.eu/eli/reg/2024/2509/oj>);

(5) the following article is inserted:

'Article 16a

Conflicts of rules

In the case of actions implementing the European Cybersecurity Alert System, the applicable rules shall be those set out in Articles 4, 5 and 9 of Regulation (EU) 2025/38. In the case of a conflict between the provisions of this Regulation and Articles 4, 5 and 9 of Regulation (EU) 2025/38, the latter shall prevail and apply to those specific actions.

In the case of EU Cybersecurity Reserve, specific rules for the participation of third countries associated to the Programme are laid down in Article 19 of Regulation (EU) 2025/38. In the case of a conflict between the provisions of this Regulation and Article 19 of Regulation (EU) 2025/38, the latter shall prevail and apply to those specific actions.';

(6) Article 19 is replaced by the following:

'Article 19

Grants

Grants under the Programme shall be awarded and managed in accordance with Title VIII of the Financial Regulation and may cover up to 100 % of the eligible costs, without prejudice to the co-financing principle as laid down in Article 190 of the Financial Regulation. Such grants shall be awarded and managed as specified for each specific objective.

Support in the form of grants may be awarded directly by the ECCC without a call for proposals to the Member States selected pursuant to Article 9 of Regulation (EU) 2025/38 and the Hosting Consortium referred to in Article 5 of Regulation (EU) 2025/38, in accordance with Article 195(1), point (d), of the Financial Regulation.

Support in the form of grants for the Cybersecurity Emergency Mechanism may be awarded directly by the ECCC to Member States without a call for proposals, in accordance with Article 195(1), point (d), of the Financial Regulation.

With regard to actions supporting mutual assistance provided for in Article 18 of Regulation (EU) 2025/38, the ECCC shall inform the Commission and ENISA about Member States' requests for direct grants without a call for proposals.

With regard to actions supporting mutual assistance provided for in Article 18 of Regulation (EU) 2025/38, and in accordance with Article 193(2), second subparagraph, point (a), of the Financial Regulation, the costs may, in duly justified cases, be considered to be eligible even if they were incurred before the grant application was submitted.’;

(7) Annexes I and II are amended in accordance with the Annex to this Regulation.

Article 23

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Article 14(7) shall be conferred on the Commission for a period of 5 years from 5 February 2025. The Commission shall draw up a report in respect of the delegation of power not later than 9 months before the end of the 5-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 3 months before the end of each period.
3. The delegation of power referred to in Article 14(7) 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. It shall take effect the day following that of the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. 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.
5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
6. A delegated act adopted pursuant to Article 14(7) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of 2 months of the notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by 2 months at the initiative of the European Parliament or of the Council.

Article 24

Committee procedure

1. The Commission shall be assisted by the Digital Europe Programme Coordination Committee referred to in Article 31(1) of Regulation (EU) 2021/694. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 25

Evaluation and review

1. By 5 February 2027 and at least every 4 years thereafter, the Commission shall evaluate the functioning of the measures provided for in this Regulation and shall submit a report to the European Parliament and to the Council.
2. The evaluation referred to in paragraph 1 shall assess, in particular:
 - (a) the number of National Cyber Hubs and Cross-Border Cyber Hubs established, the extent of information shared, including, if possible, the impact on the work of the CSIRTs network, and the extent to which those have contributed to strengthening common Union detection and situational awareness of cyber threats and incidents and to the development of state-of-the-art technologies; the use of DEP funding for cybersecurity tools, infrastructure, or services

jointly procured; and, if the information is available, the level of cooperation between National Cyber Hubs and sectoral and cross-sectoral communities of essential and important entities as referred to in Article 3 of Directive (EU) 2022/2555;

- (b) the use and effectiveness of actions under the Cybersecurity Emergency Mechanism supporting preparedness, including training, response to and initial recovery from significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents, including the use of DEP funding and the lessons learned and recommendations from the implementation of the Cybersecurity Emergency Mechanism;
- (c) the use and effectiveness of the EU Cybersecurity Reserve in relation to types of user, including the use of DEP funding, the uptake of services, including their type, the average time for responding to the requests and for the EU Cybersecurity Reserve to be deployed, the percentage of services converted into preparedness services related to incident prevention and response and the lessons learned and recommendations from the implementation of the EU Cybersecurity Reserve;
- (d) the contribution of this Regulation to strengthening the competitive position of the industry and services in the Union across the digital economy, including microenterprises and small and medium-sized enterprises as well as start-ups, and the contribution to the overall objective of reinforcing the cybersecurity skills and capacities of the workforce.

3. On the basis of the reports referred to in paragraph 1, the Commission shall, where appropriate, submit a legislative proposal to the European Parliament and to the Council to amend this Regulation.

Article 26

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 19 December 2024.

For the European Parliament

The President

R. METSOLA

For the Council

The President

BÓKA J.

ANNEX

Regulation (EU) 2021/694 is amended as follows:

(1) in Annex I, the section ‘Specific Objective 3 – Cybersecurity and Trust’ is replaced by the following:

‘Specific Objective 3 – Cybersecurity and Trust

The Programme shall stimulate the reinforcement, building and acquisition of essential capacities to secure the Union’s digital economy, society and democracy by reinforcing the Union cybersecurity industrial potential and competitiveness, as well as by improving capabilities of both the private and public sectors to protect citizens and businesses from cyber threats, including by supporting the implementation of Directive (EU) 2016/1148.

Initial and, where appropriate, subsequent actions under this objective shall include:

1. Co-investment with Member States in advanced cybersecurity equipment, infrastructure and know-how that are essential to protect critical infrastructures and the Digital Single Market at large. Such co-investment could include investments in quantum facilities and data resources for cybersecurity, situational awareness in cyberspace including National Cyber Hubs and Cross-Border Cyber Hubs forming the European Cybersecurity Alert System, as well as other tools to be made available to public and private sector across Europe.
2. Scaling up existing technological capacities and networking the competence centres in Member States and making sure that those capacities respond to public sector and industry needs, including through products and services that reinforce cybersecurity and trust within the Digital Single Market.
3. Ensuring wide deployment of effective state-of-the-art cybersecurity and trust solutions across the Member States. Such deployment includes strengthening the security and safety of products, from their design to their commercialisation.
4. Support closing the cybersecurity skills gap, taking into account gender balance by, for example, aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training.
5. Promoting solidarity among Member States in preparing for and responding to significant cybersecurity incidents and large-scale cybersecurity incidents through deployment of cybersecurity services across borders, including support for mutual assistance between public authorities and the establishment of a reserve of trusted managed security service providers at Union level.’;

(2) in Annex II, the section ‘Specific Objective 3 – Cybersecurity and Trust’ is replaced by the following:

‘Specific Objective 3 – Cybersecurity and Trust

- 3.1. The number of cybersecurity infrastructure, or tools, or both jointly procured including in the context of the European Cybersecurity Alert System
- 3.2. The number of users and user communities getting access to European cybersecurity facilities
- 3.3. The number of actions supporting preparedness for and response to cybersecurity incidents under the Cybersecurity Emergency Mechanism’.

A statement has been made with regard to this act and can be found in OJ C, C/2025/308, 15.1.2025, ELI: <http://data.europa.eu/eli/C/2025/308/oj>