



Βρυξέλλες, 26 Νοεμβρίου 2021  
(OR. en)

14337/21

---

---

**Διοργανικός φάκελος:  
2020/0359(COD)**

---

---

**CODEC 1541  
CSC 416  
CSCI 147  
CYBER 312  
DATAPROTECT 269  
JAI 1295  
MI 891  
TELECOM 435**

## **ΣΗΜΕΙΩΜΑ**

---

Αποστολέας: Γενική Γραμματεία του Συμβουλίου

Αποδέκτης: Συμβούλιο

---

αριθ. προηγ. εγγρ.: 9583/2/21, 11724/21

Αριθ. εγγρ. Επιτρ.: 14150/20

---

Θέμα: Πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148  
*- Γενική προσέγγιση*

---

## **I. ΕΙΣΑΓΩΓΗ**

1. Στις 16 Δεκεμβρίου 2020, η Επιτροπή ενέκρινε την πρόταση οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση («αναθεωρημένη οδηγία NIS» ή «NIS 2»)<sup>1</sup> με σκοπό την αντικατάσταση της ισχύουσας οδηγίας σχετικά με την ασφάλεια συστημάτων δικτύου και πληροφοριών («οδηγία NIS»)<sup>2</sup>.

---

<sup>1</sup> Πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148

<sup>2</sup> Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση

Η πρόταση ήταν μία από τις δράσεις που προβλέπονταν στη στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία<sup>3</sup> προκειμένου να διασφαλιστεί ότι οι πολίτες και οι επιχειρήσεις επωφελούνται από αξιόπιστες ψηφιακές τεχνολογίες.

2. Η πρόταση βασίζεται στο άρθρο 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) και αποσκοπεί στην περαιτέρω βελτίωση της ανθεκτικότητας και των ικανοτήτων αντιμετώπισης περιστατικών των δημόσιων και ιδιωτικών φορέων, των αρμόδιων αρχών, και της Ένωσης συνολικά.
3. Στο Ευρωπαϊκό Κοινοβούλιο αρμόδια επί της πρότασης είναι η Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας (ITRE). Η επιτροπή ITRE ενέκρινε την έκθεση του εισηγητή στις 28 Οκτωβρίου 2021.
4. Η Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή γνωμοδότησε στις 28 Απριλίου 2021.
5. Στις 3 Φεβρουαρίου 2021, η Επιτροπή των Μόνιμων Αντιπροσώπων αποφάσισε να ζητήσει τη γνωμοδότηση της Ευρωπαϊκής Επιτροπής των Περιφερειών επί της πρότασης<sup>4</sup>. Η Ευρωπαϊκή Επιτροπή των Περιφερειών δεν έχει εισέτι γνωμοδοτήσει.
6. Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων γνωμοδότησε στις 11 Μαρτίου 2021<sup>5</sup>.
7. Στα συμπεράσματά του<sup>6</sup> της 22ας Μαρτίου 2021 ως προς τη στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία, το Συμβούλιο σημείωσε τη νέα πρόταση οδηγίας η οποία βασίζεται στην οδηγία NIS, και επανέλαβε τη στήριξή του για την ενίσχυση και την εναρμόνιση των εθνικών πλαισίων κυβερνοασφάλειας και τη σταθερή συνεργασία μεταξύ των κρατών μελών.
8. Στα συμπεράσματά του της 21ης-22ας Οκτωβρίου 2021, το Ευρωπαϊκό Συμβούλιο ζήτησε να προχωρήσουν οι εργασίες σχετικά με την πρόταση αναθεώρησης της οδηγίας για την ασφάλεια δικτύων και πληροφοριών.

---

<sup>3</sup> 14133/20

<sup>4</sup> 5573/21

<sup>5</sup> Γνωμοδότηση 5/2021 σχετικά με τη στρατηγική κυβερνοασφάλειας και την οδηγία NIS 2.

<sup>6</sup> 6722/21

## **II. ΕΡΓΑΣΙΕΣ ΣΤΑ ΠΡΟΠΑΡΑΣΚΕΥΑΣΤΙΚΑ ΟΡΓΑΝΑ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ**

9. Στο Συμβούλιο, η εξέταση της πρότασης πραγματοποιήθηκε στο πλαίσιο της οριζόντιας ομάδας «Θέματα κυβερνοχώρου» (εφεξής «HWPCI»). Η εξέταση της πρότασης άρχισε κατά τη διάρκεια της πορτογαλικής Προεδρίας στις 19 Ιανουαρίου με ενδεδειγμένη ανάγνωση της πρότασης, επιτρέποντας στα κράτη μέλη να υποβάλουν τα ερωτήματά τους και να υπογραμμίσουν τις κύριες ανησυχίες τους και να λάβουν λεπτομερείς εξηγήσεις από την Επιτροπή σχετικά με τις αλλαγές στην αναθεωρημένη οδηγία.
10. Κατά τη διάρκεια της πορτογαλικής Προεδρίας, η HWPCI αφιέρωσε 17 συνεδριάσεις για την παρουσίαση και την ανάγνωση της πρότασης. Έκθεση προόδου της ανάγνωσης υποβλήθηκε στο Συμβούλιο «Μεταφορές, Τηλεπικοινωνίες και Ενέργεια» της 4ης Ιουνίου 2021.
11. Έκτοτε, οι εργασίες συνεχίστηκαν και εντατικοποιήθηκαν κατά τη διάρκεια της σλοβενικής Προεδρίας με στόχο την επίτευξη γενικής προσέγγισης κατά τη σύνοδο του Συμβουλίου (Μεταφορές, Τηλεπικοινωνίες και Ενέργεια) της 3ης Δεκεμβρίου 2021. Η σλοβενική Προεδρία αφιέρωσε 15 συνεδριάσεις στην αναθεώρηση της πρότασης NIS 2 και πολλές διμερείς συζητήσεις σε όλα τα επίπεδα.
12. Η HWPCI επικέντρωσε τις εργασίες της στην αναδιατύπωση του κειμένου της πρότασης, αρχικά, στην αλληλεπίδραση της οδηγίας NIS 2 με την τομεακή νομοθεσία και το πεδίο εφαρμογής, ιδίως όσον αφορά τη δημόσια διοίκηση, τους εξυπηρετητές πυρήνα DNS και τη ρήτρα αποκλεισμού και στη συνέχεια, μεταξύ άλλων θεμάτων, στις αξιολογήσεις από ομοτίμους, τη δικαιοδοσία και την αμοιβαία συνδρομή, τη συντονισμένη δημοσιοποίηση τρωτών σημείων, τις βάσεις δεδομένων ονομάτων τομέα και δεδομένων καταχώρισης και τη διεθνή συνεργασία, μεταξύ άλλων.
13. Μια πρώτη συμβιβαστική πρόταση για το κείμενο της προτεινόμενης οδηγίας εκδόθηκε στις 21 Σεπτεμβρίου 2021<sup>7</sup>, με βάση τις γραπτές παρατηρήσεις και τα ανεπίσημα έγγραφα που υπέβαλαν τα κράτη μέλη, καθώς και τις προηγούμενες συμβιβαστικές προτάσεις σχετικά με την αλληλεπίδραση της οδηγίας NIS 2 με την τομεακή νομοθεσία και το πεδίο εφαρμογής της οδηγίας NIS 2.

---

<sup>7</sup> 12019/21

14. Η τελευταία αναθεώρηση<sup>8</sup> της συμβιβαστικής πρότασης της Προεδρίας συζητήθηκε σε επίπεδο Ομάδας στις 22 Νοεμβρίου 2021. Ενώ οι αντιπροσωπίες εξέφρασαν εν γένει ικανοποίηση για το συμβιβαστικό κείμενο, ορισμένες εξ αυτών διατύπωσαν ωστόσο επιφυλάξεις εξέτασης ή διατύπωσαν σχόλια για τμήματα της συμβιβαστικής πρότασης. Κάποιες τεχνικές αναδιατυπώσεις είχαν προταθεί σε ορισμένα μέρη του κειμένου.

### **III. ΩΣ ΠΡΟΣ ΤΗΝ ΟΥΣΙΑ**

15. Με βάση τις συζητήσεις σε επίπεδο Ομάδας, τα ακόλουθα σημεία εντοπίστηκαν ως τα κύρια πολιτικά ζητήματα:

α) Πεδίο εφαρμογής (άρθρο 2)

Από την έναρξη των συζητήσεων σχετικά με την πρόταση NIS 2, η κύρια ανησυχία που εξέφρασαν τα κράτη μέλη ήταν η σημαντική αύξηση του αριθμού των οντοτήτων που καλύπτονται από την οδηγία και, ειδικότερα, η εισαγωγή του κανόνα του κατωτάτου ορίου μεγέθους σύμφωνα με τον οποίο όλες οι μεσαίες και μεγάλες οντότητες που δραστηριοποιούνται στους τομείς ή παρέχουν τις υπηρεσίες που καλύπτονται από την οδηγία NIS 2 εμπίπτουν στο πεδίο εφαρμογής της. Ενώ η συμβιβαστική πρόταση διατηρεί αυτόν τον γενικό κανόνα, περιλαμβάνει πρόσθετες διατάξεις για να εξασφαλιστεί η αναγκαία αναλογικότητα, υψηλότερο επίπεδο διαχείρισης κινδύνου και σαφή κριτήρια αξιολόγησης της κρισιμότητας για τον προσδιορισμό των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας. Επιπλέον, η συμβιβαστική πρόταση περιλαμβάνει ειδικές διατάξεις σχετικά με την ιεράρχηση της εφαρμογής μέτρων επιτήρησης σύμφωνα με προσέγγιση βάσει του κινδύνου.

---

<sup>8</sup> 12019/5/21 REV 5

β) Δημόσια διοίκηση (άρθρο 2 παράγραφος 2α)

Η συμπερίληψη της δημόσιας διοίκησης στο πεδίο εφαρμογής της οδηγίας NIS 2 αποτέλεσε αντικείμενο έντονης συζήτησης, δεδομένου ότι ο τομέας της δημόσιας διοίκησης είναι περισσότερο διαφοροποιημένος από άλλους τομείς που καλύπτονται από την οδηγία NIS 2. Η Προεδρία επεδίωξε μια ισορροπημένη προσέγγιση που λαμβάνει υπόψη τις ιδιαιτερότητες των εθνικών πλαισίων δημόσιας διοίκησης και εξασφαλίζει ότι τα κράτη μέλη διατηρούν κάποια ευελιξία όσον αφορά τον καθορισμό των οντοτήτων της δημόσιας διοίκησης που εμπίπτουν στο πεδίο εφαρμογής της NIS 2. Ως εκ τούτου, στο συμβιβαστικό κείμενο, η NIS 2 εφαρμόζεται σε οντότητες της δημόσιας διοίκησης κεντρικών κυβερνήσεων, ενώ τα κράτη μέλη μπορούν επίσης να ορίζουν ότι η οδηγία εφαρμόζεται σε οντότητες της δημόσιας διοίκησης σε περιφερειακό και τοπικό επίπεδο.

γ) Ρήτρα αποκλεισμού (άρθρο 2 σημεία 3α) και 3αα))

Τα κράτη μέλη επιθυμούσαν να αποσαφηνιστεί περαιτέρω η ρήτρα εξαίρεσης, δεδομένου ότι η οδηγία δεν εφαρμόζεται σε οντότητες που ασκούν κυρίως δραστηριότητες στους τομείς της άμυνας, της εθνικής ασφάλειας, της δημόσιας ασφάλειας ή της επιβολής του νόμου ή σε δραστηριότητες που αφορούν την εθνική ασφάλεια ή άμυνα. Εξαιρούνται επίσης η δικαιοσύνη, τα κοινοβούλια και οι κεντρικές τράπεζες.

δ) Η αλληλεπίδραση με την τομεακή νομοθεσία

Τα κράτη μέλη τόνισαν την ανάγκη εναρμόνισης μεταξύ της οδηγίας NIS 2 και της τομεακής νομοθεσίας, ιδίως του κανονισμού για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα («DORA») και της οδηγίας για την ανθεκτικότητα κρίσιμων οντοτήτων (οδηγία «CER»). Η οδηγία NIS 2, η οποία θα πρέπει να αποτελεί τη βάση για την ελάχιστη εναρμόνιση στον τομέα της κυβερνοασφάλειας, περιέχει ειδικό άρθρο για τις τομεακές πράξεις της Ένωσης (άρθρο 2β). Όσον αφορά την αλληλεπίδραση με την οδηγία CER, η συμβιβαστική πρόταση εξασφαλίζει μεγαλύτερη σαφήνεια όσον αφορά την προσέγγιση αντιμετώπισης όλων των κινδύνων. Άλλες σημαντικές προσθήκες σχετίζονται με ρυθμίσεις συνεργασίας μεταξύ των αρμόδιων αρχών στο πλαίσιο των αντίστοιχων νομικών πράξεων.

ε) Μάθηση από ομοτίμους (άρθρο 16)

Με ορισμένες εξαιρέσεις, τα κράτη μέλη αντιτάχθηκαν στην καθιέρωση υποχρεωτικών αξιολογήσεων από ομοτίμους από την Επιτροπή. Ο προτεινόμενος συμβιβασμός διασφαλίζει ότι ο νέος μηχανισμός αλληλοδιδασχής από ομοτίμους βασίζεται στην αμοιβαία εμπιστοσύνη και αποτελεί εθελοντική διαδικασία καθοδηγούμενη από τα κράτη μέλη.

στ) Δικαιοδοσία και εδαφικότητα (άρθρο 24) και αμοιβαία συνδρομή (άρθρο 34)

Τα κράτη μέλη διατύπωσαν ανησυχίες σχετικά με τις συνέπειες της ύπαρξης διαφοροποιημένης δικαιοδοσίας για οντότητες στον τομέα των ΤΠΕ, όπως προτείνεται από την Επιτροπή. Το συμβιβαστικό κείμενο αποσαφήνισε τη δικαιοδοσία με βάση το είδος των οντοτήτων και ενίσχυσε τη διατύπωση για την αμοιβαία συνδρομή.

ζ) Υποχρεώσεις αναφοράς περιστατικών (άρθρο 20)

Λόγω των ανησυχιών που εξέφρασαν τα κράτη μέλη, ότι θα επιβαρύνονταν υπερβολικά οι οντότητες που καλύπτονται από την οδηγία NIS 2 και θα οδηγούσε σε υπερβολική αναφορά συμβάντων, η υποχρεωτική αναφορά σημαντικών απειλών στον κυβερνοχώρο αποκλείστηκε από το συμβιβαστικό κείμενο.

#### **IV. ΣΥΜΠΕΡΑΣΜΑ**

16. Στις 24 Νοεμβρίου 2021, η Επιτροπή των Μόνιμων Αντιπροσώπων κατέληξε σε συμφωνία επί του συμβιβαστικού κειμένου ως έχει στο παράρτημα και αποφάσισε να το υποβάλει στο Συμβούλιο (Μεταφορές, Τηλεπικοινωνίες και Ενέργεια) για την έγκριση γενικής προσέγγισης.
17. Καλείται, συνεπώς, το Συμβούλιο να εγκρίνει το συμβιβαστικό κείμενο που παρουσίασε η Προεδρία ως έχει στο παράρτημα και να υιοθετήσει γενική προσέγγιση κατά τη σύνοδό του στις 3 Δεκεμβρίου 2021.

Πρόταση

**ΟΔΗΓΙΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ**

**σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) 910/2014 και της οδηγίας (ΕΕ) 2018/1972 και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148**

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 114,

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής<sup>9</sup>,

Έχοντας υπόψη τη γνώμη της Επιτροπής των Περιφερειών<sup>10</sup>,

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία,

---

<sup>9</sup> ΕΕ C της , σ. .

<sup>10</sup> ΕΕ C της , σ. .

Εκτιμώντας τα ακόλουθα:

- (1) Η οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>11</sup> αποσκοπούσε στην ανάπτυξη ικανοτήτων κυβερνοασφάλειας σε ολόκληρη την Ένωση, στον μετριασμό των απειλών για τα δικτυακά και πληροφοριακά συστήματα που χρησιμοποιούνται για την παροχή βασικών υπηρεσιών σε σημαντικούς τομείς και στη διασφάλιση της συνέχειας των υπηρεσιών αυτών κατά την αντιμετώπιση περιστατικών κυβερνοασφάλειας, ώστε να συμβάλει στην αποτελεσματική λειτουργία της οικονομίας και της κοινωνίας της Ένωσης.
- (2) Αφότου άρχισε να ισχύει η οδηγία (ΕΕ) 2016/1148, έχει σημειωθεί σημαντική πρόοδος όσον αφορά την αύξηση του επιπέδου ανθεκτικότητας της κυβερνοασφάλειας της Ένωσης. Η επανεξέταση της εν λόγω οδηγίας κατέδειξε ότι αυτή λειτούργησε ως καταλύτης για τη θεσμική και κανονιστική προσέγγιση της κυβερνοασφάλειας στην Ένωση καθώς προετοίμασε το έδαφος για μια σημαντική αλλαγή νοοτροπίας. Με την οδηγία διασφαλίστηκε η ολοκλήρωση των εθνικών πλαισίων με τον καθορισμό εθνικών [...] στρατηγικών **σχετικά με την ασφάλεια συστημάτων δικτύου και πληροφοριών**, τη θέσπιση εθνικών ικανοτήτων και την εφαρμογή ρυθμιστικών μέτρων τα οποία καλύπτουν βασικές υποδομές και φορείς που προσδιορίζονται από κάθε κράτος μέλος. Συνέβαλε επίσης στη συνεργασία σε επίπεδο Ένωσης μέσω της σύστασης της ομάδας συνεργασίας<sup>12</sup> και του [...] δικτύου εθνικών ομάδων απόκρισης για περιστατικά που αφορούν την ασφάλεια υπολογιστών («δίκτυο CSIRT»)<sup>13</sup>. Παρά τα επιτεύγματα αυτά, η επανεξέταση της οδηγίας (ΕΕ) 2016/1148 αποκάλυψε εγγενείς αδυναμίες που την εμποδίζουν να αντιμετωπίσει αποτελεσματικά τις ταυτόχρονες και αναδυόμενες προκλήσεις στον τομέα της κυβερνοασφάλειας.

---

<sup>11</sup> Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ΕΕ L 194/1 της 19.7.2016, σ. 1).

<sup>12</sup> Άρθρο 11 της οδηγίας (ΕΕ) 2016/1148.

<sup>13</sup> Άρθρο 12 της οδηγίας (ΕΕ) 2016/1148.



- (3) Τα δικτυακά και πληροφοριακά συστήματα έχουν εξελιχθεί σε κεντρικό στοιχείο της καθημερινής ζωής με τον ταχύ ψηφιακό μετασχηματισμό και τη διασύνδεση της κοινωνίας, μεταξύ άλλων στις διασυνοριακές ανταλλαγές. Η εξέλιξη αυτή έχει οδηγήσει σε επέκταση του τοπίου των απειλών για την κυβερνοασφάλεια, γεγονός που δημιουργεί νέες προκλήσεις οι οποίες απαιτούν προσαρμοσμένες, συντονισμένες και καινοτόμες αποκρίσεις σε όλα τα κράτη μέλη. Ο αριθμός, το μέγεθος, η επινοητικότητα, η συχνότητα και ο αντίκτυπος των περιστατικών κυβερνοασφάλειας αυξάνονται και συνιστούν μείζονα απειλή για τη λειτουργία των δικτυακών και πληροφοριακών συστημάτων. Ως εκ τούτου, τα κυβερνοπεριστατικά μπορούν να παρεμποδίσουν την άσκηση οικονομικών δραστηριοτήτων στην εσωτερική αγορά, να προκαλέσουν οικονομικές απώλειες, να υπονομεύσουν την εμπιστοσύνη των χρηστών και των χρηστριών και να προκαλέσουν σοβαρή ζημία στην οικονομία και την κοινωνία της Ένωσης. Ως εκ τούτου, η ετοιμότητα και η αποτελεσματικότητα στον τομέα της κυβερνοασφάλειας είναι πλέον πιο σημαντικές από ποτέ για την ορθή λειτουργία της εσωτερικής αγοράς.
- (4) Η νομική βάση της οδηγίας 1148/2016/ΕΕ ήταν το άρθρο 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), στόχος του οποίου είναι η εγκαθίδρυση και η λειτουργία της εσωτερικής αγοράς με την ενίσχυση των μέτρων για την προσέγγιση των εθνικών κανόνων. Οι απαιτήσεις κυβερνοασφάλειας που επιβάλλονται στις οντότητες που παρέχουν υπηρεσίες ή οικονομικά συναφείς δραστηριότητες ποικίλλουν σημαντικά μεταξύ των κρατών μελών ως προς το είδος της απαίτησης, τον βαθμό λεπτομερειακότητάς τους και τη μέθοδο εποπτείας. Οι διαφορές αυτές αυξάνουν το κόστος και προκαλούν δυσκολίες στις επιχειρήσεις που προσφέρουν αγαθά ή υπηρεσίες διασυνοριακά. Απαιτήσεις που επιβάλλονται από ένα κράτος μέλος και οι οποίες διαφέρουν, ή ακόμη και έρχονται σε αντίθεση με αυτές που επιβάλλει άλλο κράτος μέλος, ενδέχεται να επηρεάσουν σημαντικά τις εν λόγω διασυνοριακές δραστηριότητες.

Επιπλέον, η πιθανότητα μη βέλτιστου σχεδιασμού ή εφαρμογής [...] **μέτρων** κυβερνοασφάλειας σε ένα κράτος μέλος είναι πιθανό να επηρεάσει το επίπεδο κυβερνοασφάλειας άλλων κρατών μελών, ιδίως λόγω των έντονων διασυνοριακών ανταλλαγών. Η επανεξέταση της οδηγίας (ΕΕ) 2016/1148 κατέδειξε μεγάλη απόκλιση στην εφαρμογή της από τα κράτη μέλη, μεταξύ άλλων όσον αφορά το πεδίο εφαρμογής της, η οριοθέτηση του οποίου επαφίεται σε μεγάλο βαθμό στη διακριτική ευχέρεια των κρατών μελών. Η οδηγία (ΕΕ) 2016/1148 παρείχε επίσης ευρύτατη διακριτική ευχέρεια στα κράτη μέλη όσον αφορά την εφαρμογή των υποχρεώσεων σχετικά με την ασφάλεια και την αναφορά των περιστατικών που ορίζονται στην εν λόγω οδηγία. Ως εκ τούτου, οι υποχρεώσεις αυτές εκπληρώθηκαν με πολύ διαφορετικούς τρόπους σε εθνικό επίπεδο. Παρόμοια απόκλιση ως προς την εφαρμογή σημειώθηκε σε σχέση με τις διατάξεις της εν λόγω οδηγίας που αφορούν την εποπτεία και την επιβολή.

- (5) Όλες αυτές οι αποκλίσεις έχουν ως αποτέλεσμα τον κατακερματισμό της εσωτερικής αγοράς και ενδέχεται να έχουν αρνητικές επιπτώσεις στη λειτουργία της, επηρεάζοντας ιδίως τη διασυνοριακή παροχή υπηρεσιών και το επίπεδο ανθεκτικότητας της κυβερνοασφάλειας λόγω της εφαρμογής διαφορετικών [...] **μέτρων**. Η παρούσα οδηγία αποσκοπεί στην εξάλειψη αυτών των μεγάλων αποκλίσεων μεταξύ των κρατών μελών, ιδίως με τον καθορισμό ελάχιστων κανόνων σχετικά με τη λειτουργία ενός συντονισμένου κανονιστικού πλαισίου, με τη θέσπιση μηχανισμών για την αποτελεσματική συνεργασία μεταξύ των αρμόδιων αρχών σε κάθε κράτος μέλος, με την επικαιροποίηση του καταλόγου των τομέων και δραστηριοτήτων που υπόκεινται σε υποχρεώσεις κυβερνοασφάλειας και με τη θέσπιση αποτελεσματικών ένδικων μέσων και κυρώσεων που είναι καθοριστικής σημασίας για την αποτελεσματική επιβολή των εν λόγω υποχρεώσεων. Ως εκ τούτου, η οδηγία (ΕΕ) 2016/1148 θα πρέπει να καταργηθεί και να αντικατασταθεί από την παρούσα οδηγία.

- (6) [...] Τα κράτη μέλη **θα πρέπει να είναι σε θέση** να λαμβάνουν τα αναγκαία μέτρα για την προστασία των ουσιωδών συμφερόντων της ασφάλειας τους, τη διαφύλαξη της δημόσιας τάξης και ασφάλειας, καθώς και τη διερεύνηση, ανίχνευση και δίωξη ποινικών αδικημάτων, [...] [...]. **Η οδηγία δεν θα πρέπει να εφαρμόζεται σε ορισμένες δημόσιες ή ιδιωτικές οντότητες που ασκούν δραστηριότητες στους τομείς αυτούς. Επίσης, δεν θα πρέπει να εφαρμόζεται στις δραστηριότητες των οντοτήτων που διεξάγονται σε αυτούς τους τομείς. Επιπλέον,** κανένα κράτος μέλος δεν υποχρεούται να παρέχει πληροφορίες, η γνωστοποίηση των οποίων θα ήταν αντίθετη προς ουσιώδη συμφέροντα της δημόσιας ασφάλειάς του. [...] **Ισχύουν εθνικοί [...] ή ενωσιακοί κανόνες για την προστασία διαβαθμισμένων πληροφοριών, οι συμφωνίες εμπιστευτικότητας και οι ανεπίσημες συμφωνίες εμπιστευτικότητας, όπως το πρωτόκολλο για την ανταλλαγή πληροφοριών «Traffic Light Protocol»<sup>14</sup>.**
- (6α) **Το δίκαιο της Ένωσης για την προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής εφαρμόζεται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα δυνάμει της παρούσας οδηγίας. Ειδικότερα, η παρούσα οδηγία δεν θίγει τον κανονισμό (ΕΕ) 2016/679 και την οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και, ως εκ τούτου, δεν θα πρέπει ιδίως να θίγει τα καθήκοντα και τις εξουσίες των ανεξάρτητων εποπτικών αρχών που είναι αρμόδιες για την παρακολούθηση της συμμόρφωσης με την αντίστοιχη ενωσιακή νομοθεσία για την προστασία των δεδομένων.**

---

<sup>14</sup> Το πρωτόκολλο για την ανταλλαγή πληροφοριών «Traffic Light» (TLP) είναι μέσο που επιτρέπει σε όσους και όσες ανταλλάσσουν πληροφορίες να ενημερώνουν το ακροατήριό τους σχετικά με τυχόν περιορισμούς στην περαιτέρω διάδοση των πληροφοριών αυτών. Χρησιμοποιείται σε όλες σχεδόν τις κοινότητες των ομάδων CSIRT και σε ορισμένα κέντρα κοινοχρησίας και ανάλυσης πληροφοριών (ISAC).

- (7) Με την κατάργηση της οδηγίας (ΕΕ) 2016/1148, το πεδίο εφαρμογής ανά τομείς θα πρέπει να επεκταθεί σε μεγαλύτερο μέρος της οικονομίας υπό το πρίσμα των εκτιμήσεων που εκτίθενται στις αιτιολογικές σκέψεις (4) έως (6). Ως εκ τούτου, οι τομείς που καλύπτονται από την οδηγία (ΕΕ) 2016/1148 θα πρέπει να επεκταθούν ώστε να παρέχουν ολοκληρωμένη κάλυψη των τομέων και υπηρεσιών ζωτικής σημασίας για βασικές κοινωνιακές και οικονομικές δραστηριότητες εντός της εσωτερικής αγοράς. Οι κανόνες δεν θα πρέπει να διαφέρουν ανάλογα με το αν οι οντότητες είναι φορείς εκμετάλλευσης βασικών υπηρεσιών ή πάροχοι ψηφιακών υπηρεσιών. Η διαφοροποίηση αυτή έχει αποδειχθεί παρωχημένη, δεδομένου ότι δεν αποτυπώνει την πραγματική σημασία των τομέων ή των υπηρεσιών για τις κοινωνιακές και οικονομικές δραστηριότητες στην εσωτερική αγορά.
- (8) Σύμφωνα με την οδηγία (ΕΕ) 2016/1148, τα κράτη μέλη έφεραν την ευθύνη του προσδιορισμού των οντοτήτων που πληρούν τα κριτήρια του ορισμού του φορέα εκμετάλλευσης βασικών υπηρεσιών («διαδικασία προσδιορισμού»). Προκειμένου να εξαιρεθούν οι μεγάλες αποκλίσεις μεταξύ των κρατών μελών ως προς το θέμα αυτό και να εξασφαλιστεί ασφάλεια δικαίου για όλες τις σχετικές οντότητες όσον αφορά τις απαιτήσεις διαχείρισης κινδύνου και τις υποχρεώσεις αναφοράς περιστατικών, θα πρέπει να θεσπιστεί ενιαίο κριτήριο για τον προσδιορισμό των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας. Το κριτήριο αυτό θα πρέπει να συνίσταται στην εφαρμογή του κανόνα του κατωτάτου ορίου μεγέθους, σύμφωνα με τον οποίο όλες οι μεσαίες και μεγάλες επιχειρήσεις, όπως ορίζονται στη σύσταση 2003/361/ΕΚ<sup>15</sup> της Επιτροπής, οι οποίες δραστηριοποιούνται εντός των τομέων ή παρέχουν το είδος των υπηρεσιών που καλύπτονται από την παρούσα οδηγία, εμπίπτουν στο πεδίο εφαρμογής της. [...]

---

<sup>15</sup> Σύσταση 2003/361/ΕΚ της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων (ΕΕ L 124 της 20.5.2003, σ. 36).

- (8α) Προκειμένου να εξασφαλιστεί σαφής επισκόπηση των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, τα κράτη μέλη θα πρέπει να είναι σε θέση να θεσπίζουν εθνικούς μηχανισμούς αυτοκοινοποίησης που απαιτούν από τις οντότητες που υπόκεινται στην παρούσα οδηγία να υποβάλλουν τουλάχιστον την επωνυμία, τη διεύθυνση και τα στοιχεία επικοινωνίας τους, καθώς και τον τομέα στον οποίο δραστηριοποιούνται ή το είδος της υπηρεσίας που παρέχουν και, κατά περίπτωση, κατάλογο των κρατών μελών στα οποία η οντότητα παρέχει τις υπηρεσίες τους στις αρμόδιες αρχές δυνάμει της παρούσας οδηγίας ή σε οργανισμούς που έχουν οριστεί για τον σκοπό αυτό από τα κράτη μέλη. Τα κράτη μέλη μπορούν να αποφασίζουν σχετικά με τους κατάλληλους μηχανισμούς όπου υπάρχουν μητρώα σε εθνικό επίπεδο, που επιτρέπουν τον προσδιορισμό των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας.
- (9) Ωστόσο, θα πρέπει επίσης να καλύπτονται από την παρούσα οδηγία οι [...] πολύ μικρές ή [...] μικρές οντότητες που πληρούν ορισμένα κριτήρια τα οποία υποδηλώνουν ότι αυτές διαδραματίζουν βασικό ρόλο στις οικονομίες ή τις κοινωνίες των κρατών μελών ή σε συγκεκριμένους τομείς ή είδη υπηρεσιών. Τα κράτη μέλη θα πρέπει να είναι υπεύθυνα τουλάχιστον για την [...] υποβολή [...] στην Επιτροπή πληροφοριών σχετικών με τον αριθμό των ταυτοποιημένων οντοτήτων, τον τομέα στον οποίο ανήκουν ή το είδος της υπηρεσίας που παρέχουν, καθώς και τα ειδικά κριτήρια βάσει των οποίων προσδιορίστηκαν. Τα κράτη μέλη μπορούν επίσης να αποφασίσουν, σύμφωνα με τους εθνικούς κανόνες ασφαλείας, να υποβάλουν στην Επιτροπή τα ονόματα αυτών των οντοτήτων.
- (9α) Οι οντότητες της δημόσιας διοίκησης που ασκούν δραστηριότητες στους τομείς της εθνικής ασφάλειας, της άμυνας, της δημόσιας ασφάλειας, της επιβολής του νόμου, καθώς και η δικαιοσύνη, τα κοινοβούλια και οι κεντρικές τράπεζες εξαιρούνται από το πεδίο εφαρμογής της παρούσας οδηγίας. Για τους σκοπούς της παρούσας οδηγίας, οι φορείς με κανονιστική αρμοδιότητα δεν θεωρείται ότι ασκούν δραστηριότητες στον τομέα της επιβολής του νόμου και, ως εκ τούτου, δεν εξαιρούνται για τους λόγους αυτούς από το πεδίο εφαρμογής της παρούσας οδηγίας. Επιπλέον, οι φορείς δημόσιας διοίκησης της κεντρικής κυβέρνησης, οι οποίοι ιδρύονται από κοινού με τρίτη χώρα σύμφωνα με διεθνή συμφωνία, δεν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας.

- (9αα) Τα κράτη μέλη θα πρέπει να είναι σε θέση να διαπιστώσουν ότι οι οντότητες που προσδιορίστηκαν πριν από την έναρξη ισχύος της παρούσας οδηγίας ως φορείς εκμετάλλευσης βασικών υπηρεσιών σύμφωνα με την οδηγία (ΕΕ) 2016/1148 πρέπει να θεωρούνται βασικές οντότητες.
- (9ααα) Η παρούσα οδηγία δεν εφαρμόζεται στις διπλωματικές και προξενικές αποστολές των κρατών μελών στο εξωτερικό και στις υποδομές ΤΠΕ που χρησιμοποιούν οι εν λόγω αποστολές, εφόσον οι υποδομές αυτές βρίσκονται στο εξωτερικό ή λειτουργούν για χρήστες στο εξωτερικό.
- (10) Η Επιτροπή, σε διαβούλευση με την ομάδα συνεργασίας, μπορεί να εκδίδει κατευθυντήριες γραμμές σχετικά με την εφαρμογή των κριτηρίων που ισχύουν για τις πολύ μικρές και τις μικρές επιχειρήσεις.
- (11) [...] Οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας θα πρέπει να ταξινομηθούν σε δύο κατηγορίες: ουσιώδεις και σημαντικές που λαμβάνουν υπόψη το επίπεδο κρισιμότητας του τομέα ή του είδους των υπηρεσιών που παρέχουν, καθώς και το μέγεθός τους. Στο πλαίσιο αυτό, θα πρέπει επίσης να λαμβάνονται δεόντως υπόψη τυχόν σχετικές τομεακές εκτιμήσεις κινδύνου ή καθοδήγηση από τις αρμόδιες αρχές, κατά περίπτωση. Τόσο οι βασικές όσο και οι σημαντικές οντότητες θα πρέπει να υπόκεινται στις [...] απαιτήσεις διαχείρισης κινδύνου και στις ίδιες υποχρεώσεις αναφοράς περιστατικών. Τα καθεστώτα εποπτείας και επιβολής κυρώσεων μεταξύ αυτών των δύο κατηγοριών οντοτήτων θα πρέπει να διαφοροποιούνται ώστε να εξασφαλίζεται δίκαιη ισορροπία μεταξύ των απαιτήσεων και των υποχρεώσεων **με βάση τον κίνδυνο**, αφενός, και του διοικητικού φόρτου που προκύπτει από την εποπτεία της συμμόρφωσης, αφετέρου.

