EUROPEAN
COMMISSION

Brussels, 17.10.2024
C(2024) 7151 final

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of 17.10.2024

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

(Text with EEA relevance)

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of 17.10.2024

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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)[1], and in particular Articles 21(5), first subparagraph and 23(11), second subparagraph thereof,

Whereas:

(1) With regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers as covered by Article 3 of Directive (EU) 2022/2555 (the relevant entities), this Regulation aims to lay down the technical and the methodological requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555 and to further specify the cases in which an incident should be considered to be significant as referred to in Article 23(3) of Directive (EU) 2022/2555.

(2) Taking account of the cross-border nature of their activities and in order to ensure a coherent framework for trust service providers, this Regulation should, with respect to trust service providers, further specify the cases in which an incident shall be considered to be significant, in addition to laying down the technical and the methodological requirements of the cybersecurity risk-management measures.

(3) Following Article 21(5), third subparagraph of Directive (EU) 2022/2555, the technical and methodological requirements of the cybersecurity risk-management measures set out in the Annex to this Regulation are based on European and international standards, such as ISO/IEC 27001, ISO/IEC 27002 and ETSI EN 319

[1] OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

401, and technical specifications, such as CEN/TS 18026:2024, relevant to the security of network and information systems.

(4) As regards the implementation and application of the technical and the methodological requirements of cybersecurity risk-management measures set out in the Annex to this Regulation, in line with the principle of proportionality, due account should be taken of the divergent risk exposure of relevant entities, such as the criticality of the relevant entity, the risks to which it is exposed, the relevant entity's size and structure as well as the likelihood of occurrence of incidents and their severity, including their societal and economic impact, when complying with the technical and methodological requirements of cybersecurity risk-management measures set out in the Annex to this Regulation.

(5) In line with the principle of proportionality, where relevant entities cannot implement some of the technical and the methodological requirements of the cybersecurity risk-management measures due to their size, those entities should be able to take other compensating measures that are suitable to achieve the purpose of those requirements. For example, when defining roles, responsibilities and authorities for network and information system security within the relevant entity, micro-sized entities might find it difficult to segregate conflicting duties and conflicting areas of responsibility. Such entities should be able to consider compensating measures such as targeted oversight by the entity's management or increased monitoring and logging.

(6) Certain technical and methodological requirements set out in the Annex to this Regulation should be applied by the relevant entities where appropriate, where applicable, or to the extent feasible. Where a relevant entity considers it not appropriate, not applicable or not feasible for the relevant entity to apply certain technical and methodological requirements as provided for in the Annex to this Regulation, the relevant entity should in a comprehensible manner document its reasoning to that effect. National competent authorities may, when exercising supervision, take into account the appropriate time required for the relevant entities to implement the technical and the methodological requirements of the cybersecurity risk-management measures.

(7) ENISA or national competent authorities under Directive (EU) 2022/2555 can provide guidance to support relevant entities in the identification, analysis, and assessment of risks for the purpose of implementing the technical and the methodological requirements concerning the establishment and maintenance of an appropriate risk management framework. Such guidance can include, in particular, national and sectoral risk assessments as well as risk assessments specific for a certain type of entity. The guidance may also include tools or templates for the development of risk management framework at the level of the relevant entities. Frameworks, guidance or other mechanisms provided by Member States' national law, as well as relevant European and international standards, can also support relevant entities in demonstrating compliance with this Regulation. Moreover, ENISA or national competent authorities under Directive (EU) 2022/2555 can support relevant entities in identifying and implementing appropriate solutions to treat risks identified in such risk assessments. Such guidance should be without prejudice to the relevant entities' obligation to identify and document the risks posed to the security of network and information systems, and to the relevant entities' obligation to implement the technical and the methodological requirements of the cybersecurity risk management measures set out in the Annex to this Regulation according to their needs and resources.

(8) Network security measures in relation to: (i) the transition towards latest generation network layer communication protocols, (ii) the deployment of internationally agreed and interoperable modern e-mail communications standards, and (iii) the application of best practices for DNS security, and for Internet routing security and routing hygiene entail specific challenges regarding the identification of best available standards and deployment techniques. To achieve as soon as possible a high common level of cybersecurity across networks, the Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA) and in collaboration with competent authorities, industry – including telecommunication industry – and other stakeholders, should support the development of a multistakeholder forum tasked to identify these best available standards and deployment techniques. Such multi-stakeholder guidance should be without prejudice to the relevant entities' obligation to implement the technical and the methodological requirements of the cybersecurity risk management measures set out in the Annex to this Regulation.

