**European Parliament**
2019-2024

*Committee on Civil Liberties, Justice and Home Affairs*

**2020/0359(COD)**

10.6.2021

# DRAFT OPINION

of the Committee on Civil Liberties, Justice and Home Affairs

for the Committee on Industry, Research and Energy

on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Rapporteur for opinion (*): Lukas Mandl(*)

Associated committee – Rule 57 of the Rules of Procedure

PA_Legam

## SHORT JUSTIFICATION

The proposal for a Directive of the European Parliament and the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS2 Directive)[1] is part of a wider set of initiatives at Union level that seek to increase the resilience of public and private entities against threats. The proposal aims to address the shortcomings of the existing legislation and to enable the entities covered by its scope to respond better to the new challenges identified by the Commission in its impact assessment, which included an extensive stakeholder consultation. These challenges include in particular the increased digitisation of the internal market and the evolving security threat landscape.

The legal basis of the proposal is Article 114 TFEU, i.e. internal market. From a LIBE perspective it is however important to highlight that the measures imposed on network and information systems by the NIS2 Directive do not only serve to ensure the proper functioning of the internal market. **The Directive should also help to contribute to the security of the Union as a whole**, inter alia by avoiding diverging vulnerability to cybersecurity risks between Member States.

To this end, it is crucial to **eliminate existing divergences between Member States** resulting from different interpretations of the law by the Member States. For this reason, the Rapporteur welcomes the uniform condition established by the Regulation to determine the entities falling within the scope of the Directive. Additional suggestions are made to prevent divergence in implementation, notably to oblige the Commission to issue guidelines on the implementation of the *lex specialis* and the criteria applicable to SMEs (which should also ensure legal clarity and avoid unnecessary burden) and to require the Cooperation Group to further specify non-technical factors to be taken into account in the supply chain risk assessments. It is moreover stressed that cooperation between competent authorities need to take place both within and *between* Member States, in real time.

The draft report also takes on board a number of **recommendations made by the EDPS** in its opinion on the Cybersecurity Strategy and the NIS 2.0 Directive[2]. Most importantly, it is clarified both in the recitals and in the operative part of the text that any personal data processing under the NIS2 Directive is without prejudice to Regulation (EU) 2016/679 (GDPR)[3] and Directive 2002/58/EC[4] (ePrivacy). Given the narrower scope of the term ‘security of networks and information systems’ (only covers protection of technology) compared to ‘cybersecurity’ (also covers activities to protect users) the former term is only used when the context is purely technical. In relation to domain names and registration data, clarifications are proposed regarding 1) the legal basis of the publication of ‘relevant

[1] 2020/0359(COD).

[2] Opinion 5/2021: https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) *OJ L 119, 4.5.2016, p. 1–88.*

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ L 201, 31.7.2002, p. 37–47.*

information' for the purposes of identification and contacting, 2) the categories of data domain registration data subject to publication (based on an ICANN recommendation), and 3) the entities that might constitute 'legitimate access seekers'. It is also specified in the legal text that the proposal does not affect the attribution of jurisdiction and the competences of data protection supervisory authorities under the GDPR. Finally, a more comprehensive legal basis is provided for the cooperation and exchange of relevant information between the competent authorities under the Proposal and other relevant supervisory authorities, notably supervisory authorities under the GDPR.

**Other changes** introduced to the Commission proposal by the LIBE rapporteur relate to the following:

- To ensure coherence between the NIS2-Directive and the proposed Directive on resilience of critical entities (ECI)[5], the language of some provisions was aligned with those of the ECI proposal. In line with a similar change envisaged for the ECI Directive which should cover the same sectors as the NIS2 Directive, it is proposed to add 'food production, processing and distribution' to the scope.
- As regards personal data, it is clarified that the scanning of networks and information systems by CSIRTs should not only be in line with Regulation (EU) 2016/679 (GDPR)[6] but also with Directive 2002/58/EC[7] (ePrivacy). International transfers of personal data under this Directive should be in compliance with Chapter V of the GDPR.
- The Cooperation Group should meet twice rather than once a year to take stock of the latest developments regarding cybersecurity. The EDPB should participate in the meetings of the Cooperation Group as an observer.
- ENISA should issue annual rather than biennial reports on the state of cybersecurity in the Union. The report should also take into account the impact of cybersecurity incidents on the protection of personal data in the Union.
- The notification deadline of incidents is aligned with the deadline for the notification of breaches under the GDPR, namely 72 hours.
- While the notification of actual cybersecurity incidents by essential and important entities should indeed be mandatory, the notification of cyber threats should be voluntary to limit administrative burden and avoid over-reporting. To be considered significant, an incident should have caused actual damage and affected other natural and legal persons rather than such damage or effect being 'possible'.
- The circumstances to be taken into account when deciding on a sanction following a breach of the cybersecurity rules are aligned with the GDPR. As this would go against the current liability practice in Union law, it should not be possible to impose a temporary ban of natural persons from exercising managerial functions.

---

[5] 2020/0365(COD).

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) *OJ L 119, 4.5.2016, p. 1–88.*

[7] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ L 201, 31.7.2002, p. 37–47.*

- To avoid reputational damage, entities should not be obliged to make public aspects of non-compliance with the requirements under this Directive or the identity natural or legal persons responsible for the infringement.

