Council of the European Union

Brussels, 17 May 2016
(OR. en)

Interinstitutional File:
2013/0027 (COD)

5581/1/16
REV 1 ADD 1

TELECOM 7
DATAPROTECT 6
CYBER 4
MI 37
CSC 15
CODEC 84
PARLNAT 154

STATEMENT OF THE COUNCIL'S REASONS

Subject:	Position of the Council at first reading with a view to the adoption of a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures for a high common level of security of network and information systems across the Union – Statement of the Council's reasons – Adopted by the Council on 17 May 2016

I. INTRODUCTION

1. The Commission submitted its proposal for a Directive of the European Parliament and of the Council concerning *measures to ensure a high common level of network and information security across the Union* (hereinafter referred to as the Directive) on 12 February 2013 with article 114 TFEU as a legal basis.

2. The European Economic and Social Committee voted its Opinion on 22 May 2013 and the Committee of the Regions voted its Opinion on 3-4 July 2013.

3. The European Parliament voted its legislative resolution in first reading on 13 March 2014[1], adopting 138 Amendments.

4. The Council and the European Parliament entered into negotiations with a view to reaching an early second reading agreement in October 2014. The negotiations were successfully concluded on 7 December 2015 with the European Parliament and Council reaching a provisional agreement on a compromise text.

5. On 18 December 2015 the Committee of Permanent Representatives confirmed the compromise text of the Directive, as it had been agreed by the two institutions.

6. On 28 January 2016 the Chair of the European Parliament's IMCO Committee addressed a letter to the Chair of the Committee of Permanent Representatives stating that, should the Council transmit formally to the European Parliament its position as agreed, subject to legal-linguistic verification, she would recommend to the Plenary that the Council's position be accepted without amendments at Parliament's second reading.

7. On 29 February 2016, the Council confirmed its political agreement to the compromise text of the Directive.

---

[1] European Parliament legislative resolution of 13 March 2014 on the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security (NIS) across the Union.

II. OBJECTIVE

8. It derives from the outcome of the negotiations that the Directive lays down measures with a view to achieving a high common level of security of networks and information systems within the European Union so as to improve the functioning of the internal market.

III. ANALYSIS OF THE COUNCIL'S POSITION AT FIRST READING

A. General

9. Following the vote in plenary, the European Parliament and the Council conducted negotiations with the aim of concluding a second-reading agreement on the basis of a Council first-reading position that the Parliament could approve as such. The text of the Council's first-reading position fully reflects the compromise reached between the co-legislators.

B. Key issues

10. The main elements of the compromise reached with the European Parliament are outlined below:

a. *National capabilities*

11. Under the compromise, Member States have certain obligations with regard to their national cybersecurity capabilities. Firstly, Member States are required to adopt a national strategy defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of networks and information systems.

12. Secondly, Member States shall designate one or more national competent authorities on the security of network and information systems to monitor the application of the Directive at national level.

13. Thirdly, Member States are also required to designate a national single point of contact on the security of networks and information systems that will exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the cooperation group and the CSIRTs network. The single point of contact will also submit a yearly report on notifications received to the Cooperation Group.

14. Finally, Member States shall designate one or more Computer Security Incident Response Teams ("CSIRTs ") responsible for handling incidents and risks. The compromise text provides for requirements and tasks of CSIRTs in its Annex I.

b. *Cooperation*

15. In order to support and facilitate strategic cooperation among Member States, to develop trust and confidence and with a view to achieving a high common level of security of networks and information systems in the Union, the compromise text establishes a Cooperation Group. The Group will be composed of representatives from the Member States, the Commission and the European Union Agency for Network and Information Security ('ENISA') and will have specific tasks listed in the text, such as exchanging best practices and information on a number of issues or discussing capabilities and preparedness of Member States.

16. Furthermore, the compromise establishes a network of the national CSIRTs in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation.The network will be composed of representatives of the Member States' CSIRTs and CERT-EU and the Commission will participate in the network as an observer. ENISA will provide the secretariat and actively support the cooperation among the CSIRTs. The text provides for a list of tasks to be carried out by the network, such as exchanging information on CSIRTs services, operations and cooperation capabilities, supporting Member States in addressing cross-border incidents or, under certain conditions, exchanging and discussing information related to incidents and associated risks.

c. *Security and notification requirements*

17. The Directive lays down certain obligations for two sets of market players: operators of essential services and digital service providers.

18. Annex II of the Directive lists a number of sectors important for society and economy, namely energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution and digital infrastructure. Within these sectors Member States will identify the operators of essential services, based on precise criteria provided for in the Directive.

19. Annex III of the Directive lists three types of digital services, the providers of which will have to comply with the requirements of the Directive: online market places, online search engines and cloud computing services. All digital service providers providing the listed services will have to comply with the requirements of the Directive with the exclusion of micro and small enterprises.

20. The two sets of market players will be required to take organisational and technical measures to manage the risks posed to the security of networks and information systems and to prevent and to minimise the impact of incidents affecting the security of those systems. Moreover, incidents having a certain level of impact on the services in question will have to be notified to the national competent authorities or to CSIRTs. The Directive provides for criteria to determine the level of the impact of such incidents.

21. The Directive takes a differentiated approach with regard to the two categories of players. The security and notification requirements are lighter for digital service providers than for operators of essential services, which reflects the degree of risk that disruption to their services may pose to society and economy. Moreover, taking into account that digital service providers are often active in many Member States and in order to ensure a high level of harmonisation, the Directive prevents Member States from imposing any further security and notification requirements on those providers.

22. The compromise text also provides that entities which have not been identified as operators of essential services and are not digital service providers may notify certain incidents on a voluntary basis.

d. *Transposition*

23. Member States will be required to transpose the Directive by 21 months after the date of its entry into force and will have 6 additional months to identify their operators of essential services.

IV. CONCLUSION

24. The Council's position fully reflects the compromise reached in the negotiations between the European Parliament and the Council, with the agreement of the Commission. The compromise is confirmed by the letter that the Chair of the IMCO Committee addressed to the Chairman of the Permanent Representatives Committee on 28 January 2016.