(9) Pursuant to Article 21(2), point (a), of Directive (EU) 2022/2555, essential and important entities should have, besides policies on risk analysis, policies on information system security. For that purpose, the relevant entities should establish a policy on the security of network and information systems as well as topic-specific policies, such as policies on access control, which should be coherent with the policy on the security of network and information systems. The policy on the security of network and information systems should be the highest-level document setting out the relevant entities' overall approach to their security of network and information systems and should be approved by the management bodies of the relevant entities. The topic-specific policies should be approved by an appropriate level of management. The policy should lay down indicators and measures to monitor its implementation and the current status of relevant entities' maturity level of network and information security, in particular to facilitate the oversight of the implementation of the cybersecurity risk-management measures through the management bodies.

(10) For the purposes of the technical and the methodological requirements laid down in the Annex to this Regulation, the term 'user' should encompass all legal and natural persons which have access to the entity's network and information systems.

(11) To identify and address the risks posed to the security of network and information systems, the relevant entities should establish and maintain an appropriate risk management framework. As a part of the risk management framework, the relevant entities should establish, implement and monitor a risk treatment plan. The relevant entities may use the risk treatment plan to identify and prioritise risk treatment options and measures. Options for risk treatment include, in particular, avoiding, reducing or, in exceptional cases, accepting the risk. The choice of risk treatment options should take into account the results of the risk assessment carried out by the relevant entity, and be in accordance with the relevant entity's policy on the security of network and information systems. To give effect to the chosen risk treatment options, the relevant entities should take the appropriate risk treatment measures.

(12) To detect events, near misses and incidents, the relevant entities should monitor their network and information systems and should take actions to evaluate events, near misses and incidents. Those measures should be capable of allowing the detection of network-based attacks based on anomalous inbound and outbound traffic patterns and denial of service attacks in a timely manner.

(13) When the relevant entities conduct a business impact analysis, they are encouraged to carry out a comprehensive analysis establishing, as appropriate, maximum tolerable downtime, recovery time objectives, recovery point objectives and service delivery objectives.

(14) In order to mitigate risks stemming from a relevant entity's supply chain and its relationship with its suppliers, the relevant entities should establish a supply chain security policy which governs their relations with their direct suppliers and service providers. These entities should specify in the contracts with their direct suppliers or service providers adequate security clauses, for example by requiring, where appropriate, cybersecurity risk-management measures according to Article 21(2) of Directive (EU) 2022/2555 or other similar legal requirements.

(15) The relevant entities should regularly carry out security tests based on a dedicated policy and procedures to verify whether the cybersecurity risk-management measures are implemented and function properly. Security tests may be performed on specific network and information systems or on the relevant entity as a whole and may include automated or manual tests, penetration tests, vulnerability scanning, static and dynamic application security tests, configuration tests or security audits. The relevant entities may conduct security tests on their network and information systems at set-up, after infrastructure or application upgrades or modifications that they deem significant, or after maintenance. The findings of the security tests should inform the relevant entities' policies and procedures to assess the effectiveness of the cybersecurity risk-management measures, as well as independent reviews of their network and information security policies.

(16) In order to avoid significant disruption and harm caused by the exploitation of unpatched vulnerabilities in network and information systems, the relevant entities should set out and apply appropriate security patch management procedures which are aligned with the relevant entities' change management, vulnerability management, risk management and other relevant procedures. Relevant entities should take measures proportionate to their resources to ensure that security patches do not introduce additional vulnerabilities or instabilities. In case of planned inaccessibility to the service caused by the application of security patches, the relevant entities are encouraged to duly inform customers in advance.

(17) The relevant entities should manage the risks stemming from the acquisition of ICT products or ICT services from suppliers or service providers and should obtain assurance that the ICT products or ICT services to be acquired achieve certain cybersecurity protection levels, for example by European cybersecurity certificates and EU statements of conformity for ICT products or ICT services issued under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881 of the European Parliament and of the Council[2]. Where the relevant entities set out security requirements to apply to the ICT products to be acquired, they should take into account the essential cybersecurity requirements set out in a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements.