- (12) **Η παρούσα οδηγία καθορίζει τη βάση αναφοράς για τα μέτρα διαχείρισης της κυβερνοασφάλειας και τις υποχρεώσεις αναφοράς περιστατικών σε όλους τους τομείς που εμπíπτουν στο πεδίο εφαρμογής της. Προκειμένου να αποφευχθεί ο κατακερματισμός των διατάξεων περί κυβερνοασφάλειας των ενωσιακών νομικών πράξεων, όταν πρόσθετες ειδικές τομεακές διατάξεις σχετικά με τα μέτρα διαχείρισης κινδύνων και τις υποχρεώσεις αναφοράς περιστατικών στον τομέα της κυβερνοασφάλειας θεωρούνται αναγκαίες για τη διασφάλιση υψηλού επιπέδου ασφάλειας στον κυβερνοχώρο, η Επιτροπή θα πρέπει να αξιολογήσει κατά πόσον οι εν λόγω διατάξεις θα μπορούσαν να οριστούν σε εκτελεστική πράξη στο πλαίσιο της εξουσιοδότησης που προβλέπεται στην παρούσα οδηγία. Σε περίπτωση που οι εν λόγω πράξεις δεν είναι κατάλληλες για τον σκοπό αυτό, η τομεακή νομοθεσία θα μπορούσε να συμβάλει στη διασφάλιση υψηλού επιπέδου [...] κυβερνοασφάλειας, λαμβάνοντας πλήρως υπόψη τις ιδιαιτερότητες και την πολυπλοκότητα [...] των σχετικών τομέων. Ο λόγος για τον οποίο μια εκτελεστική πράξη στο πλαίσιο της εξουσιοδότησης που προβλέπεται στην παρούσα οδηγία δεν ήταν κατάλληλη πρέπει να εξηγηθεί στην τομεακή νομοθεσία. Ταυτόχρονα, οι εν λόγω τομεακές διατάξεις των νομικών πράξεων της Ένωσης θα πρέπει να λαμβάνουν δεόντως υπόψη την ανάγκη για ένα ολοκληρωμένο και εναρμονισμένο πλαίσιο κυβερνοασφάλειας. [...] Αυτό [...] δεν θίγει τις υφιστάμενες εκτελεστικές αρμοδιότητες που έχουν ανατεθεί [...] στην Επιτροπή σε διάφορους τομείς, συμπεριλαμβανομένων των μεταφορών και της ενέργειας.**

**(12α)** Όταν μια τομεακή νομική πράξη της Ένωσης περιέχει διατάξεις [...] που απαιτούν από βασικές ή σημαντικές οντότητες να θεσπίσουν μέτρα με τουλάχιστον ισοδύναμο αποτέλεσμα προς τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία σχετικά με τα μέτρα διαχείρισης κινδύνου στον κυβερνοχώρο [...] και τις υποχρεώσεις κοινοποίησης σημαντικών περιστατικών ή σημαντικών κυβερνοαπειλών [...], θα πρέπει να εφαρμόζονται οι εν λόγω ειδικές τομεακές διατάξεις, μεταξύ άλλων σχετικά με την εποπτεία και την επιβολή. Κατά τον καθορισμό του ισοδύναμου αποτελέσματος των υποχρεώσεων που προβλέπονται στις τομεακές διατάξεις μιας νομικής πράξης της Ένωσης, θα πρέπει να λαμβάνονται υπόψη οι ακόλουθες πτυχές: i) τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει να συνίστανται σε κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων που απειλούν την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν οι σχετικές οντότητες κατά την παροχή των υπηρεσιών τους, και θα πρέπει να περιλαμβάνουν τουλάχιστον όλα τα στοιχεία που ορίζονται στην παρούσα οδηγία· ii) η υποχρέωση κοινοποίησης σημαντικών περιστατικών και κυβερνοαπειλών θα πρέπει να είναι τουλάχιστον ισοδύναμη προς τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία όσον αφορά το περιεχόμενο, τη μορφή και τα χρονοδιαγράμματα των κοινοποιήσεων· iii) οι λεπτομέρειες αναφοράς περιστατικών από τις οντότητες και τις αρμόδιες αρχές των τομεακών νομικών πράξεων της Ένωσης θα πρέπει να είναι τουλάχιστον ισοδύναμες προς τις απαιτήσεις που ορίζονται στην παρούσα οδηγία όσον αφορά το περιεχόμενο, τη μορφή και τα χρονοδιαγράμματά τους και θα πρέπει να λαμβάνουν υπόψη τον ρόλο του δικτύου CSIRT· iv) οι απαιτήσεις διασυννοριακής συνεργασίας για τις αρμόδιες αρχές θα πρέπει να είναι τουλάχιστον ισοδύναμες με εκείνες που ορίζονται στην παρούσα οδηγία. Εάν οι τομεακές διατάξεις νομικής πράξης της Ένωσης δεν καλύπτουν όλες τις οντότητες συγκεκριμένου τομέα που εμπίπτει στο πεδίο εφαρμογής της παρούσας οδηγίας, οι σχετικές διατάξεις της παρούσας οδηγίας θα πρέπει να εξακολουθούν να εφαρμόζονται στις οντότητες που δεν καλύπτονται από τις τομεακές αυτές διατάξεις.



- (12αα) Η Επιτροπή θα πρέπει να επανεξετάζει περιοδικά την εφαρμογή των απαιτήσεων ισοδύναμου αποτελέσματος σε σχέση με τομεακές διατάξεις νομικών πράξεων της Ένωσης [...]. Η Επιτροπή πρέπει να συμβουλευτεί την ομάδα συνεργασίας κατά την προετοιμασία της περιοδικής επανεξέτασης.
- (12ααα) Οι μελλοντικές τομεακές νομικές πράξεις της Ένωσης θα πρέπει να λαμβάνουν δεόντως υπόψη τους ορισμούς που περιγράφονται στο άρθρο 4 της παρούσας οδηγίας και το πλαίσιο εποπτείας και επιβολής που προβλέπεται στο κεφάλαιο VI της παρούσας οδηγίας.
- (12αβ) Όταν τομεακές διατάξεις των νομικών πράξεων της Ένωσης απαιτούν από τις βασικές ή σημαντικές οντότητες να θεσπίσουν μέτρα με τουλάχιστον ισοδύναμο αποτέλεσμα με τις υποχρεώσεις αναφοράς περιστατικών που ορίζονται στην παρούσα οδηγία, θα πρέπει να αποφεύγονται οι αλληλεπικαλυπτόμενες υποχρεώσεις αναφοράς περιστατικών και θα πρέπει να διασφαλίζεται η συνοχή και η αποτελεσματικότητα του χειρισμού των κοινοποιήσεων κυβερνοαπειλών ή περιστατικών στον κυβερνοχώρο. Για τον σκοπό αυτό, οι εν λόγω τομεακές διατάξεις μπορούν να επιτρέψουν στα κράτη μέλη να θεσπίσουν κοινό, αυτόματο και άμεσο μηχανισμό αναφοράς για την κοινοποίηση σημαντικών περιστατικών στον κυβερνοχώρο και κυβερνοαπειλών τόσο στις αρχές των οποίων τα καθήκοντα ορίζονται στις αντίστοιχες ειδικές τομεακές διατάξεις όσο και στις αρμόδιες αρχές, συμπεριλαμβανομένου του ενιαίου σημείου επαφής και των CSIRT, κατά περίπτωση, που είναι αρμόδιες για τα καθήκοντα κυβερνοασφάλειας που προβλέπονται στην παρούσα οδηγία, ή για μηχανισμό που διασφαλίζει τη συστηματική και άμεση ανταλλαγή πληροφοριών και τη συνεργασία μεταξύ των αρμόδιων αρχών και των CSIRT όσον αφορά τον χειρισμό των εν λόγω κοινοποιήσεων. Για τους σκοπούς της απλούστευσης της αναφοράς περιστατικών και της εφαρμογής του κοινού, αυτόματου και άμεσου μηχανισμού αναφοράς, τα κράτη μέλη μπορούν, σύμφωνα με ειδικές τομεακές νομοθεσίες, να χρησιμοποιούν το ενιαίο σημείο εισόδου που καθορίζουν σύμφωνα με το άρθρο 11 παράγραφος 5α της παρούσας οδηγίας. Για να διασφαλιστεί η εναρμόνιση, οι υποχρεώσεις αναφοράς περιστατικών των τομεακών νομικών πράξεων της Ένωσης θα πρέπει να ευθυγραμμιστούν με εκείνες που ορίζονται στην παρούσα οδηγία. Τα κράτη μέλη μπορούν να ορίζουν ότι οι αρμόδιες αρχές δυνάμει της παρούσας οδηγίας ή οι εθνικές CSIRT είναι οι αποδέκτες της αναφοράς, σύμφωνα με τις τομεακές νομοθεσίες.

- (13) Ο κανονισμός XXXX/XXXX του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου θα πρέπει να θεωρείται τομεακή νομική πράξη της Ένωσης σε σχέση με την παρούσα οδηγία όσον αφορά τις οντότητες του χρηματοπιστωτικού τομέα. Αντί των διατάξεων που θεσπίζονται [...] στην παρούσα οδηγία, θα πρέπει να εφαρμόζονται οι διατάξεις του κανονισμού XXXX/XXXX σχετικά με τα μέτρα διαχείρισης κινδύνων της τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ), τη διαχείριση περιστατικών που σχετίζονται με τις ΤΠΕ και ιδίως την αναφορά περιστατικών, καθώς και σχετικά με τις δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας, τις ρυθμίσεις ανταλλαγής πληροφοριών και τον κίνδυνο τρίτων παρόχων ΤΠΕ. Ως εκ τούτου, τα κράτη μέλη δεν θα πρέπει να εφαρμόζουν τις διατάξεις της παρούσας οδηγίας σχετικά με τις υποχρεώσεις διαχείρισης κινδύνου και αναφοράς περιστατικών στον τομέα της κυβερνοασφάλειας, [...] την εποπτεία, καθώς και την επιβολή [...] στις χρηματοπιστωτικές οντότητες που καλύπτονται από τον κανονισμό XXXX/XXXX. Ταυτόχρονα, είναι σημαντικό να διατηρηθεί στενή σχέση και ανταλλαγή πληροφοριών με τον χρηματοπιστωτικό τομέα στο πλαίσιο της παρούσας οδηγίας. Προς τον σκοπό αυτό, ο κανονισμός XXXX/XXXX επιτρέπει [...] στις Ευρωπαϊκές Εποπτικές Αρχές (ΕΕΑ) για τον χρηματοπιστωτικό τομέα και στις εθνικές αρμόδιες αρχές δυνάμει του κανονισμού XXXX/XXXX να συμμετέχουν στις συζητήσεις [...] **στις [...] εργασίες [...]** της ομάδας συνεργασίας, καθώς και να ανταλλάσσουν πληροφορίες και να συνεργάζονται τόσο με τα ενιαία σημεία επαφής που ορίζονται δυνάμει της παρούσας οδηγίας, [...] **καθώς και με τις εθνικές CSIRT.** Οι αρμόδιες αρχές δυνάμει του κανονισμού XXXX/XXXX θα πρέπει να διαβιβάζουν λεπτομερή στοιχεία για σημαντικά περιστατικά που σχετίζονται με τις ΤΠΕ **και σημαντικές κυβερνοαπειλές** και στα ενιαία σημεία επαφής, **τις αρμόδιες αρχές ή τις εθνικές CSIRT** που ορίζονται δυνάμει της παρούσας οδηγίας. **Αυτό μπορεί να επιτευχθεί με την αυτόματη και άμεση διαβίβαση κοινοποιήσεων περιστατικών ή με κοινή πλατφόρμα αναφοράς.** Επιπλέον, τα κράτη μέλη θα πρέπει να συνεχίσουν να περιλαμβάνουν τον χρηματοπιστωτικό τομέα στις στρατηγικές τους για την κυβερνοασφάλεια, και οι εθνικές CSIRT [...] **μπορούν να περιλαμβάνουν τον χρηματοπιστωτικό τομέα στις δραστηριότητές τους.**

(13α) Προκειμένου να αποφευχθούν κενά και αλληλεπικαλύψεις των υποχρεώσεων κυβερνοασφάλειας που επιβάλλονται στις οντότητες του κλάδου των αεροπορικών μεταφορών που αναφέρονται στο σημείο 2 στοιχείο α) του παραρτήματος I, οι εθνικές αρχές που έχουν οριστεί βάσει των κανονισμών (ΕΚ) αριθ. 300/2008<sup>16</sup> και (ΕΕ) 2018/1139<sup>17</sup> του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και οι αρμόδιες αρχές δυνάμει της παρούσας οδηγίας θα πρέπει να συνεργάζονται όσον αφορά την εφαρμογή των μέτρων διαχείρισης κινδύνων στον κυβερνοχώρο και την εποπτεία των εν λόγω μέτρων σε εθνικό επίπεδο. Η συμμόρφωση μιας οντότητας με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας δυνάμει της παρούσας οδηγίας [...] μπορεί να θεωρηθεί από τις εθνικές αρχές που ορίζονται βάσει των κανονισμών (ΕΚ) αριθ. 300/2008 και (ΕΕ) 2018/1139 ότι συμμορφώνεται με τις απαιτήσεις που ορίζονται στους εν λόγω κανονισμούς, καθώς και στις σχετικές κατ' εξουσιοδότηση και εκτελεστικές πράξεις που εκδίδονται δυνάμει των εν λόγω κανονισμών.

---

<sup>16</sup> Κανονισμός (ΕΚ) αριθ. 300/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 2008, για τη θέσπιση κοινών κανόνων στο πεδίο της ασφάλειας της πολιτικής αεροπορίας και την κατάργηση του κανονισμού (ΕΚ) αριθ. 2320/2002 (ΕΕ L 97 της 9.4.2008, σ. 72).

<sup>17</sup> Κανονισμός (ΕΕ) 2018/1139 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4ης Ιουλίου 2018, για τη θέσπιση κοινών κανόνων στον τομέα της πολιτικής αεροπορίας και την ίδρυση Οργανισμού της Ευρωπαϊκής Ένωσης για την Αεροπορική Ασφάλεια, και για την τροποποίηση των κανονισμών (ΕΚ) αριθ. 2111/2005, (ΕΚ) αριθ. 1008/2008, (ΕΕ) αριθ. 996/2010, (ΕΕ) αριθ. 376/2014 και των οδηγιών 2014/30/ΕΕ και 2014/53/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, καθώς και για την κατάργηση των κανονισμών (ΕΚ) αριθ. 552/2004 και (ΕΚ) αριθ. 216/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και του κανονισμού (ΕΟΚ) αριθ. 3922/91 του Συμβουλίου (ΕΕ L 212 της 22.8.2018, σ. 1).

- (14) Λαμβανομένων υπόψη των διασυνδέσεων μεταξύ της κυβερνοασφάλειας και της φυσικής ασφάλειας των οντοτήτων, θα πρέπει να εξασφαλιστεί μια συνεκτική προσέγγιση μεταξύ της οδηγίας (ΕΕ) XXX/XXX του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της παρούσας οδηγίας. Για να επιτευχθεί αυτό, τα κράτη μέλη θα πρέπει να διασφαλίσουν ότι οι κρίσιμες οντότητες [και οι ισοδύναμες οντότητες], σύμφωνα με την οδηγία (ΕΕ) XXX/XXX, θεωρούνται [...] ως βασικές οντότητες δυνάμει της παρούσας οδηγίας. Τα κράτη μέλη θα πρέπει επίσης να διασφαλίζουν ότι οι στρατηγικές τους για την κυβερνοασφάλεια παρέχουν ένα πλαίσιο πολιτικής για ενισχυμένο συντονισμό μεταξύ της αρμόδιας αρχής δυνάμει της παρούσας οδηγίας και της αρμόδιας αρχής δυνάμει της οδηγίας (ΕΕ) XXX/XXX στο πλαίσιο της ανταλλαγής πληροφοριών σχετικά με περιστατικά και κυβερνοαπειλές και της άσκησης εποπτικών καθηκόντων. **Οι αρμόδιες [...] αρχές δυνάμει και των δύο οδηγιών θα πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες, ιδίως σε σχέση με τον εντοπισμό κρίσιμων οντοτήτων, τις κυβερνοαπειλές, τους κινδύνους κυβερνοασφάλειας, τα περιστατικά, καθώς και σχετικά με κινδύνους, απειλές και περιστατικά εκτός του κυβερνοχώρου, που επηρεάζουν κρίσιμες οντότητες ή οντότητες ισοδύναμες με κρίσιμες οντότητες, [...] συμπεριλαμβανομένων των μέτρων κυβερνοασφάλειας και των υλικών μέτρων που λαμβάνονται από κρίσιμες οντότητες και των αποτελεσμάτων των εποπτικών δραστηριοτήτων που διεξάγονται σε σχέση με τις εν λόγω οντότητες. Επιπλέον, προκειμένου να εξορθολογιστούν οι εποπτικές δραστηριότητες μεταξύ των αρμόδιων αρχών που ορίζονται βάσει των δύο οδηγιών και προκειμένου να ελαχιστοποιηθεί ο διοικητικός φόρτος για τις ενδιαφερόμενες οντότητες, οι αρμόδιες αρχές θα πρέπει να προσπαθήσουν να εναρμονίσουν τα υποδείγματα κοινοποίησης περιστατικών και τις εποπτικές διαδικασίες. [...] Κατά περίπτωση, οι αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) XXXX/XXXX [...] μπορούν να ζητήσουν από τις αρμόδιες αρχές δυνάμει της παρούσας οδηγίας [...] να ασκήσουν τις εποπτικές και εκτελεστικές εξουσίες τους [...] σε σχέση με ουσιώδη οντότητα η οποία προσδιορίζεται ως κρίσιμη. [...]**

- (14a) Οι οντότητες που ανήκουν στον τομέα των ψηφιακών υποδομών βασίζονται ουσιαστικά σε συστήματα δικτύου και πληροφοριών και, ως εκ τούτου, οι υποχρεώσεις που επιβάλλονται σε αυτές από την παρούσα οδηγία θα πρέπει να αντιμετωπίζονται με ολοκληρωμένο τρόπο τη φυσική ασφάλεια των εν λόγω συστημάτων στο πλαίσιο των υποχρεώσεών τους όσον αφορά τη διαχείριση κινδύνων και τις υποχρεώσεις αναφοράς περιστατικών στον τομέα της κυβερνοασφάλειας. Δεδομένου ότι τα θέματα αυτά καλύπτονται από την παρούσα οδηγία, οι υποχρεώσεις που προβλέπονται στα κεφάλαια III έως VI της οδηγίας (ΕΕ) XXX/XXX [CER] δεν ισχύουν για τις εν λόγω οντότητες.
- (15) Η υποστήριξη και η διατήρηση ενός αξιόπιστου, ανθεκτικού και ασφαλούς συστήματος ονομάτων τομέα (DNS) αποτελούν βασικό παράγοντα για τη διασφάλιση της ακεραιότητας του διαδικτύου και είναι ουσιαστικής σημασίας για τη συνεχή και σταθερή λειτουργία του, από την οποία εξαρτάται η ψηφιακή οικονομία και κοινωνία. Ως εκ τούτου, η παρούσα οδηγία θα πρέπει να εφαρμόζεται στους παρόχους υπηρεσιών DNS κατά μήκος της αλυσίδας παροχής και επίλυσης DNS, οι οποίοι είναι σημαντικοί για την εσωτερική αγορά, συμπεριλαμβανομένων [...], των μητρώων ονομάτων τομέα ανωτάτου επιπέδου (TLD), των οντοτήτων που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, των φορέων των επίσημων διακομιστών ονομάτων για ονόματα τομέα και των φορέων αναδρομικών επιλυτών. Ο όρος «πάροχος υπηρεσιών DNS» δεν θα πρέπει να εφαρμόζεται σε υπηρεσίες DNS που λειτουργούν για ίδιους σκοπούς της οικείας οντότητας και των συνδεδεμένων με αυτήν οντοτήτων. Οι υποχρεώσεις κυβερνοασφάλειας που απορρέουν από την παρούσα οδηγία για τη συγκεκριμένη κατηγορία παρόχων περιορίζονται αυστηρά σε μέτρα διαχείρισης κινδύνου και υποχρεώσεις αναφοράς περιστατικών στον τομέα της κυβερνοασφάλειας και, ως εκ τούτου, δεν θίγουν τη διακυβέρνηση του παγκόσμιου συστήματος DNS από την πολυσυμμετοχική κοινότητα.

(16) Οι υπηρεσίες νεφοϋπολογιστικής θα πρέπει να καλύπτουν τις υπηρεσίες που επιτρέπουν κατά παραγγελία και ευρεία εξ αποστάσεως πρόσβαση σε κλιμακούμενο και ελαστικό σύνολο κοινόχρηστων και κατανεμημένων υπολογιστικών πόρων. Οι εν λόγω υπολογιστικοί πόροι περιλαμβάνουν πόρους όπως δίκτυα, εξυπηρετητές ή άλλες υποδομές, λειτουργικά συστήματα, λογισμικό, αποθήκευση, εφαρμογές και υπηρεσίες. **Τα μοντέλα υπηρεσιών νεφοϋπολογιστικής περιλαμβάνουν, μεταξύ άλλων, υποδομή ως υπηρεσία (IaaS), πλατφόρμα ως υπηρεσία (PaaS), λογισμικό ως υπηρεσία (SaaS) και δίκτυο ως υπηρεσία (NaaS).** Τα μοντέλα ανάπτυξης της νεφοϋπολογιστικής θα πρέπει να περιλαμβάνουν το ιδιωτικό, το κοινοτικό, το δημόσιο και το υβριδικό υπολογιστικό νέφος. Τα προαναφερθέντα μοντέλα υπηρεσιών και ανάπτυξης έχουν την ίδια έννοια με τους όρους παροχής υπηρεσίας και μοντέλα ανάπτυξης που ορίζονται στο πρότυπο ISO/IEC 17788:2014. Η ικανότητα του χρήστη του υπολογιστικού νέφους να παρέχει μονομερώς με ίδια μέσα υπολογιστικές ικανότητες, όπως ο χρόνος εξυπηρετητή ή η δικτυακή αποθήκευση, χωρίς ανθρώπινη αλληλεπίδραση από τον πάροχο υπηρεσιών νεφοϋπολογιστικής, θα μπορούσε να περιγραφεί ως διαχείριση κατά παραγγελία. Ο όρος «ευρεία εξ αποστάσεως πρόσβαση» χρησιμοποιείται για να περιγράψει την κατάσταση κατά την οποία οι ικανότητες υπολογιστικού νέφους παρέχονται μέσω του δικτύου και η πρόσβαση σε αυτές γίνεται μέσω μηχανισμών που προωθούν τη χρήση ετερογενών πλατφορμών, λεπτών ή παχιών πελατών (συμπεριλαμβανομένων κινητών τηλεφώνων, ταμπλετών, φορητών υπολογιστών, σταθμών εργασίας).

Ο όρος «κλιμακοθετήσιμο» αναφέρεται σε υπολογιστικούς πόρους που κατανέμονται με ευελιξία από τον πάροχο των υπηρεσιών νεφοϋπολογιστικής, ανεξαρτήτως της γεωγραφικής θέσης των πόρων, προκειμένου να αντιμετωπιστούν διακυμάνσεις στη ζήτηση. Ο όρος «ελαστικό σύνολο» χρησιμοποιείται για να περιγράψει εκείνους τους υπολογιστικούς πόρους που διατίθενται και απελευθερώνονται ανάλογα με τη ζήτηση προκειμένου να καταστεί δυνατή η ταχεία αύξηση και μείωση των διαθέσιμων πόρων ανάλογα με τον φόρτο εργασίας. Ο όρος «κοινόχρηστοι» χρησιμοποιείται για να περιγράψει εκείνους τους υπολογιστικούς πόρους που παρέχονται σε πολλούς χρήστες που διαθέτουν από κοινού την πρόσβαση στην υπηρεσία, αλλά η επεξεργασία εκτελείται χωριστά για κάθε χρήστη, παρόλο που η υπηρεσία παρέχεται από τον ίδιο ηλεκτρονικό εξοπλισμό. Ο όρος «κατανεμημένοι» χρησιμοποιείται για να περιγράψει τους υπολογιστικούς πόρους που βρίσκονται σε διαφορετικούς δικτυωμένους υπολογιστές ή συσκευές και οι οποίοι επικοινωνούν και συντονίζονται μεταξύ τους μέσω διαβίβασης μηνυμάτων.

- (17) Δεδομένης της ανάδυσης καινοτόμων τεχνολογιών και νέων επιχειρηματικών μοντέλων, αναμένεται να εμφανιστούν στην αγορά νέα μοντέλα ανάπτυξης και υπηρεσιών νεφοϋπολογιστικής τα οποία θα ανταποκρίνονται στις εξελισσόμενες ανάγκες των πελατών. Στο πλαίσιο αυτό, οι υπηρεσίες νεφοϋπολογιστικής μπορούν να παρέχονται σε έντονα καταναμημένη μορφή, ακόμη πιο κοντά στον τόπο παραγωγής ή συλλογής των δεδομένων, μεταβαίνοντας έτσι από το παραδοσιακό μοντέλο σε ένα έντονα καταναμημένο μοντέλο («υπολογιστική παρυφών»).
- (18) Οι υπηρεσίες που παρέχονται από τους παρόχους υπηρεσιών κέντρων δεδομένων ενδέχεται να μην παρέχονται πάντοτε με τη μορφή υπηρεσιών νεφοϋπολογιστικής. Ως εκ τούτου, τα κέντρα δεδομένων ενδέχεται να μην αποτελούν πάντοτε μέρος της υποδομής νεφοϋπολογιστικής. Για τη διαχείριση όλων των κινδύνων για την ασφάλεια δικτυακών και πληροφοριακών συστημάτων, η παρούσα οδηγία θα πρέπει να καλύπτει επίσης τους παρόχους τέτοιων υπηρεσιών κέντρων δεδομένων που δεν είναι υπηρεσίες νεφοϋπολογιστικής. Για τους σκοπούς της παρούσας οδηγίας, ο όρος «υπηρεσία κέντρων δεδομένων» θα πρέπει να καλύπτει την παροχή υπηρεσίας που περιλαμβάνει δομές, ή ομάδες δομών, που προορίζονται για την κεντρική φιλοξενία, διασύνδεση και λειτουργία της τεχνολογίας πληροφοριών και του εξοπλισμού δικτύου που παρέχει υπηρεσίες αποθήκευσης, επεξεργασίας και μεταφοράς δεδομένων, καθώς και όλες τις εγκαταστάσεις και υποδομές διανομής ηλεκτρικής ενέργειας και περιβαλλοντικού ελέγχου. Ο όρος «υπηρεσία κέντρων δεδομένων» δεν ισχύει για ενδοεπιχειρησιακά, εταιρικά κέντρα δεδομένων που ανήκουν και λειτουργούν για ίδιους σκοπούς της οικείας οντότητας.
- (19) Οι φορείς παροχής ταχυδρομικών υπηρεσιών κατά την έννοια της οδηγίας 97/67/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>18</sup>, [...] **περιλαμβανομένων** των [...] ταχυμεταφορών [...] των παρόχων υπηρεσιών, θα πρέπει να εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας εάν παρέχουν τουλάχιστον ένα από τα στάδια της αλυσίδας ταχυδρομικής διανομής, και ιδίως την περισυλλογή, τη διαλογή ή τη διανομή, συμπεριλαμβανομένων των υπηρεσιών παραλαβής. Οι υπηρεσίες μεταφορών που δεν αναλαμβάνονται σε συνδυασμό με ένα από τα στάδια αυτά θα πρέπει να μείνουν εκτός του πεδίου των ταχυδρομικών υπηρεσιών.

---

<sup>18</sup> Οδηγία 97/67/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Δεκεμβρίου 1997, σχετικά με τους κοινούς κανόνες για την ανάπτυξη της εσωτερικής αγοράς κοινοτικών ταχυδρομικών υπηρεσιών και τη βελτίωση της ποιότητας των παρεχομένων υπηρεσιών (ΕΕ L 15 της 21.1.1998, σ. 14).

- (20) Αυτές οι αυξανόμενες αλληλεξαρτήσεις είναι αποτέλεσμα ενός ολοένα και περισσότερο διασυνοριακού και αλληλεξαρτώμενου δικτύου παροχής υπηρεσιών που χρησιμοποιεί βασικές υποδομές σε ολόκληρη την Ένωση στους τομείς της ενέργειας, των μεταφορών, των ψηφιακών υποδομών, του πόσιμου νερού και των λυμάτων, της υγείας, ορισμένων πτυχών της δημόσιας διοίκησης, καθώς και του διαστήματος, στον βαθμό που αφορά την παροχή ορισμένων υπηρεσιών που εξαρτώνται από επίγειες υποδομές των οποίων η κυριότητα, η διαχείριση και η λειτουργία ανήκει είτε σε κράτη μέλη είτε σε ιδιώτες, και, ως εκ τούτου, δεν καλύπτει τις υποδομές των οποίων η κυριότητα, η διαχείριση και η λειτουργία ανήκει στην Ένωση, ή γίνεται εξ ονόματος αυτής, στο πλαίσιο των διαστημικών προγραμμάτων της. Λόγω των αλληλεξαρτήσεων αυτών, οποιαδήποτε διαταραχή, ακόμη και αν αρχικά περιοριζόταν σε μία οντότητα ή σε έναν τομέα, μπορεί να έχει ευρύτερες αλυσιδωτές επιπτώσεις, με δυννητικά μεγάλης κλίμακας και μακροχρόνιο αρνητικό αντίκτυπο στην παροχή υπηρεσιών σε ολόκληρη την εσωτερική αγορά. Η πανδημία της COVID-19 κατέδειξε την τρωτότητα των ολοένα και πιο αλληλεξαρτώμενων κοινωνιών μας απέναντι σε κινδύνους χαμηλής πιθανότητας.
- (20α) Για τους σκοπούς της επίτευξης και διατήρησης υψηλού επιπέδου κυβερνοασφάλειας, οι εθνικές στρατηγικές κυβερνοασφάλειας που απαιτούνται από την παρούσα οδηγία θα πρέπει να αποτελούνται από συνεκτικά πλαίσια που προβλέπουν διακυβέρνηση στον τομέα της κυβερνοασφάλειας. Οι στρατηγικές αυτές μπορούν να αποτελούνται από ένα ή περισσότερα έγγραφα νομοθετικού ή μη νομοθετικού χαρακτήρα.**
- (21) Με δεδομένες τις διαφορές των εθνικών δομών διακυβέρνησης και προκειμένου να διασφαλιστούν οι ήδη υφιστάμενες τομεακές ρυθμίσεις ή οι εποπτικοί και ρυθμιστικοί φορείς της Ένωσης, τα κράτη μέλη θα πρέπει να είναι σε θέση να ορίζουν περισσότερες από μία αρμόδιες εθνικές αρχές για την εκτέλεση των καθηκόντων που συνδέονται με την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων βασικών και σημαντικών οντοτήτων δυνάμει της παρούσας οδηγίας. Τα κράτη μέλη θα πρέπει να έχουν τη δυνατότητα να αναθέτουν τον ρόλο αυτόν σε υφιστάμενη αρχή.



- (22) Για τη διευκόλυνση της διασυνοριακής συνεργασίας και επικοινωνίας μεταξύ των αρχών, και για να καταστεί δυνατή η αποτελεσματική εφαρμογή της παρούσας οδηγίας, είναι ανάγκη κάθε κράτος μέλος να ορίζει ένα εθνικό ενιαίο σημείο επαφής υπεύθυνο για τον συντονισμό θεμάτων σχετικά με την ασφάλεια δικτυακών και πληροφοριακών συστημάτων και με τη διασυνοριακή συνεργασία σε επίπεδο Ένωσης.
- (23) Οι αρμόδιες αρχές ή οι CSIRT θα πρέπει να λαμβάνουν κοινοποιήσεις περιστατικών από οντότητες με αποτελεσματικό και αποδοτικό τρόπο, **μεταξύ άλλων με σκοπό τη διευκόλυνση, κατά περίπτωση, της έγκαιρης αντίδρασης σε περιστατικά και την παροχή απάντησης στην κοινοποιούσα οντότητα**. Τα ενιαία σημεία επαφής θα πρέπει να είναι επιφορτισμένα με τη διαβίβαση των κοινοποιήσεων περιστατικών στα ενιαία κέντρα επαφής άλλων επηρεαζόμενων κρατών μελών. [...]

- (23α) Οι τομεακές νομικές πράξεις της Ένωσης που απαιτούν μέτρα διαχείρισης κινδύνου κυβερνοασφάλειας ή υποχρεώσεις αναφοράς περιστατικών τουλάχιστον ισοδύναμου αποτελέσματος με εκείνες που ορίζονται στην παρούσα οδηγία θα μπορούσαν να προβλέπουν ότι οι ορισθείσες αρμόδιες αρχές τους ασκούν τις εποπτικές και εκτελεστικές εξουσίες τους σε σχέση με τα εν λόγω μέτρα ή υποχρεώσεις με τη βοήθεια των αρμόδιων αρχών που ορίζονται σύμφωνα με την παρούσα οδηγία. Οι ενδιαφερόμενες αρμόδιες αρχές θα μπορούσαν να θεσπίσουν ρυθμίσεις συνεργασίας για τον σκοπό αυτό. Οι εν λόγω ρυθμίσεις συνεργασίας θα μπορούσαν να καθορίζουν, μεταξύ άλλων, τις διαδικασίες που αφορούν τον συντονισμό των εποπτικών δραστηριοτήτων, συμπεριλαμβανομένων των διαδικασιών ερευνών και επιτόπιων επιθεωρήσεων σύμφωνα με το εθνικό δίκαιο, καθώς και μηχανισμό ανταλλαγής συναφών πληροφοριών μεταξύ των αρμόδιων αρχών για την εποπτεία και την επιβολή, συμπεριλαμβανομένης της πρόσβασης σε πληροφορίες σχετικές με τον κυβερνοχώρο που ζητούν οι αρμόδιες αρχές που ορίζονται σύμφωνα με την παρούσα οδηγία.
- (24) Τα κράτη μέλη θα πρέπει να διαθέτουν τον κατάλληλο εξοπλισμό, τόσο σε τεχνικές όσο και σε οργανωτικές ικανότητες, για την πρόληψη, τον εντοπισμό, την αντιμετώπιση και τον μετριασμό περιστατικών και κινδύνων σε δικτυακά και πληροφοριακά συστήματα. Τα κράτη μέλη θα πρέπει επομένως να φροντίσουν να διαθέτουν εύρυθμα λειτουργούσες CSIRT, γνωστές επίσης ως «ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική» (Computer Emergency Response Teams – CERT), οι οποίες να συμμορφώνονται με τις βασικές απαιτήσεις ώστε να διασφαλίζεται τόσο η ύπαρξη αποτελεσματικών και συμβατών ικανοτήτων αντιμετώπισης περιστατικών και κινδύνων όσο και η αποτελεσματική συνεργασία σε ενωσιακό επίπεδο. Προκειμένου να ενισχυθεί η σχέση εμπιστοσύνης μεταξύ των οντοτήτων και των CSIRT, στις περιπτώσεις που μια CSIRT αποτελεί μέρος της αρμόδιας αρχής, τα κράτη μέλη [...] **μπορούν** να εξετάσουν το ενδεχόμενο λειτουργικού διαχωρισμού μεταξύ των επιχειρησιακών καθηκόντων που επιτελούν οι CSIRT, ιδίως όσον αφορά την ανταλλαγή πληροφοριών και τη στήριξη προς τις οντότητες, και των εποπτικών δραστηριοτήτων των αρμόδιων αρχών.