## AMENDMENTS

The Committee on Civil Liberties, Justice and Home Affairs calls on the Committee on Civil Liberties, Justice and Home Affairs, as the committee responsible, to take into account the following amendments:

**Amendment 1**

**Proposal for a directive**
**Recital 1**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (1) Directive (EU) 2016/1148 of the European Parliament and the Council[11] aimed at building cybersecurity capabilities across the Union, mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing cybersecurity incidents, thus contributing to the Union's economy and society to function effectively. | (1) Directive (EU) 2016/1148 of the European Parliament and the Council[11] aimed at building cybersecurity capabilities across the Union, mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing cybersecurity incidents, thus contributing to the Union's ***security and to the effective functioning of its*** economy and society to function effectively. |
| [11] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1, 19.7.2016 p. 1). | [11] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1, 19.7.2016 p. 1). |

Or. en

**Amendment 2**

**Proposal for a directive**
**Recital 5**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different standards. This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for the effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and sanctions which are instrumental to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive. | (5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different standards. ***Ultimately, these divergences can lead to higher vulnerability of some Member States to cybersecurity threats, with potential spillover effects across the Union.*** This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for the effective ***and real time*** cooperation among the responsible authorities in each Member State***, and between the competent authorities of the Member States***, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and sanctions which are instrumental to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive. |

Or. en

**Amendment 3**

**Proposal for a directive**
**Recital 6**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (6) This Directive leaves unaffected the ability of Member States to take the necessary measures to ensure the protection of the essential interests of their security, to safeguard public policy and public security, and to allow for the | (6) This Directive leaves unaffected the ability of Member States to take the necessary measures to ensure the protection of the essential interests of their ***national*** security, to safeguard public policy and public security, and to allow for |

investigation, detection and prosecution of criminal offences, in compliance with Union law. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[14] , are of relevance.

[14] The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).

the ***prevention,*** investigation, detection and prosecution of criminal offences, in compliance with Union law. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[14] , are of relevance.

[14] The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).

Or. en

**Amendment 4**

**Proposal for a directive**
**Recital 8**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (8) In accordance with Directive (EU) 2016/1148, Member States were responsible for determining which entities meet the criteria to qualify as operators of essential services ('identification process'). ***In order to eliminate the*** wide divergences among Member States in that regard ***and ensure legal certainty for the risk management requirements and reporting obligations for all relevant entities***, a uniform criterion should be established that determines the entities falling within the scope of application of this Directive. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by | (8) ***The responsibility of Member States*** in accordance with Directive (EU) 2016/1148, Member States were responsible for determining which entities meet the criteria to qualify as operators of essential services ('identification process') ***has led to*** wide divergences among Member States in that regard***. Without prejudice to the specific exceptions provided in this Directive***, a uniform criterion should be established that determines the entities falling within the scope of application of this Directive ***to eliminate these divergences and ensure legal certainty regarding the risk management requirements and reporting*** |

| | |
|---|---|
| Commission Recommendation 2003/361/EC[15] , that operate within the sectors or provide the type of services covered by this Directive, fall within its scope. Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion. | ***obligations for all relevant entities***. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[15] , that operate within the sectors or provide the type of services covered by this Directive, fall within its scope. Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion. |
| [15] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36). | [15] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36). |

Or. en

**Amendment 5**

**Proposal for a directive**
**Recital 9**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (9) ***However,*** small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive. Member States should be responsible for establishing a list of such entities, and submit it to the Commission. | (9) Small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services ***based on a risk-assessment, including entities defined as critical entities or entities equivalent to critical entities under Directive (EU) XXX/XXX of the European Parliament and the Council[1a]***, should also be covered by this Directive. Member States should be responsible for establishing a list of such entities, and submit it to the Commission. |
| | ***[1a] Directive (EU)[XXX/XXX]of the European Parliament and of the Council of XXX on the resilience of critical*** |

***entities (OJ...).***

Or. en

**Amendment 6**

**Proposal for a directive**
**Recital 10**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (10) The Commission, in cooperation with the Cooperation Group, ***may*** issue guidelines on the implementation of the criteria applicable to micro and small ***enterprises***. | (10) The Commission, in cooperation with the Cooperation Group, ***should*** issue guidelines on the implementation of the criteria applicable to micro and small ***entities***. |

Or. en

**Amendment 7**

**Proposal for a directive**
**Recital 12**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission ***may*** issue guidelines in relation to the implementation of the lex specialis. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures | (12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission ***should*** issue guidelines in relation to the implementation of the lex specialis. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures |

and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

Or. en

**Amendment 8**

**Proposal for a directive**
**Recital 14**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[17] and this Directive. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent ***authority*** under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on incidents and cyber threats and the exercise of supervisory tasks. Authorities under both Directives should cooperate and exchange information, particularly ***in*** relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents affecting critical entities as well as on the cybersecurity measures taken by critical entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities under this Directive should be allowed to ***exercise their supervisory and enforcement powers on an*** essential entity | (14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[17] and this Directive***, wherever possible and appropriate***. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent ***authorities within and between Member States,*** under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on ***cyber*** incidents and cyber threats and the exercise of supervisory tasks. Authorities under both Directives ***within and between Member States*** should cooperate and exchange information, particularly ***on*** relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents affecting critical entities as well as on the cybersecurity measures taken by ***competent authorities under this Directive relevant for*** critical entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities |

identified as critical. Both authorities should cooperate and exchange information for this purpose.

