**DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**of 14 December 2022**

**on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)**

(Text with EEA relevance)

CHAPTER I

**GENERAL PROVISIONS**

*Article 1*

**Subject matter**

1.   This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market.

2.   To that end, this Directive lays down:

(a) obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);

(b) cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive (EU) 2022/2557;

(c) rules and obligations on cybersecurity information sharing;

(d) supervisory and enforcement obligations on Member States.

*Article 2*

**Scope**

1.   This Directive applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union.

Article 3(4) of the Annex to that Recommendation shall not apply for the purposes of this Directive.

2.   Regardless of their size, this Directive also applies to entities of a type referred to in Annex I or II, where:

(a) services are provided by:

(i) providers of public electronic communications networks or of publicly available electronic communications services;

(ii) trust service providers;

(iii) top-level domain name registries and domain name system service providers;

(b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;

(c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;

(d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;

(e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;

(f) the entity is a public administration entity:

(i) of central government as defined by a Member State in accordance with national law; or

(ii) at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities.

3.   Regardless of their size, this Directive applies to entities identified as critical entities under Directive (EU) 2022/2557.

4.   Regardless of their size, this Directive applies to entities providing domain name registration services.

5.   Member States may provide for this Directive to apply to:

(a) public administration entities at local level;

(b) education institutions, in particular where they carry out critical research activities.

6.   This Directive is without prejudice to the Member States’ responsibility for safeguarding national security and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.

7.   This Directive does not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.

8.   Member States may exempt specific entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in paragraph 7 of this Article, from the obligations laid down in Article 21 or 23 with regard to those activities or services. In such cases, the supervisory and enforcement measures referred to in Chapter VII shall not apply in relation to those specific activities or services. Where the entities carry out activities or provide services exclusively of the type referred to in this paragraph, Member States may decide also to exempt those entities from the obligations laid down in Articles 3 and 27.

9.   Paragraphs 7 and 8 shall not apply where an entity acts as a trust service provider.

10.  This Directive does not apply to entities which Member States have exempted from the scope of Regulation (EU) 2022/2554 in accordance with Article 2(4) of that Regulation.

11.  The obligations laid down in this Directive shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States’ national security, public security or defence.

12.  This Directive applies without prejudice to Regulation (EU) 2016/679, Directive 2002/58/EC, Directives 2011/93/EU ([1](https://eur-lex.europa.eu/eli/dir/2022/2555#E0001)) and 2013/40/EU ([2](https://eur-lex.europa.eu/eli/dir/2022/2555#E0002)) of the European Parliament and of the Council and Directive (EU) 2022/2557.

13.  Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities in accordance with this Directive only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of entities concerned.

14.  Entities, the competent authorities, the single points of contact and the CSIRTs shall process personal data to the extent necessary for the purposes of this Directive and in accordance with Regulation (EU) 2016/679, in particular such processing shall rely on Article 6 thereof.

The processing of personal data pursuant to this Directive by providers of public electronic communications networks or providers of publicly available electronic communications services shall be carried out in accordance with Union data protection law and Union privacy law, in particular Directive 2002/58/EC.