[2] 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, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(18) In order to protect against cyber threats and support the prevention and containment of data breaches, the relevant entities should implement network security solutions. Typical solutions for network security include the use of firewalls to protect the relevant entities' internal networks, the limitation of connections and access to services where connections and access are absolutely needed, and the use of virtual private networks for remote access and allowing connections of service providers only after an authorisation request and for a set time period such as the duration of a maintenance operation.

(19) In order to protect the networks of the relevant entities and their information systems against malicious and unauthorised software, those entities should implement controls that prevent or detect the use of unauthorised software and should, where appropriate, use detection and response software. The relevant entities should also consider implementing measures to minimize the attack surface, reduce vulnerabilities that can be exploited by attackers, control the execution of applications on endpoints, and deploy email and web application filters to reduce exposure to malicious content.

(20) Pursuant to Article 21(2), point (g), of Directive (EU) 2022/2555, Member States are to ensure that essential and important entities apply basic cyber hygiene practices and cybersecurity training. Basic cyber hygiene practices can include zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Cyber hygiene practices are a part of different technical and methodological requirements of the cybersecurity risk management measures set out in the Annex to this Regulation. With regard to basic cyber hygiene practices for users, the relevant entities should consider practices such as clear desk and screen policy, use of multi-factor and other authentication means, safe email use and web browsing, protection from phishing and social engineering, secure remote working practices.

(21) In order to prevent unauthorised access to the relevant entities' assets, the relevant entities should establish and implement a topic-specific policy addressing access by persons and by network and information systems, such as applications.

(22) In order to avoid that employees can misuse, for instance, access rights within the relevant entity to harm and cause damage, relevant entities should consider adequate employee security management measures and raise awareness among personnel about such risks. The relevant entities should establish, communicate and maintain a disciplinary process for handling violations of the relevant entities' network and information system security policies, which may be embedded in other disciplinary processes established by the relevant entities. Verification of the background of the employees and where applicable the direct suppliers and service providers of the relevant entities should contribute to the goal of human resources security in the relevant entities, and may include measures such as checks of the person's criminal record or past professional duties, as appropriate for the person's duties in the relevant entity and in line with the relevant entity's policy on the security of network and information systems.

(23) Multi-factor authentication can enhance the entities' cybersecurity and should be considered by the entities in particular when users access network and information systems from remote locations, or when they access sensitive information or privileged accounts and system administration accounts. Multi-factor authentication can be combined with other techniques to require additional factors under specific

circumstances, based on predefined rules and patterns, such as access from an unusual location, from an unusual device or at an unusual time.

(24) The relevant entities should manage and protect the assets which are of value to them through a sound asset management which should also serve as the basis for the risk analysis and business continuity management. The relevant entities should manage both tangible and intangible assets and should create an asset inventory, associate the assets with a defined classification level, handle and track the assets and take steps to protect the assets throughout their lifecycle.

(25) Asset management should involve classifying assets by their type, sensitivity, risk level, and security requirements and applying appropriate measures and controls to ensure their availability, integrity, confidentiality, and authenticity. By classifying assets by risk level, the relevant entities should be able to apply appropriate security measures and controls to protect assets such as encryption, access control including perimeter and physical and logical access control, backups, logging and monitoring, retention and disposal. When conducting a business impact analysis, the relevant entities may determine the classification level based on the consequences of disruption of assets for the entities. All employees of the entities handling assets should be familiar with the asset handling policies and instructions.

(26) The granularity of the asset inventory should be appropriate for the needs of the relevant entities. A comprehensive asset inventory could include, for each asset, at least a unique identifier, the owner of the asset, a description of the asset, the location of the asset, the type of asset, the type and classification of information processed in the asset, the date of last update or patch of the asset, the classification of the asset under the risk assessment, and the end of life of the asset. When identifying the owner of an asset, the relevant entities should also identify the person responsible for protecting said asset.

(27) The allocation and organisation of cybersecurity roles, responsibilities and authorities should establish a consistent structure for the governance and implementation of cybersecurity within the relevant entities, and should ensure effective communication in case of incidents. When defining and assigning responsibilities for certain roles, the relevant entities should consider roles such as chief information security officer, information security officer, incident handling officer, auditor, or comparable equivalents. Relevant entities may assign roles and responsibilities to external parties, such as ICT third-party service providers.