[17] [insert the full title and OJ publication reference when known]

under this Directive should be allowed to ***assess the cybersecurity of*** essential entity identified as critical. Both authorities should cooperate and exchange information ***in real time*** for this purpose.

[17] [insert the full title and OJ publication reference when known]

Or. en

**Amendment 9**

**Proposal for a directive**
**Recital 18**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (18) Services offered by data centre service providers may not always be provided in a form of cloud computing service. Accordingly, data centres may not always constitute a part of cloud computing infrastructure. In order to manage all the risks posed to ***the*** security ***of network and information systems***, this Directive should cover also providers of such data centre services that are not cloud computing services. For the purpose of this Directive, the term 'data centre service' should cover provision of a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control. The term 'data centre service' does not apply to in-house, corporate data centres owned and operated for own purposes of the concerned entity. | (18) Services offered by data centre service providers may not always be provided in a form of cloud computing service. Accordingly, data centres may not always constitute a part of cloud computing infrastructure. In order to manage all the risks posed to ***cyber***security, this Directive should cover also providers of such data centre services that are not cloud computing services. For the purpose of this Directive, the term 'data centre service' should cover provision of a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control. The term 'data centre service' does not apply to in-house, corporate data centres owned and operated for own purposes of the concerned entity. |

Or. en

**Amendment 10**

**Proposal for a directive**
**Recital 20**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks. | (20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water***, food production, processing and distribution***, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks. |

Or. en

**Amendment 11**

**Proposal for a directive**
**Recital 22**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (22) In order to facilitate cross-border | (22) In order to facilitate cross-border |

| | |
|---|---|
| cooperation and communication among authorities and to enable this Directive to be implemented effectively, it is necessary for each Member State to designate a national single point of contact responsible for coordinating issues related to ***the security of network and information systems*** and cross-border cooperation at Union level. | cooperation and communication among authorities and to enable this Directive to be implemented effectively, it is necessary for each Member State to designate a national single point of contact responsible for coordinating issues related to ***cybersecurity*** and cross-border cooperation at Union level. |

Or. en

**Amendment 12**

**Proposal for a directive**
**Recital 23**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (23) Competent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way. The single points of contact should be tasked with forwarding incident notifications to the single points of contact of other ***affected*** Member States. At the level of Member States' authorities, to ensure one single entry point in every Member States, the single points of contacts should also be the addressees of relevant information on incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which they should be able to forward, as appropriate, to the relevant national competent authorities or CSIRTs under this Directive. | (23) Competent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way. The single points of contact should be tasked with forwarding incident notifications ***in real time*** to the single points of contact of ***all*** other Member States. At the level of Member States' authorities, to ensure one single entry point in every Member States, the single points of contacts should also be the addressees of relevant information on incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which they should be able to forward, as appropriate, to the relevant national competent authorities or CSIRTs under this Directive. |

Or. en

**Amendment 13**

**Proposal for a directive**
**Recital 25**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] ***as regards personal data***, on behalf of and upon request by an entity under this Directive, a proactive scanning of the network and information systems used for the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs. | (25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] ***and with Directive 2002/58/EC***, on behalf of and upon request by an entity under this Directive, a proactive scanning of the network and information systems used for the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs. |
| [19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1). | [19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1). |

Or. en

**Amendment 14**

**Proposal for a directive**
**Recital 27**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20] , a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. | (27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20] , a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. |

| | |
|---|---|
| Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union. | Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market ***or posing serious public security risks in several Member States or the Union as a whole***. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union. |
| [20] 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). | [20] 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). |

Or. en

**Amendment 15**

**Proposal for a directive**
**Recital 33**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (33) When developing guidance documents, the Cooperation Group should consistently: map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations to be addressed through better implementation of existing rules. | (33) When developing guidance documents, the Cooperation Group should consistently: map national ***and sectoral*** solutions and experiences, assess the impact of Cooperation Group deliverables on national ***and sectoral*** approaches, discuss implementation challenges and formulate specific recommendations to be addressed through better implementation of existing rules. |

Or. en

**Amendment 16**

**Proposal for a directive**
**Recital 34**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (34) The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should ***consider inviting*** Union bodies and agencies involved in cybersecurity policy, ***such as the European Cybercrime Centre (EC3)***, the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work. | (34) The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should ***invite relevant*** Union bodies and agencies involved in cybersecurity policy, ***notably Europol***, the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work. |

Or. en

**Amendment 17**

**Proposal for a directive**
**Recital 36**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (36) The Union should, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group and the CSIRTs network. ***Such agreements*** should ***ensure adequate protection of data***. | (36) The Union should, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group and the CSIRTs network. ***To the extent that personal data is transferred to a third country or international organisation, Chapter V of Regulation (EU) 2016/679*** should ***be respected***. |

Or. en

**Amendment 18**

**Proposal for a directive**
**Recital 47**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors ***including*** those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities. | (47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors ***that should be further specified by the Coordination Group, and which include*** those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities. |