- (25) Όσον αφορά τα δεδομένα προσωπικού χαρακτήρα, οι CSIRT θα πρέπει να είναι σε θέση να παρέχουν, σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>19</sup> όσον αφορά τα δεδομένα προσωπικού χαρακτήρα, εξ ονόματος και κατόπιν αιτήματος οντότητας δυνάμει της παρούσας οδηγίας, προδραστική σάρωση των δικτυακών και πληροφοριακών συστημάτων που χρησιμοποιούνται για την παροχή των υπηρεσιών τους. **Κατά περίπτωση**, τα κράτη μέλη θα πρέπει να στοχεύουν στην εξασφάλιση του ίδιου επιπέδου τεχνικών ικανοτήτων για όλες τις τομεακές CSIRT. Για την ανάπτυξη των εθνικών τους CSIRT, τα κράτη μέλη μπορούν να ζητούν τη συνδρομή του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA).
- (26) Δεδομένης της σημασίας της διεθνούς συνεργασίας για την κυβερνοασφάλεια, οι CSIRT θα πρέπει να έχουν τη δυνατότητα να συμμετέχουν σε διεθνή δίκτυα συνεργασίας πέραν του δικτύου CSIRT που θεσπίζεται με την παρούσα οδηγία. **Ως εκ τούτου, οι CSIRT και οι αρμόδιες αρχές θα μπορούσαν να ανταλλάσσουν πληροφορίες, συμπεριλαμβανομένων των δεδομένων προσωπικού χαρακτήρα, με CSIRT τρίτων χωρών ή με τις αρχές τους για την εκτέλεση των καθηκόντων τους σύμφωνα με τον κανονισμό (ΕΕ) 2016/679. Σε περιπτώσεις απουσίας απόφασης περί επάρκειας που εκδίδεται σύμφωνα με το άρθρο 45 του κανονισμού (ΕΕ) 2016/679 ή κατάλληλων εγγυήσεων δυνάμει του άρθρου 46 του εν λόγω κανονισμού, η ανταλλαγή δεδομένων προσωπικού χαρακτήρα που κρίνεται αναγκαία για τον μετριασμό σημαντικών κυβερνοαπειλών και την αντιμετώπιση εν εξελίξει σημαντικού περιστατικού θα μπορούσε να θεωρηθεί σημαντικός λόγος δημόσιου συμφέροντος κατά την έννοια του άρθρου 49 παράγραφος 1 στοιχείο δ) του κανονισμού (ΕΕ) 2016/679.**

---

<sup>19</sup> Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

- (27) Σύμφωνα με το παράρτημα της σύστασης (ΕΕ) 2017/1548 της Επιτροπής για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο («προσχέδιο»)<sup>20</sup>, ως περιστατικό μεγάλης κλίμακας θα πρέπει να νοείται εκείνο που έχει ευρείες συνέπειες σε τουλάχιστον δύο κράτη μέλη ή το οποίο προκαλεί διαταραχή που υπερβαίνει την ικανότητα ενός κράτους μέλους να ανταποκριθεί σε αυτή. Ανάλογα με την αιτία και τις συνέπειές τους, τα περιστατικά μεγάλης κλίμακας ενδέχεται να κλιμακωθούν και να μετατραπούν σε πραγματικές κρίσεις που καθιστούν αδύνατη την ομαλή λειτουργία της εσωτερικής αγοράς. Δεδομένου των ευρέων συνεπειών και, στις περισσότερες περιπτώσεις, του διασυννοριακού χαρακτήρα τέτοιων περιστατικών, τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης θα πρέπει να συνεργάζονται σε τεχνικό, επιχειρησιακό και πολιτικό επίπεδο για τον κατάλληλο συντονισμό της αντιμετώπισής τους σε ολόκληρη την Ένωση.
- (28) Δεδομένου ότι η εκμετάλλευση των τρωτών σημείων στα δικτυακά και πληροφοριακά συστήματα μπορεί να προκαλέσει σημαντικές διαταραχές και βλάβες, ο άμεσος εντοπισμός και η διόρθωση αυτών των τρωτών σημείων αποτελεί σημαντικό παράγοντα για τη μείωση του κινδύνου για την κυβερνοασφάλεια. Οι οντότητες που αναπτύσσουν ή **διαχειρίζονται** τέτοια συστήματα θα πρέπει, ως εκ τούτου, να θεσπίσουν κατάλληλες διαδικασίες για την αντιμετώπιση των τρωτών σημείων όταν εντοπίζονται. Δεδομένου ότι τα τρωτά σημεία συχνά εντοπίζονται και αναφέρονται (γνωστοποιούνται) από τρίτους (αναφέρουσες οντότητες), ο κατασκευαστής ή ο πάροχος προϊόντων ή υπηρεσιών ΤΠΕ θα πρέπει επίσης να θεσπίσει τις αναγκαίες διαδικασίες για τη λήψη πληροφοριών από τρίτους σχετικά με τρωτά σημεία. Στο πλαίσιο αυτό, τα διεθνή πρότυπα ISO/IEC 30111 και ISO/IEC [...] **29147** παρέχουν καθοδήγηση σχετικά με τον χειρισμό τρωτών σημείων και τη γνωστοποίηση τρωτών σημείων, αντίστοιχα. Όσον αφορά τη γνωστοποίηση τρωτών σημείων, είναι ιδιαίτερα σημαντικός ο συντονισμός μεταξύ των αναφερουσών οντοτήτων και των κατασκευαστών ή παρόχων προϊόντων ή υπηρεσιών ΤΠΕ. Η συντονισμένη γνωστοποίηση τρωτών σημείων προσδιορίζει μια διαρθρωμένη διαδικασία μέσω της οποίας τα τρωτά σημεία αναφέρονται σε οργανισμούς κατά τρόπο που να επιτρέπει στον οργανισμό να διαγνώσει και να διορθώσει το τρωτό σημείο πριν να αποκαλυφθούν σε τρίτα μέρη ή στο ευρύ κοινό λεπτομερείς πληροφορίες σχετικά με τα τρωτά σημεία. Η συντονισμένη γνωστοποίηση τρωτών σημείων θα πρέπει επίσης να περιλαμβάνει τον συντονισμό μεταξύ της αναφέρουσας οντότητας και του οργανισμού όσον αφορά το χρονοδιάγραμμα διόρθωσης και δημοσιοποίησης των τρωτών σημείων.

---

<sup>20</sup> Σύσταση (ΕΕ) 2017/1584 της Επιτροπής, της 13ης Σεπτεμβρίου 2017, για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο (ΕΕ L 239 της 19.9.2017, σ. 36).

- (29) Ως εκ τούτου, τα κράτη μέλη οφείλουν να λάβουν μέτρα για να διευκολύνουν τη συντονισμένη γνωστοποίηση τρωτών σημείων με τη θέσπιση σχετικής εθνικής πολιτικής. **Στο πλαίσιο της εθνικής πολιτικής τους, τα κράτη μέλη θα πρέπει να στοχεύουν στην αντιμετώπιση, στο μέτρο του δυνατού, των προκλήσεων που αντιμετωπίζουν οι ευάλωτοι ερευνητές, συμπεριλαμβανομένης της ενδεχόμενης έκθεσής τους σε ποινική ευθύνη, σύμφωνα με την εθνική έννομη τάξη τους.** [...] Τα κράτη μέλη θα πρέπει να ορίσουν μια CSIRT η οποία θα αναλάβει ρόλο «συντονίστριας», ενεργώντας ως διαμεσολαβήτρια μεταξύ των αναφερουσών οντοτήτων και των κατασκευαστών ή παρόχων προϊόντων ή υπηρεσιών ΤΠΕ, όπου απαιτείται. Τα καθήκοντα της συντονίστριας CSIRT θα πρέπει να περιλαμβάνουν ιδίως τον προσδιορισμό και την επικοινωνία με τις σχετικές οντότητες, την υποστήριξη των αναφερουσών οντοτήτων, τη διαπραγμάτευση των χρονοδιαγραμμάτων γνωστοποίησης και τη διαχείριση των τρωτών σημείων που επηρεάζουν πολλαπλούς οργανισμούς (συντονισμένη γνωστοποίηση τρωτών σημείων που αφορούν πολλά μέρη). Όταν **το αναφερόμενο** τρωτό σημείο **θα μπορούσε δυνητικά να έχει σημαντικό αντίκτυπο σε οντότητες** [...] σε περισσότερα του ενός κράτη μέλη, οι ορισθείσες CSIRT [...] θα πρέπει να συνεργάζονται στο πλαίσιο του δικτύου CSIRT, **κατά περίπτωση.**
- (30) Η πρόσβαση σε ορθές και έγκαιρες πληροφορίες σχετικά με τα τρωτά σημεία που επηρεάζουν τα προϊόντα και τις υπηρεσίες ΤΠΕ συμβάλλει στην ενίσχυση της διαχείρισης κινδύνων κυβερνοασφάλειας. Στο πλαίσιο αυτό, οι πηγές δημόσια διαθέσιμων πληροφοριών σχετικά με τα τρωτά σημεία αποτελούν σημαντικό εργαλείο για τις οντότητες και τους χρήστες τους, αλλά και για τις εθνικές αρμόδιες αρχές και τις CSIRT. Για τον λόγο αυτό, ο ENISA θα πρέπει να καταρτίσει μητρώο τρωτών σημείων στο οποίο βασικές και σημαντικές οντότητες και οι πάροχοί τους, καθώς και οντότητες που δεν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, **ή οι ορισθείσες CSIRT** θα μπορούν, σε εθελοντική βάση, να γνωστοποιούν τρωτά σημεία και να παρέχουν τις πληροφορίες σχετικά με τρωτά σημεία οι οποίες επιτρέπουν στους χρήστες να λάβουν κατάλληλα μέτρα μετριασμού.

- (31) Μολονότι υπάρχουν παρόμοια μητρώα ή βάσεις δεδομένων τρωτών σημείων, αυτά φιλοξενούνται και τηρούνται από οντότητες που δεν είναι εγκατεστημένες στην Ένωση. Ένα ευρωπαϊκό μητρώο τρωτών σημείων που θα τηρείται από τον ENISA θα προσέφερε βελτιωμένη διαφάνεια όσον αφορά τη διαδικασία δημοσίευσης πριν από την επίσημη γνωστοποίηση του τρωτού σημείου, καθώς και ανθεκτικότητα σε περιπτώσεις διαταραχών ή διακοπών της παροχής παρόμοιων υπηρεσιών. Για να αποφευχθεί η αλληλεπικάλυψη των προσπαθειών και να επιδιωχθεί η συμπληρωματικότητα στο μέτρο του δυνατού, ο ENISA θα πρέπει να εξετάσει τη δυνατότητα σύναψης συμφωνιών διαρθρωμένης συνεργασίας με παρόμοια μητρώα σε δικαιοδοσίες τρίτων χωρών. **Ειδικότερα, ο ENISA θα πρέπει να διερευνήσει τη δυνατότητα στενής συνεργασίας με τους φορείς εκμετάλλευσης του κοινού συστήματος τρωτών σημείων και ανοιγμάτων (CVE), συμπεριλαμβανομένης της δυνατότητας να καταστεί βασική αρχή αριθμοδότησης CVE.**
- (32) **Η ομάδα συνεργασίας θα πρέπει να συνεχίσει να στηρίζει και να διευκολύνει τη στρατηγική συνεργασία και την ανταλλαγή πληροφοριών, καθώς και να ενισχύει την εμπιστοσύνη μεταξύ των κρατών μελών.** Η ομάδα συνεργασίας θα πρέπει να καταρτίζει ανά διετία πρόγραμμα εργασίας, συμπεριλαμβανομένων των δράσεων που πρέπει να αναληφθούν από την ομάδα για την υλοποίηση των στόχων και των καθηκόντων της. Το χρονοδιάγραμμα του πρώτου προγράμματος που θα εγκριθεί δυνάμει της παρούσας οδηγίας θα πρέπει να ευθυγραμμίζεται με το χρονοδιάγραμμα του τελευταίου προγράμματος που εγκρίθηκε δυνάμει της οδηγίας (ΕΕ) 2016/1148, ώστε να αποφευχθούν ενδεχόμενες διαταραχές στις εργασίες της ομάδας.
- (33) Κάθε φορά που καταρτίζει έγγραφα καθοδήγησης, η ομάδα συνεργασίας θα πρέπει: να καταγράφει τις εθνικές λύσεις και εμπειρίες, να αξιολογεί τον αντίκτυπο των παραδοτέων της ομάδας συνεργασίας στις εθνικές προσεγγίσεις, να συζητά τις προκλήσεις όσον αφορά την εφαρμογή και να διατυπώνει ειδικές συστάσεις που πρέπει να λαμβάνονται υπόψη μέσω της καλύτερης εφαρμογής των υφιστάμενων κανόνων.

- (34) Η ομάδα συνεργασίας θα πρέπει να παραμείνει ένα ευέλικτο φόρουμ και να είναι σε θέση να αντιδρά σε μεταβαλλόμενες και νέες πολιτικές προτεραιότητες και προκλήσεις, λαμβάνοντας παράλληλα υπόψη τη διαθεσιμότητα των πόρων. Θα πρέπει να διοργανώνει τακτικές κοινές συνεδριάσεις με σχετικούς ιδιωτικούς ενδιαφερόμενους φορείς από ολόκληρη την Ένωση για να συζητά δραστηριότητες που πραγματοποιεί η ομάδα και να συγκεντρώνει στοιχεία σχετικά με αναδυόμενες προκλήσεις πολιτικής. Προκειμένου να ενισχύσει τη συνεργασία σε επίπεδο Ένωσης, η ομάδα θα πρέπει να εξετάσει το ενδεχόμενο να προσκαλέσει για να συμμετάσχουν στις εργασίες της φορείς και οργανισμούς της Ένωσης που εμπλέκονται στην πολιτική για την κυβερνοασφάλεια, όπως το Ευρωπαϊκό Κέντρο για το Κυβερνοέγκλημα (EC3), ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια της Αεροπορίας (EASA) και ο Οργανισμός της Ευρωπαϊκής Ένωσης για το Διαστημικό Πρόγραμμα (EUSPA).
- (35) Οι αρμόδιες αρχές και οι CSIRT θα πρέπει να εξουσιοδοτηθούν να συμμετέχουν σε προγράμματα ανταλλαγής υπαλλήλων από άλλα κράτη μέλη με σκοπό τη βελτίωση της συνεργασίας. Οι αρμόδιες αρχές θα πρέπει να λαμβάνουν τα αναγκαία μέτρα ώστε οι υπάλληλοι από άλλα κράτη μέλη να είναι σε θέση να συμμετέχουν αποτελεσματικά στις δραστηριότητες της φιλοξενούσας αρμόδιας αρχής.
- (35α) Το δίκτυο CSIRT θα πρέπει να συνεχίσει να συμβάλλει στην ενίσχυση της αξιοπιστίας και της εμπιστοσύνης και να προωθεί την ταχεία και αποτελεσματική επιχειρησιακή συνεργασία μεταξύ των κρατών μελών. Για να ενισχυθεί η επιχειρησιακή συνεργασία σε επίπεδο Ένωσης, το δίκτυο CSIRT θα πρέπει να εξετάσει το ενδεχόμενο να προσκαλέσει όργανα και οργανισμούς της Ένωσης που εμπλέκονται στην πολιτική για την κυβερνοασφάλεια, όπως η Ευρωπόλ, να συμμετάσχουν στις εργασίες του.**
- (36) [...]

- (36α) Για να διευκολυνθεί η αποτελεσματική εφαρμογή των διατάξεων της παρούσας οδηγίας, όπως η διαχείριση των τρωτών σημείων, η διαχείριση κινδύνων στον τομέα της κυβερνοασφάλειας, τα μέτρα αναφοράς περιστατικών και οι ρυθμίσεις ανταλλαγής πληροφοριών, τα κράτη μέλη μπορούν να συνεργάζονται με τρίτες χώρες και να αναλαμβάνουν δραστηριότητες που κρίνονται κατάλληλες για τον σκοπό αυτό, όπως ανταλλαγή πληροφοριών σχετικά με απειλές, περιστατικά, τρωτά σημεία, εργαλεία και μεθόδους, τακτικές, τεχνικές και διαδικασίες, σχετικά με την ετοιμότητα και τις ασκήσεις για τη διαχείριση κρίσεων στον κυβερνοχώρο, την κατάρτιση, την οικοδόμηση εμπιστοσύνης και τις ρυθμίσεις διαρθρωμένης ανταλλαγής πληροφοριών. Οι εν λόγω συμφωνίες συνεργασίας θα πρέπει να συμμορφώνονται με το δίκαιο της Ένωσης για την προστασία των δεδομένων.
- (37) Τα κράτη μέλη θα πρέπει να συμβάλουν στη δημιουργία του πλαισίου της ΕΕ για την αντιμετώπιση κρίσεων στον κυβερνοχώρο που ορίζεται στη σύσταση (ΕΕ) 2017/1584 μέσω των υφιστάμενων δικτύων συνεργασίας, ιδίως μέσω του **ευρωπαϊκού** δικτύου οργανώσεων διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (EU-CyCLONe), του δικτύου CSIRT και της ομάδας συνεργασίας. Το EU-CyCLONe και το δίκτυο CSIRT θα πρέπει να συνεργάζονται βάσει διαδικαστικών ρυθμίσεων που θα καθορίζουν τις λεπτομέρειες της εν λόγω συνεργασίας **και να αποφεύγουν τυχόν επικάλυψη εργασιών**. Οι διαδικαστικοί κανόνες του EU-CyCLONe θα πρέπει να προσδιορίζουν περαιτέρω τις λεπτομέρειες λειτουργίας του δικτύου, συμπεριλαμβανομένων, μεταξύ άλλων, των ρόλων, των τρόπων συνεργασίας, των αλληλεπιδράσεων με άλλους σχετικούς παράγοντες και των υποδειγμάτων για την ανταλλαγή πληροφοριών, καθώς και των μέσων επικοινωνίας. Για τη διαχείριση κρίσεων σε ενωσιακό **πολιτικό** επίπεδο, τα ενδιαφερόμενα μέρη θα πρέπει να βασίζονται στις ολοκληρωμένες ρυθμίσεις για την πολιτική αντιμετώπιση κρίσεων (IPCR). Η Επιτροπή θα πρέπει να χρησιμοποιήσει για τον σκοπό αυτό την υψηλού επιπέδου διαδικασία ARGUS για τον συντονισμό σε περιπτώσεις διατομεακών κρίσεων. Εάν η κρίση ενέχει σημαντική εξωτερική διάσταση ή διάσταση κοινής πολιτικής ασφάλειας και άμυνας (ΚΠΑΑ), θα πρέπει να ενεργοποιείται ο Μηχανισμός Αντιμετώπισης Κρίσεων (CRM) της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης (EYED).



- (37α)** Το EU-CyCLONe θα πρέπει να λειτουργεί ως ενδιάμεσο δίκτυο μεταξύ τεχνικού και πολιτικού επιπέδου κατά τη διάρκεια περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας. Θα πρέπει να ενισχύει τη συνεργασία σε επιχειρησιακό επίπεδο, αξιοποιώντας τα ευρήματα του δικτύου CSIRT και χρησιμοποιώντας τις δικές του δυνατότητες για την εκπόνηση εκτιμήσεων επιπτώσεων των περιστατικών και των κρίσεων μεγάλης κλίμακας, και υποστηρίζοντας τη λήψη αποφάσεων σε πολιτικό επίπεδο. Τα θεσμικά και λοιπά όργανα και οργανισμοί της ΕΕ θα πρέπει να ορίσουν ως μέλος του EU-CyCLONe μια αρμόδια αρχή για τη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας.
- (38) [...]
- (39) [...]
- (39α)** Η ευθύνη για την εξασφάλιση της ασφάλειας των δικτυακών και πληροφοριακών συστημάτων εναπόκειται σε μεγάλο βαθμό στις βασικές και στις σημαντικές οντότητες. Θα πρέπει να προαχθεί και να αναπτυχθεί μια νοοτροπία διαχείρισης κινδύνων, που να περιλαμβάνει εκτίμηση των κινδύνων και την εφαρμογή μέτρων ασφάλειας προσαρμοσμένων στους εκάστοτε κινδύνους.
- (40) Τα μέτρα για τη διαχείριση του κινδύνου θα πρέπει να λαμβάνουν υπόψη τον βαθμό εξάρτησης της οντότητας από δικτυακά και πληροφοριακά συστήματα και να περιλαμβάνουν μέτρα για τον εντοπισμό τυχόν κινδύνων περιστατικών, καθώς και μέτρα για την πρόληψη, την ανίχνευση και την αντιμετώπιση περιστατικών και για τον μετριασμό του αντίκτυπού τους. Η ασφάλεια δικτυακών και πληροφοριακών συστημάτων θα πρέπει να περιλαμβάνει την ασφάλεια των δεδομένων που αποθηκεύονται, μεταδίδονται και υποβάλλονται σε επεξεργασία.

- (40α) Δεδομένου ότι οι απειλές για την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων μπορεί να έχουν διαφορετική προέλευση, η παρούσα οδηγία εφαρμόζει μια προσέγγιση «παντός κινδύνου» που περιλαμβάνει την προστασία των δικτυακών και πληροφοριακών συστημάτων και του φυσικού τους περιβάλλοντος από κάθε συμβάν, όπως κλοπή, πυρκαγιά, πλημμύρα, διακοπές τηλεπικοινωνιών ή ρεύματος, ή από κάθε μη εξουσιοδοτημένη φυσική πρόσβαση και πρόκληση βλάβης και παρεμβολή στις εγκαταστάσεις πληροφόρησης και επεξεργασίας πληροφοριών της οντότητας, που θα μπορούσε να θέσει σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων που αποθηκεύονται, μεταδίδονται και υποβάλλονται σε επεξεργασία ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω δικτυακών και πληροφοριακών συστημάτων. Συνεπώς, τα μέτρα διαχείρισης κινδύνων θα πρέπει επίσης να καλύπτουν την υλική και περιβαλλοντική ασφάλεια, περιλαμβάνοντας μέτρα για την προστασία των δικτυακών και πληροφοριακών συστημάτων της οντότητας από βλάβες των συστημάτων, ανθρώπινα σφάλματα, κακόβουλες ενέργειες ή φυσικά φαινόμενα, σύμφωνα με ευρωπαϊκά ή διεθνώς αναγνωρισμένα πρότυπα, όπως αυτά που περιλαμβάνονται στη σειρά ISO 27000. Εν προκειμένω, οι οντότητες θα πρέπει, στο πλαίσιο των μέτρων διαχείρισης κινδύνων που εφαρμόζουν, να μεριμνούν και για την ασφάλεια των ανθρώπινων πόρων και να εφαρμόζουν κατάλληλες πολιτικές ελέγχου της πρόσβασης. Τα μέτρα αυτά θα πρέπει να συνάδουν με την οδηγία XXXX [οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων].
- (40β) Ελλείψει κατάλληλων ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας εγκεκριμένων σύμφωνα με τον κανονισμό (ΕΕ) 2019/881, τα κράτη μέλη θα μπορούσαν να απαιτούν από τις οντότητες να χρησιμοποιούν πιστοποιημένα προϊόντα, υπηρεσίες και διαδικασίες ΤΠΕ ή να αποκτούν πιστοποιητικό στο πλαίσιο των διαθέσιμων εθνικών συστημάτων κυβερνοασφάλειας με σκοπό τη συμμόρφωση με τις απαιτήσεις διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας δυνάμει της παρούσας οδηγίας.

- (41) Για να αποφευχθεί η δυσανάλογη οικονομική και διοικητική επιβάρυνση των βασικών και των σημαντικών οντοτήτων, οι απαιτήσεις σχετικά με τη διαχείριση κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει να είναι ανάλογες προς τον κίνδυνο που ενέχει [...] **το σχετικό δικτυακό και πληροφοριακό σύστημα, λαμβανομένων υπόψη των πλέον πρόσφατων τεχνικών δυνατοτήτων όσον αφορά τα σχετικά μέτρα, καθώς και του κόστους εφαρμογής των μέτρων αυτών. Θα πρέπει επίσης να λαμβάνεται δεόντως υπόψη το μέγεθος της οντότητας, καθώς και η πιθανότητα επέλευσης περιστατικών και η σοβαρότητά τους.**
- (41α) **Για να μειωθούν οι ρυθμιστικές επιβαρύνσεις, οι απαιτήσεις για την εφαρμογή μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας από τις μεσαίες, μικρές ή πολύ μικρές οντότητες θα πρέπει καταρχήν να είναι λιγότερο αυστηρές, εκτός εάν τα κριτήρια κρισιμότητας ή οι εθνικές εκτιμήσεις επικινδυνότητας δικαιολογούν αυστηρότερες απαιτήσεις, ιδίως όσον αφορά τις οντότητες οι οποίες πληρούν τα κριτήρια κρισιμότητας που ορίζονται στην παρούσα οδηγία.**
- (42) Οι βασικές και οι σημαντικές οντότητες θα πρέπει να εγγυώνται την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων που χρησιμοποιούν στις δραστηριότητές τους. Κατά κύριο λόγο πρόκειται για ιδιωτικά δικτυακά και πληροφοριακά συστήματα τα οποία διαχειρίζεται το εσωτερικά απασχολούμενο προσωπικό πληροφορικής ή των οποίων η ασφάλεια έχει ανατεθεί σε τρίτους. Οι απαιτήσεις για τη διαχείριση των κινδύνων και την αναφορά περιστατικών σχετικά με την κυβερνοασφάλεια σύμφωνα με την παρούσα οδηγία θα πρέπει να εφαρμόζονται στις σχετικές βασικές και σημαντικές οντότητες, ανεξάρτητα από το αν εκτελούν τη συντήρηση των δικτυακών και πληροφοριακών συστημάτων τους εσωτερικά ή αν την αναθέτουν σε τρίτους.
- (42αα) **Λαμβανομένης υπόψη της διασυνοριακής φύσης τους, οι πάροχοι υπηρεσιών DNS, τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD, οι πάροχοι υπηρεσιών νεφοϋπολογιστικής, οι πάροχοι υπηρεσιών κέντρου δεδομένων, οι πάροχοι δικτύων διανομής περιεχομένου, οι πάροχοι υπηρεσιών διαχείρισης και οι πάροχοι υπηρεσιών διαχείρισης ασφάλειας θα πρέπει να υπόκεινται σε υψηλότερο βαθμό εναρμόνισης σε επίπεδο Ένωσης. Ως εκ τούτου, η εφαρμογή των μέτρων κυβερνοασφάλειας θα πρέπει να διευκολυνθεί με εκτελεστική πράξη.**

- (43) Η αντιμετώπιση των κινδύνων κυβερνοασφάλειας που γεννώνται από την αλυσίδα εφοδιασμού μιας οντότητας και τη σχέση της με τους προμηθευτές της είναι ιδιαίτερα σημαντική, δεδομένης της συχνής εμφάνισης περιστατικών κατά τα οποία οι οντότητες καθίστανται θύματα κυβερνοεπιθέσεων και στα οποία κακόβουλοι παράγοντες κατόρθωσαν να θέσουν σε κίνδυνο την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων μιας οντότητας εκμεταλλευόμενοι τρωτά σημεία που επηρεάζουν προϊόντα και υπηρεσίες τρίτων. Ως εκ τούτου, οι οντότητες θα πρέπει να αξιολογούν και να λαμβάνουν υπόψη τη συνολική ποιότητα των προϊόντων και τις πρακτικές κυβερνοασφάλειας των προμηθευτών και των παρόχων υπηρεσιών τους, συμπεριλαμβανομένων των ασφαλών τους διαδικασιών ανάπτυξης.
- (44) Μεταξύ των παρόχων υπηρεσιών, οι πάροχοι υπηρεσιών διαχείρισης ασφάλειας (managed security services providers – MSSP) σε τομείς όπως η αντιμετώπιση περιστατικών, οι δοκιμές διείσδυσης, οι έλεγχοι ασφάλειας και η παροχή συμβουλών διαδραματίζουν ιδιαίτερα σημαντικό ρόλο στην παροχή συνδρομής σε οντότητες που καταβάλλουν προσπάθειες για τον εντοπισμό και την αντιμετώπιση περιστατικών. Ωστόσο, οι ίδιοι οι MSSP αποτελούν επίσης στόχους κυβερνοεπιθέσεων και, μέσω της στενής ενσωμάτωσής τους στις λειτουργίες των φορέων εκμετάλλευσης, συνιστούν ιδιαίτερο κίνδυνο για την κυβερνοασφάλεια. Ως εκ τούτου, οι οντότητες θα πρέπει να επιδεικνύουν αυξημένη επιμέλεια κατά την επιλογή ενός MSSP.
- (44α) Οι αρμόδιες εθνικές αρχές, στο πλαίσιο των εποπτικών καθηκόντων τους, μπορούν επίσης να επωφελούνται από υπηρεσίες κυβερνοασφάλειας, όπως οι έλεγχοι ασφάλειας και οι δοκιμές διείσδυσης ή η αντιμετώπιση περιστατικών. Για να βοηθήσει τις οντότητες, καθώς και τις αρμόδιες εθνικές αρχές, στην επιλογή ειδικευμένων και αξιόπιστων παρόχων υπηρεσιών κυβερνοασφάλειας, η Επιτροπή, με τη συνδρομή της ομάδας συνεργασίας και του ENISA, θα πρέπει να εξετάσει το ενδεχόμενο να ζητήσει ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας σύμφωνα με το άρθρο 48 του κανονισμού (ΕΕ) 2019/881.**

- (45) Οι οντότητες θα πρέπει επίσης να αντιμετωπίζουν τους κινδύνους για την κυβερνοασφάλεια που γεννώνται από τις αλληλεπιδράσεις και τις σχέσεις τους με άλλα ενδιαφερόμενα μέρη εντός ενός ευρύτερου οικοσυστήματος. Ειδικότερα, οι οντότητες θα πρέπει να λαμβάνουν τα κατάλληλα μέτρα ώστε η συνεργασία τους με ακαδημαϊκά και ερευνητικά ιδρύματα να πραγματοποιείται σύμφωνα με τις πολιτικές τους για την κυβερνοασφάλεια και να ακολουθεί τις ορθές πρακτικές όσον αφορά την ασφαλή πρόσβαση και διάδοση των πληροφοριών εν γένει και την προστασία της διανοητικής ιδιοκτησίας ειδικότερα. Ομοίως, δεδομένης της σημασίας και της αξίας που έχουν τα δεδομένα για τις δραστηριότητες των οντοτήτων, όταν βασίζονται σε υπηρεσίες μετασχηματισμού και ανάλυσης δεδομένων από τρίτα μέρη, οι οντότητες θα πρέπει να λαμβάνουν όλα τα κατάλληλα μέτρα κυβερνοασφάλειας.
- (46) Για την περαιτέρω αντιμετώπιση των βασικών κινδύνων της αλυσίδας εφοδιασμού και την παροχή βοήθειας σε οντότητες οι οποίες δραστηριοποιούνται σε τομείς που καλύπτονται από την παρούσα οδηγία με σκοπό την κατάλληλη διαχείριση των κινδύνων για την κυβερνοασφάλεια που σχετίζονται με την αλυσίδα εφοδιασμού και τους προμηθευτές, η ομάδα συνεργασίας στην οποία συμμετέχουν αρμόδιες εθνικές αρχές, σε συνεργασία με την Επιτροπή και τον ENISA, θα πρέπει να διενεργεί συντονισμένες τομεακές εκτιμήσεις κινδύνου στην αλυσίδα εφοδιασμού, όπως έγινε ήδη για τα δίκτυα 5G κατόπιν της σύστασης (ΕΕ) 2019/534 για την κυβερνοασφάλεια των δικτύων 5G<sup>21</sup>, με στόχο τον εντοπισμό ανά τομέα των κρίσιμων υπηρεσιών, συστημάτων ή προϊόντων ΤΠΕ, των σχετικών απειλών και των τρωτών σημείων.

---

<sup>21</sup> Σύσταση (ΕΕ) 2019/534 της Επιτροπής, της 26ης Μαρτίου 2019, Κυβερνοασφάλεια δικτύων 5G (ΕΕ L 88 της 29.3.2019, σ. 42).

- (47) Οι εκτιμήσεις κινδύνου στην αλυσίδα εφοδιασμού, υπό το πρίσμα των χαρακτηριστικών του οικείου τομέα, θα πρέπει να λαμβάνουν υπόψη τόσο τεχνικούς όσο και, κατά περίπτωση, μη τεχνικούς παράγοντες, συμπεριλαμβανομένων εκείνων που ορίζονται στη σύσταση (ΕΕ) 2019/534, στην πανευρωπαϊκή συντονισμένη εκτίμηση κινδύνου της ασφάλειας των δικτύων 5G και στην εργαλειοθήκη της ΕΕ για την κυβερνοασφάλεια των δικτύων 5G που συμφωνήθηκε από την ομάδα συνεργασίας. Ο προσδιορισμός των αλυσίδων εφοδιασμού που θα πρέπει να υποβάλλονται σε συντονισμένη εκτίμηση κινδύνου θα πρέπει να γίνεται με γνώμονα τα ακόλουθα κριτήρια: i) τον βαθμό στον οποίο βασικές και σημαντικές οντότητες χρησιμοποιούν και βασίζονται σε συγκεκριμένες κρίσιμες υπηρεσίες, συστήματα ή προϊόντα ΤΠΕ· ii) τη σημασία συγκεκριμένων κρίσιμων υπηρεσιών, συστημάτων ή προϊόντων ΤΠΕ για την εκτέλεση κρίσιμων ή ευαίσθητων λειτουργιών, συμπεριλαμβανομένης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· iii) τη διαθεσιμότητα εναλλακτικών υπηρεσιών, συστημάτων ή προϊόντων ΤΠΕ· iv) την ανθεκτικότητα του συνόλου της αλυσίδας εφοδιασμού υπηρεσιών, συστημάτων ή προϊόντων ΤΠΕ έναντι γεγονότων που προκαλούν διαταραχές και v) όσον αφορά αναδιδόμενες υπηρεσίες, συστήματα ή προϊόντα ΤΠΕ, τη δυνητική μελλοντική τους σημασία για τις δραστηριότητες των οντοτήτων.
- (48) Για τον εξορθολογισμό των νομικών υποχρεώσεων που επιβάλλονται στους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών και στους παρόχους υπηρεσιών εμπιστοσύνης που σχετίζονται με την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων, καθώς και για να δοθεί η δυνατότητα στις εν λόγω οντότητες και στις αντίστοιχες αρμόδιες αρχές τους να επωφεληθούν από το νομικό πλαίσιο που θεσπίζεται με την παρούσα οδηγία (συμπεριλαμβανομένου του ορισμού των CSIRT που είναι υπεύθυνες για τον χειρισμό κινδύνων και περιστατικών, της συμμετοχής των αρμόδιων αρχών και φορέων στις εργασίες της ομάδας συνεργασίας και του δικτύου CSIRT), θα πρέπει να συμπεριληφθούν στο πεδίο εφαρμογής της παρούσας οδηγίας. Συνεπώς, οι αντίστοιχες διατάξεις του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>22</sup> και της οδηγίας (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>23</sup> σχετικά με την επιβολή απαιτήσεων ασφάλειας και κοινοποίησης σε αυτούς τους τύπους οντοτήτων, θα πρέπει να καταργηθούν.

