180717
DLA input in tracked changes 23/8 rev

FINAL
CA6
Security

The CA covers Art 2(22), 40-41 and related recitals. All relevant AMs, including AMs 213, 214, 332, 565-581, 732 as well as IMCO xx, ~~CULT yy,~~ LIBE ~~zz~~9, 17, 26-35, fall.

Recitals

(90) Providers of public electronic communications networks or publicly available electronic communications services, or of both, should be required to take measures to safeguard the security of their networks and services, respectively***, and to prevent*** ***or*** ~~***and***~~ ***minimise the impact of security incidents, including incidents caused by hijacking of devices.***[1] Having regard to the state of the art, those measures should ensure a level of security of networks and services appropriate to the risks posed. Security measures should take into account, as a minimum, all the relevant aspects of the following elements: as regards security of networks and facilities: physical and environmental security, security of supplies, access control to networks and integrity of networks; as regards incident handling: incident-handling procedures, incident detection capability, incident reporting and communication; as regards business continuity management: service continuity strategy and contingency plans, disaster recovery capabilities; and as regards monitoring, auditing and testing: monitoring and logging policies, exercise contingency plans, network and service testing, security assessments and compliance monitoring; and compliance with international standards.

(91) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that they are also subject to appropriate security requirements in accordance with their specific nature and economic importance. Providers of such services should thus ensure a level of security commensurate with the degree of risk posed to the security of the electronic communications services they provide. 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 lower than for traditional electronic communications services. Therefore, whenever it is justified by the actual assessment of the security risks involved, the security requirements for number-independent interpersonal communications services should be lighter. In that context, the providers should be able to decide about the measures they consider appropriate to manage the risks posed to the security of their services. The same approach should apply mutatis mutandis to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission.

(91a) Providers of public communications networks or publicly available electronic communications services should inform users of measures they can take to protect

1 To reflect AM 580 Kumpula-Natri. DLA input.

the security of their communications, for instance by using specific types of software or encryption technologies. The requirement to inform users of particular security risks should not discharge a provider from the obligation to take, at its own costs, appropriate and immediate measures to seek to prevent or remedy any new, unforeseen security risks and restore the normal security level. The provision of information about security risks to the subscriber should be free of charge.[2]

(91b) In order to safeguard security and integrity of networks and services, the use of end-to-end encryption should be promoted and, where necessary, should be mandatory in accordance with the principles of security and privacy by default and design;[3]

(92) Competent authorities should ensure that the integrity and availability of public communications networks are maintained. The European Network and Information Security Agency ('ENISA') should contribute to an enhanced level of security of electronic communications by, amongst other things, ***assisting Member States in preventing and resolving potential internal market problems due to conflicting particular security measures, issue guidelines, in close cooperation with BEREC and the Commission on security criteria,***[4] providing expertise and advice, and promoting the exchange of best practices. The competent authorities should have the necessary means to perform their duties, including powers to request the information necessary to assess the level of security of networks or services. They should also have the power to request comprehensive and reliable data about actual security incidents that have had a significant impact on the operation of networks or services. They should, where necessary, be assisted by Computer Security Incident Response Teams (CSIRTs) established under Article 9 of Directive (EU) 2016/1148. In particular, CSIRTs may be required to provide competent authorities with information about risks and incidents affecting public communications networks and publicly available electronic communications services and recommend ways to address them.

Articles

Art 2(22) (Definitions)

'security' of networks and services means the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those networks or services.

TITLE V: SECURITY AND INTEGRITY

Article 40

Security of networks and services

1. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services take appropriate ***and proportionate***[5] technical and organisational measures to appropriately manage the risks posed to security of

2 AM 213 Kumpula-Natri. DLA input.

3 Part of AM 214 Kallas (slightly amended). Linked AM 565/566/568, 567, 570. The phrase "...principles of data protection by design and privacy by design..." could possibly be replaced by "principle of security by design" for the purpose of the EECC

4 Poss additional text, cf AM 578

5 Cf Presidency 12/4 doc

networks and services. Having regard to the state of the art, these measures shall ensure a level of security appropriate to the risk presented. In particular, measures shall be taken to ***ensure that, when necessary for confidentiality, electronic communications content is encrypted from end-to-end by default, in order to***[6] prevent and minimise the impact of security incidents on users**,** other networks ***or*** services.