Or. en

**Amendment 19**

**Proposal for a directive**
**Recital 50**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. Providers of such services should thus also ensure a level of security ***of network and information systems*** appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission. | (50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. Providers of such services should thus also ensure a level of ***cyber*** security appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission. |

Or. en

**Amendment 20**

**Proposal for a directive**
**Recital 52**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (52) Where appropriate, entities should inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves. The requirement to inform those recipients of such threats should not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such information about security threats | (52) Where appropriate, entities should ***be enabled to*** inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves. The requirement to inform those recipients of such threats should not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such |

| | |
|---|---|
| to the recipients should be free of charge. | information about security threats to the recipients should be free of charge. |

Or. en

**Amendment 21**

**Proposal for a directive**
**Recital 53**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (53) In particular, providers of public electronic communications networks or publicly available electronic communications services, should inform the service recipients of particular and significant cyber threats and of measures they can take to protect the security of their communications, for instance by using specific types of software or encryption technologies. | (53) In particular, providers of public electronic communications networks or publicly available electronic communications services, should ***be enabled to*** inform the service recipients of particular and significant cyber threats and of measures they can take to protect the security of their communications, for instance by using specific types of software or encryption technologies. |

Or. en

**Amendment 22**

**Proposal for a directive**
**Recital 54**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The use of end-to-end encryption should be reconciled with the Member State' ***powers*** to ensure the protection of their essential security | (54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The use of end-to-end encryption should be reconciled with the Member State' ***responsibility*** to ensure the protection of their essential security |

| | |
|---|---|
| interests and public security, and to permit the ***investigation***, detection and prosecution of criminal offences in compliance with Union law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime. | interests and public security, and to permit the ***prevention***, detection and prosecution of criminal offences in compliance with Union ***and national*** law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime. |

Or. en

**Amendment 23**

**Proposal for a directive**
**Recital 55**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification within ***24*** hours, followed by a final report not later than one month after. The initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that | (55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification within ***72*** hours, followed by a final report not later than one month after. The initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that |

should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines of ***24*** hours for the initial notification and one month for the final report.

should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines of ***72*** hours for the initial notification and one month for the final report.

Or. en

**Amendment 24**

**Proposal for a directive**
**Recital 56**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (56) Essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, for the purposes of simplifying the reporting of security incidents, Member States should establish a single entry point ***for all notifications*** required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. ENISA, in cooperation with the Cooperation Group should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union law and decrease the burdens for companies. | (56) Essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, for the purposes of simplifying the reporting of security incidents, Member States should establish a single entry point required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. ENISA, in cooperation with the Cooperation Group ***and the European Data Protection Board,*** should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union law and decrease the burdens for companies. |

Or. en

**Amendment 25**

**Proposal for a directive**
**Recital 57**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (57) Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage essential and important entities, on the basis of applicable criminal proceedings rules in compliance with Union law, to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, and without prejudice to the personal data protection rules applying to Europol, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the ***EC3*** and ENISA. | (57) Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage essential and important entities, on the basis of applicable criminal proceedings rules in compliance with Union law, to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, and without prejudice to the personal data protection rules applying to Europol, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the ***European Cybercrime Centre (EC3) of Europol*** and ENISA. |

Or. en

**Amendment 26**

**Proposal for a directive**
**Recital 58**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (58) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities should cooperate and exchange information on all relevant matters with data protection authorities and the supervisory authorities pursuant to Directive 2002/58/EC. | (58) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities should cooperate and exchange information on all relevant matters with data protection authorities and the supervisory authorities pursuant to ***Regulation (EU) 2016/679 and*** Directive 2002/58/EC. |

Or. en

**Amendment 27**

**Proposal for a directive**
**Recital 59**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (59) Maintaining accurate and complete databases of domain names and registration data (so called 'WHOIS data') and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with Union data protection law. | (59) Maintaining accurate and complete databases of domain names and registration data (so called 'WHOIS data') and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with ***applicable*** Union data protection law. |

Or. en

**Amendment 28**

**Proposal for a directive**
**Recital 60**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (60) The availability and timely accessibility of these data to public authorities, including competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CERTs, (CSIRTs, and as regards the data of their clients to providers of electronic communications networks and services and providers of cybersecurity technologies and services acting on behalf of those clients, is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents. Such access should | (60) The availability and timely accessibility of these data to public authorities, including competent authorities under Union or national law for the prevention, ***detection,*** investigation or prosecution of criminal offences, CERTs, (CSIRTs, and as regards the data of their clients**,** to providers of electronic communications networks and services and providers of cybersecurity technologies and services acting on behalf of those clients, is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents. Such access should |

comply with Union data protection law insofar as it is related to personal data.

comply with Union data protection law insofar as it is related to personal data.