<sup>22</sup> Κανονισμός (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ (ΕΕ L 257 της 28.8.2014, σ. 73).

<sup>23</sup> Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (ΕΕ L 321 της 17.12.2018, σ. 36).

- (48a) Οι υποχρεώσεις ασφάλειας που ορίζονται στην παρούσα οδηγία θα πρέπει να θεωρούνται συμπληρωματικές προς τις απαιτήσεις που επιβάλλονται στους παρόχους υπηρεσιών εμπιστοσύνης δυνάμει του κανονισμού (ΕΕ) αριθ. 910/2014 (κανονισμός eIDAS). Θα πρέπει να ζητείται από τους παρόχους υπηρεσιών εμπιστοσύνης να λαμβάνουν όλα τα κατάλληλα και αναλογικά μέτρα για τη διαχείριση των κινδύνων που διατρέχουν οι υπηρεσίες τους, μεταξύ άλλων έναντι των πελατών και των εξαρτώμενων τρίτων μερών, και να αναφέρουν περιστατικά ασφάλειας δυνάμει της παρούσας οδηγίας. Οι εν λόγω υποχρεώσεις ασφάλειας και αναφοράς περιστατικών θα πρέπει να αφορούν και τη φυσική προστασία της παρεχόμενης υπηρεσίας. Το άρθρο 24 του κανονισμού (ΕΕ) αριθ. 910/2014 εξακολουθεί να ισχύει.
- (48α) Τα κράτη μέλη μπορούν να αναθέσουν τον ρόλο των αρμόδιων αρχών για τις υπηρεσίες εμπιστοσύνης στους εποπτικούς φορείς που προβλέπει ο κανονισμός eIDAS (εποπτικοί φορείς eIDAS), προκειμένου να εξασφαλιστεί η συνέχιση των τρεχουσών πρακτικών και να αξιοποιηθούν οι γνώσεις και η πείρα που έχουν αποκτηθεί κατά την εφαρμογή του κανονισμού eIDAS. Όταν ο ρόλος αυτός ανατίθεται σε διαφορετικό φορέα, οι αρμόδιες εθνικές αρχές δυνάμει της παρούσας οδηγίας θα πρέπει να συνεργάζονται μαζί του στενά και εγκαίρως, ανταλλάσσοντας τις σχετικές πληροφορίες, προκειμένου να εξασφαλίζεται η αποτελεσματική εποπτεία και συμμόρφωση των παρόχων υπηρεσιών εμπιστοσύνης με τις απαιτήσεις που ορίζονται στην παρούσα οδηγία και στον κανονισμό [XXXX/XXXX].

Κατά περίπτωση, η αρμόδια εθνική αρχή δυνάμει της παρούσας οδηγίας θα πρέπει να ενημερώνει αμέσως τον εποπτικό φορέα eIDAS για τυχόν κοινοποιηθείσα σημαντική απειλή ή περιστατικό κυβερνοασφάλειας με επιπτώσεις σε υπηρεσίες εμπιστοσύνης, καθώς και για τυχόν μη συμμόρφωση ενός παρόχου υπηρεσιών εμπιστοσύνης με τις απαιτήσεις της παρούσας οδηγίας. Για τους σκοπούς της αναφοράς, τα κράτη μέλη μπορούν να χρησιμοποιούν, κατά περίπτωση, το ενιαίο σημείο εισόδου που έχει θεσπιστεί για την επίτευξη κοινής και αυτόματης αναφοράς περιστατικών τόσο στον εποπτικό φορέα eIDAS όσο και στην αρμόδια αρχή δυνάμει της παρούσας οδηγίας. Οι κανόνες σχετικά με τις υποχρεώσεις αναφοράς περιστατικών δεν θα πρέπει να θίγουν τον κανονισμό (ΕΕ) 2016/679 και την οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>24</sup>.

<sup>24</sup> Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ L 201 της 31.7.2002, σ. 37).

- (49) Κατά περίπτωση, και για την αποφυγή περιττών διαταραχών, οι υφιστάμενες εθνικές κατευθυντήριες γραμμές [...] που έχουν θεσπιστεί για τη μεταφορά στο εθνικό δίκαιο των κανόνων σχετικά με τα μέτρα ασφάλειας που ορίζονται στο άρθρο 40 [...] και στο άρθρο 41 της οδηγίας (ΕΕ) 2018/1972, [...] **θα πρέπει να ληφθούν υπόψη στις ρυθμίσεις που εφαρμόζουν τα κράτη μέλη για τη μεταφορά της παρούσας οδηγίας στο εθνικό δίκαιο, ώστε να αξιοποιηθούν οι γνώσεις και οι δεξιότητες που αποκτήθηκαν στο πλαίσιο της οδηγίας (ΕΕ) 2018/1972 σχετικά με τα μέτρα διαχείρισης κινδύνων ασφάλειας και τις κοινοποιήσεις περιστατικών. Ο ENISA μπορεί επίσης να καταρτίσει κατευθυντήριες γραμμές σχετικά με τις απαιτήσεις ασφάλειας και αναφοράς περιστατικών για τους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, προκειμένου να διευκολυνθούν η εναρμόνιση, η μετάβαση και η ελαχιστοποίηση των διαταραχών. Τα κράτη μέλη μπορούν να αναθέσουν στις εθνικές ρυθμιστικές αρχές τον ρόλο των αρμόδιων αρχών για τις ηλεκτρονικές επικοινωνίες, προκειμένου να εξασφαλιστεί η συνέχιση των τρεχουσών πρακτικών και να αξιοποιηθούν οι γνώσεις και η πείρα που αποκτήθηκαν στο πλαίσιο της οδηγίας (ΕΕ) 2018/1972.**
- (50) Δεδομένης της αυξανόμενης σημασίας των υπηρεσιών διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμών, είναι αναγκαίο να εξασφαλίζεται ότι οι εν λόγω υπηρεσίες θα υπόκεινται επίσης σε κατάλληλες απαιτήσεις ασφάλειας σύμφωνα με τον συγκεκριμένο χαρακτήρα τους και την οικονομική τους σημασία. Οι πάροχοι των εν λόγω υπηρεσιών θα πρέπει, συνεπώς, να διασφαλίζουν επίσης ένα επίπεδο ασφάλειας των δικτυακών και πληροφοριακών συστημάτων ανάλογο προς τον εκάστοτε κίνδυνο. Δεδομένου ότι οι πάροχοι υπηρεσιών διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμών κατά κανόνα δεν ασκούν πραγματικό έλεγχο επί της μετάδοσης σημάτων μέσω δικτύων, ο βαθμός κινδύνου για τις εν λόγω υπηρεσίες μπορεί να θεωρηθεί, από ορισμένες απόψεις, χαμηλότερος από ό,τι για τις παραδοσιακές υπηρεσίες ηλεκτρονικών επικοινωνιών. Το ίδιο ισχύει και για τις υπηρεσίες διαπροσωπικών επικοινωνιών που χρησιμοποιούν αριθμούς και δεν ασκούν πραγματικό έλεγχο επί της μετάδοσης σημάτων.



- (51) Η εσωτερική αγορά εξαρτάται περισσότερο από ποτέ από τη λειτουργία του διαδικτύου. Οι υπηρεσίες όλων, σχεδόν, των βασικών και των σημαντικών οντοτήτων εξαρτώνται από τις υπηρεσίες που παρέχονται μέσω του διαδικτύου. Προκειμένου να διασφαλιστεί η ομαλή παροχή υπηρεσιών που παρέχονται από βασικές και σημαντικές οντότητες, είναι σημαντικά τα δημόσια δίκτυα ηλεκτρονικών επικοινωνιών, όπως, για παράδειγμα, οι βασικοί κορμοί του διαδικτύου ή τα υποβρύχια καλώδια επικοινωνιών, να διαθέτουν κατάλληλα μέτρα κυβερνοασφάλειας και να αναφέρουν τα σχετικά περιστατικά.
- (52) Κατά [...] **περίπτωση**, οι οντότητες θα πρέπει να ενημερώνουν τους αποδέκτες των υπηρεσιών τους για συγκεκριμένα [...] μέτρα που μπορούν να λάβουν για να μετριάσουν τον κίνδυνο που συνεπάγεται γι' αυτές **μια σημαντική κυβερνοαπειλή. Οι οντότητες θα πρέπει, κατά περίπτωση, και ιδίως σε περιπτώσεις στις οποίες μπορεί να πραγματοποιηθεί η σημαντική κυβερνοαπειλή, να ενημερώνουν και τους αποδέκτες των υπηρεσιών τους, παράλληλα με τις αρμόδιες αρχές ή τις CSIRT, σχετικά με την ίδια την απειλή.** Η απαίτηση να ενημερώνονται οι εν λόγω αποδέκτες σχετικά με τέτοιες απειλές, δεν θα πρέπει να απαλλάσσει τις οντότητες από την υποχρέωση να λαμβάνουν, με ίδιες δαπάνες, κατάλληλα και άμεσα μέτρα για την αποτροπή κυβερνοαπειλών ή την επανόρθωση τυχόν συνεπειών τους και για την αποκατάσταση του κανονικού επιπέδου ασφάλειας. Η σχετική ενημέρωση προς τους αποδέκτες σχετικά με **κυβερνοαπειλές [...]** θα πρέπει να παρέχεται δωρεάν.
- (53) Ειδικότερα, οι πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών θα πρέπει να ενημερώνουν τους αποδέκτες υπηρεσιών σχετικά με ιδιαίτερες και σημαντικές κυβερνοαπειλές και σχετικά με τα μέτρα προστασίας που μπορούν να λαμβάνουν για την ασφάλεια των επικοινωνιών τους, για παράδειγμα χρησιμοποιώντας συγκεκριμένους τύπους λογισμικού ή τεχνολογίες κρυπτογράφησης.

- (54) Προκειμένου να διαφυλαχθεί η ασφάλεια των δικτύων και των υπηρεσιών ηλεκτρονικών επικοινωνιών, θα πρέπει να προωθηθεί η χρήση της κρυπτογράφησης, και ιδίως της διατερματικής κρυπτογράφησης, και, όπου απαιτείται, αυτή θα πρέπει να είναι υποχρεωτική για τους παρόχους των εν λόγω υπηρεσιών και δικτύων, σύμφωνα με τις αρχές της ασφάλειας και της ιδιωτικότητας εκ προεπιλογής και εκ σχεδιασμού, για τους σκοπούς του άρθρου 18. Η χρήση της διατερματικής κρυπτογράφησης θα πρέπει να συμβιβάζεται με τις εξουσίες των κρατών μελών να διασφαλίζουν την προστασία των ουσιωδών συμφερόντων ασφάλειας και δημόσιας ασφάλειάς τους και να επιτρέπουν τη διερεύνηση, τον εντοπισμό και τη δίωξη ποινικών αδικημάτων σύμφωνα με το δίκαιο της Ένωσης. Οι λύσεις για τη νόμιμη πρόσβαση σε πληροφορίες σε διατερματικές κρυπτογραφημένες επικοινωνίες θα πρέπει να διατηρούν την αποτελεσματικότητα της κρυπτογράφησης όσον αφορά την προστασία της ιδιωτικής ζωής και της ασφάλειας των επικοινωνιών, παρέχοντας παράλληλα αποτελεσματική άμυνα κατά της εγκληματικότητας.
- (55) Η παρούσα οδηγία θεσπίζει μια προσέγγιση δύο σταδίων ως προς την αναφορά περιστατικών, προκειμένου να επιτευχθεί η σωστή ισορροπία μεταξύ, αφενός, της ταχείας αναφοράς, που συμβάλλει στον μετριασμό της πιθανής εξάπλωσης συμβάντων και επιτρέπει στις οντότητες να αναζητούν στήριξη και, αφετέρου, της υποβολής εμπειρισταωμένων αναφορών που αντλούν πολύτιμα διδάγματα από μεμονωμένα περιστατικά και βελτιώνουν με την πάροδο του χρόνου την ανθεκτικότητα μεμονωμένων εταιρειών και ολόκληρων τομέων έναντι των κυβερνοαπειλών. Όταν οι οντότητες λαμβάνουν γνώση περιστατικού, θα πρέπει να υποχρεούνται να υποβάλουν αρχική κοινοποίηση εντός 24 ωρών, ακολουθούμενη από τελική έκθεση το αργότερο ένα μήνα μετά. Η αρχική κοινοποίηση θα πρέπει να περιλαμβάνει μόνο τις πληροφορίες που είναι απολύτως αναγκαίες για να ενημερωθούν οι αρμόδιες αρχές σχετικά με το περιστατικό και να δοθεί η δυνατότητα στην οντότητα να ζητήσει συνδρομή, εφόσον απαιτείται. Η εν λόγω κοινοποίηση, κατά περίπτωση, θα πρέπει να αναφέρει εάν το περιστατικό είναι πιθανόν να οφείλεται σε παράνομη ή κακόβουλη ενέργεια. Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι η απαίτηση υποβολής αυτής της αρχικής κοινοποίησης δεν εκτρέπει τους πόρους της αναφέρουσας οντότητας από δραστηριότητες που σχετίζονται με τον χειρισμό περιστατικών, στις οποίες θα πρέπει να δίνεται προτεραιότητα. Για να αποτραπεί το μελλοντικό ενδεχόμενο οι υποχρεώσεις αναφοράς περιστατικών είτε να εκτρέπουν πόρους από τον χειρισμό της αντιμετώπισης περιστατικών είτε να μπορούν με άλλον τρόπο να θέσουν σε κίνδυνο τις σχετικές προσπάθειες των οντοτήτων, τα κράτη μέλη θα πρέπει επίσης να προβλέπουν ότι, σε δεόντως αιτιολογημένες περιπτώσεις και σε συμφωνία με τις αρμόδιες αρχές ή την CSIRT, η εν λόγω οντότητα θα μπορεί να παρεκκλίνει από τις προθεσμίες των 24 ωρών για την αρχική κοινοποίηση και του ενός μήνα για την τελική έκθεση.

- (55a) Μια προορατική προσέγγιση όσον αφορά τις κυβερνοαπειλές αποτελεί ζωτικό στοιχείο της διαχείρισης κινδύνων κυβερνοασφάλειας που θα επιτρέψει στις αρμόδιες αρχές να αποτρέπουν αποτελεσματικά τη μετατροπή των κυβερνοαπειλών σε πραγματικά περιστατικά που ενδέχεται να προκαλέσουν σημαντικές υλικές ή μη υλικές ζημιές. Για τον σκοπό αυτό, η κοινοποίηση σημαντικών κυβερνοαπειλών είναι καίριας σημασίας.
- (56) Οι βασικές και οι σημαντικές οντότητες βρίσκονται συχνά αντιμέτωπες με καταστάσεις κατά τις οποίες ένα συγκεκριμένο περιστατικό, λόγω των χαρακτηριστικών του, πρέπει να αναφερθεί σε διαφορετικές αρχές, ως αποτέλεσμα των υποχρεώσεων κοινοποίησης που περιλαμβάνονται σε διάφορες νομικές πράξεις. Οι περιπτώσεις αυτές δημιουργούν πρόσθετες επιβαρύνσεις και ενδέχεται επίσης να οδηγήσουν σε αβεβαιότητες όσον αφορά τη μορφή και τις διαδικασίες των εν λόγω κοινοποιήσεων. Με βάση τα ανωτέρω και για τους σκοπούς της αναφοράς περιστατικών που θέτουν σε κίνδυνο την ασφάλεια, τα κράτη μέλη [...] **θα μπορούσαν** να θεσπίσουν ενιαίο σημείο εισόδου για όλες τις κοινοποιήσεις που απαιτούνται βάσει της παρούσας οδηγίας, καθώς και βάσει άλλων νομοθετικών πράξεων της Ένωσης, όπως ο κανονισμός (ΕΕ) 2016/679 και η οδηγία 2002/58/ΕΚ. Ο ENISA, σε συνεργασία με την ομάδα συνεργασίας, θα πρέπει να αναπτύξει κοινά υποδείγματα κοινοποίησης μέσω κατευθυντήριων γραμμών που θα απλουστεύουν και θα εξορθολογίζουν τις πληροφορίες αναφοράς που απαιτούνται από το δίκαιο της Ένωσης και θα μειώνουν τον φόρτο για τις εταιρείες.
- (57) Όταν υπάρχει υπόνοια ότι ένα περιστατικό σχετίζεται με σοβαρές εγκληματικές δραστηριότητες δυνάμει ενωσιακής ή εθνικής νομοθεσίας, τα κράτη μέλη θα πρέπει να παροτρύνουν τις βασικές και τις σημαντικές οντότητες με βάση τους ισχύοντες στο ενωσιακό δίκαιο κανόνες ποινικών διαδικασιών, να αναφέρουν περιστατικά εικαζόμενης σοβαρής εγκληματικής φύσεως στις αρμόδιες αρχές επιβολής του νόμου. Κατά περίπτωση, και με την επιφύλαξη των κανόνων προστασίας των δεδομένων προσωπικού χαρακτήρα που ισχύουν για την Ευρώπη, είναι επιθυμητό ο συντονισμός μεταξύ των αρμόδιων αρχών και των αρχών επιβολής του νόμου των διαφόρων κρατών μελών να διευκολύνεται από το EC3 και από τον ENISA.

- (58) Ως αποτέλεσμα περιστατικών, σε πολλές περιπτώσεις διακυβεύονται δεδομένα προσωπικού χαρακτήρα. Στο πλαίσιο αυτό, οι αρμόδιες αρχές θα πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες για όλα τα σχετικά θέματα με τις αρχές προστασίας δεδομένων και τις εποπτικές αρχές, σύμφωνα με την οδηγία 2002/58/ΕΚ.
- (59) Η διατήρηση ακριβών και πλήρων βάσεων δεδομένων ονομάτων τομέα και δεδομένων καταχώρισης (τα λεγόμενα «δεδομένα WHOIS») και η παροχή νόμιμης πρόσβασης στα εν λόγω δεδομένα είναι ουσιαστικής σημασίας για τη διασφάλιση της ασφάλειας, της σταθερότητας και της ανθεκτικότητας του DNS, γεγονός που με τη σειρά του συμβάλλει σε υψηλό κοινό επίπεδο κυβερνοασφάλειας εντός της Ένωσης. Όταν η επεξεργασία περιλαμβάνει δεδομένα προσωπικού χαρακτήρα, η εν λόγω επεξεργασία συμμορφώνεται με το δίκαιο της Ένωσης για την προστασία των δεδομένων.
- (60) Η διαθεσιμότητα των εν λόγω δεδομένων για τις δημόσιες αρχές και η έγκαιρη προσβασιμότητά τους από αυτές, συμπεριλαμβανομένων των αρμόδιων αρχών βάσει του ενωσιακού ή του εθνικού δικαίου για την πρόληψη, τη διερεύνηση ή τη δίωξη ποινικών αδικημάτων, των CERT, [...] των CSIRT και, όσον αφορά τα δεδομένα των πελατών τους, για παρόχους δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών και για παρόχους τεχνολογιών και υπηρεσιών κυβερνοασφάλειας που ενεργούν για λογαριασμό των εν λόγω πελατών, είναι ουσιαστικής σημασίας για την πρόληψη και την καταπολέμηση της κατάχρησης του συστήματος ονομάτων τομέα, ιδίως για την πρόληψη, τον εντοπισμό και την αντιμετώπιση περιστατικών κυβερνοασφάλειας. Η εν λόγω πρόσβαση θα πρέπει να συμμορφώνεται με τη νομοθεσία της Ένωσης για την προστασία των δεδομένων στον βαθμό που σχετίζεται με δεδομένα προσωπικού χαρακτήρα.
- (61) Προκειμένου να διασφαλιστεί η διαθεσιμότητα ακριβών και πλήρων δεδομένων καταχώρισης ονομάτων τομέα, τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD (οι αποκαλούμενοι καταχωρητές), θα πρέπει να συλλέγουν και να εγγυώνται την ακεραιότητα και τη διαθεσιμότητα των δεδομένων καταχώρισης ονομάτων τομέα. **Όσον αφορά τα δεδομένα καταχώρισης, οι οντότητες θα πρέπει ιδίως να επαληθεύουν την επωνυμία και τη διεύθυνση ηλεκτρονικού ταχυδρομείου του καταχωρίζοντος.** [...] Τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD θα πρέπει να θεσπίσουν πολιτικές και διαδικασίες για τη συλλογή και τη διατήρηση ακριβών και πλήρων δεδομένων καταχώρισης, καθώς και για την πρόληψη και διόρθωση ανακριβών δεδομένων καταχώρισης σύμφωνα με τους κανόνες της Ένωσης για την προστασία των δεδομένων.

(62) Τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για αυτά θα πρέπει να δημοσιοποιούν δεδομένα καταχώρισης ονομάτων τομέα που δεν εμπίπτουν στο πεδίο εφαρμογής των κανόνων της Ένωσης για την προστασία των δεδομένων, όπως δεδομένα που αφορούν νομικά πρόσωπα<sup>25</sup>. Τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD θα πρέπει επίσης να καθιστούν δυνατή τη νόμιμη πρόσβαση από νόμιμους αιτούντες πρόσβαση σε συγκεκριμένα δεδομένα καταχώρισης ονομάτων τομέα που αφορούν φυσικά πρόσωπα, σύμφωνα με το δίκαιο της Ένωσης για την προστασία των δεδομένων. Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για λογαριασμό τους θα πρέπει να ανταποκρίνονται χωρίς αδικαιολόγητη καθυστέρηση σε αιτήματα [...] που αφορούν τη γνωστοποίηση δεδομένων καταχώρισης ονομάτων τομέα **από νόμιμους αιτούντες πρόσβαση, όπως αρμόδιες αρχές βάσει του ενωσιακού ή του εθνικού δικαίου στον τομέα της εθνικής ασφάλειας και της ποινικής δικαιοσύνης ή CSIRT**. Τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για λογαριασμό τους θα πρέπει να θεσπίσουν πολιτικές και διαδικασίες για τη δημοσίευση και γνωστοποίηση δεδομένων καταχώρισης, συμπεριλαμβανομένων συμφωνιών σε επίπεδο υπηρεσιών για την αντιμετώπιση αιτημάτων πρόσβασης από νόμιμους αιτούντες πρόσβαση. Η διαδικασία πρόσβασης μπορεί επίσης να περιλαμβάνει τη χρήση διεπαφής, πύλης ή άλλου τεχνικού εργαλείου για την παροχή αποτελεσματικού συστήματος υποβολής αιτημάτων για δεδομένα καταχώρισης και την πρόσβαση σε αυτά. **Τα κράτη μέλη θα πρέπει να εξασφαλίζουν ότι κάθε είδους πρόσβαση σε δεδομένα καταχώρισης τομέα (δεδομένα προσωπικού και μη προσωπικού χαρακτήρα) παρέχεται δωρεάν**. Με σκοπό την προώθηση εναρμονισμένων πρακτικών σε ολόκληρη την εσωτερική αγορά, η Επιτροπή μπορεί να εκδίδει κατευθυντήριες γραμμές σχετικά με τις εν λόγω διαδικασίες, με την επιφύλαξη των αρμοδιοτήτων του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, **σύμφωνα με τα διεθνή πρότυπα που έχει αναπτύξει η πολυμερής κοινότητα και συμπληρωματικά προς αυτά**.

<sup>25</sup> Κανονισμός (ΕΕ) 2016/679 [...] του [...] Ευρωπαϊκού Κοινοβουλίου [...] και [...] του [...] Συμβουλίου, αιτιολογική σκέψη (14) βάσει της οποίας «ο παρών κανονισμός δεν καλύπτει την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν νομικά πρόσωπα και ιδίως επιχειρήσεις συσταθείσες ως νομικά πρόσωπα, περιλαμβανομένων της επωνυμίας, του τύπου και των στοιχείων επικοινωνίας του νομικού προσώπου».

- (63) [...] Οι βασικές και οι σημαντικές οντότητες δυνάμει της παρούσας οδηγίας θα πρέπει να υπάγονται στη δικαιοδοσία του κράτους μέλους στο οποίο παρέχουν τις υπηρεσίες τους. **Οι οντότητες των σημείων 1 έως 7 και 10 του παραρτήματος I, οι πάροχοι υπηρεσιών εμπιστοσύνης και οι πάροχοι σημείων ανταλλαγής κίνησης διαδικτύου του σημείου 8 του παραρτήματος I και των σημείων 1 έως 5 του παραρτήματος II της παρούσας οδηγίας θα πρέπει να υπάγονται στη δικαιοδοσία του κράτους μέλους στο οποίο είναι εγκατεστημένοι.** Εάν η οντότητα παρέχει υπηρεσίες ή έχει εγκατάσταση σε περισσότερα του ενός κράτη μέλη, θα πρέπει να υπάγεται στη χωριστή και συντρέχουσα δικαιοδοσία καθενός από τα εν λόγω κράτη μέλη. Οι αρμόδιες αρχές των εν λόγω κρατών μελών θα πρέπει να συνεργάζονται, να παρέχουν αμοιβαία συνδρομή μεταξύ τους και, κατά περίπτωση, να εκτελούν κοινές εποπτικές δράσεις. **Όταν τα κράτη μέλη αποφασίζουν να ασκήσουν δικαιοδοσία, θα πρέπει να αποφεύγουν την επιβολή περισσότερων της μίας κυρώσεων για την ίδια συμπεριφορά που συνιστά παράβαση των υποχρεώσεων που προβλέπονται στην παρούσα οδηγία.**
- (64) Προκειμένου να ληφθεί υπόψη ο διασυνοριακός χαρακτήρας των υπηρεσιών και των δραστηριοτήτων των παρόχων υπηρεσιών DNS, των μητρώων ονομάτων TLD, **των οντοτήτων που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD**, των παρόχων δικτύου διανομής περιεχομένου, των παρόχων υπηρεσιών νεφοϋπολογιστικής, των παρόχων υπηρεσιών κέντρου δεδομένων και των παρόχων ψηφιακών υπηρεσιών, μόνο ένα κράτος μέλος θα πρέπει να έχει δικαιοδοσία επί των εν λόγω οντοτήτων. Η δικαιοδοσία θα πρέπει να ανατίθεται στο κράτος μέλος στο οποίο η αντίστοιχη οντότητα έχει την κύρια εγκατάστασή της στην Ένωση. Το κριτήριο της εγκατάστασης για τους σκοπούς της παρούσας οδηγίας συνεπάγεται την πραγματική άσκηση δραστηριότητας μέσω σταθερών εγκαταστάσεων. Από αυτή την άποψη, ο νομικός τύπος των ρυθμίσεων αυτών, είτε πρόκειται για παράρτημα είτε για θυγατρική με νομική προσωπικότητα, δεν είναι καθοριστικής σημασίας.

Το κατά πόσον πληρούται το κριτήριο αυτό δεν θα πρέπει να εξαρτάται από το αν τα δικτυακά και πληροφοριακά συστήματα βρίσκονται σε συγκεκριμένο τόπο· η παρουσία και η χρήση τέτοιων συστημάτων δεν συνιστούν από μόνες τους βασική εγκατάσταση και συνεπώς δεν συνιστούν αποφασιστικά κριτήρια για τον καθορισμό της βασικής εγκατάστασης. Η κύρια εγκατάσταση θα πρέπει να είναι ο τόπος όπου λαμβάνονται **κατά κύριο λόγο** στην Ένωση οι αποφάσεις που σχετίζονται με τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας. Αυτό συνήθως αντιστοιχεί στον τόπο της κεντρικής διοίκησης των εταιρειών εντός της Ένωσης. **Εάν δεν μπορεί να καθοριστεί ο τόπος όπου λαμβάνονται κατά κύριο λόγο οι αποφάσεις αυτές ή εάν οι αποφάσεις αυτές δεν λαμβάνονται εντός της Ένωσης**, η κύρια εγκατάσταση θα πρέπει να θεωρείται ότι βρίσκεται στα κράτη μέλη όπου η οντότητα διαθέτει εγκατάσταση με τον μεγαλύτερο αριθμό εργαζομένων στην Ένωση. Όταν οι υπηρεσίες παρέχονται από όμιλο επιχειρήσεων, η κύρια εγκατάσταση της ελέγχουσας επιχείρησης θα πρέπει να θεωρείται ως η κύρια εγκατάσταση του ομίλου επιχειρήσεων.

**(64α)** Όταν ένας πάροχος δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών παρέχει υπηρεσία αναδρομικής επίλυσης ονομάτων τομέα μόνο ως μέρος της υπηρεσίας πρόσβασης στο διαδίκτυο, η οντότητα θα πρέπει να θεωρείται ότι υπάγεται στη δικαιοδοσία όλων των κρατών μελών στα οποία παρέχει τις υπηρεσίες της.

**(64αα)** Προκειμένου να εξασφαλιστεί σαφής επισκόπηση των παρόχων υπηρεσιών DNS, των μητρικών ονομάτων TLD, των οντοτήτων που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD, των παρόχων δικτύων διανομής περιεχομένου, των παρόχων υπηρεσιών νεφοϋπολογιστικής, των παρόχων υπηρεσιών κέντρου δεδομένων και των ψηφιακών παρόχων που παρέχουν υπηρεσίες σε ολόκληρη την Ένωση και εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, ο ENISA θα πρέπει να δημιουργήσει και να διατηρεί μητρώο για τις εν λόγω οντότητες, βάσει κοινοποιήσεων που λαμβάνουν τα κράτη μέλη, κατά περίπτωση μέσω των εθνικών τους μηχανισμών αυτοκοινοποίησης. Προκειμένου να εξασφαλιστεί η ακρίβεια και η πληρότητα των πληροφοριών που θα πρέπει να περιλαμβάνονται στο μητρώο αυτό, τα κράτη μέλη θα πρέπει να υποβάλλουν στον ENISA τις πληροφορίες που είναι διαθέσιμες στα εθνικά τους μητρώα σχετικά με τις εν λόγω οντότητες. Ο ENISA και τα κράτη μέλη θα πρέπει να λάβουν μέτρα για να διευκολύνουν τη διαλειτουργικότητα των εν λόγω μητρώων, διασφαλίζοντας παράλληλα την προστασία των εμπιστευτικών ή διαβαθμισμένων πληροφοριών.

(65) Σε περιπτώσεις που πάροχος υπηρεσιών DNS, μητρώο ονομάτων TLD, πάροχος δικτύου διανομής περιεχομένου, πάροχος υπηρεσιών νεφούπολογιστικής, πάροχος υπηρεσιών κέντρου δεδομένων και πάροχος ψηφιακών υπηρεσιών ο οποίος δεν είναι εγκατεστημένος στην Ένωση προσφέρει υπηρεσίες εντός της Ένωσης, θα πρέπει να ορίσει εκπρόσωπο. Για να προσδιοριστεί κατά πόσον μια τέτοια οντότητα προσφέρει υπηρεσίες εντός της Ένωσης, θα πρέπει να εξακριβώνεται αν είναι προφανές ότι η εν λόγω οντότητα σκοπεύει να προσφέρει υπηρεσίες σε πρόσωπα σε ένα ή περισσότερα κράτη μέλη. Η προσβασιμότητα εντός της Ένωσης του ιστοτόπου της οντότητας ή μεσάζοντα ή διεύθυνσης ηλεκτρονικού ταχυδρομείου και άλλων στοιχείων επικοινωνίας, ή η χρήση γλώσσας που χρησιμοποιείται γενικά στην τρίτη χώρα όπου είναι εγκατεστημένος ο πάροχος ψηφιακών υπηρεσιών δεν αρκούν από μόνες τους για να εξακριβωθεί τέτοια πρόθεση. Ωστόσο, άλλοι παράγοντες όπως η χρήση γλώσσας ή νομίσιματος που χρησιμοποιείται γενικά σε ένα ή περισσότερα κράτη μέλη με δυνατότητα παραγγελίας υπηρεσιών σε αυτή την άλλη γλώσσα ή οι αναφορές σε καταναλωτές ή χρήστες που βρίσκονται στην Ένωση μπορούν να καθιστούν προφανή την πρόθεση της οντότητας να προσφέρει υπηρεσίες εντός της Ένωσης. Ο εκπρόσωπος πρέπει να ενεργεί εξ ονόματος της οντότητας και οι αρμόδιες αρχές ή οι CSIRT θα πρέπει να έχουν τη δυνατότητα να έρχονται σε επαφή με αυτόν. Ο εκπρόσωπος θα πρέπει να ορίζεται ρητώς με γραπτή εντολή της οντότητας να ενεργεί για λογαριασμό του τελευταίου όσον αφορά τις υποχρεώσεις του που απορρέουν από την παρούσα οδηγία, συμπεριλαμβανομένης της αναφοράς περιστατικών.



- (66) Σε περίπτωση ανταλλαγής, αναφοράς ή με άλλο τρόπο κοινοποίησης πληροφοριών που θεωρούνται διαβαθμισμένες σύμφωνα με το εθνικό ή το ενωσιακό δίκαιο δυνάμει των διατάξεων της παρούσας οδηγίας, θα πρέπει να εφαρμόζονται οι αντίστοιχοι ειδικοί κανόνες για τον χειρισμό διαβαθμισμένων πληροφοριών.
- (67) Καθώς οι κυβερνοαπειλές καθίστανται ολοένα και πιο πολύπλοκες και εξελιγμένες, η λήψη άρτιων μέτρων εντοπισμού και πρόληψης εξαρτώνται σε μεγάλο βαθμό από την τακτική ανταλλαγή πληροφοριών και στοιχείων μεταξύ των οντοτήτων σχετικά με τις απειλές και τα τρωτά σημεία. Η ανταλλαγή πληροφοριών συμβάλλει στην αύξηση της ευαισθητοποίησης σχετικά με τις κυβερνοαπειλές, η οποία ενισχύει με τη σειρά της την ικανότητα των οντοτήτων να αποτρέπουν τη μετατροπή απειλών σε πραγματικά περιστατικά, ενώ παρέχει επίσης στις οντότητες τη δυνατότητα να περιορίζουν καλύτερα τις επιπτώσεις των περιστατικών και να εξασφαλίζουν την αποκατάστασή τους με αποτελεσματικότερο τρόπο. Ελλείψει καθοδήγησης σε επίπεδο Ένωσης, φαίνεται ότι η παρεμπόδιση της ανταλλαγής στοιχείων αυτού του είδους οφείλεται σε διάφορους παράγοντες, κυρίως στην αβεβαιότητα ως προς τη συμβατότητα με τους κανόνες ανταγωνισμού και τους κανόνες περί ευθύνης.
- (68) Οι οντότητες θα πρέπει να ενθαρρύνονται να αξιοποιούν συλλογικά τις επιμέρους γνώσεις και την πρακτική εμπειρία που διαθέτουν σε στρατηγικό, τακτικό και επιχειρησιακό επίπεδο, με σκοπό την ενίσχυση των ικανοτήτων τους ώστε να είναι σε θέση να αξιολογούν, να παρακολουθούν, να υπερασπίζονται και να αντιμετωπίζουν δεόντως κυβερνοαπειλές. Ως εκ τούτου, είναι αναγκαίο να καταστεί δυνατή η δημιουργία μηχανισμών εθελούσιας ανταλλαγής πληροφοριών σε επίπεδο Ένωσης. Για τον σκοπό αυτό, τα κράτη μέλη θα πρέπει να υποστηρίζουν ενεργά και να ενθαρρύνουν επίσης τις σχετικές οντότητες που δεν καλύπτονται από το πεδίο εφαρμογής της παρούσας οδηγίας να συμμετέχουν στους εν λόγω μηχανισμούς ανταλλαγής πληροφοριών. Οι εν λόγω μηχανισμοί θα πρέπει να εφαρμόζονται σε πλήρη συμμόρφωση με τους κανόνες ανταγωνισμού της Ένωσης, καθώς και με τους κανόνες του ενωσιακού δικαίου για την προστασία των δεδομένων.