(28) In accordance with Article 21(2) of Directive (EU) 2022/2555, the cybersecurity risk-management measures are to be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from events such as theft, fire, flood, telecommunication or power failures, or unauthorised physical access and damage to, and interference with, an essential or important entity’s information and information processing facilities, which could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. The technical and the methodological requirements of the cybersecurity risk-management measures should therefore also address the physical and environmental security of network and information systems by including measures to protect such systems from system failures, human error, malicious acts or natural phenomena. Further examples of physical and environmental threats can include earthquakes, explosions, sabotage, insider threat, civil unrest, toxic waste, and environmental

emissions. Prevention of loss, damage or compromise of network and information systems or interruption to their operations due to the failure and disruption of supporting utilities should contribute to the goal of business continuity in the relevant entities. Moreover, protection against physical and environmental threats should contribute to security of network and information systems maintenance in the relevant entities.

(29) Relevant entities should design and implement protection measures against physical and environmental threats and determine minimum and maximum control thresholds for physical and environmental threats and monitor environmental parameters. For example, they should consider installing systems to detect at an early stage the flooding of areas where network and information systems are located. Regarding fire hazard, the relevant entities should consider the establishment of a separate fire compartment for the data centre, the use of fire-resistant materials, sensors for monitoring temperature and humidity, the connection of the building to a fire alarm system with an automated notification to the local fire department, and early fire detection and extinguishing systems. The relevant entities should also carry out regular fire drills and fire inspections. Furthermore, to ensure power supply, the relevant entities should consider overvoltage protection and corresponding emergency power supply, in accordance with relevant standards. Moreover, as overheating poses a risk to the availability of network and information systems, relevant entities, in particular data centre service providers, could consider adequate, continuous and redundant air conditioning systems.

(30) This Regulation is to further specify the cases in which an incident should be considered to be significant for the purpose of Article 23(3) of Directive (EU) 2022/2555. The criteria should be such that relevant entities are able to assess whether an incident is significant, in order to notify the incident in accordance with Directive (EU) 2022/2555. Furthermore, the criteria set out in this Regulation should be considered exhaustive, without prejudice to Article 5 of Directive (EU) 2022/2555. This regulation specifies the cases in which an incident should be considered to be significant by setting out horizontal as well as entity-type specific cases.

(31) Pursuant to Article 23(4) of Directive (EU) 2022/2555, relevant entities should be required to notify significant incidents within the deadlines set by that provision. Those notification deadlines are running from the moment the entity becomes aware of such significant incidents. The relevant entity is therefore required to report incidents that, based on its initial assessment, could cause severe operational disruption of the services or financial loss for that entity or affect other natural or legal persons by causing considerable material or non-material damage. Therefore, when a relevant entity has detected a suspicious event, or after a potential incident has been brought to its attention by a third party, such as an individual, a customer, an entity, an authority, a media organisation, or another source, the relevant entity should assess in a timely manner the suspicious event to determine whether it constitutes an incident and, if so, determine its nature and severity. The relevant entity is therefore to be regarded as having become “aware” of the significant incident when, after such initial assessment, that entity has a reasonable degree of certainty that a significant incident has occurred.

(32) With a view to establishing whether an incident is significant, where relevant, relevant entities should count the number of users impacted by the incident, taking into consideration business and end customers with whom the relevant entities have a contractual relationship as well as natural and legal persons that are associated with business customers. Where a relevant entity is unable to calculate the number of

impacted users, the relevant entity's estimate of the possible maximum number of affected users should be considered for the purpose of calculating the total number of users affected by the incident. The significance of an incident involving a trust service should not only be determined by the number of users but also by the number of relying parties as these can be equally affected by a significant incident involving a trust service in regard to operational disruption and material or non-material damage. Therefore, trust service providers should, where applicable, also take into account the number of relying parties when establishing whether an incident is significant. For that purpose, relying parties should be understood as natural or legal persons that rely upon a trust service.

(33) Maintenance operations resulting in the limited availability or unavailability of the services should not be considered as significant incidents if the limited availability or unavailability of the service occurs according to a scheduled maintenance operation. Moreover, where a service is unavailable due to scheduled interruptions such as interruptions or non-availability based on pre-determined contractual agreement should not be considered as significant incident.