Or. en

**Amendment 29**

**Proposal for a directive**
**Recital 62**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (62) TLD registries and the entities providing domain name registration services for them should make ***publically*** available domain name registration data ***that fall outside the scope of Union data protection rules***, such as ***data that concern*** legal ***persons***[25] . TLD registries and the entities providing domain name registration services for the TLD should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with ***Union data protection law***. Member States should ensure that TLD registries and the entities providing domain name registration services for them should respond without undue delay to requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and the entities providing domain name registration services for them should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of | (62) ***To comply with a legal obligation in terms of Article 6(1)(c) and Article 6(3) of Regulation (EU) 2016/679,*** TLD registries and the entities providing domain name registration services for them should make ***publicly*** available ***certain*** domain name registration data ***specified in the Member State law to which they are subject***, such as ***the domain name and the name of the*** legal ***person***. TLD registries and the entities providing domain name registration services for the TLD should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, ***notably to competent authorities under this Directive or supervisory authorities under Regulation (EU) 2016/679*** in accordance with ***their powers***. Member States should ensure that TLD registries and the entities providing domain name registration services for them should respond without undue delay to ***lawful and duly justified*** requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and the entities providing domain name registration services for them should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tool to |

| | |
|---|---|
| the European Data Protection Board. | provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board. |
| [25] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL recital (14) whereby "this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person". | [25] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL recital (14) whereby "this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person". |

Or. en

**Amendment 30**

**Proposal for a directive**
**Recital 63**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (63) All essential and important entities under this Directive should fall under the jurisdiction of the Member State where they provide their services. If the entity provides services in more than one Member State, it should fall under the separate and concurrent jurisdiction of each of these Member States. The competent authorities of these Member States should cooperate, provide mutual assistance to each other and where appropriate, carry out joint supervisory actions. | (63) ***Fur the purposes of this Directive,*** all essential and important entities under this Directive should fall under the jurisdiction of the Member State where they provide their services. If the entity provides services in more than one Member State, it should fall under the separate and concurrent jurisdiction of each of these Member States. The competent authorities of these Member States should ***agree on constituent classifications,*** cooperate ***wherever possible***, provide ***real time*** mutual assistance to each other and where appropriate, carry out joint supervisory actions. |

Or. en

**Amendment 31**

**Proposal for a directive**
**Recital 64**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (64) In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, content delivery network providers, cloud computing service providers, data centre service providers and digital providers, only one Member State should have jurisdiction over these entities. Jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether this criterion is fulfilled should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be the place where the decisions related to the cybersecurity risk management measures are taken in the Union. This will typically correspond to the place of the companies' central administration in the Union. If such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States where the entity has an establishment with the highest number of employees in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings. | (64) In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, content delivery network providers, cloud computing service providers, data centre service providers and digital providers, only one Member State should have jurisdiction over these entities. ***For the purposes of this Directive,*** jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether this criterion is fulfilled should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be the place where the decisions related to the cybersecurity risk management measures are taken in the Union. This will typically correspond to the place of the companies' central administration in the Union. If such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States where the entity has an establishment with the highest number of employees in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of |

the group of undertakings.

Or. en

**Amendment 32**

**Proposal for a directive**
**Recital 69**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of ***the following types*** of personal data***:*** IP addresses, uniform resources locators (URLs), domain names, and email addresses. | (69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services ***is necessary for compliance with their legal obligations under national law transposing this Directive, and is therefore covered by Articles 6(1)(c) and 6(3) of Regulation (EU) 2016/679. Moreover, such processing*** should constitute a legitimate interest of the data controller concerned, as referred to in ***Article 6(1)(f) of*** Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of ***certain categories*** of personal data***, including*** IP addresses, uniform resources locators (URLs), domain names, and email addresses. |

Or. en

**Amendment 33**

**Proposal for a directive**
**Recital 71**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (71) In order to make enforcement effective, a minimum list of administrative sanctions for breach of the cybersecurity risk management and reporting obligations provided by this Directive should be laid down, setting up a clear and consistent framework for such sanctions across the Union. Due regard should be given to the ***nature, gravity*** and duration of the infringement, the actual damage caused or losses incurred or potential damage or losses that could have been triggered, the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The ***imposition of*** penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection and due process. | (71) In order to make enforcement effective, a minimum list of administrative sanctions for breach of the cybersecurity risk management and reporting obligations provided by this Directive should be laid down, setting up a clear and consistent framework for such sanctions across the Union. Due regard should be given to the ***seriousness*** and duration of the infringement, the actual damage caused or losses incurred or potential damage or losses that could have been triggered***, any relevant previous infringements, the manner in which the infringement became known to the competent authority***, the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The penalties ***imposed,*** including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection and due process. |

Or. en

**Amendment 34**

**Proposal for a directive**
**Recital 74**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (74) Member States should be able to lay down the rules on criminal penalties for infringements of the national rules transposing this Directive. However, the imposition of criminal penalties for infringements of such national rules and of related administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice. | (74) Member States should be able to lay down the rules on criminal penalties for infringements of the national rules transposing this Directive***. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation***. However, the imposition of criminal penalties for infringements of such national rules and of related administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice. |

Or. en

**Amendment 35**

**Proposal for a directive**
**Recital 76**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning part or all the services provided by an essential entity ***and the imposition of a temporary ban from the exercise of managerial functions by a natural person***. Given their ***severity*** and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or | (76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning part or all the services provided by an essential entity. Given their ***seriousness*** and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such sanctions should only be applied as ultima ratio, meaning only |

losses suffered. Such sanctions should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial ***protection***, due process, presumption of innocence and right of defence.

after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial ***remedies***, due process, presumption of innocence and right of defence.