- (69) [...] Στον βαθμό που είναι απολύτως αναγκαία και αναλογική για τους σκοπούς της προστασίας της δικτυακής και πληροφοριακής ασφάλειας, **η επεξεργασία δεδομένων προσωπικού χαρακτήρα από βασικές και σημαντικές οντότητες [...]** και από παρόχους τεχνολογιών και υπηρεσιών ασφάλειας **θα μπορούσε να θεωρείται απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση ή [...]** να συνιστά έννομο συμφέρον του ενδιαφερόμενου υπευθύνου επεξεργασίας δεδομένων [...], όπως αναφέρεται στον κανονισμό (ΕΕ) 2016/679. Στο πλαίσιο αυτό θα **μπορούσαν [...]** να περιλαμβάνονται μέτρα σχετικά με την πρόληψη, τον εντοπισμό, την ανάλυση και την αντιμετώπιση περιστατικών, μέτρα για την ευαισθητοποίηση σχετικά με συγκεκριμένες κυβερνοαπειλές, την ανταλλαγή πληροφοριών στο πλαίσιο της αποκατάστασης τρωτών σημείων και της συντονισμένης γνωστοποίησης, καθώς και την εθελούσια ανταλλαγή πληροφοριών σχετικά με τα εν λόγω περιστατικά, [...] τις κυβερνοαπειλές και τα τρωτά σημεία, τους δείκτες συμβιβασμού, τις τακτικές, τις τεχνικές και τις διαδικασίες, τις ειδοποιήσεις επαγρύπνησης για την κυβερνοασφάλεια και τα εργαλεία διαμόρφωσης. Τα μέτρα αυτά μπορεί να απαιτούν την επεξεργασία [...] **διάφορων τύπων δεδομένων προσωπικού χαρακτήρα, όπως:** διευθύνσεις IP, ενιαίους εντοπιστές πόρων (URL), ονόματα τομέα και διευθύνσεις ηλεκτρονικού ταχυδρομείου. **Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές, SPOC και CSIRT θα πρέπει να ορίζεται στην εθνική νομοθεσία και να θεωρείται απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση ή για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, όπως αναφέρεται στο άρθρο 6 παράγραφος 1 στοιχείο γ) ή ε) του κανονισμού (ΕΕ) 2016/679.**
- (69α) Τα κράτη μέλη μπορούν να θεσπίζουν νομοθετικές διατάξεις που επιτρέπουν στις αρμόδιες αρχές, τα SPOC και τις CSIRT, στον βαθμό που αυτό είναι απολύτως αναγκαίο και αναλογικό για τον σκοπό της διασφάλισης της ασφάλειας των δικτυακών και πληροφοριακών συστημάτων των βασικών και των σημαντικών οντοτήτων, να επεξεργάζονται ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα σύμφωνα με το άρθρο 9 [...] του κανονισμού (ΕΕ) 2016/679, ιδίως με την πρόβλεψη κατάλληλων και ειδικών μέτρων για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων των φυσικών προσώπων, μεταξύ των οποίων τεχνικοί περιορισμοί όσον αφορά την περαιτέρω χρήση των εν λόγω δεδομένων και η χρήση προηγμένων μέτρων ασφάλειας και προστασίας της ιδιωτικής ζωής, όπως η ψευδωνυμοποίηση, ή η κρυπτογράφηση όταν η ανωνυμοποίηση ενδέχεται να επηρεάσει τον επιδιωκόμενο σκοπό.

(70) Προκειμένου να ενισχυθούν οι εποπτικές εξουσίες και οι δράσεις που συμβάλλουν στη διασφάλιση της αποτελεσματικής συμμόρφωσης, η παρούσα οδηγία θα πρέπει να προβλέπει έναν ελάχιστο κατάλογο εποπτικών δράσεων και μέσων με τα οποία οι αρμόδιες αρχές **μπορούν [...] να εποπτεύουν βασικές και σημαντικές οντότητες.** Επιπλέον, η παρούσα οδηγία θα πρέπει να καθιερώνει μια διαφοροποίηση του εποπτικού καθεστώτος μεταξύ βασικών και σημαντικών οντοτήτων, με σκοπό την εξασφάλιση δίκαιης ισορροπίας των υποχρεώσεων τόσο για τις οντότητες όσο και για τις αρμόδιες αρχές. Ως εκ τούτου, οι βασικές οντότητες θα πρέπει να υπόκεινται σε πλήρες καθεστώς εποπτείας (εκ των προτέρων και εκ των υστέρων), ενώ οι σημαντικές οντότητες θα πρέπει να υπόκεινται σε απλοποιημένο, μόνο εκ των υστέρων, εποπτικό καθεστώς. Για την τελευταία περίπτωση, αυτό σημαίνει ότι οι σημαντικές οντότητες δεν θα πρέπει να **υποχρεούνται να [...] τεκμηριώνουν** συστηματικά τη συμμόρφωση με τις απαιτήσεις διαχείρισης κινδύνων κυβερνοασφάλειας, ενώ οι αρμόδιες αρχές θα πρέπει να εφαρμόζουν μια εκ των υστέρων προσέγγιση αντίδρασης όσον αφορά την εποπτεία και, ως εκ τούτου, να μην έχουν γενική υποχρέωση εποπτείας των εν λόγω οντοτήτων. **Για τις σημαντικές οντότητες, η εκ των υστέρων εποπτεία θα μπορούσε να ενεργοποιείται με αποδεικτικά στοιχεία ή οποιαδήποτε ένδειξη ή πληροφορία που τίθεται υπόψη των αρμόδιων αρχών και θεωρείται από τις αρχές αυτές ότι υποδηλώνει πιθανή μη συμμόρφωση με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία.** Για παράδειγμα, τέτοια αποδεικτικά στοιχεία, ενδείξεις ή πληροφορίες θα μπορούσαν να είναι του είδους που παρέχονται στις αρμόδιες αρχές από άλλες αρχές, οντότητες, πολίτες, μέσα ενημέρωσης ή άλλες πηγές, να είναι πληροφορίες διαθέσιμες στο κοινό ή να προκύπτουν από άλλες δραστηριότητες που διεξάγουν οι αρμόδιες αρχές κατά την εκτέλεση των καθηκόντων τους.

(70α) Στο πλαίσιο της άσκησης της εκ των προτέρων εποπτείας, οι αρμόδιες αρχές θα πρέπει να είναι σε θέση να αποφασίζουν πώς θα ιεραρχήσουν τη χρήση των εποπτικών δράσεων και μέσων που έχουν στη διάθεσή τους με αναλογικό τρόπο. Τούτο συνεπάγεται ότι οι αρμόδιες αρχές μπορούν να αποφασίζουν σχετικά με την εν λόγω ιεράρχηση βάσει εποπτικών μεθοδολογιών οι οποίες θα πρέπει να ακολουθούν προσέγγιση που βασίζεται στους κινδύνους. Πιο συγκεκριμένα, οι μεθοδολογίες αυτές θα μπορούσαν να περιλαμβάνουν κριτήρια ή στοιχεία αναφοράς για την κατάταξη των βασικών οντοτήτων σε κατηγορίες κινδύνου, και αντίστοιχες εποπτικές δράσεις και μέσα που συνιστώνται ανά κατηγορία κινδύνου, όπως χρήση, συχνότητα ή είδος επιτόπιων επιθεωρήσεων ή στοχευμένων ελέγχων ασφαλείας ή σαρώσεων ασφαλείας, είδος πληροφοριών που πρέπει να ζητούνται και βαθμός λεπτομέρειας των εν λόγω πληροφοριών. Οι εν λόγω εποπτικές μεθοδολογίες μπορούν επίσης να συνοδεύονται από προγράμματα εργασίας και να αξιολογούνται και να επανεξετάζονται τακτικά, μεταξύ άλλων όσον αφορά πτυχές όπως η κατανομή των πόρων και οι ανάγκες σε πόρους.

(70αα) Όσον αφορά τις οντότητες της δημόσιας διοίκησης, οι εποπτικές εξουσίες θα πρέπει να ασκούνται σύμφωνα με τα εθνικά πλαίσια και την εθνική έννομη τάξη. Τα κράτη μέλη θα πρέπει να είναι σε θέση να αποφασίζουν σχετικά με την επιβολή κατάλληλων, αναλογικών και αποτελεσματικών μέτρων εποπτείας και επιβολής σε σχέση με τις εν λόγω οντότητες.

(70ααα) Προκειμένου να αποδειχθεί η συμμόρφωση με ορισμένα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας, τα κράτη μέλη θα μπορούσαν να απαιτούν από τις βασικές και τις σημαντικές οντότητες να χρησιμοποιούν αναγνωρισμένες υπηρεσίες εμπιστοσύνης ή κοινοποιημένα συστήματα ηλεκτρονικής ταυτοποίησης δυνάμει του κανονισμού (ΕΕ) αριθ. 910/2014.

- (71) Προκειμένου να καταστεί αποτελεσματική η επιβολή της νομοθεσίας, θα πρέπει να καταρτιστεί ένας ελάχιστος κατάλογος διοικητικών κυρώσεων για παραβίαση των υποχρεώσεων διαχείρισης κινδύνου και αναφοράς περιστατικών στον τομέα της κυβερνοασφάλειας που προβλέπονται από την παρούσα οδηγία, με τη θέσπιση σαφούς και συνεκτικού πλαισίου για τις εν λόγω κυρώσεις σε ολόκληρη την Ένωση. Θα πρέπει να λαμβάνονται δεόντως υπόψη η φύση, η σοβαρότητα και η διάρκεια της παράβασης, η πραγματική ζημία που προκλήθηκε ή οι ζημίες που προκλήθηκαν ή οι δυνητικές ζημίες που θα μπορούσαν να προκληθούν, ο εκ προθέσεως ή εξ αμελείας χαρακτήρας της παράβασης, τα μέτρα που ελήφθησαν για την πρόληψη ή τον μετριασμό της ζημίας ή/και των απωλειών που σημειώθηκαν, ο βαθμός ευθύνης ή τυχόν σχετικών προηγούμενων παραβάσεων, ο βαθμός συνεργασίας με την αρμόδια αρχή και κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο. Η επιβολή κυρώσεων, συμπεριλαμβανομένων των διοικητικών προστίμων, θα πρέπει να υπόκειται σε κατάλληλες δικονομικές εγγυήσεις σύμφωνα με τις γενικές αρχές του ενωσιακού δικαίου και του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, συμπεριλαμβανομένης της πραγματικής δικαστικής προστασίας και της ορθής διαδικασίας.
- (71a) Οι διατάξεις σχετικά με την ευθύνη φυσικών προσώπων που έχουν ορισμένες αρμοδιότητες εντός μιας οντότητας για παράβαση του καθήκοντός τους να διασφαλίζουν τη συμμόρφωση με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία δεν απαιτούν από τα κράτη μέλη να διασφαλίζουν την ποινική δίωξη ή την αστική ευθύνη για ζημίες που προκαλούνται από την εν λόγω παράβαση σε τρίτους.**
- (72) Προκειμένου να διασφαλιστεί η αποτελεσματική επιβολή των υποχρεώσεων που ορίζονται στην παρούσα οδηγία, κάθε αρμόδια αρχή θα πρέπει να έχει την εξουσία να επιβάλλει ή να ζητεί την επιβολή διοικητικών προστίμων.

- (73) Σε περίπτωση που τα διοικητικά πρόστιμα επιβάλλονται σε επιχείρηση, μια επιχείρηση θα πρέπει να νοείται επιχείρηση σύμφωνα με τα άρθρα 101 και 102 ΣΛΕΕ για τους σκοπούς αυτούς. Σε περίπτωση που τα διοικητικά πρόστιμα επιβάλλονται σε πρόσωπα που δεν είναι επιχειρήσεις, η εποπτική αρχή θα πρέπει να λαμβάνει υπόψη το γενικό επίπεδο εισοδημάτων στο κράτος μέλος, καθώς και την οικονομική κατάσταση του προσώπου, όταν εξετάζει το ενδεδειγμένο ποσό του προστίμου. Θα πρέπει να εναπόκειται στα κράτη μέλη να αποφασίζουν εάν και σε ποιο βαθμό μπορούν να επιβάλλονται διοικητικά πρόστιμα σε δημόσιες αρχές. Η επιβολή διοικητικού προστίμου δεν θίγει την άσκηση άλλων εξουσιών από τις αρμόδιες αρχές ή άλλων κυρώσεων που προβλέπονται στους εθνικούς κανόνες μεταφοράς της παρούσας οδηγίας.
- (74) Τα κράτη μέλη [...] **μπορούν** να θεσπίζουν κανόνες σχετικά με τις ποινικές κυρώσεις για παραβάσεις των εθνικών κανόνων μεταφοράς της παρούσας οδηγίας. Ωστόσο, η επιβολή ποινικών κυρώσεων για παραβάσεις τέτοιων εθνικών κανόνων και συναφών διοικητικών κυρώσεων δεν θα πρέπει να οδηγεί σε παραβίαση της αρχής *ne bis in idem*, όπως την ερμηνεύει το Δικαστήριο.
- (75) Όταν η παρούσα οδηγία δεν εναρμονίζει διοικητικές ποινές ή αν είναι αναγκαίο σε άλλες περιπτώσεις, λόγω χάρη σε περιπτώσεις σοβαρών παραβάσεων των υποχρεώσεων που ορίζονται στην παρούσα οδηγία, τα κράτη μέλη θα πρέπει να εφαρμόζουν ένα σύστημα αποτελεσματικών, αναλογικών και αποτρεπτικών ποινών. Η φύση των εν λόγω ποινών, ποινικών ή διοικητικών, θα πρέπει να προσδιορίζεται από το δίκαιο των κρατών μελών.

- (76) Προκειμένου να ενισχυθεί περαιτέρω η αποτελεσματικότητα και η αποτρεπτικότητα των κυρώσεων που επιβάλλονται σε περίπτωση παράβασης των υποχρεώσεων που καθορίζονται δυνάμει της παρούσας οδηγίας, οι αρμόδιες αρχές θα πρέπει να έχουν την εξουσία να επιβάλλουν κυρώσεις που συνίστανται στην αναστολή πιστοποίησης ή εξουσιοδότησης όσον αφορά μέρος ή το σύνολο των υπηρεσιών που παρέχονται από βασική οντότητα και στην επιβολή προσωρινής απαγόρευσης της άσκησης διαχειριστικών καθηκόντων από φυσικό πρόσωπο. Δεδομένης της σοβαρότητας και του αντικτύπου τους στις δραστηριότητες των οντοτήτων και, τελικά, στους καταναλωτές τους, οι εν λόγω κυρώσεις θα πρέπει να επιβάλλονται μόνο αναλογικά με τη σοβαρότητα της παράβασης και λαμβάνοντας υπόψη τις ειδικές περιστάσεις κάθε περίπτωσης, συμπεριλαμβανομένου του εκ προθέσεως ή εξ αμελείας χαρακτήρα της παράβασης, των μέτρων που λαμβάνονται για την πρόληψη ή τον μετριασμό της ζημίας ή/και των ζημιών που σημειώθηκαν. Οι κυρώσεις αυτές θα πρέπει να επιβάλλονται μόνο ως ultima ratio, δηλαδή μόνο μετά την εξάντληση των άλλων σχετικών μέτρων επιβολής που προβλέπονται στην παρούσα οδηγία, και μόνο για το χρονικό διάστημα έως ότου οι οντότητες στις οποίες εφαρμόζονται λάβουν τα αναγκαία μέτρα για να συμπληρωθούν οι ελλείψεις ή για τη συμμόρφωση με τις απαιτήσεις της αρμόδιας αρχής για την οποία επιβλήθηκαν οι εν λόγω κυρώσεις. Η επιβολή των εν λόγω κυρώσεων, θα πρέπει να υπόκειται σε κατάλληλες δικονομικές εγγυήσεις σύμφωνα με τις γενικές αρχές του ενωσιακού δικαίου και του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, συμπεριλαμβανομένης της αποτελεσματικής δικαστικής προστασίας, της ορθής διαδικασίας, του τεκμηρίου αθωότητας και του δικαιώματος της υπεράσπισης.
- (76α) Προκειμένου να εξασφαλιστεί η αποτελεσματική εποπτεία και επιβολή, ιδίως σε υποθέσεις με διασυνοριακή διάσταση, τα κράτη μέλη που έχουν λάβει αίτημα αμοιβαίας συνδρομής θα πρέπει, στον βαθμό που αυτό ζητείται, να λαμβάνουν τα κατάλληλα μέτρα εποπτείας και επιβολής σε σχέση με την οικεία οντότητα που παρέχει υπηρεσίες ή που έχει το δικτυακό και πληροφοριακό σύστημα στην επικράτειά τους.**

- (77) Η παρούσα οδηγία θα πρέπει να θεσπίσει κανόνες συνεργασίας μεταξύ των αρμόδιων αρχών και των εποπτικών αρχών σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 για την αντιμετώπιση παραβάσεων που σχετίζονται με δεδομένα προσωπικού χαρακτήρα.
- (78) Η παρούσα οδηγία θα πρέπει να αποσκοπεί στη διασφάλιση υψηλού επιπέδου ευθύνης για τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας και τις υποχρεώσεις αναφοράς περιστατικών σε επίπεδο οργανισμών. Για τους λόγους αυτούς, τα διοικητικά όργανα των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας θα πρέπει να εγκρίνουν τα μέτρα κινδύνου για την κυβερνοασφάλεια και να εποπτεύουν την εφαρμογή τους.
- (79) Θα πρέπει να θεσπιστεί [...] **σύστημα [...] μάθησης από ομοτίμους για να συμβάλει στην ενίσχυση της αμοιβαίας εμπιστοσύνης και στη μάθηση από ορθές πρακτικές και εμπειρίες**, το οποίο θα επιτρέπει [...] τις ανταλλαγές μεταξύ ομότιμων εμπειρογνομόνων που ορίζονται από τα κράτη μέλη σχετικά με [...] την εφαρμογή των πολιτικών κυβερνοασφάλειας [...]. **Κατά την εφαρμογή του συστήματος μάθησης από ομοτίμους, θα πρέπει να δίνεται ιδιαίτερη προσοχή ώστε να εξασφαλίζεται ότι δεν επιβαρύνει άσκοπα ή δυσανάλογα τις αρμόδιες αρχές των κρατών μελών. Η Επιτροπή θα πρέπει να διερευνήσει όλες τις δυνατότητες προκειμένου να εξασφαλίσει δυνητικά την οικονομική κάλυψη των δαπανών που ενδέχεται να προκύψουν από την οργάνωση αποστολών αλληλοδιδαχής από ομοτίμους. Επιπλέον, το σύστημα μάθησης από ομοτίμους θα πρέπει να λαμβάνει υπόψη τα αποτελέσματα παρόμοιων μηχανισμών, όπως το σύστημα αξιολόγησης από ομοτίμους του δικτύου CSIRT, να προσθέτει αξία και να αποφεύγει τις επικαλύψεις. Η εφαρμογή του συστήματος μάθησης από ομοτίμους δεν θα πρέπει να θίγει την εθνική ή ενωσιακή νομοθεσία για την προστασία των εμπιστευτικών και διαβαθμισμένων πληροφοριών. Πριν από την έναρξη των κύκλων μάθησης από ομοτίμους, τα κράτη μέλη μπορούν να διενεργούν αυτοαξιολόγηση των σχετικών πτυχών. Κατόπιν αιτήματος της ομάδας συνεργασίας, ο ENISA μπορεί να παρέχει καθοδήγηση σχετικά με την αυτοαξιολόγηση και τα σχετικά υποδείγματα, όπου απαιτείται. Τα κράτη μέλη θα μπορούσαν να αποφασίσουν να δημοσιοποιήσουν τις αντίστοιχες εκθέσεις τους.**



- (80) [...]
- (81) Προκειμένου να εξασφαλιστούν ενιαίοι όροι για την εφαρμογή των σχετικών διατάξεων της παρούσας οδηγίας σχετικά με τις διαδικαστικές ρυθμίσεις που απαιτούνται για τη λειτουργία της ομάδας συνεργασίας, τα τεχνικά στοιχεία που σχετίζονται με τα μέτρα διαχείρισης του κινδύνου ή το είδος των πληροφοριών, τη μορφή και τη διαδικασία των κοινοποιήσεων περιστατικών, **τις κατηγορίες των οντοτήτων που πρέπει να υποχρεούνται να χρησιμοποιούν ορισμένα πιστοποιημένα προϊόντα, υπηρεσίες και διαδικασίες ΤΠΕ**, θα πρέπει να ανατεθούν εκτελεστικές αρμοδιότητες στην Επιτροπή. Οι εν λόγω αρμοδιότητες θα πρέπει να ασκούνται σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 182/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>26</sup>.
- (82) Η Επιτροπή θα πρέπει να επανεξετάζει περιοδικά την παρούσα οδηγία, σε διαβούλευση με τα ενδιαφερόμενα μέρη, ιδίως προκειμένου να εξακριβώνεται αν απαιτείται τροποποίησή της υπό το πρίσμα της μεταβολής συνθηκών στην κοινωνία, την πολιτική, την τεχνολογία ή τις αγορές.

---

<sup>26</sup> Κανονισμός (ΕΕ) αριθ. 182/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Φεβρουαρίου 2011, για τη θέσπιση κανόνων και γενικών αρχών σχετικά με τους τρόπους ελέγχου από τα κράτη μέλη της άσκησης των εκτελεστικών αρμοδιοτήτων από την Επιτροπή (ΕΕ L 55 της 28.2.2011, σ. 13).

- (83) Δεδομένου ότι ο στόχος της παρούσας οδηγίας, ήτοι η επίτευξη υψηλού ενιαίου επιπέδου κυβερνοασφάλειας στην Ένωση, δεν μπορεί να επιτευχθεί ικανοποιητικά από τα κράτη μέλη αλλά μπορεί, λόγω των επιπτώσεων της δράσης, να επιτευχθεί καλύτερα σε ενωσιακό επίπεδο, η Ένωση μπορεί να λάβει μέτρα, σύμφωνα με την αρχή της επικουρικότητας του άρθρου 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Σύμφωνα με την αρχή της αναλογικότητας του ίδιου άρθρου, η παρούσα οδηγία δεν υπερβαίνει τα αναγκαία για την επίτευξη του στόχου αυτού.
- (84) Η παρούσα οδηγία σέβεται τα θεμελιώδη δικαιώματα και τηρεί τις αρχές που αναγνωρίζονται από τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, ιδιαίτερα δε το δικαίωμα στον σεβασμό της ιδιωτικής ζωής και των επικοινωνιών, την προστασία των δεδομένων προσωπικού χαρακτήρα, την επιχειρηματική ελευθερία, το δικαίωμα ιδιοκτησίας, το δικαίωμα πραγματικής προσφυγής ενώπιον δικαστηρίου και το δικαίωμα ακρόασης. Η παρούσα οδηγία θα πρέπει να εφαρμόζεται σύμφωνα με τα δικαιώματα και τις αρχές αυτές,

## ΚΕΦΑΛΑΙΟ Ι

### *Γενικές διατάξεις*

#### *Άρθρο 1*

#### *Αντικείμενο*

1. Η παρούσα οδηγία θεσπίζει μέτρα για τη διασφάλιση υψηλού κοινού επιπέδου κυβερνοασφάλειας εντός της Ένωσης **προκειμένου να βελτιωθεί η λειτουργία της εσωτερικής αγοράς.**
2. Για τον σκοπό αυτό, η οδηγία:
  - α) θεσπίζει υποχρεώσεις για τα κράτη μέλη όσον αφορά την έγκριση εθνικών στρατηγικών κυβερνοασφάλειας, τον ορισμό αρμόδιων εθνικών αρχών, ενιαίων σημείων επαφής και ομάδων αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT)·
  - β) καθορίζει υποχρεώσεις διαχείρισης κινδύνου και αναφοράς περιστατικών στον τομέα της κυβερνοασφάλειας για οντότητες του είδους που αναφέρεται [...] στα **παραρτήματα Ι και ΙΙ** [...].
  - γ) θεσπίζει **κανόνες και υποχρεώσεις** σχετικά με την ανταλλαγή πληροφοριών για την κυβερνοασφάλεια.

## Άρθρο 2

### Πεδίο εφαρμογής

1. Η παρούσα οδηγία εφαρμόζεται σε δημόσιες και ιδιωτικές οντότητες των ειδών που **απαριθμούνται στα παραρτήματα I και II [...] μεγέθους ίσου ή ανώτερου από τα ανώτατα όρια για μεσαίες επιχειρήσεις**[...] κατά την έννοια της σύστασης 2003/361/EK της Επιτροπής<sup>27</sup>. **Το άρθρο 3 παράγραφος 4 και το άρθρο 6 παράγραφος 2 δεύτερο και τρίτο εδάφιο του παραρτήματος της εν λόγω σύστασης δεν εφαρμόζονται για τους σκοπούς της παρούσας οδηγίας.**
2. [...]Ανεξάρτητα από το μέγεθος[...] **των οντοτήτων της παραγράφου 1**, η παρούσα οδηγία εφαρμόζεται επίσης **όταν:** [...]
  - α) οι υπηρεσίες παρέχονται από μία από τις ακόλουθες οντότητες:
    - (i) **παρόχους δημόσιων δικτύων** ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών που αναφέρονται στο Παράρτημα I σημείο 8·
    - (ii) **εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης που αναφέρονται στο παράρτημα I σημείο XX·**
    - (iii) **μη εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης που αναφέρονται στο παράρτημα I σημείο XX·**
    - (iv) μητρώα ονομάτων τομέα ανωτάτου επιπέδου [...] που αναφέρονται στο παράρτημα I σημείο 8·
  - β) [...]

<sup>27</sup> Σύσταση 2003/361/EK της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων (EE L 124 της 20.5.2003, σ. 36).

- γ) η οντότητα είναι ο μοναδικός πάροχος, σε ένα κράτος μέλος, [...] υπηρεσίας που είναι ουσιώδης για τη διατήρηση κρίσιμων κοινωνικών ή οικονομικών δραστηριοτήτων·
- δ) ενδεχόμενη διατάραξη της υπηρεσίας που παρέχει η οντότητα θα μπορούσε να έχει [...] σημαντικό αντίκτυπο στη δημόσια ασφάλεια, στη δημόσια προστασία ή στη δημόσια υγεία·
- ε) ενδεχόμενη διατάραξη της υπηρεσίας που παρέχεται από την οντότητα θα μπορούσε να προκαλέσει [...] σημαντικούς συστημικούς κινδύνους, ιδίως για τους τομείς στους οποίους η διατάραξη αυτή θα μπορούσε να έχει διασυνοριακό αντίκτυπο·
- στ) [...].
- ζ) η οντότητα χαρακτηρίζεται ως κρίσιμη οντότητα σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>28</sup> [οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων] [ή ως οντότητα ισοδύναμη με κρίσιμη οντότητα, σύμφωνα με το άρθρο 7 της εν λόγω οδηγίας].

**2α. Ανεξάρτητα από το μέγεθός τους, η παρούσα οδηγία εφαρμόζεται επίσης σε φορείς δημόσιας διοίκησης κεντρικών κυβερνήσεων που αναγνωρίζονται ως τέτοιοι σε ένα κράτος μέλος σύμφωνα με το εθνικό δίκαιο και αναφέρονται στο σημείο 9 του παραρτήματος Ι. Τα κράτη μέλη μπορούν να ορίζουν ότι η παρούσα οδηγία εφαρμόζεται επίσης σε φορείς δημόσιας διοίκησης σε περιφερειακό και τοπικό επίπεδο.**

---

<sup>28</sup> [να αναγραφεί ο πλήρης τίτλος και τα στοιχεία δημοσίευσης της ΕΕ όταν είναι γνωστά]

3. [...]

**Η παρούσα οδηγία δεν θίγει τις αρμοδιότητες των κρατών μελών να διαφυλάσσουν την εθνική ασφάλεια ή την εξουσία τους να διασφαλίζουν άλλες ουσιώδεις λειτουργίες του κράτους, περιλαμβανομένης της διασφάλισης της εδαφικής ακεραιότητας του κράτους και της τήρησης της δημόσιας τάξης.**

**3α. (1) Η παρούσα οδηγία δεν εφαρμόζεται σε:**

**α) οντότητες που δεν εμπίπτουν στο πεδίο εφαρμογής του ενωσιακού δικαίου και, σε κάθε περίπτωση, σε όλες τις οντότητες που ασκούν κατά κύριο λόγο δραστηριότητες στους τομείς της άμυνας, της εθνικής ασφάλειας, της δημόσιας ασφάλειας ή της επιβολής του νόμου ασχέτως του ποια οντότητα ασκεί τις δραστηριότητες και αν είναι δημόσια ή ιδιωτική οντότητα, με την επιφύλαξη του σημείου 2)·**

β) οντότητες που εκτελούν δραστηριότητες στους τομείς της δικαστικής εξουσίας, στα κοινοβούλια και σε κεντρικές τράπεζες.[...]

2) Όταν οι φορείς δημόσιας διοίκησης ασκούν δραστηριότητες στους τομείς αυτούς μόνο ως τμήμα των συνολικών δραστηριοτήτων τους, εξαιρούνται στο σύνολό τους από το πεδίο εφαρμογής της παρούσας οδηγίας.

**3αα.** Η παρούσα οδηγία δεν εφαρμόζεται σε:

- i) δραστηριότητες οντοτήτων που δεν εμπίπτουν στο πεδίο εφαρμογής του ενωσιακού δικαίου και, σε κάθε περίπτωση, σε όλες τις δραστηριότητες που αφορούν την εθνική ασφάλεια ή άμυνα, ασχέτως του ποια οντότητα ασκεί τις δραστηριότητες αυτές και αν πρόκειται για δημόσια ή ιδιωτική οντότητα·
- ii) δραστηριότητες οντοτήτων στον τομέα της δικαιοσύνης, κοινοβουλίων, κεντρικών τραπεζών και στον τομέα δημόσιας ασφάλειας, περιλαμβανομένων φορέων δημόσιας διοίκησης που ασκούν δραστηριότητες επιβολής του νόμου για τους σκοπούς της πρόληψης, διερεύνησης, ανάχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων.

**3ααα.** Οι υποχρεώσεις που προβλέπονται στην παρούσα οδηγία δεν συνεπάγονται την παροχή πληροφοριών, η αποκάλυψη των οποίων αντίκειται στα ουσιώδη συμφέροντα εθνικής ασφάλειας, δημόσιας ασφάλειας ή άμυνας των κρατών μελών.

**3αααα. Η παρούσα οδηγία δεν θίγει το ενωσιακό δίκαιο περί προστασίας δεδομένων προσωπικού χαρακτήρα, ειδικότερα δε τον κανονισμό (ΕΕ) 2016/679 και την οδηγία 2002/58/ΕΚ.**

**3β. Η παρούσα οδηγία δεν εφαρμόζεται σε οντότητες που εξαιρούνται από τον κανονισμό (ΕΕ) XXXX/XXXX του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [κανονισμός DORA] σύμφωνα με το άρθρο 2 παράγραφος 4 του κανονισμού DORA.**

4. Η παρούσα οδηγία εφαρμόζεται με την επιφύλαξη [...] <sup>29</sup> [...] των οδηγιών 2011/93/ΕΕ <sup>30</sup> και 2013/40/ΕΕ <sup>31</sup> του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

5. Με την επιφύλαξη του άρθρου 346 της ΣΛΕΕ, πληροφορίες που είναι εμπιστευτικές σύμφωνα με ενωσιακούς και εθνικούς κανόνες, όπως κανόνες περί επιχειρηματικού απορρήτου, ανταλλάσσονται με την Επιτροπή και άλλες αρμόδιες αρχές **σύμφωνα με την παρούσα οδηγία** μόνον εφόσον η ανταλλαγή αυτή είναι αναγκαία για την εφαρμογή της παρούσας οδηγίας. Οι ανταλλασσόμενες πληροφορίες περιορίζονται σε ό,τι είναι συναφές και αναλογικό προς τον σκοπό της ανταλλαγής αυτής. Η ανταλλαγή πληροφοριών διαφυλάσσει το απόρρητο αυτών των πληροφοριών και προστατεύει τα συμφέροντα ασφάλειας και τα εμπορικά συμφέροντα των βασικών ή σημαντικών οντοτήτων.

---

<sup>29</sup> [...]

<sup>30</sup> Οδηγία 2011/93/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2011, σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου (ΕΕ L 335 της 17.12.2011, σ. 1).

<sup>31</sup> Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου (ΕΕ L 218 της 14.8.2013, σ. 8).



## *Άρθρο 2α*

### *Βασικές και σημαντικές οντότητες.*

1. Από τις οντότητες στις οποίες εφαρμόζεται η παρούσα οδηγία, βασικές θεωρούνται:
  - i) οι οντότητες του τύπου που προβλέπεται στα σημεία 1 έως 8α και 10 του παραρτήματος I της παρούσας οδηγίας, οι οποίες υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις, όπως ορίζονται στη σύσταση 2003/361/ΕΚ της Επιτροπής·
  - ii) οι μεσαίες οντότητες του άρθρου 2 παράγραφος 2 στοιχείο α) σημείο i)·
  - iii) οι οντότητες του άρθρου 2 παράγραφος 2 στοιχείο α) σημεία ii) και iv) της παρούσας οδηγίας, ανεξαρτήτως μεγέθους·
  - iv) οι οντότητες του άρθρου 2 παράγραφος 2 στοιχείο ζ) και στο άρθρο 2 παράγραφος 2α της παρούσας οδηγίας, ανεξαρτήτως μεγέθους·
  - v) εάν έχουν συσταθεί από τα κράτη μέλη, οι οντότητες τις οποίες τα κράτη μέλη προσδιόρισαν πριν από την έναρξη ισχύος της παρούσας οδηγίας ως φορείς εκμετάλλευσης βασικών υπηρεσιών σύμφωνα με την οδηγία (ΕΕ) 2016/1148 ή το εθνικό δίκαιο·
  - vi) οι οντότητες που υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις, όπως ορίζονται στη σύσταση 2003/361/ΕΚ της Επιτροπής, του τύπου που προβλέπεται στο παράρτημα II, τις οποίες τα κράτη μέλη ορίζουν ως βασικές βάσει των κριτηρίων του άρθρου 2 παράγραφος 2 στοιχεία γ) έως ε)·

(vii) οι μεσαίες οντότητες κατά την έννοια της σύστασης 2003/361/ΕΚ της Επιτροπής, τις οποίες τα κράτη μέλη ορίζουν ως βασικές βάσει των κριτηρίων του άρθρου 2 παράγραφος 2 στοιχεία γ) έως ε)·

viii) οι πολύ μικρές ή μικρές οντότητες κατά την έννοια της σύστασης 2003/361/ΕΚ της Επιτροπής που μνημονεύονται στην παράγραφο 2) στοιχείο α) σημείο i) ή που προσδιορίζεται σύμφωνα με την παράγραφο 2) στοιχεία γ) έως ε) του παρόντος άρθρου, τις οποίες τα κράτη μέλη τις ορίζουν ως ουσιώδεις βάσει εθνικών εκτιμήσεων κινδύνου.