(34) The duration of an incident which impacts availability of a service should be measured from the disruption of the proper provision of such service until the time of recovery. Where a relevant entity is unable to determine the moment when the disruption began, the duration of the incident should be measured from the moment the incident was detected, or from the moment when the incident was recorded in network or system logs or other data sources, whichever is earlier.

(35) Complete unavailability of a service should be measured from the moment the service is fully unavailable to users, to the moment when regular activities or operations have been restored to the level of service that was provided prior to the incident. Where a relevant entity is unable to determine when the complete unavailability of a service began, the unavailability should be measured from the moment it was detected by that entity.

(36) For the purpose of determining the direct financial losses resulting from an incident, relevant entities should take into account all the financial losses which they have incurred as a result of the incident, such as costs for replacement or relocation of software, hardware or infrastructure, staff costs, including costs associated with replacement or relocation of staff, recruitment of extra staff, remuneration of overtime and recovery of lost or impaired skills, fees due to non-compliance with contractual obligations, costs for redress and compensation to customers, losses due to forgone revenues, costs associated with internal and external communication, advisory costs, including costs associated with legal counselling, forensic services and remediation services, and other costs associated to the incident. However, administrative fines, as well as costs that are necessary for the day-to-day operation of the business, should not be considered as financial losses resulting from an incident, including costs for general maintenance of infrastructure, equipment, hardware and software, keeping skills of staff up to date, internal or external costs to enhance the business after the incident, including upgrades, improvements and risk assessment initiatives, and insurance premiums. The relevant entities should calculate the amounts of financial losses based on available data and, where the actual amounts of financial losses cannot be determined, the entities should estimate those amounts.

(37) Relevant entities should also be obliged to report incidents that have caused or are capable of causing the death of natural persons or considerable damage to natural

persons' health as such incidents are particularly serious cases of causing considerable material or non-material damage. For instance, an incident affecting a relevant entity could cause unavailability of healthcare or emergency services, or the loss of confidentiality or integrity of data with an effect on the health of natural persons. For the purpose of determining whether an incident has caused or is capable of causing considerable damage to a natural person's health, relevant entities should take into account whether the incident caused or is capable of causing severe injuries and ill-health. For that purpose, the relevant entities should not be required to collect additional information to which they do not have access.

(38) Limited availability should be considered to occur in particular when a service provided by a relevant entity is considerably slower than average response time, or where not all functionalities of a service are available. Where possible, objective criteria based on the average response times of services provided by the relevant entities should be used to assess delays in response time. A functionality of a service may be, for instance, a chat functionality or an image search functionality.

(39) Successful, suspectedly malicious and unauthorised access to a relevant entity's network and information systems should be regarded as a significant incident, where such access is capable of causing severe operational disruption. For instance, where a cyber threat actor pre-positions itself in a relevant entity's network and information systems with a view to causing disruption of services in the future, the incident should be considered to be significant.

(40) Recurring incidents that are linked through the same apparent root cause, which individually do not meet the criteria of a significant incident, should collectively be considered to be a significant incident, provided that they collectively meet the criterion for financial loss, and that they have occurred at least twice within six months. Such recurring incidents can indicate significant deficiencies and weaknesses in the relevant entity's cybersecurity risk management procedures and their level of cybersecurity maturity. Moreover, such recurring incidents are capable of causing significant financial loss for the relevant entity.

(41) The Commission has exchanged advice and cooperated with the Cooperation Group and ENISA on the draft implementing act, in accordance with Articles 21(5) and 23(11) of Directive (EU) 2022/2555.

(42) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[3], and delivered its opinion on 1 September 2024.

(43) The measures provided for in this Regulation are in accordance with the opinion of the committee established in accordance with Article 39 of Directive (EU) 2022/2555,

[3] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

HAS ADOPTED THIS REGULATION:

Article 1

Subject matter

This Regulation, with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers (the relevant entities) lays down the technical and the methodological requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555 and further specifies the cases in which an incident shall be considered to be significant as referred to in Article 23(3) of Directive (EU) 2022/2555.

Article 2

Technical and methodological requirements

1. For the relevant entities the technical and methodological requirements of cybersecurity risk-management measures referred to in Article 21(2), points (a) to (j), of Directive (EU) 2022/2555 are set out in the Annex to this Regulation.

