Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (Text with EEA relevance)

PART I

FRAMEWORK (GENERAL RULES FOR THE ORGANISATION OF THE SECTOR)

TITLE V

SECURITY

Article 40

Security of networks and services

1 Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. Having regard to the state of the art, those measures shall ensure a level of security appropriate to the risk presented. In particular, measures, including encryption where appropriate, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services.

The European Union Agency for Network and Information Security ('ENISA') shall facilitate, in accordance with Regulation (EU) No 526/2013 of the European Parliament and of the Council[(1)], the coordination of Member States to avoid diverging national requirements that may create security risks and barriers to the internal market.

2 Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services.

In order to determine the significance of the impact of a security incident, where available the following parameters shall, in particular, be taken into account:

a the number of users affected by the security incident;

b the duration of the security incident;

c the geographical spread of the area affected by the security incident;

d the extent to which the functioning of the network or service is affected;

e the extent of impact on economic and societal activities.

Where appropriate, the competent authority concerned shall inform the competent authorities in other Member States and ENISA. The competent authority concerned may inform the public or require the providers to do so, where it determines that disclosure of the security incident is in the public interest.

Once a year, the competent authority concerned shall submit a summary report to the Commission and to ENISA on the notifications received and the action taken in accordance with this paragraph.

3 Member States shall ensure that in the case of a particular and significant threat of a security incident in public electronic communications networks or publicly available electronic communications services, providers of such networks or services shall inform their users potentially affected by such a threat of any possible protective measures or remedies which can be taken by the users. Where appropriate, providers shall also inform their users of the threat itself.

4 This Article is without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC.

5 The Commission, taking utmost account of ENISA's opinion, may adopt implementing acts detailing the technical and organisational measures referred to in paragraph 1, as well as the circumstances, format and procedures applicable to notification requirements pursuant to paragraph 2. They shall be based on European and international standards to the greatest extent possible, and shall not prevent Member States from adopting additional requirements in order to pursue the objectives set out in paragraph 1.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(4).

Article 41

Implementation and enforcement

1 Member States shall ensure that, in order to implement Article 40, the competent authorities have the power to issue binding instructions, including those regarding the measures required to remedy a security incident or prevent one from occurring when a significant threat has been identified and time-limits for implementation, to providers of public electronic communications networks or publicly available electronic communications services.

2 Member States shall ensure that competent authorities have the power to require providers of public electronic communications networks or publicly available electronic communications services to:

a provide information needed to assess the security of their networks and services, including documented security policies; and

b submit to a security audit carried out by a qualified independent body or a competent authority and make the results thereof available to the competent authority; the cost of the audit shall be paid by the provider.

3 Member States shall ensure that the competent authorities have all the powers necessary to investigate cases of non-compliance and the effects thereof on the security of the networks and services.

4 Member States shall ensure that, in order to implement Article 40, the competent authorities have the power to obtain the assistance of a Computer Security Incident Response Team ('CSIRT') designated pursuant to Article 9 of Directive (EU) 2016/1148 in relation to issues falling within the tasks of the CSIRTs pursuant to point 2 of Annex I to that Directive.

5 The competent authorities shall, where appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities, the competent authorities within the meaning of Article 8(1) of Directive (EU) 2016/1148 and the national data protection authorities.

(**1**) Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (OJ L 165, 18.6.2013, p. 41).