Or. en

**Amendment 36**

**Proposal for a directive**
**Recital 77**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (77) This Directive should establish cooperation rules between the competent authorities and the supervisory ***authorities in accordance with*** Regulation (EU) 2016/679 to deal with infringements related to personal data. | (77) This Directive should establish cooperation rules between the competent authorities ***under this Directive*** and the supervisory ***under*** Regulation (EU) 2016/679 to deal with infringements related to personal data. |

Or. en

**Amendment 37**

**Proposal for a directive**
**Recital 84**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (84) This Directive respects the | (84) This Directive respects the |

| | |
|---|---|
| fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles, | fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles, ***and in full compliance with existing Union legislation regulating these issues. Any processing of personal data under this Directive is subject to Regulation (EU) 2016/679 and Directive 2002/58/EC, in their respective scope of application, including the tasks and powers of the supervisory authorities competent to monitor compliance with those legal instruments,*** |

Or. en

**Amendment 38**

**Proposal for a directive**
**Article 2 – paragraph 1**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small ***enterprises*** within the meaning of Commission Recommendation 2003/361/EC.[28] | 1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small ***entities*** within the meaning of Commission Recommendation 2003/361/EC.[28] |
| [28] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36). | [28] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36). |

Or. en

**Amendment 39**

**Proposal for a directive**
**Article 2 – paragraph 2 – introductory part**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where: | 2. However, regardless of their size ***and based on a risk assessment according to Article 18***, this Directive also applies to entities referred to in Annexes I and II, where: |

Or. en

**Amendment 40**

**Proposal for a directive**
**Article 2 – paragraph 4 a (new)**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| | ***4a. Any processing of personal data under this Directive shall comply with Regulation (EU) 2016/679 and with Directive 2002/58/EC and shall be limited to what is strictly necessary and proportionate for the purposes of this Directive.*** |

Or. en

**Amendment 41**

**Proposal for a directive**
**Article 4 – paragraph 1 – point 1 – point b**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform | (b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform |

| | |
|---|---|
| automatic processing of digital data; | automatic processing of digital data***, and that are integrated into the IT system and are used for the provision of their intended services***; |

Or. en

**Amendment 42**

**Proposal for a directive**
**Article 4 – paragraph 1 – point 4**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (4) 'national strategy on cybersecurity' means a coherent framework of a Member State providing strategic objectives and priorities on the ***security of network and information systems*** in that Member State; | (4) 'national strategy on cybersecurity' means a coherent framework of a Member State providing strategic objectives and priorities on the ***cybersecurity*** in that Member State; |

Or. en

**Amendment 43**

**Proposal for a directive**
**Article 4 – paragraph 1 – point 24**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (24) 'entity' means any natural ***or*** legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations; | (24) 'entity' means any natural ***person or any*** legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations; |

Or. en

**Amendment 44**

**Proposal for a directive**
**Article 5 – paragraph 1 – point f**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council[38] [Resilience of Critical Entities Directive] for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks. | (f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council[38] [Resilience of Critical Entities Directive]***, both within and between Member States,*** for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks. |
| [38] [insert the full title and OJ publication reference when known] | [38] [insert the full title and OJ publication reference when known] |

Or. en

**Amendment 45**

**Proposal for a directive**
**Article 5 – paragraph 2 – point h**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats. | (h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats ***and their capability to respond to cybersecurity incidents***. |

Or. en

**Amendment 46**

**Proposal for a directive**
**Article 11 – paragraph 4**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 4. To the extent necessary to | 4. To the extent necessary to |

| | |
|---|---|
| effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State. | effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State ***in line with their respective competences***. |
| [39] [insert the full title and OJ publication reference when known] | [39] [insert the full title and OJ publication reference when known] |

Or. en

**Amendment 47**

**Proposal for a directive**
**Article 11 – paragraph 5**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 5. Member States shall ensure that their competent authorities regularly provide information to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] on cybersecurity risks, cyber threats and incidents affecting essential entities identified as critical, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], as well as the measures taken by competent authorities in response to those risks and incidents. | 5. Member States shall ensure that their competent authorities regularly ***and timely*** provide information to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] on cybersecurity risks, cyber threats and incidents affecting essential entities identified as critical, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], as well as the measures taken by competent authorities in response to those risks and incidents. |

Or. en

**Amendment 48**

**Proposal for a directive**
**Article 12 – paragraph 3 – introductory part**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) in accordance with Article 17(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group. | 3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service ***and the European Data Protection Board*** shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) in accordance with Article 17(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group. |

Or. en

**Amendment 49**

**Proposal for a directive**
**Article 12 – paragraph 8**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 8. The Cooperation Group shall meet regularly and at least ***once*** a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to ***promote*** strategic cooperation and ***exchange of*** information. | 8. The Cooperation Group shall meet regularly and at least ***twice*** a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to ***facilitate*** strategic cooperation and ***real time*** information ***exchange***. |

Or. en

**Amendment 50**

**Proposal for a directive**
**Article 15 – paragraph 1 – introductory part**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 1. ENISA shall issue, in cooperation with the Commission, ***a biennial*** report on the state of cybersecurity in the Union. The report shall in particular include an assessment of the following: | 1. ENISA shall issue, in cooperation with the Commission, ***an annual*** report on the state of cybersecurity in the Union. The report shall in particular include an assessment of the following: |

Or. en

**Amendment 51**

**Proposal for a directive**
**Article 15 – paragraph 1 – point c a (new)**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| | ***(ca) the impact of cybersecurity incidents on the protection of personal data in the Union.*** |