2. The relevant entities shall ensure a level of security of network and information systems appropriate to the risks posed when implementing and applying the technical and methodological requirements of cybersecurity risk-management measures set out in the Annex to this Regulation. For that purpose, they shall take due account of the degree of their exposure to risks, their size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact, when complying with the technical and methodological requirements of cybersecurity risk-management measures set out in the Annex to this Regulation.

   Where the Annex to this Regulation provides that a technical or methodological requirement of a cybersecurity risk-management measure shall be applied “where appropriate”, “where applicable” or “to the extent feasible”, and where a relevant entity considers it not appropriate, not applicable or not feasible for the relevant entity to apply certain such technical and methodological requirements, the relevant entity shall in a comprehensible manner document its reasoning to that effect.

Article 3

Significant incidents

1. An incident shall be considered to be significant for the purposes of Article 23(3) of Directive 2022/2555 with regard to the relevant entities where one or more of the following criteria are fulfilled:

(a) the incident has caused or is capable of causing direct financial loss for the relevant entity that exceeds EUR 500 000 or 5 % of the relevant entity’s total annual turnover in the preceding financial year, whichever is lower;

(b) the incident has caused or is capable of causing the exfiltration of trade secrets as set out in Article 2 point (1), of Directive (EU) 2016/943 of the relevant entity;

(c) the incident has caused or is capable of causing the death of a natural person;

(d) the incident has caused or is capable of causing considerable damage to a natural person's health;

(e) a successful, suspectedly malicious and unauthorised access to network and information systems occurred, which is capable of causing severe operational disruption;

(f) the incident meets the criteria set out in Article 4;

(g) the incident meets one or more of the criteria set out in Articles 5 to 14.

(2) Scheduled interruptions of service and planned consequences of scheduled maintenance operations carried out by or on behalf of the relevant entities shall not be considered to be significant incidents.

(3) When calculating the number of users impacted by an incident for the purpose of Articles 7 and 9 to 14, the relevant entities shall consider all of the following:

(a) the number of customers that have a contract with the relevant entity which grants them access to the relevant entity's network and information systems or services offered by, or accessible via, those network and information systems;

(b) the number of natural and legal persons associated with business customers that use the entities' network and information systems or services offered by, or accessible via, those network and information systems.

Article 4

Recurring incidents

Incidents that individually are not considered a significant incident within the meaning of Article 3, shall be considered collectively as one significant incident where they meet all of the following criteria:

(a) they have occurred at least twice within 6 months;

(b) they have the same apparent root cause;

(c) they collectively meet the criteria set out in Article 3(1)(a).

Article 5

Significant incidents with regard to DNS service providers

With regard to DNS service providers, an incident shall be considered significant under Article 3(1)(g), where it fulfils one or more of the following criteria:

(a) a recursive or authoritative domain name resolution service is completely unavailable for more than 30 minutes;

(b) for a period of more than one hour, the average response time of a recursive or authoritative domain name resolution service to DNS requests is more than 10 seconds;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the authoritative domain name resolution service is compromised, except in cases where the data of fewer than 1 000 domain names managed by the DNS service provider, amounting to no more than 1 % of the domain names managed by the DNS service provider, are not correct because of misconfiguration.

Article 6

Significant incidents with regard to TLD name registries

With regard to TLD name registries, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) an authoritative domain name resolution service is completely unavailable;

(b) for a period of more than one hour, the average response time of an authoritative domain name resolution service to DNS requests is more than 10 seconds,

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the technical operation of the TLD is compromised.

Article 7

Significant incidents with regard to cloud computing service providers

With regard to cloud computing service providers, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) a cloud computing service provided is completely unavailable for more than 30 minutes;

(b) the availability of a cloud computing service of a provider is limited for more than 5 % of the cloud computing service's users in the Union, or for more than 1 million of the cloud computing service's users in the Union, whichever number is smaller, for a duration of more than one hour;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a cloud computing service is compromised as a result of a suspectedly malicious action,

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a cloud computing service is compromised with an impact on more than 5 % of that cloud computing service's users in the Union, or on more than 1 million of that cloud computing service's users in the Union, whichever number is smaller.

Article 8

Significant incidents with regard to data centre service providers

With regard to data centre service providers, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) a data centre service of a data centre operated by the provider is completely unavailable;

(b) the availability of a data centre service of a data centre operated by the provider is limited for a duration of more than one hour;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a data centre service is compromised as a result of a suspectedly malicious action;

(d) physical access to a data centre operated by the provider is compromised.