2. Από τις οντότητες στις οποίες εφαρμόζεται η παρούσα οδηγία θεωρούνται σημαντικές οι εξής:

i) οι οντότητες τύπου που προβλέπεται στο παράρτημα I της παρούσας οδηγίας, οι οποίες χαρακτηρίζονται ως μεσαίες επιχειρήσεις κατά την έννοια της σύστασης 2003/361/ΕΚ της Επιτροπής και οι οντότητες τύπου που προβλέπεται στο παράρτημα II μεγέθους ίσου ή ανώτερου από τα ανώτατα όρια για μεσαίες επιχειρήσεις κατά την έννοια της σύστασης 2003/361/ΕΚ της Επιτροπής<sup>32</sup>

ii) οι οντότητες του άρθρου 2 παράγραφος 2 στοιχείο α) σημείο iii) της παρούσας οδηγίας, ανεξαρτήτως μεγέθους·

iii) οι μικρές και πολύ μικρές επιχειρήσεις του άρθρου 2 παράγραφος 2 στοιχείο α) σημείο i)·

(iv) οι μικρές και πολύ μικρές οντότητες τις οποίες τα κράτη μέλη προσδιορίζουν ως σημαντικές βάσει του άρθρου 2 παράγραφος 2 στοιχεία γ) έως ε).

---

<sup>32</sup> Σύσταση 2003/361/ΕΚ της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων (ΕΕ L 124 της 20.5.2003, σ. 36).

## *Άρθρο 2α*

### *Μηχανισμοί κοινοποίησης*

1. Τα κράτη μέλη μπορούν να θεσπίσουν εθνικό μηχανισμό αυτο-κοινοποίησης ο οποίος να απαιτεί από όλες τις οντότητες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας να υποβάλλουν τουλάχιστον την επωνυμία, τη διεύθυνση, τα στοιχεία επικοινωνίας τους, τον τομέα στον οποίο δραστηριοποιούνται ή το είδος της υπηρεσίας που παρέχουν και, κατά περίπτωση, τον κατάλογο των κρατών μελών στα οποία παρέχουν υπηρεσίες υποκείμενες στην παρούσα οδηγία, στις αρμόδιες αρχές δυνάμει της παρούσας οδηγίας ή σε οργανισμούς ορισμένους προς τούτο από τα κράτη μέλη.
2. Τα κράτη μέλη [...] υποβάλλουν στην Επιτροπή, σε σχέση με τις οντότητες που έχουν προσδιορίσει σύμφωνα με το άρθρο 2 παράγραφος 2 στοιχεία β) έως ε), τουλάχιστον σχετικές πληροφορίες για τον αριθμό των ταυτοποιημένων οντοτήτων, τον τομέα στον οποίο ανήκουν ή το είδος της υπηρεσίας που παρέχουν σύμφωνα με τα παραρτήματα, και την (τις) ειδική (-ές) διάταξη (-εις) του άρθρου 2 παράγραφος 2 βάσει των οποίων προσδιορίστηκαν έως [12 μήνες μετά την προθεσμία μεταφοράς της παρούσας οδηγίας στο εθνικό δίκαιο]. Σε τακτική βάση και τουλάχιστον ανά διετία, τα κράτη μέλη επανεξετάζουν και, εφόσον απαιτείται, επικαιροποιούν [...] τις πληροφορίες αυτές [...].

## Άρθρο 2β

### Τομεακές πράξεις της Ένωσης

1. Όταν τομεακές [...] **νομικές πράξεις της Ένωσης**[...] απαιτούν από βασικές ή σημαντικές οντότητες [...] να θεσπίζουν μέτρα διαχείρισης κινδύνου για την κυβερνοασφάλεια [...] ή να κοινοποιούν **σημαντικά** περιστατικά ή [...] κυβερνοαπειλές, και όταν οι απαιτήσεις αυτές είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία, **περιλαμβανομένων των διατάξεων περί εποπτείας και επιβολής του κεφαλαίου VI**, στις οντότητες αυτές δεν εφαρμόζονται οι σχετικές διατάξεις της παρούσας οδηγίας. **Εάν τομεακές νομικές πράξεις της Ένωσης δεν καλύπτουν όλες τις οντότητες συγκεκριμένου τομέα που εμπίπτει στο πεδίο εφαρμογής της παρούσας οδηγίας, οι σχετικές διατάξεις της παρούσας οδηγίας εξακολουθούν να εφαρμόζονται στις οντότητες που δεν καλύπτονται από τις τομεακές αυτές διατάξεις.**
2. Οι απαιτήσεις της παραγράφου 1 του παρόντος άρθρου θεωρούνται ισοδύναμες ως προς το αποτέλεσμα με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία εάν η αντίστοιχη τομεακή πράξη της Ένωσης προβλέπει άμεση πρόσβαση, κατά περίπτωση αυτόματα και απευθείας, στις κοινοποιήσεις περιστατικών από τις αρμόδιες αρχές δυνάμει της παρούσας οδηγίας ή από τις ορισθείσες CSIRT και εάν:
  - α) τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας είναι τουλάχιστον ισοδύναμα ως προς το αποτέλεσμα με εκείνα που ορίζονται στο άρθρο 18 παράγραφοι 1 και 2 της παρούσας οδηγίας· ή
  - β) οι απαιτήσεις για κοινοποίηση σημαντικών περιστατικών είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με εκείνες που ορίζονται στο άρθρο 20 παράγραφοι 1 έως 6.

3. **Η Επιτροπή επανεξετάζει περιοδικά την εφαρμογή των απαιτήσεων ισοδύναμου αποτελέσματος που προβλέπονται στις παραγράφους 1 και 2 του παρόντος άρθρου σε σχέση με τομεακές διατάξεις νομικών πράξεων της Ένωσης. Η Επιτροπή συμβουλεύεται την ομάδα συνεργασίας και τον ENISA κατά την προετοιμασία των περιοδικών αυτών επανεξετάσεων.**

#### *Άρθρο 3*

#### **Ελάχιστη εναρμόνιση**

Με την επιφύλαξη των λοιπών υποχρεώσεών τους βάσει του δικαίου της Ένωσης, τα κράτη μέλη μπορούν [...] να θεσπίζουν ή να διατηρούν διατάξεις που διασφαλίζουν υψηλότερο επίπεδο κυβερνοασφάλειας **στους τομείς που καλύπτει η παρούσα οδηγία.**

#### *Άρθρο 4*

#### **Ορισμοί**

Για τους σκοπούς της παρούσας οδηγίας, ισχύουν οι ακόλουθοι ορισμοί:

- (1) «δικτυακό και πληροφοριακό σύστημα»:
- α) δίκτυο ηλεκτρονικών επικοινωνιών κατά την έννοια του άρθρου 2 σημείο 1) της οδηγίας (ΕΕ) 2018/1972·
  - β) κάθε συσκευή ή ομάδα διασυνδεδεμένων ή σχετιζόμενων συσκευών από τις οποίες μία ή περισσότερες εκτελούν, βάσει προγράμματος, αυτόματη επεξεργασία ψηφιακών δεδομένων,
  - γ) ψηφιακά δεδομένα που αποθηκεύονται, υποβάλλονται σε επεξεργασία, ανακτώνται ή μεταδίδονται από στοιχεία που καλύπτονται στα στοιχεία α) και β) για τους σκοπούς της λειτουργίας, χρήσης, προστασίας και συντήρησής τους·

- 2) «ικανότητα δικτυακών και πληροφοριακών συστημάτων»: η ικανότητα των δικτυακών και πληροφοριακών συστημάτων να ανθίστανται, σε δεδομένο βαθμό αξιοπιστίας, σε κάθε **συμβάν που μπορεί να** πλήξει [...] τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω δικτυακών και πληροφοριακών συστημάτων·
- 2α) «υπηρεσίες ηλεκτρονικών επικοινωνιών»: υπηρεσίες ηλεκτρονικών επικοινωνιών κατά την έννοια του άρθρου 2 σημείο 4) της οδηγίας (ΕΕ) 2018/1972·**
- 3) κυβερνοασφάλεια κατά την έννοια του άρθρου 2 σημείο 1) του κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>33</sup>.
- 4) «εθνική στρατηγική **κυβερνοασφάλειας** [...] συνεκτικό πλαίσιο κράτους μέλους το οποίο παρέχει διακυβέρνηση για να επιτευχθούν στρατηγικοί στόχοι και προτεραιότητες **στον τομέα** [...] της **κυβερνοασφάλειας** [...] στο εν λόγω κράτος μέλος·
- 5) «περιστατικό»: κάθε συμβάν που θέτει σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των [...] υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω δικτυακών και πληροφοριακών συστημάτων·
- 5α) «περιστατικό κυβερνοασφάλειας μεγάλης κλίμακας»: περιστατικό με σημαντικό αντίκτυπο σε τουλάχιστον δύο κράτη μέλη ή το οποίο προκαλεί διατάραξη που υπερβαίνει την ικανότητα ενός κράτους μέλους να αντεπεξέλθει.**

---

<sup>33</sup> Κανονισμός (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) (ΕΕ L 151 της 7.6.2019, σ. 15).

- 6) «χειρισμός περιστατικών»: όλες οι ενέργειες και διαδικασίες που αποσκοπούν στον εντοπισμό, την ανάλυση και την ανάλυση ενός περιστατικού και στην αντιμετώπισή του·
- 6α) «κίνδυνος»:** η πιθανότητα ζημίας ή διατάραξης που προκαλείται από περιστατικό και εκφράζεται ως συνδυασμός της έκτασης της εν λόγω ζημίας ή διατάραξης και της πιθανότητας επέλευσης του εν λόγω περιστατικού·
- 7) «κυβερνοαπειλή»: κυβερνοαπειλή κατά την έννοια του άρθρου 2 σημείο 8) του κανονισμού (ΕΕ) 2019/881·
- (7α) «σημαντική κυβερνοαπειλή»:** κυβερνοαπειλή η οποία, με βάση τα τεχνικά της χαρακτηριστικά, μπορεί να θεωρηθεί ότι έχει τη δυνατότητα να επηρεάσει σοβαρά τα συστήματα δικτύου και πληροφοριών μιας οντότητας ή τους χρήστες της, προκαλώντας σημαντικές υλικές ή μη υλικές ζημιές·
- 8) «τρωτό σημείο»: αδυναμία, ευαισθησία ή ελάττωμα πάγιου στοιχείου ΤΠΕ ή συστήματος [...] που μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης από κυβερνοαπειλή·
- 8α) –«παρ’ ολίγον περιστατικά»:** συμβάν το οποίο θα μπορούσε δυνητικά να προκαλέσει βλάβη στα συστήματα δικτύου και πληροφοριών μιας οντότητας ή των χρηστών της, αλλά του οποίου η συντέλεση εμποδίστηκε επιτυχώς.
- 9) «εκπρόσωπος»: κάθε φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ένωση που έχει οριστεί ρητά για να ενεργεί για λογαριασμό i) παρόχου υπηρεσιών DNS, μητρώου ονομάτων τομέα ανωτάτου επιπέδου (TLD), παρόχου υπηρεσιών νεφροϋπολογιστικής, παρόχου υπηρεσιών κέντρου δεδομένων, παρόχου δικτύου διανομής περιεχομένου όπως αναφέρεται στο Παράρτημα I σημείο 8 ή ii) των οντοτήτων που αναφέρονται στο Παράρτημα II σημείο 6 οι οποίες δεν είναι εγκατεστημένες στην Ένωση, στο οποίο μπορούν να απευθύνονται οι εθνικές αρμόδιες αρχές ή τις CSIRT αντί για την οντότητα όσον αφορά τις υποχρεώσεις της εν λόγω οντότητας δυνάμει της παρούσας οδηγίας·

- 10) «πρότυπο»: πρότυπο κατά την έννοια του άρθρου 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>34</sup>.
- 11) «τεχνική προδιαγραφή»: τεχνική προδιαγραφή κατά την έννοια του άρθρου 2 σημείο 4) του κανονισμού (ΕΕ) αριθ. 1025/2012.
- 12) «σημείο ανταλλαγής κίνησης διαδικτύου (Internet Exchange Point — IXP)»: δικτυακή υποδομή που επιτρέπει τη διασύνδεση περισσότερων από δύο ανεξάρτητων δικτύων (αυτόνομων συστημάτων), κυρίως με σκοπό τη διευκόλυνση της ανταλλαγής κίνησης διαδικτύου και η οποία διασυνδέει μόνον αυτόνομα συστήματα· και η οποία διασυνδέει μόνον αυτόνομα συστήματα· το IXP δεν απαιτεί η κίνηση διαδικτύου που διέρχεται μεταξύ οποιουδήποτε ζεύγους συμμετεχόντων αυτόνομων συστημάτων να διέλθει από τρίτο αυτόνομο σύστημα ούτε την τροποποιεί ούτε παρεμβαίνει με άλλον τρόπο σε αυτήν·
- 13) «σύστημα ονομάτων τομέα (DNS)»: ιεραρχικό και κατανεμημένο σύστημα ονοματοδοσίας το οποίο παρέχει στους τελικούς χρήστες πρόσβαση σε υπηρεσίες και πόρους του διαδικτύου·
- 14) «πάροχος υπηρεσιών DNS»: οντότητα που παρέχει υπηρεσίες αναδρομικής ή αυθεντικής επίλυσης ονομάτων τομέα **για[...] χρήση εκ μέρους τρίτων, εξαιρουμένων των εξυπηρετητών ονομάτων ρίζας [...]**.

---

<sup>34</sup> Κανονισμός (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Οκτωβρίου 2012 σχετικά με την ευρωπαϊκή τυποποίηση, την τροποποίηση των οδηγιών του Συμβουλίου 89/686/ΕΟΚ και 93/15/ΕΟΚ και των οδηγιών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 94/9/ΕΚ, 94/25/ΕΚ, 95/16/ΕΚ, 97/23/ΕΚ, 98/34/ΕΚ, 2004/22/ΕΚ, 2007/23/ΕΚ, 2009/23/ΕΚ και 2009/105/ΕΚ και την κατάργηση της απόφασης 87/95/ΕΟΚ του Συμβουλίου και της απόφασης αριθ. 1673/2006/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ L 316 της 14.11.2012, σ. 12).



- 15) «μητρώο ονομάτων τομέα ανωτάτου επιπέδου»: οντότητα στην οποία έχει ανατεθεί συγκεκριμένος τομέας ανωτάτου επιπέδου (TLD) και η οποία είναι υπεύθυνη για τη διοίκηση του TLD, περιλαμβανομένης της καταχώρισης ονομάτων τομέα στον TLD και της τεχνικής λειτουργίας του, στην οποία περιλαμβάνεται η λειτουργία των εξυπηρετητών ονομάτων του, η συντήρηση των βάσεων δεδομένων του και η κατανομή των αρχείων ζώνης TLD μεταξύ των εξυπηρετητών ονομάτων, **ενώ εξαιρούνται οι περιπτώσεις στις οποίες τα ονόματα τομέα ανωτάτου επιπέδου χρησιμοποιούνται από ένα μητρώο μόνο για ίδια χρήση**.
- 15α) «οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD»:**  
**μητρώα ονομάτων TLD, καταχωριστές για τους TLD και αντιπρόσωποι καταχωριστών, όπως μεταπωλητές και πάροχοι υπηρεσιών διακομιστή διαμεσολάβησης**
- 16) «ψηφιακή υπηρεσία»: υπηρεσία κατά την έννοια του άρθρου 1 παράγραφος 1 στοιχείο β) της οδηγίας (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>35</sup>.
- 16α) «υπηρεσίες εμπιστοσύνης»:** οι υπηρεσίες εμπιστοσύνης κατά την έννοια του άρθρου 3 σημείο 16) του κανονισμού (ΕΕ) αριθ. 910/2014.

---

<sup>35</sup> Οδηγία (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Σεπτεμβρίου 2015, για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών (ΕΕ L 241 της 17.9.2015, σ. 1).

- 16β) «εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης»: εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης κατά την έννοια του άρθρου 3 σημείο 20) του κανονισμού (ΕΕ) αριθ. 910/2014.
- 17) «επιγραμμική αγορά»: ψηφιακή υπηρεσία κατά την έννοια του άρθρου 2 στοιχείο ιδ) της οδηγίας 2005/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>36</sup>.
- 18) «επιγραμμική μηχανή αναζήτησης»: ψηφιακή υπηρεσία κατά την έννοια του άρθρου 2 σημείο 5) του κανονισμού (ΕΕ) 2019/1150 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>37</sup>.
- 19) «υπηρεσία νεφούπολογιστικής»: ψηφιακή υπηρεσία που επιτρέπει κατά παραγγελία διαχείριση και ευρεία εξ αποστάσεως πρόσβαση σε κλιμακούμενο και ελαστικό σύνολο κοινόχρηστων [...] υπολογιστικών πόρων, **ακόμη και όταν αυτοί κατανέμονται σε περισσότερες τοποθεσίες**.
- 20) «υπηρεσία κέντρου δεδομένων»: υπηρεσία που περιλαμβάνει δομές, ή ομάδες δομών, οι οποίες προορίζονται για την κεντρική φιλοξενία, διασύνδεση και λειτουργία εξοπλισμού τεχνολογίας πληροφοριών και δικτύων και παρέχουν υπηρεσίες αποθήκευσης, επεξεργασίας και μεταφοράς δεδομένων, καθώς και όλες τις εγκαταστάσεις και υποδομές διανομής ισχύος και περιβαλλοντικού ελέγχου.

---

<sup>36</sup> Οδηγία 2005/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαΐου 2005, για τις αθέμιτες εμπορικές πρακτικές των επιχειρήσεων προς τους καταναλωτές στην εσωτερική αγορά και για την τροποποίηση της οδηγίας 84/450/ΕΟΚ του Συμβουλίου, των οδηγιών 97/7/ΕΚ, 98/27/ΕΚ, 2002/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και του κανονισμού (ΕΚ) αριθ. 2006/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου («Οδηγία για τις αθέμιτες εμπορικές πρακτικές») (ΕΕ L 149 της 11.6.2005, σ. 22).

<sup>37</sup> Κανονισμός (ΕΕ) 2019/1150 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Ιουνίου 2019, για την προώθηση της δίκαιης μεταχείρισης και της διαφάνειας για τους επιχειρηματικούς χρήστες επιγραμμικών υπηρεσιών διαμεσολάβησης (ΕΕ L 186 της 11.7.2019, σ. 57).

- 21) «δίκτυο διανομής περιεχομένου»: δίκτυο γεωγραφικά κατανεμημένων εξυπηρετητών που αποσκοπεί στη διασφάλιση υψηλής διαθεσιμότητας και προσβασιμότητας ή ταχείας παράδοσης ψηφιακού περιεχομένου και ψηφιακών υπηρεσιών στους χρήστες του διαδικτύου για λογαριασμό παρόχων περιεχομένου και υπηρεσιών·
- 22) «πλατφόρμα υπηρεσιών κοινωνικής δικτύωσης»: πλατφόρμα που επιτρέπει στους τελικούς χρήστες να συνδέονται, να ανταλλάσσουν, να ανακαλύπτουν και να επικοινωνούν μεταξύ τους μέσω πολλαπλών συσκευών, και ιδίως μέσω συνομιλιών, αναρτήσεων, βίντεο και συστάσεων·[...]
- 23) «φορέας δημόσιας διοίκησης»: οντότητα που **αναγνωρίζεται ως τέτοια σε ένα κράτος μέλος σύμφωνα με το εθνικό δίκαιο και [...]** πληροί τα ακόλουθα κριτήρια:
- α) έχει συσταθεί με σκοπό την κάλυψη αναγκών γενικού συμφέροντος και δεν έχει βιομηχανικό ή εμπορικό χαρακτήρα·
  - β) Έχει νομική προσωπικότητα **ή δικαιούται εκ του νόμου να ενεργεί για λογαριασμό άλλης οντότητας με νομική προσωπικότητα·**
  - γ) χρηματοδοτείται κατά το μεγαλύτερο μέρος από το κράτος, περιφερειακές αρχές ή άλλους οργανισμούς δημοσίου δικαίου ή η διαχείρισή του υπόκειται στην εποπτεία των ανωτέρω αρχών ή οργανισμών· ή περισσότερο από το ήμισυ των μελών του διοικητικού, του διευθυντικού ή του εποπτικού συμβουλίου του διορίζεται από το κράτος, τις περιφερειακές αρχές αυτοδιοίκησης ή άλλους οργανισμούς δημοσίου δικαίου·
  - δ) έχει την εξουσία να εκδίδει διοικητικές ή κανονιστικές αποφάσεις που απευθύνονται σε φυσικά ή νομικά πρόσωπα και επηρεάζουν τα δικαιώματά τους στη διασυνοριακή κυκλοφορία προσώπων, αγαθών, υπηρεσιών ή κεφαλαίων.
- 24) «οντότητα»: κάθε φυσικό ή νομικό πρόσωπο που έχει συσταθεί και αναγνωρίζεται ως τέτοιο σύμφωνα με το εθνικό δίκαιο του τόπου εγκατάστασής του, το οποίο μπορεί, ενεργώντας εξ ιδίου ονόματος, να ασκεί δικαιώματα και να αναλαμβάνει υποχρεώσεις·

- 25) «βασική οντότητα»: κάθε οντότητα τύπου που [...] προβλέπεται στο παράρτημα I και χαρακτηρίζεται ως «βασική» σύμφωνα με το άρθρο 2α παράγραφος 1·
- 26) «σημαντική οντότητα»: κάθε οντότητα τύπου που [...] προβλέπεται στα παραρτήματα I και II και χαρακτηρίζονται ως «σημαντική» σύμφωνα με το άρθρο 2α παράγραφος 2·
- 26α) «προϊόν ΤΠΕ»: προϊόν ΤΠΕ κατά την έννοια του άρθρου 2 σημείο 12) του κανονισμού (ΕΕ) αριθ. 2019/881·
- 26αα) «υπηρεσία ΤΠΕ»: υπηρεσία ΤΠΕ κατά την έννοια του άρθρου 2 σημείο 13) του κανονισμού (ΕΕ) αριθ. 2019/881·
- 26αβ) «διαδικασία ΤΠΕ»: διαδικασία ΤΠΕ κατά την έννοια του άρθρου 2 σημείο 14) του κανονισμού (ΕΕ) 2019/881·
- 26αγ) «Πάροχος υπηρεσιών διαχείρισης»: κάθε οντότητα που παρέχει υπηρεσίες όπως υπηρεσίες δικτύου, εφαρμογών, υποδομής και ασφάλειας, μέσω συνεχούς και τακτικής διαχείρισης, υποστήριξης και ενεργού διοίκησης στις εγκαταστάσεις των πελατών, στο κέντρο δεδομένων του δικού τους παρόχου υπηρεσιών διαχείρισης (φιλοξενία) ή σε κέντρο δεδομένων τρίτων.
- 26αδ) «Πάροχος υπηρεσιών διαχείρισης ασφάλειας»: κάθε οντότητα που παρέχει παρακολούθηση και διαχείριση συσκευών και συστημάτων ασφάλειας κατ' εξωτερική ανάθεση. Οι κοινές υπηρεσίες περιλαμβάνουν υπηρεσίες διαχείρισης τειχών προστασίας, ανίχνευσης εισβολών, εικονικού ιδιωτικού δικτύου, σάρωσης τρωτών σημείων και αντιϊκές υπηρεσίες.
- Περιλαμβάνει επίσης τη χρήση κέντρων επιχειρήσεων ασφάλειας υψηλής διαθεσιμότητας (είτε από δικές τους εγκαταστάσεις είτε από άλλους παρόχους κέντρων δεδομένων) για την παροχή υπηρεσιών 24/7 με σκοπό τη μείωση του αριθμού του προσωπικού επιχειρησιακής ασφάλειας που χρειάζεται να προσλάβει, να εκπαιδεύσει και να κρατήσει μια επιχείρηση προκειμένου να διατηρήσει μια αποδεκτή πολιτική ασφάλειας.

## ΚΕΦΑΛΑΙΟ ΙΙ

### Συντονισμένα κανονιστικά πλαίσια κυβερνοασφάλειας

#### Άρθρο 5

#### **Εθνική στρατηγική κυβερνοασφάλειας**

1. Κάθε κράτος μέλος θεσπίζει εθνική στρατηγική κυβερνοασφάλειας, η οποία καθορίζει τους στρατηγικούς στόχους και κατάλληλα μέτρα πολιτικής και κανονιστικά μέτρα, με σκοπό την επίτευξη και τη διατήρηση υψηλού επιπέδου κυβερνοασφάλειας. Η εθνική στρατηγική κυβερνοασφάλειας περιλαμβάνει, συγκεκριμένα, τα εξής:
  - α) [...] τους στόχους και τις προτεραιότητες της στρατηγικής των κρατών μελών στον τομέα της κυβερνοασφάλειας·
  - β) πλαίσιο διακυβέρνησης για την επίτευξη των εν λόγω στόχων και προτεραιοτήτων, περιλαμβανομένων των πολιτικών που αναφέρονται στην παράγραφο 2 και των ρόλων και των αρμοδιοτήτων των διάφορων αρχών και δρώντων που εμπλέκονται στην υλοποίηση της στρατηγικής [...].
  - γ) [...] **καθοδήγηση** για τον προσδιορισμό σχετικών άγιων στοιχείων και την αξιολόγηση κινδύνων για την κυβερνοασφάλεια στο εν λόγω κράτος μέλος [...]
  - δ) προσδιορισμό των μέτρων που διασφαλίζουν την ετοιμότητα για περιστατικά, την αντιμετώπισή τους και την αποκατάσταση των συστημάτων, περιλαμβανομένης της συνεργασίας μεταξύ δημόσιου και ιδιωτικού τομέα·
  - ε) [...]

στ) πλαίσιο πολιτικής για την ενίσχυση του συντονισμού μεταξύ των αρμόδιων αρχών δυνάμει της παρούσας οδηγίας και της οδηγίας (ΕΕ) XXXX/XXXX του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>38</sup> [οδηγία για την ανθεκτικότητα κρίσιμων οντοτήτων] με σκοπό την ανταλλαγή πληροφοριών σχετικά με **κινδύνους κυβερνοασφάλειας, [...] κυβερνοαπειλές και περιστατικά καθώς και σχετικά με κινδύνους, απειλές και περιστατικά εκτός του κυβερνοχώρου**, και την άσκηση εποπτικών καθηκόντων, **όπως ενδείκνυται**.

στα) **πλαίσιο πολιτικής για συντονισμό και συνεργασία μεταξύ των αρμόδιων αρχών δυνάμει της παρούσας οδηγίας και των αρμόδιων αρχών που ορίζονται βάσει της τομεακής νομοθεσίας.**

2. Στο πλαίσιο της εθνικής στρατηγικής κυβερνοασφάλειας, τα κράτη μέλη θεσπίζουν ιδίως τις ακόλουθες πολιτικές:

- α) πολιτική σχετικά με την κυβερνοασφάλεια στην αλυσίδα εφοδιασμού προϊόντων και υπηρεσιών ΤΠΕ που χρησιμοποιούνται από [...] οντότητες για την παροχή των υπηρεσιών τους·
- β) **πολιτική [...] σχετικά με τη συμπερίληψη και τον προσδιορισμό απαιτήσεων σχετικών με την κυβερνοασφάλεια όσον αφορά προϊόντα και υπηρεσίες ΤΠΕ στις δημόσιες συμβάσεις, περιλαμβανομένης και της πιστοποίησης κυβερνοασφάλειας·**
- γ) πολιτική [...] **για τη διαχείριση τρωτών σημείων, που να εμπερικλείει την προαγωγή και τη διευκόλυνση [...] της εθελοντικής συντονισμένης γνωστοποίησης τρωτών σημείων κατά την έννοια του άρθρου 6 παράγραφος 1·**
- δ) πολιτική σχετικά με τη διατήρηση της γενικής διαθεσιμότητας, [...] της ακεραιότητας **και του απορρήτου** του δημόσιου πυρήνα του ανοικτού διαδικτύου·
- ε) πολιτική για την προώθηση και την ανάπτυξη **εκπαίδευσης και κατάρτισης, δεξιοτήτων, δραστηριοτήτων ευαισθητοποίησης και πρωτοβουλιών έρευνας και ανάπτυξης στον τομέα της κυβερνοασφάλειας·**

---

<sup>38</sup> [να αναγραφεί ο πλήρης τίτλος και τα στοιχεία δημοσίευσης στην ΕΕ όταν είναι γνωστά]

- στ) πολιτική για τη στήριξη των πανεπιστημιακών και ερευνητικών ιδρυμάτων με σκοπό την ανάπτυξη εργαλείων κυβερνοασφάλειας και ασφαλών δικτυακών υποδομών·
  - ζ) πολιτική, σχετικές διαδικασίες και κατάλληλα εργαλεία ανταλλαγής πληροφοριών για τη στήριξη της εθελούσιας ανταλλαγής πληροφοριών σχετικά με την κυβερνοασφάλεια μεταξύ εταιρειών σύμφωνα με το δίκαιο της Ένωσης·
  - η) πολιτική για την αντιμετώπιση ειδικών αναγκών των ΜΜΕ, ιδίως εκείνων που εξαιρούνται από το πεδίο εφαρμογής της παρούσας οδηγίας, όσον αφορά την καθοδήγηση και τη στήριξή τους για τη βελτίωση της ανθεκτικότητάς τους έναντι [...] κυβερνοαπειλών.
3. Τα κράτη μέλη κοινοποιούν τις εθνικές στρατηγικές κυβερνοασφάλειας στην Επιτροπή εντός τριών μηνών από την έγκρισή τους. Τα κράτη μέλη μπορούν να εξαιρούν **από την κοινοποίηση αυτή στοιχεία της στρατηγικής που συνδέονται με την εθνική ασφάλεια.**
4. Τα κράτη μέλη αξιολογούν τις εθνικές στρατηγικές κυβερνοασφάλειας σε τακτική βάση και τουλάχιστον ανά [...] **πενταετία** με βάση βασικούς δείκτες επιδόσεων και τις τροποποιούν αν κρίνεται απαραίτητο. Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) επικουρεί τα κράτη μέλη, κατόπιν αιτήματός τους, στην ανάπτυξη εθνικής στρατηγικής και βασικών δεικτών επιδόσεων για την αξιολόγηση της στρατηγικής τους.

**Συντονισμένη γνωστοποίηση τρωτών σημείων και ευρωπαϊκό μητρώο τρωτών σημείων**

1. Κάθε κράτος μέλος ορίζει μία από τις CSIRT του, οι οποίες αναφέρονται στο άρθρο 9, ως συντονίστρια για τον σκοπό της συντονισμένης γνωστοποίησης τρωτών σημείων. Η ορισθείσα CSIRT ενεργεί ως αξιόπιστος ενδιάμεσος φορέας, διευκολύνοντας, αν είναι αναγκαίο, την επικοινωνία μεταξύ της αναφέρουσας οντότητας, **του υπεύθυνου για τα δυνητικά τρωτά σημεία** και του κατασκευαστή ή του παρόχου προϊόντων ή υπηρεσιών ΤΠΕ. **Κάθε φυσικό ή νομικό πρόσωπο μπορεί να κοινοποιεί στην ορισθείσα CSIRT, ενδεχομένως ανώνυμα, τρωτά σημεία του άρθρου 4 παράγραφος 8. Η ορισθείσα CSIRT διασφαλίζει την επιμελή επακολούθηση της καταγγελίας και το απόρρητο της ταυτότητας του προσώπου που κοινοποιεί το τρωτό σημείο.** Όταν το κοινοποιούμενο τρωτό σημείο [...] θα μπορούσε δυνητικά να έχει σημαντικό αντίκτυπο σε οντότητες σε περισσότερα του ενός κράτη μέλη, η ορισθείσα CSIRT κάθε ενδιαφερόμενου κράτους μέλους, όπου ενδείκνυται, συνεργάζεται με άλλες ορισθείσες CSIRT στο πλαίσιο του δικτύου CSIRT.
2. Ο ENISA αναπτύσσει και διατηρεί ευρωπαϊκό μητρώο τρωτών σημείων, **σε διαβούλευση με την ομάδα συνεργασίας.** Για τον σκοπό αυτό, ο ENISA δημιουργεί και διατηρεί κατάλληλα πληροφοριακά συστήματα και κατάλληλες πολιτικές και διαδικασίες προκειμένου, ιδίως, να παρέχει τη δυνατότητα στις σημαντικές και στις βασικές οντότητες και στους προμηθευτές δικτυακών και πληροφοριακών συστημάτων τους να γνωστοποιούν και να καταγράφουν, **σε εθελοντική βάση, δημοσίως γνωστά** τρωτά σημεία που παρατηρούνται σε προϊόντα ΤΠΕ ή υπηρεσίες ΤΠΕ, καθώς και να παρέχει πρόσβαση στις πληροφορίες σχετικά με τρωτά σημεία που περιλαμβάνονται στο μητρώο σε όλα τα ενδιαφερόμενα μέρη. Το μητρώο περιλαμβάνει, συγκεκριμένα, πληροφορίες που περιγράφουν το τρωτό σημείο, το προϊόν ΤΠΕ ή τις υπηρεσίες ΤΠΕ που επηρεάζονται και τη σοβαρότητα του τρωτού σημείου από την άποψη των περιστάσεων υπό τις οποίες μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης, τη διαθεσιμότητα σχετικών διορθωτικών προγραμμάτων και, ελλείψει διαθέσιμων διορθωτικών προγραμμάτων, υλικό καθοδήγησης που **εκδίδουν οι αρμόδιες εθνικές αρχές ή οι CSIRT και απευθύνεται** στους χρήστες τρωτών προϊόντων και υπηρεσιών σχετικά με τον τρόπο μετριασμού των κινδύνων που απορρέουν από τα γνωστοποιημένα τρωτά σημεία. **Η ENISA μεριμνά ώστε το ευρωπαϊκό μητρώο τρωτών σημείων να χρησιμοποιεί ασφαλή και ανθεκτική υποδομή επικοινωνιών και πληροφοριών.**



## Άρθρο 7

### **Εθνικά πλαίσια διαχείρισης κρίσεων κυβερνοασφάλειας**

1. Κάθε κράτος μέλος ορίζει μία ή περισσότερες αρμόδιες αρχές ως υπεύθυνες για τη διαχείριση περιστατικών και κρίσεων **κυβερνοασφάλειας** μεγάλης κλίμακας. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές διαθέτουν επαρκείς πόρους για την αποτελεσματική και αποδοτική εκτέλεση των καθηκόντων που τους ανατίθενται. **Τα κράτη μέλη εξασφαλίζουν τη συνοχή με τα υφιστάμενα πλαίσια γενικής διαχείρισης κρίσεων.**
2. Κάθε κράτος μέλος προσδιορίζει τις ικανότητες, τα πάγια στοιχεία και τις διαδικασίες που μπορούν να χρησιμοποιηθούν σε περίπτωση κρίσης για τους σκοπούς της παρούσας οδηγίας.
3. Κάθε κράτος μέλος θεσπίζει εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας, στο οποίο καθορίζονται στόχοι και λεπτομέρειες της διαχείρισης περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας. Στο σχέδιο αυτό καθορίζονται, συγκεκριμένα, τα εξής:
  - α) οι στόχοι των εθνικών μέτρων και δραστηριοτήτων ετοιμότητας·
  - β) τα καθήκοντα και οι αρμοδιότητες των εθνικών αρμόδιων αρχών·
  - γ) διαδικασίες διαχείρισης κρίσεων κυβερνοασφάλειας, **περιλαμβανομένης της ενσωμάτωσής τους στο γενικό εθνικό πλαίσιο διαχείρισης κρίσεων** και τους διαύλους ανταλλαγής πληροφοριών·
  - δ) μέτρα ετοιμότητας, περιλαμβανομένων τακτικών ασκήσεων και δραστηριοτήτων κατάρτισης·
  - ε) τα συναφή [...] μέρη και οι εμπλεκόμενες υποδομές του δημόσιου και του ιδιωτικού τομέα·
  - στ) εθνικές διαδικασίες και ρυθμίσεις μεταξύ των αρμόδιων εθνικών αρχών και φορέων για να διασφαλίζεται η αποτελεσματική συμμετοχή και η παροχή υποστήριξης εκ μέρους του κράτους μέλους στη συντονισμένη διαχείριση περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας σε επίπεδο Ένωσης.

