Council of the
European Union

Brussels, 19 June 2019

10140/19

Interinstitutional File:
2017/0225 (COD)

JUR 321
CYBER 201
TELECOM 256
COPEN 271
COPS 182
COSI 128
CSC 167
CSCI 78
IND 192
JAI 672
JAIEX 98
POLMIL 65
RELEX 596
CODEC 1209

LEGISLATIVE ACTS AND OTHER INSTRUMENTS: CORRIGENDUM/RECTIFICATIF

Subject:	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) *(Official Journal of the European Union L 151 of 7 June 2019)*

LANGUAGE concerned: **EL**

PROCEDURE APPLICABLE (according to Council document R/2521/75):

— Procedure 2(b) (obvious errors in one language version)

This text has also been transmitted to the European Parliament.

TIME LIMIT for the observations by Member States: 8 days

OBSERVATIONS to be notified to: dql.rectificatifs@consilium.europa.eu

(DQL RECTIFICATIFS (JUR 7), Directorate Quality of Legislation, Legal Service)

ΠΑΡΑΡΤΗΜΑ

ΔΙΟΡΘΩΤΙΚΟ

του κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια)

(Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης L 151 της 7ης Ιουνίου 2019)

1. Ο όρος «σύστημα» αντικαθίσταται από τον όρο «σχήμα» σε ολόκληρο το κείμενο του κανονισμού στον οικείο γραμματικό τύπο, με εξαίρεση:

α) στις αιτιολογικές σκέψεις 1 (σελίδα 15), 2 (σελίδα 15), 3 (σελίδα 15), 11 (σελίδα 16), 23 (σελίδα 19), 25 (σελίδα 19), 26 (σελίδα 19), 30 (σελίδα 19), 35 (σελίδα 20), 44 (σελίδα 22), 49 (σελίδα 22), 65 (σελίδα 24), 66 (σελίδα 25), 68 (σελίδα 25), 92 (σελίδα 29), 99 (σελίδα 30), 100 (σελίδα 30) και 102 (σελίδα 31),

β) στο άρθρο 2 σημεία 1), 2), 3), 8), 12) και 13) (σελίδες 32 και 33), στο άρθρο 4 παράγραφος 3 (σελίδα 34), στο άρθρο 6 παράγραφος 1 στοιχείο ε) (σελίδα 36) και στο άρθρο 9 στοιχείο γ) (σελίδα 39) και

γ) στην υποσημείωση 9 (σελίδα 17).

2. Στη σελίδα 29, αιτιολογική σκέψη 92

αντί:

«(92) Σε ορισμένους τομείς, μπορεί να χρειαστεί στο μέλλον να επιβληθούν συγκεκριμένες απαιτήσεις κυβερνοασφάλειας και η πιστοποίησή τους να γίνει υποχρεωτική για ορισμένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ ή διαδικασίες ΤΠΕ, προκειμένου να βελτιωθεί το επίπεδο κυβερνοασφάλειας στην Ένωση. Η Επιτροπή θα πρέπει να παρακολουθεί τακτικά τις επιπτώσεις των εγκριθέντων ευρωπαϊκών συστημάτων πιστοποίησης κυβερνοασφάλειας στη διαθεσιμότητα ασφαλών προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ στην εσωτερική αγορά και θα πρέπει να αξιολογεί τακτικά το επίπεδο χρησιμοποίησης των συστημάτων πιστοποίησης από τους κατασκευαστές ή τους παρόχους προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ στην Ένωση. Η αποτελεσματικότητα των ευρωπαϊκών συστημάτων πιστοποίησης κυβερνοασφάλειας και το κατά πόσο συγκεκριμένα καθεστώτα θα πρέπει να καταστούν υποχρεωτικά θα πρέπει να αξιολογείται υπό το πρίσμα της νομοθεσίας της Ένωσης που αφορά την κυβερνοασφάλεια, ιδίως της οδηγίας (ΕΕ) 2016/1148, λαμβάνοντας υπόψη την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούνται από τους φορείς εκμετάλλευσης βασικών υπηρεσιών.»,

διάβαζε:

«(92) Σε ορισμένους τομείς, μπορεί να χρειαστεί στο μέλλον να επιβληθούν συγκεκριμένες απαιτήσεις κυβερνοασφάλειας και η πιστοποίησή τους να γίνει υποχρεωτική για ορισμένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ ή διαδικασίες ΤΠΕ, προκειμένου να βελτιωθεί το επίπεδο κυβερνοασφάλειας στην Ένωση. Η Επιτροπή θα πρέπει να παρακολουθεί τακτικά τις επιπτώσεις των εγκριθέντων ευρωπαϊκών σχημάτων πιστοποίησης κυβερνοασφάλειας στη διαθεσιμότητα ασφαλών προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ στην εσωτερική αγορά και θα πρέπει να αξιολογεί τακτικά το επίπεδο χρησιμοποίησης των σχημάτων πιστοποίησης από τους κατασκευαστές ή τους παρόχους προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ στην Ένωση. Η αποτελεσματικότητα των ευρωπαϊκών σχημάτων πιστοποίησης κυβερνοασφάλειας και το κατά πόσο συγκεκριμένα σχήματα θα πρέπει να καταστούν υποχρεωτικά θα πρέπει να αξιολογείται υπό το πρίσμα της νομοθεσίας της Ένωσης που αφορά την κυβερνοασφάλεια, ιδίως της οδηγίας (ΕΕ) 2016/1148, λαμβάνοντας υπόψη την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούνται από τους φορείς εκμετάλλευσης βασικών υπηρεσιών.».