Article 9

Significant incidents with regard to content delivery network providers

With regard to content delivery network providers, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) a content delivery network is completely unavailable for more than 30 minutes;

(b) the availability of a content delivery network is limited for more than 5 % of the content delivery network's users in the Union, or for more than 1 million of the content delivery network's users in the Union, whichever number is smaller, for a duration of more than one hour;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a content delivery network is compromised as a result of a suspectedly malicious action;

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a content delivery network is compromised with an impact on more than 5 % of that content delivery network's users in the Union, or on more than 1 million of that content delivery network's users in the Union, whichever number is smaller.

Article 10

Significant incidents with regard to managed service providers and managed security service providers

With regard to managed service providers and managed security service providers, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) a managed service or managed security service is completely unavailable for more than 30 minutes;

(b) the availability of a managed service or managed security service is limited for more than 5 % of the service's users in the Union, or for more than 1 million of the service's users in the Union, whichever number is smaller, for a duration of more than one hour;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a managed service or managed security service is compromised as a result of a suspectedly malicious action;

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a managed service or a managed security service, is compromised with an impact on more than 5 % of that managed service's or that managed security service's users in the Union, or on more than 1 million of the service users in the Union, whichever number is smaller.

Article 11

Significant incidents with regard to providers of online marketplaces

With regard to providers of online marketplaces, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) an online marketplace is completely unavailable for more than 5 % of an online marketplace's users in the Union, or for more than 1 million of an online marketplace's users in the Union, whichever number is smaller;

(b) more than 5 % of an online marketplace's users in the Union, or more than 1 million of an online marketplace's users in the Union, whichever number is smaller, are impacted by limited availability of that online marketplace;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of an online marketplace is compromised as a result of a suspectedly malicious action;

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of an online marketplace is compromised with an impact on more than 5 % of that online marketplace's users in the Union, or on more than 1 million of that online marketplace's users in the Union, whichever number is smaller.

Article 12

Significant incidents with regard to providers of online search engines

With regard to providers of online search engines, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) an online search engine is completely unavailable for more than 5 % of that online search engine's users in the Union, or for more than 1 million of that online search engine's users in the Union, whichever number is smaller;

(b) more than 5 % of an online search engine's users in the Union, or more than 1 million of an online search engine's users in the Union, whichever number is smaller, are impacted by limited availability of that online search engine;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of an online search engine is compromised as a result of a suspectedly malicious action;

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of an online search engine is compromised with an impact on more than 5 % of that online search engine's users in the Union, or on more than 1 million of that online search engine's users in the Union, whichever number is smaller.

Article 13

Significant incidents with regard to providers of social networking services platforms

With regard to providers of social networking services platforms, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) a social networking service platform is completely unavailable for more than 5 % of that social networking service platform's users in the Union, or for more than 1 million of that social networking service platform's users in the Union, whichever number is smaller;

(b) more than 5 % of a social networking service platform's users in the Union, or more than 1 million of a social networking service platform's users in the Union, whichever number is smaller, are impacted by limited availability of that social networking service platform;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a social networking service platform is compromised as a result of a suspectedly malicious action;

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a social networking service platform is compromised with an impact on more than 5 % of that social networking service platform's users in the Union, or on more than 1 million of that social networking service platform's users in the Union, whichever number is smaller.

Article 14

Significant incidents with regard to trust service providers

With regard to trust service providers, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) a trust service is completely unavailable for more than 20 minutes;

(b) a trust service is unavailable to users, or relying parties, for more than one hour calculated on a calendar week basis;

(c) more than 1 % of the users or relying parties in the Union, or more than 200 000 users or relying parties in the Union, whichever number is smaller, are impacted by limited availability of a trust service;

(d) physical access to an area where network and information systems are located and to which access is restricted to trusted personnel of the trust service provider, or the protection of such physical access, is compromised;

(e) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a trust service is compromised with an impact on more than 0,1 % of users or relying parties, or more than 100 of users or relying parties, whichever number is smaller, of the trust service in the Union.

Article 15

Repeal

Commission Implementing Regulation (EU) 2018/151[4] is repealed.

Article 16

Entry into force and application

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

[4] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact (OJ L 26, 31.1.2018, p. 48, ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

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

Done at Brussels, 17.10.2024

For the Commission
The President
Ursula VON DER LEYEN