1a. Member States shall not impose any obligation on undertakings providing public communications networks or publicly available electronic communications services that would result in a weakening of the security of their networks or services.[7]

Where Member States impose additional security requirements on undertakings providing public communications networks or publicly available electronic communications services in more than one Member State, they shall notify those measures to the Commission and ENISA. ENISA shall assist Member States in coordinating the measures taken to avoid duplication or diverging requirements that may create security risks and barriers to the internal market.[8]

2. Member States shall ensure that undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks.[9]

3. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify without undue delay the competent authority of a security ***incident***[10] ***or loss of integrity***[11] 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, the following parameters shall, in particular, be taken into account:

(a) the number of users affected by the ***incident***;[12]

(b) the duration of the ***incident***;

(c) the geographical spread of the area affected by the ***incident***;

(d) the extent to which the functioning of the ***network or***[13] service is ***affected***.[14]

(e) the impact on economic and societal activities.

Where appropriate, the competent authority concerned shall inform the competent authorities in other Member States and the European Network and Information Security Agency (ENISA). The competent authority concerned may inform the public or require the ***providers***[15] to do so, where it determines that disclosure of the ***incident*** is in the public interest.

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

---

6 AM 565/566 Kumpula-Natri, 567 Reimon, 568 Kallas
7 AM 570 Kallas (sligthly amended)
8 AM 577 Kallas (moved and slightly amended)
9 Presidency 12/4 doc proposes to delete this par
10 AM 571 Tošenovský, leading to consequential changes later on
11 Possible addition of "integrity", cf AM 214. To add "or loss of integrity" would mean retaining the current wording of FD Art 13a proposed deleted by the COM
12 Consequence of AM 571
13 AM 572 Tošenovský
14 Cf Presidency 12/4 doc
15 Cf Presidency 12/4 doc

Member States shall ensure that, in the case of a particular risk of a security incident in public communications networks or publicly available electronic communications services, providers of such networks or services inform their users of such a risk and of any possible protective measures or remedies which can be taken by the users.[16]

4. This Article is without prejudice to Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

5. The Commission, shall adopt delegated acts in accordance with Article 109 with a view to specifying the measures referred to in paragraphs 1 and 2, including measures defining the circumstances, format and procedures applicable to notification requirements. The delegated acts 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 paragraphs 1 and 2. ***The first such delegated acts shall be adopted by [insert date].***[17]

5a. In order to contribute to the consistent application of measures for the security of networks and services, ENISA shall, by...[date], after consulting stakeholders and in close cooperation with the Commission and BEREC, issue guidelines on minimum criteria and common approaches for the security of networks and services and the promotion of the use of end-to-end encryption.[18]

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 ***prevent or***[19] remedy ***an incident*** and time-limits for implementation, to undertakings providing public communications networks or publicly available electronic communications services.2. Member States shall ensure that competent authorities have the power to require undertakings providing public communications networks or publicly available electronic communications services to:

(a) provide information needed to assess the security and/or integrity of their services and networks, 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 undertaking.

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 Computer Security Incident Response Teams ('CSIRTs') under Article 9 of Directive (EU) 2016/1148/EU in relation to issues falling within the tasks of the CSIRTs pursuant to Annex I, point 2 of that Directive.

---

16 AM 575 Kumpula-Natri (slightly amended). Proposed deletion of "end" as 40(1) refers to "users".

17 AM 84 Del Castillo (a horizontal AM to oblige the COM to adopt delegated/implementing acts by a certain date where it's considered necessary to have such acts, as opposed to merely giving the COM the possibility to do so).

18 AM 578 Kallas

19 AM 579 Tošenovský

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