4. Τα κράτη μέλη [...] ενημερώνουν την Επιτροπή για τον ορισμό των αρμόδιων αρχών που αναφέρονται στην παράγραφο 1 και υποβάλλουν **συναφή πληροφόρηση που συνδέεται με τις απαιτήσεις της παραγράφου 3 του παρόντος άρθρου σχετικά με τα εθνικά τους σχέδια αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας [...]** εντός τριών μηνών από τον ορισμό των εν λόγω αρχών και από την έγκριση των εν λόγω σχεδίων. Τα κράτη μέλη μπορούν να εξαιρούν συγκεκριμένες πληροφορίες [...] στις περιπτώσεις και στον βαθμό που είναι απολύτως αναγκαίο για την εθνική τους ασφάλεια, **τη δημόσια ασφάλεια ή την άμυνα.**

#### *Άρθρο 8*

#### ***Εθνικές αρμόδιες αρχές και ενιαία σημεία επαφής***

1. Κάθε κράτος μέλος ορίζει μία ή περισσότερες αρμόδιες αρχές ως υπεύθυνες για την κυβερνοασφάλεια και για τα εποπτικά καθήκοντα που αναφέρονται στο κεφάλαιο VI της παρούσας οδηγίας. Για τον σκοπό αυτόν, τα κράτη μέλη μπορούν να ορίσουν υφιστάμενη αρχή ή υφιστάμενες αρχές.
2. Οι αρμόδιες αρχές της παραγράφου 1 παρακολουθούν την εφαρμογή της παρούσας οδηγίας σε εθνικό επίπεδο.
3. Κάθε κράτος μέλος ορίζει ένα εθνικό ενιαίο σημείο επαφής για θέματα κυβερνοασφάλειας («ενιαίο σημείο επαφής»). Εάν κάποιο κράτος μέλος ορίσει μόνο μία αρμόδια αρχή, η εν λόγω αρμόδια αρχή αποτελεί επίσης το ενιαίο σημείο επαφής του εν λόγω κράτους μέλους.
4. Κάθε ενιαίο σημείο επαφής ασκεί καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών του οικείου κράτους μέλους με τις σχετικές αρχές άλλων κρατών μελών, καθώς και για τη διασφάλιση της διατομεακής συνεργασίας με άλλες εθνικές αρμόδιες αρχές εντός του οικείου κράτους μέλους.

5. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές της παραγράφου 1 και τα ενιαία σημεία επαφής διαθέτουν επαρκείς πόρους για να επιτελούν αποτελεσματικά και αποδοτικά τα καθήκοντα που τους ανατίθενται και να επιτυγχάνουν, με τον τρόπο αυτό, τους στόχους της παρούσας οδηγίας. Τα κράτη μέλη μεριμνούν για την αποτελεσματική, αποδοτική και ασφαλή συνεργασία των εκπροσώπων που ορίζουν στο πλαίσιο της ομάδας συνεργασίας που αναφέρεται στο άρθρο 12.
6. Κάθε κράτος μέλος κοινοποιεί στην Επιτροπή, χωρίς αδικαιολόγητη καθυστέρηση, τον ορισμό της αρμόδιας αρχής της παραγράφου 1 και του ενιαίου σημείου επαφής της παραγράφου 3, τα καθήκοντά τους καθώς και κάθε μεταγενέστερη τροποποίηση των στοιχείων αυτών. Κάθε κράτος μέλος δημοσιοποιεί την αρμόδια αρχή και το ενιαίο σημείο επαφής που έχει ορίσει. Η Επιτροπή δημοσιεύει τον κατάλογο των ορισθέντων ενιαίων σημείων επαφής.

#### *Άρθρο 9*

#### ***Ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT)***

1. Κάθε κράτος μέλος ορίζει μία ή περισσότερες CSIRT, οι οποίες συμμορφώνονται με τις απαιτήσεις που ορίζονται στο άρθρο 10 παράγραφος 1, καλύπτουν τουλάχιστον τους τομείς, τους επιμέρους τομείς ή τις οντότητες που αναφέρονται στα Παραρτήματα I και II, και είναι υπεύθυνες για τον χειρισμό περιστατικών βάσει σαφώς καθορισμένης διαδικασίας. Η CSIRT μπορεί να συσταθεί εντός της αρμόδιας αρχής που αναφέρεται στο άρθρο 8.
2. Τα κράτη μέλη εξασφαλίζουν ότι κάθε CSIRT διαθέτει επαρκείς πόρους για την αποτελεσματική εκτέλεση των καθηκόντων της που περιγράφονται στο άρθρο 10 παράγραφος 2. **Κατά την εκτέλεση των καθηκόντων αυτών, οι CSIRT μπορούν να δίνουν προτεραιότητα στην παροχή συγκεκριμένων υπηρεσιών σε οντότητες σύμφωνα με προσέγγιση βάσει κινδύνου.**
3. Τα κράτη μέλη διασφαλίζουν ότι κάθε CSIRT διαθέτει κατάλληλη, ασφαλή και ανθεκτική υποδομή επικοινωνίας και πληροφοριών για την ανταλλαγή πληροφοριών με βασικές και σημαντικές οντότητες και άλλα σχετικά ενδιαφερόμενα μέρη. Για τον σκοπό αυτόν, τα κράτη μέλη διασφαλίζουν ότι οι CSIRT συμβάλλουν στην εγκατάσταση ασφαλών εργαλείων ανταλλαγής πληροφοριών.

4. Οι CSIRT συνεργάζονται και, κατά περίπτωση, ανταλλάσσουν σχετικές πληροφορίες σύμφωνα με το άρθρο 26 με αξιόπιστες τομεακές ή διατομεακές κοινότητες βασικών και σημαντικών οντοτήτων.
5. Οι CSIRT συμμετέχουν σε [...] **μάθηση** από ομοτίμους που διοργανώνεται σύμφωνα με το άρθρο 16.
6. Τα κράτη μέλη μεριμνούν για την αποτελεσματική, αποδοτική και ασφαλή συνεργασία των CSIRT τους στο πλαίσιο του δικτύου CSIRT που αναφέρεται στο άρθρο 13.
7. Τα κράτη μέλη κοινοποιούν χωρίς αδικαιολόγητη καθυστέρηση στην Επιτροπή τις CSIRT που έχουν ορίσει σύμφωνα με την παράγραφο 1, τον συντονιστή CSIRT που έχουν ορίσει σύμφωνα με το άρθρο 6 παράγραφος 1 και τα αντίστοιχα καθήκοντά τους σε σχέση με τις οντότητες που αναφέρονται στα Παραρτήματα I και II.
8. Τα κράτη μέλη μπορούν να ζητούν τη συνδρομή του ENISA για τη δημιουργία των εθνικών τους CSIRT.

#### *Άρθρο 10*

#### ***Απαιτήσεις και καθήκοντα των CSIRT***

1. Οι CSIRT συμμορφώνονται με τις ακόλουθες απαιτήσεις:
  - α) οι CSIRT εξασφαλίζουν υψηλό επίπεδο διαθεσιμότητας των [...] **επικοινωνιακών τους διαύλων** αποφεύγοντας μοναδικά σημεία αστοχίας και διαθέτουν διάφορους τρόπους για εισερχόμενη και εξερχόμενη επικοινωνία με τρίτους ανά πάσα στιγμή. Οι CSIRT προσδιορίζουν σαφώς τους διαύλους επικοινωνίας και τους γνωστοποιούν στα μέλη της περιοχής ευθύνης τους και στους συνεργαζόμενους εταίρους·
  - β) τα γραφεία των CSIRT και τα υποστηρικτικά πληροφοριακά συστήματα εγκαθίστανται σε ασφαλείς τοποθεσίες·

- γ) οι CSIRT είναι εφοδιασμένες με κατάλληλο σύστημα διαχείρισης και δρομολόγησης αιτημάτων, ιδίως προκειμένου να διευκολύνεται η αποτελεσματική και αποδοτική παράδοση καθηκόντων·
- δ) οι CSIRT είναι επαρκώς στελεχωμένες ώστε να εξασφαλίζεται η διαθεσιμότητά τους ανά πάσα στιγμή,
- ε) οι CSIRT είναι εξοπλισμένες με πλεονάζοντα συστήματα και εφεδρικό χώρο εργασίας, ώστε να εξασφαλίζεται η συνέχεια των υπηρεσιών τους·
- στ) οι CSIRT έχουν τη δυνατότητα να συμμετέχουν σε διεθνή δίκτυα συνεργασίας.

2. Οι CSIRT έχουν τα ακόλουθα καθήκοντα:

- α) παρακολουθούν κυβερνοαπειλές, τρωτά σημεία και περιστατικά σε εθνικό επίπεδο·
- β) παρέχουν έγκαιρες προειδοποιήσεις, ειδοποιήσεις επαγρύπνησης και ανακοινώσεις και διάδοση πληροφοριών στις βασικές και στις σημαντικές οντότητες, καθώς και **στις αρμόδιες αρχές και σε άλλα ενδιαφερόμενα μέρη σχετικά με κυβερνοαπειλές, τρωτά σημεία και περιστατικά·**
- γ) αντιμετωπίζουν περιστατικά·
- δ) συλλέγουν και αναλύουν εγκληματολογικά δεδομένα και παρέχουν δυναμική ανάλυση κινδύνων και περιστατικών και επίγνωση της κατάστασης όσον αφορά την κυβερνοασφάλεια·
- ε) παρέχουν [...] προδραστική σάρωση των δικτυακών και πληροφοριακών συστημάτων [...] **με σκοπό τον εντοπισμό τρωτών σημείων με δυνητικές σημαντικές επιπτώσεις, υπό την προϋπόθεση ότι, όταν δεν υπάρχει συναίνεση της εν λόγω οντότητας, δεν υπάρχει παρεμβολή στα συστήματα δικτύου και πληροφοριών, ούτε επηρεάζεται αρνητικά η λειτουργία τους·**

στ) συμμετέχουν στο δίκτυο CSIRT και, ανάλογα με τις ικανότητες και τις αρμοδιότητές τους, παρέχουν αμοιβαία συνδρομή σε άλλα μέλη του δικτύου κατόπιν αιτήματός τους.

**στα) όπου συντρέχει περίπτωση, ενεργούν ως συντονίστριες για τους σκοπούς της συντονισμένης διαδικασίας γνωστοποίησης τρωτών σημείων του άρθρου 6 παράγραφος 1, η οποία περιλαμβάνει ιδίως διευκόλυνση της διάδρασης μεταξύ των κοινοποιουσών οντοτήτων, του υπεύθυνου για τα δυνητικά τρωτά σημεία και του κατασκευαστή ή του παρόχου προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ στις περιπτώσεις που αυτό είναι αναγκαίο, εντοπίζουν και έρχονται σε επαφή με τις οικείες οντότητες, στηρίζουν τις κοινοποιούσες οντότητες, διαπραγματεύονται προθεσμίες γνωστοποίησης και διαχειρίζονται τρωτά σημεία που επηρεάζουν πολλαπλούς οργανισμούς (πολυμερής συντονισμένη γνωστοποίηση τρωτών σημείων).**

3. Οι CSIRT αναπτύσσουν σχέσεις συνεργασίας με σχετικούς φορείς του ιδιωτικού τομέα, με σκοπό την καλύτερη επίτευξη των στόχων της οδηγίας.

**3α. Οι CSIRT μπορούν να δημιουργούν σχέσεις συνεργασίας με εθνικές CSIRT τρίτων χωρών. Στο πλαίσιο αυτής της συνεργασίας, μπορούν να ανταλλάσσουν σχετικές πληροφορίες, περιλαμβανομένων και δεδομένων προσωπικού χαρακτήρα, σύμφωνα με το δίκαιο της Ένωσης για την προστασία των δεδομένων.**

4. Προκειμένου να διευκολύνουν τη συνεργασία, οι CSIRT προωθούν την έκδοση και χρήση κοινών ή τυποποιημένων πρακτικών, συστημάτων ταξινόμησης και ταξινομιών σε σχέση με τα ακόλουθα:

α) διαδικασίες χειρισμού περιστατικών·

β) τη διαχείριση κρίσεων κυβερνοασφάλειας·

γ) τη συντονισμένη γνωστοποίηση τρωτών σημείων.

## Άρθρο 11

### *Δημοσίευση σε εθνικό επίπεδο*

1. Εφόσον πρόκειται για διακριτές οντότητες, οι αρμόδιες αρχές που αναφέρονται στο άρθρο 8, το ενιαίο σημείο επαφής και η/οι CSIRT του ίδιου κράτους μέλους συνεργάζονται μεταξύ τους για τους σκοπούς της τήρησης των υποχρεώσεων που προβλέπονται στην παρούσα οδηγία.
2. Τα κράτη μέλη διασφαλίζουν ότι είτε οι αρμόδιες αρχές τους είτε οι CSIRT τους λαμβάνουν κοινοποιήσεις για περιστατικά, σημαντικές κυβερνοαπειλές και παρ' ολίγον περιστατικά που υποβάλλονται σύμφωνα με την παρούσα οδηγία. Αν ένα κράτος μέλος αποφασίσει ότι οι CSIRT του δεν θα λαμβάνουν τις κοινοποιήσεις αυτές, παρέχεται στις CSIRT, στον βαθμό που είναι αναγκαίος για την εκτέλεση των καθηκόντων τους, πρόσβαση σε δεδομένα σχετικά με περιστατικά που κοινοποιούνται από τις βασικές ή τις σημαντικές οντότητες, σύμφωνα με το άρθρο 20.
3. Κάθε κράτος μέλος μεριμνά ώστε οι αρμόδιες αρχές ή οι CSIRT του να ενημερώνουν το ενιαίο σημείο επαφής του για κοινοποιήσεις σχετικά με περιστατικά, σημαντικές κυβερνοαπειλές και παρ' ολίγον περιστατικά που υποβάλλονται σύμφωνα με την παρούσα οδηγία.

4. Στον βαθμό που απαιτείται για την αποτελεσματική εκτέλεση των καθηκόντων και υποχρεώσεων που ορίζονται στην παρούσα οδηγία, τα κράτη μέλη μεριμνούν για την κατάλληλη συνεργασία μεταξύ αρμόδιων αρχών, **CSIRT**, ενιαίων σημείων επαφής καθώς και αρχών επιβολής του νόμου, αρχών προστασίας δεδομένων και των **αρμόδιων αρχών που ορίζονται** [...] σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων], [...] **των αρμόδιων βάσει του εκτελεστικού κανονισμού (ΕΕ) αριθ. 2019/1583 αρχών, των εθνικών αρχών που ορίζονται σύμφωνα με το άρθρο 17 του κανονισμού (ΕΕ) αριθ. 910/2014,** [...] των εθνικών χρηματοπιστωτικών αρχών που ορίζονται σύμφωνα με τον κανονισμό (ΕΕ) XXXX/XXXX του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [κανονισμός DORA], καθώς και **αρμόδιων αρχών που ορίζονται από άλλες τομεακές νομικές πράξεις της Ένωσης** εντός του εν λόγω κράτους μέλους.
5. Τα κράτη μέλη μεριμνούν ώστε **οι αρμόδιες δυνάμει της παρούσας οδηγίας αρχές τους και οι αρμόδιες αρχές που έχουν οριστεί σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων]** να ανταλλάσσουν τακτικά πληροφορίες [...] σχετικά με τον εντοπισμό κρίσιμων οντοτήτων, τους κινδύνους κυβερνοασφάλειας, κυβερνοαπειλές και περιστατικά καθώς και σχετικά με κινδύνους, απειλές και περιστατικά εκτός του κυβερνοχώρου που επηρεάζουν βασικές οντότητες που έχουν χαρακτηριστεί κρίσιμες [ή οντότητες ισοδύναμες με κρίσιμες οντότητες] σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων], καθώς και με τα μέτρα που λήφθηκαν [...] για την αντιμετώπιση των εν λόγω κινδύνων και περιστατικών. Τα κράτη μέλη επίσης μεριμνούν ώστε **οι αρμόδιες δυνάμει της παρούσας οδηγίας αρχές τους [...] και οι αρμόδιες αρχές που έχουν οριστεί σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία DORA], την οδηγία 2018/1972 και τον κανονισμό (ΕΕ) 910/2014 ανταλλάσσουν τακτικά συναφείς πληροφορίες.**



**Όσον** αφορά παρόχους υπηρεσιών εμπιστοσύνης και [...], ιδίως, [...] σε περιπτώσεις όπου αυτός ο εποπτικός ρόλος δυνάμει της παρούσας οδηγίας ανατίθεται σε φορέα διαφορετικό από τους εποπτικούς φορείς που ορίζονται σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014, οι αρμόδιες δυνάμει της παρούσας οδηγίας εθνικές αρχές συνεργάζονται στενά, σε εύθετο χρόνο, ανταλλάσσοντας τις σχετικές πληροφορίες προκειμένου να διασφαλίσουν αποτελεσματική εποπτεία και συμμόρφωση των παρόχων υπηρεσιών εμπιστοσύνης με τις απαιτήσεις που ορίζονται στην παρούσα οδηγία και στον κανονισμό [XXXX/XXXX] **και, κατά περίπτωση, η εθνική αρμόδια αρχή δυνάμει της παρούσας οδηγίας ενημερώνει, χωρίς αδικαιολόγητη καθυστέρηση, τον εποπτικό φορέα eIDAS σχετικά με κάθε κοινοποιημένη σημαντική κυβερνοαπειλή ή συμβάν που έχει αντίκτυπο στις υπηρεσίες εμπιστοσύνης.**

- 5α. Με σκοπό [...] την απλούστευση της αναφοράς περιστατικών, τα κράτη μέλη μπορούν να δημιουργήσουν ένα ενιαίο σημείο εισόδου για όλες τις κοινοποιήσεις που απαιτούνται βάσει της παρούσας οδηγίας, καθώς και δυνάμει του κανονισμού (ΕΕ) 2016/679 και της οδηγίας 2002/58/ΕΚ, όπου ενδείκνυται. Τα κράτη μέλη μπορούν να χρησιμοποιούν το ενιαίο σημείο εισόδου για κοινοποιήσεις που απαιτούνται βάσει άλλων τομεακών νομικών πράξεων της Ένωσης. Το εν λόγω σημείο ενιαίας εξυπηρέτησης δεν θίγει την εφαρμογή των διατάξεων του κανονισμού (ΕΕ) 2016/679 και της οδηγίας 2002/58/ΕΚ, ιδίως εκείνων που αφορούν τις ανεξάρτητες εποπτικές αρχές.**

## ΚΕΦΑΛΑΙΟ ΙΙΙ

### *Ενωσιακή συνεργασία*

#### *Άρθρο 12*

#### **Ομάδα συνεργασίας**

1. Συγκροτείται ομάδα συνεργασίας με σκοπό να υποστηριχθεί και να διευκολυνθεί η στρατηγική συνεργασία και η ανταλλαγή πληροφοριών μεταξύ κρατών μελών [...] **καθώς και να αναπτυχθεί η εμπιστοσύνη και η αξιοπιστία.**
2. Η ομάδα συνεργασίας εκτελεί τα καθήκοντά της βάσει διετών προγραμμάτων εργασιών τα οποία αναφέρονται στην παράγραφο 6.
3. Η ομάδα συνεργασίας *απαρτίζεται από εκπροσώπους των κρατών μελών, της Επιτροπής και του ENISA. Η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης συμμετέχει στις δραστηριότητες της ομάδας συνεργασίας ως παρατηρητής. Οι Ευρωπαϊκές Εποπτικές Αρχές (ΕΕΑ) και οι αρμόδιες αρχές που έχουν οριστεί σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία DORA]* μπορούν να συμμετέχουν στις δραστηριότητες της ομάδας συνεργασίας **σύμφωνα με το άρθρο 42 παράγραφος 1 της οδηγίας (ΕΕ) XXXX/XXXX [οδηγία DORA].**

Ανάλογα με την περίπτωση, η ομάδα συνεργασίας μπορεί να καλεί εκπροσώπους σχετικών ενδιαφερόμενων φορέων για να συμμετάσχουν στις εργασίες της.

Η Επιτροπή παρέχει τη γραμματειακή υποστήριξη.

4. Τα καθήκοντα της ομάδας συνεργασίας είναι τα εξής:
  - α) παροχή καθοδήγησης στις αρμόδιες αρχές όσον αφορά τη μεταφορά στο εθνικό δίκαιο και την εφαρμογή της παρούσας οδηγίας·
  - (αα) παροχή καθοδήγησης σε σχέση με την ανάπτυξη και την εφαρμογή πολιτικών για τη συντονισμένη δημοσιοποίηση τρωτών σημείων, όπως αναφέρεται στο άρθρο 5 παράγραφος 2 στοιχείο γ) και στο άρθρο 6 παράγραφος 1·**

- β) ανταλλάσσει βέλτιστες πρακτικές και πληροφοριών σχετικά με την εφαρμογή της παρούσας οδηγίας, μεταξύ άλλων όσον αφορά κυβερνοαπειλές, περιστατικά, τρωτά σημεία, παρ' ολίγον περιστατικά, πρωτοβουλίες ευαισθητοποίησης, προγράμματα κατάρτισης, ασκήσεις και δεξιότητες, ανάπτυξη ικανότητες, καθώς και πρότυπα και τεχνικές προδιαγραφές·
- γ) ανταλλάσσει συμβουλές και συνεργασία με την Επιτροπή σχετικά με αναδυόμενες πρωτοβουλίες πολιτικής σε θέματα κυβερνοασφάλειας·
- δ) ανταλλάσσει συμβουλές και συνεργασία με την Επιτροπή σχετικά με σχέδια εκτελεστικών [...] πράξεων της Επιτροπής που εκδίδονται δυνάμει της παρούσας οδηγίας·
- ε) ανταλλάσσει βέλτιστες πρακτικές και πληροφοριών με τα σχετικά θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης·
- (εα) ανταλλάσσει απόψεις σχετικά με την εφαρμογή τομεακής νομοθεσίας με πτυχές κυβερνοασφάλειας·**
- στ) συζητά τις εκθέσεις σχετικά με τη [...] **μάθηση** από ομοτίμους που αναφέρεται στο άρθρο 16 παράγραφος 7·
- ζ) Συζητά **εμπειρίες** [...] από κοινές εποπτικές δραστηριότητες σε διασυνοριακές υποθέσεις, όπως αναφέρεται στο άρθρο 34·
- η) παρέχει στρατηγική καθοδήγηση στο δίκτυο CSIRT **και το EU-CyCLONe** σχετικά με συγκεκριμένα αναδυόμενα ζητήματα·

- ηα) ανταλλάσσει απόψεις σχετικά με την επακολούθηση της πολιτικής για περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας με βάση τα διδάγματα που αντλήθηκαν από το δίκτυο CSIRT και το EU-CyCLONe·
- θ) συνεισφέρει στις ικανότητες κυβερνοασφάλειας όλων των χωρών της Ένωσης διευκολύνοντας τη ανταλλαγή εθνικών υπαλλήλων μέσω προγράμματος ανάπτυξης ικανοτήτων με τη συμμετοχή προσωπικού από τις αρμόδιες αρχές ή τις CSIRT των κρατών μελών·
- ι) διοργάνωση τακτικών κοινών συνεδριάσεων με σχετικούς ιδιωτικούς ενδιαφερόμενους φορείς από ολόκληρη την Ένωση για τη συζήτηση των δραστηριοτήτων που πραγματοποιεί η ομάδα και τη συγκέντρωση στοιχείων σχετικά με αναδυόμενες προκλήσεις πολιτικής·
- ια) συζήτηση των εργασιών που σχετίζονται με τις ασκήσεις κυβερνοασφάλειας, συμπεριλαμβανομένων των εργασιών που εκτελεί ο ENISA·
- ιβ) θέσπιση του μηχανισμού αμοιβαίας μάθησης σύμφωνα με το άρθρο 16 της παρούσας οδηγίας.**

5. Η ομάδα συνεργασίας μπορεί να ζητήσει από το δίκτυο CSIRT να εκπονήσει τεχνική έκθεση σχετικά με επιλεγμένα θέματα.
6. Έως ... [24 μήνες μετά την ημερομηνία έναρξης ισχύος της παρούσας οδηγίας] και ανά διετία στη συνέχεια, η ομάδα συνεργασίας καταρτίζει πρόγραμμα εργασιών σχετικά με τις δράσεις που πρέπει να αναληφθούν για την υλοποίηση των στόχων και των καθηκόντων της. Το χρονοδιάγραμμα του πρώτου προγράμματος που θα εγκριθεί δυνάμει της παρούσας οδηγίας ευθυγραμμίζεται με το χρονοδιάγραμμα του τελευταίου προγράμματος που εγκρίθηκε δυνάμει της οδηγίας (ΕΕ) 2016/1148.

7. Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις που καθορίζουν τις διαδικαστικές ρυθμίσεις που είναι αναγκαίες για τη λειτουργία της ομάδας συνεργασίας. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 37 παράγραφος 2.
8. Η ομάδα συνεργασίας συνεδριάζει τακτικά και τουλάχιστον μία φορά ετησίως με την ομάδα ανθεκτικότητας κρίσιμων οντοτήτων που συστάθηκε βάσει της οδηγίας (ΕΕ) XXXX/XXXX [οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων] με σκοπό την προώθηση της στρατηγικής συνεργασίας και **τη διευκόλυνση** της ανταλλαγής πληροφοριών.

### *Άρθρο 13*

#### ***Δίκτυο CSIRT***

1. Δημιουργείται δίκτυο εθνικών CSIRT με σκοπό τη συμβολή στην ανάπτυξη πίστης και εμπιστοσύνης και την προώθηση ταχείας και αποτελεσματικής επιχειρησιακής συνεργασίας μεταξύ των κρατών μελών.
2. Το δίκτυο CSIRT απαρτίζεται από εκπροσώπους των CSIRT των κρατών μελών **που ορίζονται σύμφωνα με το άρθρο 9** και της CERT-EU. Η Επιτροπή συμμετέχει στο δίκτυο CSIRT ως παρατηρητής. Ο ENISA παρέχει τη γραμματειακή υποστήριξη και υποστηρίζει ενεργά τη συνεργασία μεταξύ των CSIRT.
3. Τα καθήκοντα του δικτύου CSIRT είναι τα εξής:
  - α) ανταλλαγή πληροφοριών σχετικά με τις ικανότητες των CSIRT·
  - β) ανταλλαγή σημαντικών πληροφοριών σχετικά με περιστατικά, παρ' ολίγον περιστατικά, κυβερνοαπειλές, κινδύνους και τρωτά σημεία·

- (βα) ανταλλαγή πληροφοριών σχετικά με δημοσιεύσεις και συστάσεις για την κυβερνοασφάλεια·
- (ββ) ανταλλαγή τεχνικών λύσεων που διευκολύνουν τον τεχνικό χειρισμό περιστατικών·
- (βγ) ανταλλαγή βέλτιστων πρακτικών, εργαλείων και διαδικασιών όσον αφορά τα καθήκοντα των CSIRT·
- γ) κατόπιν αιτήματος [...] μέλους του δικτύου CSIRT που έχει ενδεχομένως επηρεαστεί από περιστατικό, ανταλλαγή και συζήτηση πληροφοριών σχετικά με το εν λόγω περιστατικό και τις συναφείς κυβερνοαπειλές, τους κινδύνους και τα τρωτά σημεία·
- δ) κατόπιν αιτήματος [...] μέλους του δικτύου CSIRT, συζήτηση και, αν είναι δυνατόν, εφαρμογή συντονισμένης αντιμετώπισης περιστατικού που έχει διαπιστωθεί εντός της δικαιοδοσίας του συγκεκριμένου κράτους μέλους·
- ε) παροχή στήριξης στα κράτη μέλη για την αντιμετώπιση διασυνοριακών περιστατικών σύμφωνα με την παρούσα οδηγία·
- στ) συνεργασία, **ανταλλαγή βέλτιστων πρακτικών** και παροχή συνδρομής στις ορισθείσες CSIRT που αναφέρονται στο άρθρο 6 όσον αφορά τη διαχείριση της [...] συντονισμένης γνωστοποίησης τρωτών σημείων που επηρεάζουν πολλαπλούς κατασκευαστές ή παρόχους προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ που είναι εγκατεστημένοι σε διαφορετικά κράτη μέλη·
- ζ) συζήτηση και προσδιορισμός περαιτέρω μορφών επιχειρησιακής συνεργασίας, μεταξύ άλλων όσον αφορά:
- i) τις κατηγορίες κυβερνοαπειλών και περιστατικών·
  - ii) τις έγκαιρες προειδοποιήσεις·
  - iii) την αμοιβαία συνδρομή·

- iv) τις αρχές και τις λεπτομέρειες του συντονισμού για την αντιμετώπιση διασυνοριακών κινδύνων και περιστατικών·
- v) τη συμβολή στο εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας που αναφέρεται στο άρθρο 7 παράγραφος 3 **κατόπιν αιτήματος κράτους μέλους**·
- η) ενημέρωση της ομάδας συνεργασίας σχετικά με τις δραστηριότητές του και τις περαιτέρω μορφές επιχειρησιακής συνεργασίας που συζητούνται σύμφωνα με το στοιχείο ζ) **και**, όπου κρίνεται απαραίτητο, υποβολή σχετικού αιτήματος καθοδήγησης·
- θ) άντληση διδαγμάτων από ασκήσεις κυβερνοασφάλειας, μεταξύ άλλων από τις ασκήσεις που διοργανώνει ο ENISA·
- ι) κατόπιν αιτήματος επιμέρους CSIRT, συζήτηση των ικανοτήτων και της ετοιμότητας του εν λόγω CSIRT·
- ια) συνεργασία και ανταλλαγή πληροφοριών με περιφερειακά και ενωσιακά κέντρα επιχειρήσεων ασφάλειας (SOCs) με σκοπό τη βελτίωση της κοινής επίγνωσης της κατάστασης σχετικά με περιστατικά και απειλές σε ολόκληρη την Ένωση·
- ιβ) συζήτηση των εκθέσεων **μάθησης** από ομοτίμους του άρθρου 16 παράγραφος 7·
- ιγ) έκδοση κατευθυντήριων γραμμών προκειμένου να διευκολυνθεί η σύγκλιση των επιχειρησιακών πρακτικών όσον αφορά την εφαρμογή των διατάξεων του παρόντος άρθρου σχετικά με την επιχειρησιακή συνεργασία.

4. Για τους σκοπούς της επανεξέτασης που αναφέρεται στο άρθρο 35 και έως [24 μήνες μετά την ημερομηνία έναρξης ισχύος της παρούσας οδηγίας], και ανά διετία στη συνέχεια, το δίκτυο CSIRT αξιολογεί την πρόοδο που έχει σημειωθεί στον τομέα της επιχειρησιακής συνεργασίας και συντάσσει σχετική έκθεση. Ειδικότερα, στην έκθεση συνάγονται συμπεράσματα σχετικά με τα αποτελέσματα της **μάθησης** [...] από ομοτίμους που αναφέρονται στο άρθρο 16, οι οποίες διενεργούνται σχετικά με τις εθνικές CSIRT, περιλαμβανομένων συμπερασμάτων και συστάσεων, δυνάμει του εν λόγω άρθρου. Η έκθεση αυτή υποβάλλεται επίσης στην ομάδα συνεργασίας.
5. Το δίκτυο CSIRT εγκρίνει τον εσωτερικό του κανονισμό.
6. **Το δίκτυο CSIRT συνεργάζεται με το EU-CyCLONe βάσει συμφωνημένων διαδικαστικών ρυθμίσεων.**

#### *Άρθρο 14*

#### ***Ευρωπαϊκό δίκτυο οργανώσεων διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (EU - CyCLONe)***

1. Δημιουργείται το ευρωπαϊκό δίκτυο οργανώσεων διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (EU - CyCLONe) με σκοπό τη στήριξη της συντονισμένης διαχείρισης περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας σε επιχειρησιακό επίπεδο και τη διασφάλιση της τακτικής ανταλλαγής πληροφοριών μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης.
2. Το δίκτυο EU-CyCLONe απαρτίζεται από τους εκπροσώπους των αρχών διαχείρισης κυβερνοκρίσεων των κρατών μελών που ορίζονται σύμφωνα με το άρθρο 7[...]. **Η Επιτροπή συμμετέχει στις δραστηριότητες του δικτύου ως παρατηρητής.** Η ENISA παρέχει γραμματειακή υποστήριξη στο δίκτυο και υποστηρίζει την ασφαλή ανταλλαγή πληροφοριών. **Επίσης παρέχει τα απαραίτητα εργαλεία για τη στήριξη της συνεργασίας μεταξύ κρατών μελών, διασφαλίζοντας ασφαλή ανταλλαγή πληροφοριών.**

**Ανάλογα με την περίπτωση, το EU-CyCLONe μπορεί να καλεί εκπροσώπους σχετικών ενδιαφερόμενων φορέων να συμμετάσχουν στις εργασίες της.**



3. Τα καθήκοντα του EU-CyCLONe είναι τα εξής:
- α) αύξηση του επιπέδου ετοιμότητας για τη διαχείριση περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας·
  - β) ανάπτυξη κοινής επίγνωσης της κατάστασης [...] για περιστατικά και κρίσεις κυβερνοασφάλειας μεγάλης κλίμακας·
  - (βα) αξιολόγηση των συνεπειών και των επιπτώσεων των σχετικών περιστατικών μεγάλης κλίμακας στον κυβερνοχώρο και πρόταση πιθανών μέτρων μετριασμού·**
  - γ) συντονισμός της **διαχείρισης** περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας και κρίσεων [...] και υποστήριξη της λήψης αποφάσεων σε πολιτικό επίπεδο όσον αφορά τα εν λόγω περιστατικά και τις κρίσεις·
  - δ) **κατόπιν αιτήματος κράτους μέλους**, συζήτηση των εθνικών του σχεδίων αντιμετώπισης περιστατικών και **κρίσεων** κυβερνοασφάλειας που αναφέρονται στο άρθρο 7 παράγραφος 3[...]·[...]
4. Το EU-CyCLONe εγκρίνει τον εσωτερικό κανονισμό του.
5. Το EU-CyCLONe υποβάλλει τακτικά εκθέσεις στην ομάδα συνεργασίας σχετικά με **τη διαχείριση περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας και τη διαχείριση κρίσεων**, [...] εστιάζοντας ιδίως στον αντίκτυπό τους στις βασικές και τις σημαντικές οντότητες.
6. Το EU-CyCLONe συνεργάζεται με το δίκτυο CSIRT βάσει συμφωνημένων διαδικαστικών ρυθμίσεων.
7. **Το EU-CyCLONe υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο έκθεση αξιολόγησης των εργασιών της έως τις [24 μήνες από την ημερομηνία έναρξης ισχύος της παρούσας οδηγίας].**

## *Άρθρο 14α*

### *Διεθνής συνεργασία*

Η Ένωση μπορεί, κατά περίπτωση, να συνάπτει διεθνείς συμφωνίες σύμφωνα με το άρθρο 218 της ΣΛΕΕ με τρίτες χώρες ή διεθνείς οργανισμούς επιτρέποντας και οργανώνοντας τη συμμετοχή τους σε ορισμένες δραστηριότητες της ομάδας συνεργασίας, του δικτύου CSIRT και του EU-CyCLONe, δυνάμει του δικαίου της Ένωσης για την προστασία των δεδομένων.