Or. en

**Amendment 52**

**Proposal for a directive**
**Article 17 – paragraph 2**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 2. Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity. | 2. Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess ***evolving*** cybersecurity risks and management practices and their impact on the operations of the entity. |

Or. en

**Amendment 53**

**Proposal for a directive**
**Article 18 – paragraph 1**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the ***security*** of network and information systems ***which those entities use in*** the provision of their services. Having regard to the state of the art, those measures shall ensure a level of ***security*** of network and information systems appropriate to the risk presented. | 1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the ***cybersecurity*** of network and information systems ***used for*** the provision of their ***services, and in view of assuring the continuity of these*** services. Having regard to the state of the art, those measures shall ensure a level of ***cybersecurity*** of network and information systems appropriate to the risk presented. |

Or. en

**Amendment 54**

**Proposal for a directive**
**Article 18 – paragraph 3**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. | 3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. ***Competent authorities shall provide guidance to entities on the practical and proportionate application.*** |

Or. en

**Amendment 55**

**Proposal for a directive**
**Article 20 – paragraph 2 – introductory part**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 2. Member States shall ***ensure*** that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident. | 2. Member States shall ***foresee*** that essential and important entities ***may*** notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident. |

Or. en

**Amendment 56**

**Proposal for a directive**
**Article 20 – paragraph 2 – subparagraph 1**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| Where applicable, those entities ***shall*** notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability. | Where applicable, those entities ***may*** notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability. |

Or. en

**Amendment 57**

**Proposal for a directive**
**Article 20 – paragraph 4 – point a**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (a) without undue delay and in any | (a) without undue delay and in any |

| | |
|---|---|
| event within ***24*** hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action; | event within ***72*** hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action; |

Or. en

**Amendment 58**

**Proposal for a directive**
**Article 20 – paragraph 4 – point c – introductory part**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (c) a ***final*** report not later than one month after the submission of the report under point (a), including at least the following: | (c) a ***comprehensive*** report not later than one month after the submission of the report under point (a), including at least the following: |

Or. en

**Amendment 59**

**Proposal for a directive**
**Article 20 – paragraph 4 – point c – point ii**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (ii) the type of threat or root cause that likely triggered the incident; | (ii) the type of ***cyber*** threat or root cause that likely triggered the incident; |

Or. en

**Amendment 60**

**Proposal for a directive**
**Article 20 – paragraph 4 – point c – point iii**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (iii) applied and ongoing mitigation measures. | (iii) applied and ongoing mitigation measures ***or remedies***. |

Or. en

**Amendment 61**

**Proposal for a directive**
**Article 20 – paragraph 6**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States and ENISA of the incident. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided. | 6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States and ENISA of the incident ***in real time***. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided. |

Or. en

**Amendment 62**

**Proposal for a directive**
**Article 23 – paragraph 1**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD ***registries and the entities providing domain name registration services for the TLD shall collect and maintain*** accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data. | 1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD ***have policies and procedures in place to ensure that*** accurate and complete domain name registration data ***is collected and maintained*** in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data. ***Member States shall ensure that such policies and procedures are made publicly available.*** |

Or. en

**Amendment 63**

**Proposal for a directive**
**Article 23 – paragraph 2**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain ***relevant*** information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs. | 2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain ***the*** information ***necessary*** to identify and contact the holders of the domain names***, namely their name, their physical and e-mail address as well as their telephone number,*** and the points of contact administering the domain names under the TLDs. |

Or. en

**Amendment 64**

**Proposal for a directive**
**Article 23 – paragraph 3**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| ***3. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the databases include accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.*** | ***deleted*** |

Or. en

*Justification*

*This paragraph has been included in Article 23(1).*

**Amendment 65**

**Proposal for a directive**
**Article 23 – paragraph 4**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 4. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, without undue delay after the registration of a domain name, domain registration data ***which are not personal data***. | 4. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, ***in accordance with Article 6(1)(c) and Article 6(3) of Regulation (EU) 2016/679 and*** without undue delay after the registration of a domain name, ***certain*** domain ***name*** registration data***, such as the domain name and the name of the legal person***. |

Or. en

**Amendment 66**

**Proposal for a directive**
**Article 23 – paragraph 5**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 5. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD reply without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available. | 5. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD reply without undue delay to all ***lawful and duly notified*** requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available. |

Or. en

**Amendment 67**

**Proposal for a directive**
**Article 24 – paragraph 3**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 3. If an entity referred to in paragraph 1 is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under this Article, any Member State in which the entity provides services may take legal actions against the entity for non-compliance with the obligations under this Directive. | 3. If an entity referred to in paragraph 1 is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. ***Without prejudice to the competences of the supervisory authorities under Regulation (EU) 2016/679,*** such entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under this Article, any Member State in which the entity provides services may take legal actions against the entity for non-compliance with the obligations under this Directive. |

Or. en

**Amendment 68**

**Proposal for a directive**
**Article 26 – paragraph 1 – introductory part**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 1. Without prejudice to Regulation (EU) 2016/679, Member States shall ensure that essential and important entities may exchange relevant cybersecurity information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools, where such information sharing: | 1. Without prejudice to Regulation (EU) 2016/679 ***or Directive 2002/58/EC***, Member States shall ensure that essential and important entities may exchange relevant cybersecurity information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools, ***and the location or identity of the attacker*** where such |

information sharing:

Or. en

**Amendment 69**

**Proposal for a directive**
**Article 28 – paragraph 2**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 2. Competent authorities shall work in close cooperation with ***data protection*** authorities when addressing incidents resulting in personal data breaches. | 2. Competent authorities shall work in close cooperation with ***supervisory*** authorities ***competent under Regulation (EU) 2016/679*** when addressing incidents resulting in personal data breaches. ***To this end, competent authorities and supervisory authorities shall exchange information relevant for their respective area of competence. Moreover, competent authorities shall, upon request of the competent supervisory authorities, provide them all information obtained in the context of any audits and investigations that relate to the processing of personal data.*** |

Or. en

**Amendment 70**

**Proposal for a directive**
**Article 29 – paragraph 4 – point h**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| ***(h) order those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner;*** | ***deleted*** |

Or. en

**Amendment 71**

**Proposal for a directive**
**Article 29 – paragraph 5 – point b**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| ***(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.*** | ***deleted*** |

Or. en

**Amendment 72**

**Proposal for a directive**
**Article 29 – paragraph 5 – subparagraph 1**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| ***These sanctions*** shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. | ***This sanction*** shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. |

Or. en

**Amendment 73**

**Proposal for a directive**
**Article 29 – paragraph 7 – point c**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (c) the actual damage caused ***or losses incurred or potential damage*** or losses that could have been triggered, insofar as | (c) the actual damage caused or losses that could have been triggered, insofar as they can be determined. Where evaluating |

| | |
|---|---|
| they can be determined. Where evaluating this aspect, account shall be taken, amongst others, of actual or ***potential financial or*** economic losses, effects on other services, number of users affected or potentially affected; | this aspect, account shall be taken, amongst others, of actual or economic losses, effects on other services, ***and*** number of users affected or potentially affected; |

Or. en

**Amendment 74**

**Proposal for a directive**
**Article 29 – paragraph 7 – point c a (new)**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| | ***(ca) any relevant previous infringements by the entity concerned;*** |

Or. en

**Amendment 75**

**Proposal for a directive**
**Article 29 – paragraph 7 – point c b (new)**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| | ***(cb) the manner in which the infringement became known to the competent authority, in particular whether, and if so to what extent, the entity notified the infringement;*** |

Or. en

**Amendment 76**

**Proposal for a directive**
**Article 29 – paragraph 7 – point g**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| (g) the level of cooperation ***of the natural or legal person(s) held responsible*** with the competent authorities***.*** | (g) the level of cooperation with the competent authorities ***in order to remedy the infringement and mitigate possible adverse effects of the infringements;*** |

Or. en

**Amendment 77**

**Proposal for a directive**
**Article 29 – paragraph 7 – point g a (new)**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| | ***(ga) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained or losses avoided, directly or indirectly, from the infringement.*** |

Or. en

**Amendment 78**

**Proposal for a directive**
**Article 29 – paragraph 9**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 9. Member States shall ensure that their competent authorities inform the relevant competent authorities of ***the*** Member ***State concerned*** designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, or as an entity equivalent to a critical entity, under Directive (EU) XXXX/XXXX [Resilience of Critical | 9. Member States shall ensure that their competent authorities inform ***in real time*** the relevant competent authorities of ***all*** Member ***States*** designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, or as an entity equivalent to a critical entity, under Directive (EU) XXXX/XXXX [Resilience of Critical |

| | |
|---|---|
| Entities Directive] with the obligations pursuant to this Directive. Upon request of competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], competent authorities may exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent. | Entities Directive] with the obligations pursuant to this Directive. Upon request of competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], competent authorities may exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent. |

Or. en

**Amendment 79**

**Proposal for a directive**
**Article 30 – paragraph 4 – point g**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| ***(g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner;*** | ***deleted*** |

Or. en

**Amendment 80**

**Proposal for a directive**
**Article 30 – paragraph 4 – point h**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| ***(h) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;*** | ***deleted*** |

Or. en

**Amendment 81**

**Proposal for a directive**
**Article 31 – paragraph 2**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 2. Administrative fines shall***, depending on the circumstances of each individual case,*** be imposed in addition to, or instead of, measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4). | 2. Administrative fines shall be imposed in addition to, or instead of, measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4)***, depending on the circumstances of each individual case***. |

Or. en

**Amendment 82**

**Proposal for a directive**
**Article 31 – paragraph 3**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 3. ***Where*** deciding whether to impose an administrative fine ***and*** deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article 29(7). | 3. Deciding whether to impose an administrative fine ***shall depend on the circumstances of each individual case, and when*** deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article 29(7). |

Or. en

**Amendment 83**

**Proposal for a directive**
**Article 31 – paragraph 5**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| ***5. Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement in accordance with a prior*** | ***deleted*** |

***decision of the competent authority.***

Or. en

**Amendment 84**

**Proposal for a directive**
**Article 32 – paragraph 1**

| *Text proposed by the Commission* | *Amendment* |
|---|---|
| 1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation ***within a reasonable period of time***. | 1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation ***without undue delay***. |

Or. en