## *Άρθρο 15*

### *Έκθεση σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση*

1. Ο ENISA εκδίδει, σε συνεργασία με την Επιτροπή και την ομάδα συνεργασίας, έκθεση ανά διετία σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση. **Ειδικότερα, σ[...]**την έκθεση θα [...] περιλαμβάνονται [...] τα ακόλουθα:

**(αα) εκτίμηση κινδύνου κυβερνοασφάλειας σε ενωσιακό επίπεδο, λαμβανομένου υπόψη του τοπίου των απειλών·**

α) [...] **αξιολόγηση της** ανάπτυξης ικανοτήτων κυβερνοασφάλειας στον δημόσιο και τον ιδιωτικό τομέα σε ολόκληρη την Ένωση·

β) [...]

γ) **συγκεντρωτική αξιολόγηση με βάση ποσοτικούς και ποιοτικούς δείκτες [...]** κυβερνοασφάλειας, η οποία παρέχει [...] **επισκόπηση** του επιπέδου ωριμότητας των ικανοτήτων κυβερνοασφάλειας, **συμπεριλαμβανομένων των ειδικών ανά τομέα ικανοτήτων.**

2. Η έκθεση περιλαμβάνει συγκεκριμένες συστάσεις πολιτικής για την αύξηση του επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση και σύνοψη των ευρημάτων που αφορούν τη συγκεκριμένη περίοδο από τις τεχνικές εκθέσεις για την κατάσταση της κυβερνοασφάλειας στην ΕΕ που εκδίδει ο ENISA σύμφωνα με το άρθρο 7 παράγραφος 6 του κανονισμού (ΕΕ) 2019/881.

## Άρθρο 16

### Μάθηση από ομοτίμους

1. **Με σκοπό την ενίσχυση της αμοιβαίας εμπιστοσύνης, την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας, καθώς και την ενίσχυση των ικανοτήτων και των πολιτικών των κρατών μελών στον τομέα της κυβερνοασφάλειας που απαιτούνται για την αποτελεσματική εφαρμογή της παρούσας οδηγίας, η ομάδα συνεργασίας [...] θεσπίζει, με την υποστήριξη της Επιτροπής και μετά από διαβούλευση με [...] τον ENISA και, κατά περίπτωση, το δίκτυο CSIRT, και το αργότερο εντός 24 [...] μηνών από την έναρξη ισχύος της παρούσας οδηγίας, τη μεθοδολογία [...] ενός συστήματος αντικειμενικής, αμερόληπτης και δίκαιης μάθησης από [...] ομοτίμους [...] όσον αφορά την εφαρμογή της παρούσας οδηγίας [...] από τα κράτη μέλη. Η συμμετοχή στη μάθηση από ομοτίμους είναι προαιρετική. Το σύστημα αποτελείται από κύκλους αξιολόγησης [...] που διεξάγονται από [...] εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας που προέρχονται από κράτη μέλη [...] και καλύπτουν [...] μία ή περισσότερες από τις ακόλουθες πτυχές:**
- (i) την [...] εφαρμογή των απαιτήσεων διαχείρισης κινδύνων για την κυβερνοασφάλεια και των υποχρεώσεων αναφοράς περιστατικών που αναφέρονται στα άρθρα 18 και 20·
  - (ii) τις [...] ικανότητες, συμπεριλαμβανομένων των διαθέσιμων [...] πόρων, και την [...] άσκηση των καθηκόντων εκ μέρους των εθνικών αρμόδιων αρχών που αναφέρονται στο άρθρο 8 και των CSIRT που αναφέρονται στο άρθρο 9·

[...]

(iii[...]) την εφαρμογή αμοιβαίας συνδρομής που αναφέρεται στο άρθρο 34·

(iv) την [...] εφαρμογή του πλαισίου ανταλλαγής πληροφοριών που αναφέρεται στο άρθρο 26 [...].

2. **Τα κριτήρια βάσει των οποίων τα κράτη μέλη ορίζουν εμπειρογνώμονες επιλέξιμους για συμμετοχή στους κύκλους μάθησης από ομοτίμους πρέπει να είναι [...] αντικειμενικά, αμερόληπτα, δίκαια και διαφανή [...] και να περιλαμβάνονται στη μεθοδολογία που αναφέρεται στην παράγραφο 1. Ο ENISA και η Επιτροπή [...] μπορούν να ορίζουν εμπειρογνώμονες οι οποίοι συμμετέχουν ως παρατηρητές [...] στους κύκλους μάθησης από ομοτίμους. [...]**
3. [...] .

- 3α. Πριν από την έναρξη των κύκλων μάθησης από ομοτίμους, τα κράτη μέλη μπορούν να διενεργούν αυτοαξιολόγηση των πτυχών που καλύπτονται από τον συγκεκριμένο κύκλο μάθησης από ομοτίμους και να παρέχουν την αυτοαξιολόγηση στους ορισθέντες εμπειρογνώμονες της παραγράφου 2.**
4. Η **μάθηση** [...] από ομοτίμους [...] **μπορεί να συνεπάγεται [...] πραγματικές ή εικονικές επιτόπιες επισκέψεις και ανταλλαγές εκτός των εγκαταστάσεων. Με γνώμονα την αρχή της καλής συνεργασίας, τα [...] κράτη μέλη που συμμετέχουν στη μάθηση από ομοτίμους παρέχουν στους ορισθέντες εμπειρογνώμονες τις [...] πληροφορίες που είναι αναγκαίες για την αξιολόγηση [...], με την επιφύλαξη της εθνικής ή της ενωσιακής νομοθεσίας σχετικά με την προστασία εμπιστευτικών ή διαβαθμισμένων πληροφοριών ή τη διασφάλιση ουσιωδών λειτουργιών του κράτους, όπως η εθνική ασφάλεια. Κάθε πληροφορία που λαμβάνεται μέσω της διαδικασίας [...] μάθησης από ομοτίμους χρησιμοποιείται αποκλειστικά για τον σκοπό αυτό. Οι εμπειρογνώμονες που συμμετέχουν στη [...] μάθηση από ομοτίμους δεν αποκαλύπτουν σε τρίτους τυχόν ευαίσθητες ή εμπιστευτικές πληροφορίες που [...] απέκτησαν στο πλαίσιο αυτό. Το κράτος μέλος που συμμετέχει στη μάθηση από ομοτίμους μπορεί να αντιταχθεί στον ορισμό συγκεκριμένων εμπειρογνομόνων για δεόντως αιτιολογημένους λόγους που κοινοποιούνται στην ομάδα συνεργασίας.**

5. Εφόσον **υποβληθούν σε κύκλο μάθησης από ομοτίμους [...]** οι ίδιες πτυχές δεν υπόκεινται σε περαιτέρω γύρους [...] **μάθησης από ομοτίμους [...]** για τα συμμετέχοντα κράτη μέλη κατά τη διάρκεια των [...] **τεσσάρων ετών** μετά την ολοκλήρωση του εν λόγω [...] γύρου **μάθησης από ομοτίμους, εκτός εάν το ενδιαφερόμενο κράτος μέλος το ζητήσει ή συμφωνήσει σχετικά με την πρόταση [...]** από την ομάδα συνεργασίας [...].
6. [...]
7. Οι εμπειρογνώμονες που συμμετέχουν [...] σε κύκλους **μάθησης από ομοτίμους** συντάσσουν εκθέσεις με τα ευρήματα και τα συμπεράσματα των [...] **αξιολογήσεων. Τα κράτη μέλη έχουν τη δυνατότητα να υποβάλουν παρατηρήσεις σχετικά με τα αντίστοιχα σχέδια έκθεσής τους, τα οποία επισυνάπτονται στην έκθεση.** Οι τελικές εκθέσεις υποβάλλονται [...] στην ομάδα συνεργασίας [...] **Τα κράτη μέλη μπορούν να αποφασίσουν να δημοσιοποιήσουν τις αντίστοιχες εκθέσεις τους.**

## ΚΕΦΑΛΑΙΟ IV

*Διαχείριση κινδύνων στον τομέα της κυβερνοασφάλειας και υποχρεώσεις αναφοράς περιστατικών*

### ΤΜΗΜΑ I

*Διαχείριση κινδύνων στον τομέα της κυβερνοασφάλειας και αναφορά περιστατικών*

#### *Άρθρο 17*

#### **Διακυβέρνηση**

1. Τα κράτη μέλη διασφαλίζουν ότι τα διοικητικά όργανα βασικών και σημαντικών οντοτήτων εγκρίνουν τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που λαμβάνονται από τις εν λόγω οντότητες προκειμένου να συμμορφωθούν με το άρθρο 18, [...] **επιβλέπουν** την εφαρμογή του και **μπορούν να θεωρηθούν υπόλογα** για τη μη συμμόρφωση των οντοτήτων με τις υποχρεώσεις που απορρέουν από το παρόν άρθρο.

**Η εφαρμογή της παρούσας παραγράφου δεν θίγει τις εθνικές νομοθεσίες των κρατών μελών σχετικά με τους κανόνες περί ευθύνης στους δημόσιους οργανισμούς, καθώς και την ευθύνη των δημοσίων υπαλλήλων και των εκλεγμένων και διορισμένων αξιωματούχων.**

2. Τα κράτη μέλη διασφαλίζουν ότι **τα μέλη του διοικητικού οργάνου** [...] **υποχρεούνται να** παρακολουθούν, σε τακτική βάση, [...] προγράμματα κατάρτισης για την απόκτηση επαρκών γνώσεων και δεξιοτήτων ώστε να αντιλαμβάνονται και να αξιολογούν τους κινδύνους για την κυβερνοασφάλεια και τις πρακτικές διαχείρισής τους, καθώς και τον αντίκτυπό τους στις δραστηριότητες της οντότητας.

*Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας*

- 1α. Η παρούσα οδηγία εφαρμόζει μια προσέγγιση «παντός κινδύνου» που περιλαμβάνει την προστασία των συστημάτων δικτύου και πληροφοριών και του φυσικού τους περιβάλλοντος από κάθε περιστατικό που θα μπορούσε να θέσει σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω δικτυακών και πληροφοριακών συστημάτων.
1. Τα κράτη μέλη εξασφαλίζουν ότι οι βασικές και σημαντικές οντότητες [...] λαμβάνουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων που παρουσιάζονται για την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων που χρησιμοποιούν οι εν λόγω οντότητες κατά την παροχή των υπηρεσιών τους. Λαμβανομένων υπόψη των πλέον πρόσφατων τεχνικών δυνατοτήτων και του κόστους εφαρμογής, τα μέτρα αυτά διασφαλίζουν επίπεδο ασφάλειας δικτυακών και πληροφοριακών συστημάτων ανάλογο προς τον εκάστοτε κίνδυνο. **Κατά την αξιολόγηση της αναλογικότητας των μέτρων αυτών, λαμβάνεται δεόντως υπόψη ο βαθμός έκθεσης της οντότητας σε κινδύνους, το μέγεθός της, η πιθανότητα επέλευσης περιστατικών και η σοβαρότητά τους. Λαμβανομένων υπόψη του επιπέδου και του είδους του κινδύνου που διατρέχει η κοινωνία σε περίπτωση περιστατικών που επηρεάζουν βασικές ή σημαντικές οντότητες, τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που επιβάλλονται σε σημαντικές οντότητες μπορούν να είναι λιγότερο αυστηρά από εκείνα που επιβάλλονται σε βασικές οντότητες.**



2. Στα μέτρα που αναφέρονται στην παράγραφο 1 περιλαμβάνονται τουλάχιστον τα ακόλουθα:
- α) πολιτικές ανάλυσης κινδύνων και ασφάλειας του πληροφοριακού συστήματος·
  - β) χειρισμός περιστατικών (πρόληψη, ανίχνευση, [...] αντιμετώπιση περιστατικών και **ανάκαμψη από αυτά**)·
  - γ) συνέχιση των δραστηριοτήτων και διαχείριση των κρίσεων·
  - δ) η ασφάλεια της αλυσίδας εφοδιασμού, συμπεριλαμβανομένων των σχετικών με την ασφάλεια πτυχών που αφορούν τις σχέσεις μεταξύ της κάθε οντότητας και των **άμεσων** προμηθευτών της ή των παρόχων υπηρεσιών, όπως οι πάροχοι υπηρεσιών αποθήκευσης και επεξεργασίας δεδομένων ή υπηρεσιών διαχείρισης ασφάλειας·
  - ε) η ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση δικτυακών και πληροφοριακών συστημάτων, συμπεριλαμβανομένου του χειρισμού και της γνωστοποίησης τρωτών σημείων·
  - στ) πολιτικές και διαδικασίες [...] για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας·
  - ζ) **πολιτική για** τη χρήση της κρυπτογράφησης και της κρυπτοθέτησης·
  - ζα) **Ασφάλεια ανθρώπινων πόρων, πολιτικές ελέγχου πρόσβασης και διαχείριση περιουσιακών στοιχείων.**
3. Τα κράτη μέλη διασφαλίζουν ότι, κατά την εξέταση των κατάλληλων μέτρων που αναφέρονται στην παράγραφο 2 στοιχείο δ), οι οντότητες [...] **υποχρεούνται να** λαμβάνουν υπόψη τα τρωτά σημεία που χαρακτηρίζουν κάθε **άμεσο** προμηθευτή και πάροχο υπηρεσιών, καθώς και τη συνολική ποιότητα των προϊόντων και πρακτικών κυβερνοασφάλειας των προμηθευτών και των παρόχων υπηρεσιών τους, συμπεριλαμβανομένων των ασφαλών διαδικασιών ανάπτυξής τους. **Τα κράτη μέλη διασφαλίζουν επίσης ότι, κατά την εξέταση των κατάλληλων μέτρων που αναφέρονται στην παράγραφο 2 στοιχείο δ), οι οντότητες υποχρεούνται να λαμβάνουν υπόψη τα αποτελέσματα των συντονισμένων εκτιμήσεων κινδύνου που διενεργούνται σύμφωνα με το άρθρο 19 παράγραφος 1.**

4. Τα κράτη μέλη διασφαλίζουν ότι, όταν μια οντότητα διαπιστώνει ότι οι υπηρεσίες ή τα καθήκοντά της, αντίστοιχα, δεν συνάδουν με τις απαιτήσεις της παραγράφου 2, λαμβάνει, χωρίς αδικαιολόγητη καθυστέρηση, όλα τα αναγκαία διορθωτικά μέτρα για να εξασφαλίσει τη συμμόρφωση της σχετικής υπηρεσίας.
5. Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις για τον καθορισμό των τεχνικών και μεθοδολογικών προδιαγραφών, **καθώς και τομεακών ιδιαιτεροτήτων, εφόσον απαιτείται, των στοιχείων που αναφέρονται στην παράγραφο 2 του παρόντος άρθρου. Η Επιτροπή εκδίδει έως τις [18 μήνες από την έναρξη ισχύος της παρούσας οδηγίας] εκτελεστικές πράξεις προκειμένου να καθοριστούν οι τεχνικές και μεθοδολογικές προδιαγραφές για τις οντότητες που αναφέρονται στο άρθρο 24 παράγραφος 1 και τους παρόχους υπηρεσιών εμπιστοσύνης που αναφέρονται στο σημείο 8 του παραρτήματος Ι. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 37 παράγραφος 2. Κατά [...] την εκπόνηση [...] των εν λόγω εκτελεστικών πράξεων, η Επιτροπή [...] ακολουθεί, στον μέγιστο δυνατό βαθμό, τα διεθνή και ευρωπαϊκά πρότυπα, καθώς και τις σχετικές τεχνικές προδιαγραφές και ανταλλάσσει συμβουλές με την ομάδα συνεργασίας και την ENISA για το σχέδιο εκτελεστικής πράξης σύμφωνα με το άρθρο 12 παράγραφος 4 στοιχείο δ).**
6. [...]

#### *Άρθρο 19*

##### *Συντονισμένες από την ΕΕ εκτιμήσεις κινδύνου για τις κρίσιμες αλυσίδες εφοδιασμού*

1. Η ομάδα συνεργασίας, σε συνεργασία με την Επιτροπή και τον ENISA, μπορεί να διενεργεί συντονισμένες εκτιμήσεις κινδύνου για την ασφάλεια συγκεκριμένων κρίσιμων υπηρεσιών, συστημάτων ή προϊόντων αλυσίδων εφοδιασμού ΤΠΕ, λαμβάνοντας υπόψη τεχνικούς και, κατά περίπτωση, μη τεχνικούς παράγοντες κινδύνου.

2. Η Επιτροπή, κατόπιν διαβούλευσης με την ομάδα συνεργασίας και τον ENISA, προσδιορίζει τις συγκεκριμένες κρίσιμες υπηρεσίες, συστήματα ή προϊόντα ΤΠΕ που ενδέχεται να υπόκεινται στη συντονισμένη εκτίμηση κινδύνου που αναφέρεται στην παράγραφο 1.

## Άρθρο 20

### Υποχρεώσεις αναφοράς περιστατικών

1. Τα κράτη μέλη διασφαλίζουν ότι οι βασικές και σημαντικές οντότητες κοινοποιούν, χωρίς αδικαιολόγητη καθυστέρηση, στις αρμόδιες αρχές ή στην CSIRT, σύμφωνα με τις παραγράφους 3 και 4, κάθε περιστατικό που έχει σημαντικό αντίκτυπο στην παροχή των υπηρεσιών τους. Κατά περίπτωση, οι εν λόγω οντότητες κοινοποιούν στους αποδέκτες των υπηρεσιών τους, χωρίς αδικαιολόγητη καθυστέρηση, **τα περιστατικά εκείνα** που ενδέχεται να επηρεάσουν δυσμενώς την παροχή των εν λόγω υπηρεσιών. Τα κράτη μέλη διασφαλίζουν ότι οι εν λόγω οντότητες αναφέρουν, μεταξύ άλλων, κάθε πληροφορία που επιτρέπει στις αρμόδιες αρχές ή στην CSIRT να προσδιορίσουν τυχόν διασυννοριακές επιπτώσεις του περιστατικού. **Η πράξη της κοινοποίησης καθαυτή δεν συνεπάγεται αυξημένη ευθύνη για την κοινοποιούσα οντότητα.**
2. [...]

Κατά περίπτωση, [...] **οι βασικές και σημαντικές** οντότητες κοινοποιούν, χωρίς αδικαιολόγητη καθυστέρηση, στους αποδέκτες των υπηρεσιών τους που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή τυχόν μέτρα ή διορθωτικά μέτρα που μπορούν να λάβουν οι εν λόγω αποδέκτες για την αντιμετώπιση της εν λόγω απειλής. Κατά περίπτωση, οι οντότητες ενημερώνουν επίσης τους εν λόγω αποδέκτες για την ίδια την απειλή. **Η πράξη της κοινοποίησης καθαυτή** δεν συνεπάγεται αυξημένη ευθύνη για τη σχετική οντότητα.

3. Ένα περιστατικό θεωρείται σημαντικό σε περίπτωση που:
- α) προκάλεσε ή έχει τη δυνατότητα να προκαλέσει **σοβαρή** [...] λειτουργική διαταραχή **της υπηρεσίας** ή οικονομικές ζημιές στην οικεία οντότητα·
  - β) έχει επηρεάσει ή έχει τη δυνατότητα να επηρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντικές υλικές ή μη υλικές ζημιές.
4. Τα κράτη μέλη διασφαλίζουν ότι, για τους σκοπούς της κοινοποίησης δυνάμει της παραγράφου 1, οι οικείες οντότητες υποβάλλουν στις αρμόδιες αρχές ή στην CSIRT:
- α) χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που έλαβαν γνώση του περιστατικού, μια αρχική κοινοποίηση **ως έγκαιρη προειδοποίηση**, στην οποία, κατά περίπτωση, αναφέρεται αν το περιστατικό προκλήθηκε πιθανώς από παράνομη ή κακόβουλη ενέργεια·
  - β) κατόπιν αιτήματος αρμόδιας αρχής ή CSIRT, ενδιάμεση έκθεση σχετικά με την εξέλιξη της κατάστασης·
  - γ) **τελική** έκθεση το αργότερο ένα μήνα μετά την υποβολή της [...] **αρχικής κοινοποίησης** βάσει του στοιχείου α), η οποία περιλαμβάνει τουλάχιστον τα ακόλουθα:
    - i) λεπτομερή περιγραφή του περιστατικού, της σοβαρότητάς του και των επιπτώσεών του·
    - ii) το είδος της απειλής ή τη βασική αιτία που ενδεχομένως προκάλεσε το περιστατικό·
    - iii) εφαρμοζόμενα και εν εξέλιξη μέτρα μετριασμού.

Τα κράτη μέλη προβλέπουν ότι, σε δεόντως αιτιολογημένες περιπτώσεις και σε συμφωνία με τις αρμόδιες αρχές ή την CSIRT, η οικεία οντότητα μπορεί να παρεκκλίνει από τις προθεσμίες που ορίζονται στα στοιχεία α) και γ). **Ειδικότερα, παρέκκλιση από την προθεσμία του στοιχείου γ) μπορεί να δικαιολογηθεί σε περιπτώσεις κατά τις οποίες το περιστατικό βρίσκεται ακόμη σε εξέλιξη.**

5. Οι αρμόδιες εθνικές αρχές ή η CSIRT παρέχουν, [...] **χωρίς αδικαιολόγητη καθυστέρηση** μετά την παραλαβή της αρχικής κοινοποίησης που αναφέρεται στην παράγραφο 4 στοιχείο α), απάντηση στην κοινοποιούσα οντότητα, συμπεριλαμβανομένης αρχικής ανατροφοδότησης σχετικά με το περιστατικό και, κατόπιν αιτήματος της οντότητας, καθοδήγηση σχετικά με την εφαρμογή πιθανών μέτρων μετριασμού. Σε περίπτωση που η CSIRT δεν έλαβε τη κοινοποίηση που αναφέρεται στην παράγραφο 1, η καθοδήγηση παρέχεται από την αρμόδια αρχή σε συνεργασία με την CSIRT. Η CSIRT παρέχει πρόσθετη τεχνική υποστήριξη κατόπιν αιτήματος της ενδιαφερόμενης οντότητας. Όταν υπάρχουν υπόνοιες ότι το περιστατικό είναι εγκληματικού χαρακτήρα, οι αρμόδιες εθνικές αρχές ή η CSIRT παρέχουν επίσης καθοδήγηση σχετικά με την αναφορά του περιστατικού στις αρχές επιβολής του νόμου.
6. Κατά περίπτωση, και ιδίως όταν το περιστατικό που αναφέρεται στην παράγραφο 1 αφορά δύο ή περισσότερα κράτη μέλη, η αρμόδια αρχή, η CSIRT ή **το ενιαίο σημείο επαφής** ενημερώνουν τα λοιπά επηρεαζόμενα κράτη μέλη και τον ENISA για το περιστατικό. **Οι πληροφορίες αυτές περιλαμβάνουν τουλάχιστον τα στοιχεία που προβλέπονται στην παράγραφο 4 του παρόντος άρθρου.** Στο πλαίσιο της ενημέρωσης αυτής, οι αρμόδιες αρχές, οι CSIRT και τα ενιαία σημεία επαφής, σύμφωνα με το ενωσιακό δίκαιο, ή με την εθνική νομοθεσία που είναι σύμφωνη προς το ενωσιακό δίκαιο, διαφυλάσσουν την ασφάλεια και τα εμπορικά συμφέροντα της οντότητας, καθώς και το απόρρητο των πληροφοριών που έχουν παρασχεθεί.
7. Όταν η ευαισθητοποίηση του κοινού είναι απαραίτητη για την πρόληψη περιστατικού ή για την αντιμετώπιση εν εξελίξει περιστατικού, ή όταν η γνωστοποίηση του περιστατικού εξυπηρετεί άλλως το δημόσιο συμφέρον, η αρμόδια αρχή ή η CSIRT και, κατά περίπτωση, οι αρχές ή οι CSIRT άλλων ενδιαφερόμενων κρατών μελών μπορούν, κατόπιν διαβούλευσης με την ενδιαφερόμενη οντότητα, να ενημερώνουν το κοινό σχετικά με το περιστατικό ή να απαιτούν από την οντότητα να το πράξει.

8. Κατόπιν αιτήματος της αρμόδιας αρχής ή της CSIRT, το ενιαίο σημείο επαφής διαβιβάζει τις κοινοποιήσεις που παραλήφθηκαν δυνάμει της παραγράφου[...] 1 [...] στα ενιαία κέντρα επαφής άλλων επηρεαζόμενων κρατών μελών.
9. Το ενιαίο σημείο επαφής υποβάλλει στον ENISA [...] **κάθε έξι μήνες** συνοπτική έκθεση που περιλαμβάνει ανωνυμοποιημένα και συγκεντρωτικά δεδομένα σχετικά με περιστατικά, σημαντικές κυβερνοαπειλές και παρ' ολίγον περιστατικά που κοινοποιούνται σύμφωνα με την παράγραφο[...] 1 [...] και σύμφωνα με το άρθρο 27. Προκειμένου να συμβάλει στην παροχή συγκρίσιμων πληροφοριών, ο ENISA μπορεί να εκδώσει τεχνική καθοδήγηση σχετικά με τις παραμέτρους των πληροφοριών που περιλαμβάνονται στη συνοπτική έκθεση. **Η ENISA ενημερώνει κάθε έξι μήνες την ομάδα συνεργασίας και το δίκτυο CSIRT για τα πορίσματά της σχετικά με τις κοινοποιήσεις που παραλήφθηκαν.**
10. Οι αρμόδιες αρχές παρέχουν στις αρμόδιες αρχές που έχουν οριστεί σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων] πληροφορίες σχετικά με περιστατικά και κυβερνοαπειλές που κοινοποιούνται σύμφωνα με τις παραγράφους 1 και 2 από βασικές οντότητες που έχουν χαρακτηριστεί κρίσιμες οντότητες [ή οντότητες ισοδύναμες με κρίσιμες οντότητες,] σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων].
11. Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις με τις οποίες προσδιορίζεται περαιτέρω το είδος των πληροφοριών, το μορφότυπο και η διαδικασία κοινοποίησης που υποβάλλεται σύμφωνα με τις παραγράφους 1 και 2. Η Επιτροπή μπορεί επίσης να εκδίδει εκτελεστικές πράξεις για τον περαιτέρω προσδιορισμό των περιπτώσεων στις οποίες ένα περιστατικό θεωρείται σημαντικό, όπως αναφέρεται στην παράγραφο 3. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 37 παράγραφος 2.

**Χρήση των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας**

1. Προκειμένου να αποδειχθεί η συμμόρφωση με ορισμένες απαιτήσεις του άρθρου 18, **τα κράτη μέλη μπορούν να απαιτούν από τις οντότητες να χρησιμοποιούν συγκεκριμένα προϊόντα, [...] υπηρεσίες και [...] διαδικασίες ΤΠΕ που πιστοποιούνται** στο πλαίσιο συγκεκριμένων ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας που εγκρίνονται σύμφωνα με το άρθρο 49 του κανονισμού (ΕΕ) 2019/881. Τα προϊόντα, οι υπηρεσίες και οι διαδικασίες ΤΠΕ που υπόκεινται σε πιστοποίηση μπορούν να αναπτυχθούν από βασική ή σημαντική οντότητα ή να παρασχεθούν από τρίτους.
2. Η Επιτροπή μπορεί [...] να εκδίδει [...] **εκτελεστικές πράξεις** με τις οποίες θα προσδιορίζεται από ποιες κατηγορίες βασικών ή σημαντικών οντοτήτων θα απαιτείται η **χρήση πιστοποιημένων προϊόντων, υπηρεσιών και διαδικασιών** ή η λήψη πιστοποιητικού [...] και δυνάμει ποιων [...] ευρωπαϊκών συστημάτων πιστοποίησης που **καθορίζονται βάσει του άρθρου 49 του κανονισμού (ΕΕ) 2019/881[...]**. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης του άρθρου 37 παράγραφος 2. Κατά την κατάρτιση των εν λόγω εκτελεστικών πράξεων, η Επιτροπή, σύμφωνα με το άρθρο 56 του κανονισμού (ΕΕ) 2019/881:
  - i) λαμβάνει υπόψη τον αντίκτυπο των μέτρων στους κατασκευαστές ή παρόχους των εν λόγω προϊόντων, υπηρεσιών ή διαδικασιών ΤΠΕ και στους χρήστες από άποψη κόστους των εν λόγω μέτρων και τα κοινωνικά ή οικονομικά οφέλη που προκύπτουν από το αναμενόμενο βελτιωμένο επίπεδο ασφάλειας για τα στοχευόμενα προϊόντα, υπηρεσίες και διαδικασίες ΤΠΕ, καθώς και τη διαθεσιμότητα εναλλακτικών στην αγορά·
  - ii) προβαίνει σε ανοικτή, διαφανή και χωρίς αποκλεισμούς διαδικασία διαβούλευσης με όλους τους σχετικούς ενδιαφερόμενους φορείς και τα κράτη μέλη·

- (iii) λαμβάνει υπόψη τις προθεσμίες εφαρμογής, τα μεταβατικά μέτρα και χρονικά διαστήματα, ιδίως όσον αφορά τον πιθανό αντίκτυπο των μέτρων στους κατασκευαστές ή παρόχους προϊόντων, υπηρεσιών ή διαδικασιών ΤΠΕ, ή τους χρήστες αυτών, ιδίως των ΜΜΕ·
  - (iv) λαμβάνει υπόψη την ύπαρξη και την εφαρμογή σχετικής νομοθεσίας των κρατών μελών.
3. Η Επιτροπή μπορεί να ζητήσει από τον ENISA να καταρτίσει υποψήφιο σύστημα ή να επανεξετάσει υφιστάμενο ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας σύμφωνα με το άρθρο 48 παράγραφος 2 του κανονισμού (ΕΕ) 2019/881 στις περιπτώσεις που δεν υπάρχει διαθέσιμο κατάλληλο ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας για τους σκοπούς της παραγράφου 2 του παρόντος άρθρου.

#### *Άρθρο 22*

#### ***Τυποποίηση***

1. Για να προωθήσουν τη συγκλίνουσα εφαρμογή του άρθρου 18 παράγραφοι 1 και 2, τα κράτη μέλη, χωρίς να επιβάλλουν ούτε να ευνοούν τη χρησιμοποίηση συγκεκριμένου είδους τεχνολογίας, ενθαρρύνουν τη χρήση ευρωπαϊκών ή διεθνώς αποδεκτών προτύπων και προδιαγραφών σχετικών με την ασφάλεια δικτυακών και πληροφοριακών συστημάτων.
2. Ο ENISA, σε συνεργασία με τα κράτη μέλη, εκδίδει συμβουλές και κατευθυντήριες γραμμές όσον αφορά τους τεχνικούς τομείς που θα πρέπει να εξεταστούν σε σχέση με την παράγραφο 1, καθώς και όσον αφορά ήδη υφιστάμενα πρότυπα, συμπεριλαμβανομένων των εθνικών προτύπων των κρατών μελών, για την κάλυψη αυτών των τομέων.



## Άρθρο 23

### **Βάσεις δεδομένων με ονόματα τομέα και δεδομένα καταχώρισης**

1. Για τους σκοπούς της συμβολής στην ασφάλεια, τη σταθερότητα και την ανθεκτικότητα του συστήματος ονομάτων τομέα (DNS), τα κράτη μέλη διασφαλίζουν ότι τα μητρώα **ονομάτων** TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για μητρώα TLD συλλέγουν και διατηρούν ακριβή, [...] και πλήρη δεδομένα καταχώρισης ονομάτων τομέα σε ειδική βάση δεδομένων με τη δέουσα επιμέλεια **σύμφωνα με τη** [...] νομοθεσία της Ένωσης για την προστασία των δεδομένων όσον αφορά τα δεδομένα προσωπικού χαρακτήρα.
2. Τα κράτη μέλη διασφαλίζουν ότι οι βάσεις δεδομένων καταχώρισης ονομάτων τομέα που αναφέρονται στην παράγραφο 1 περιέχουν σχετικές πληροφορίες για τον εντοπισμό και την επικοινωνία με τους κατόχους των ονομάτων τομέα και τα σημεία επαφής που διαχειρίζονται τα ονόματα τομέα στο πλαίσιο των TLD, **περιλαμβάνουν δε τουλάχιστον τα ακόλουθα δεδομένα:**
  - α) **όνομα τομέα**
  - β) **ημερομηνία καταχώρισης**
  - γ) **δεδομένα καταχώρισης, τα οποία περιλαμβάνουν:**
    - i) **για φυσικά πρόσωπα – όνομα, επώνυμο και διεύθυνση ηλεκτρονικού ταχυδρομείου·**
    - ii) **για νομικά πρόσωπα: – επωνυμία και διεύθυνση ηλεκτρονικού ταχυδρομείου.**

3. Τα κράτη μέλη διασφαλίζουν ότι τα μητρώα **ονομάτων** TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD διαθέτουν πολιτικές και διαδικασίες που διασφαλίζουν ότι οι βάσεις δεδομένων περιλαμβάνουν ακριβείς και πλήρεις πληροφορίες. Τα κράτη μέλη διασφαλίζουν ότι οι εν λόγω πολιτικές και διαδικασίες δημοσιοποιούνται.
4. Τα κράτη μέλη διασφαλίζουν ότι τα μητρώα **ονομάτων** TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD δημοσιεύουν, χωρίς αδικαιολόγητη καθυστέρηση μετά την καταχώριση ονόματος τομέα, τα δεδομένα καταχώρισης τομέα που δεν αποτελούν δεδομένα προσωπικού χαρακτήρα.
5. Τα κράτη μέλη διασφαλίζουν ότι τα μητρώα **ονομάτων** TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD παρέχουν πρόσβαση σε συγκεκριμένα δεδομένα καταχώρισης ονομάτων τομέα κατόπιν νόμιμων και δεόντως αιτιολογημένων αιτημάτων νόμιμων αιτούντων πρόσβαση, σύμφωνα με τη νομοθεσία της Ένωσης για την προστασία των δεδομένων. Τα κράτη μέλη διασφαλίζουν ότι τα μητρώα **ονομάτων** TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD ανταποκρίνονται χωρίς αδικαιολόγητη καθυστέρηση, **και σε κάθε περίπτωση εντός 72 ωρών**, σε όλα τα αιτήματα πρόσβασης. Τα κράτη μέλη διασφαλίζουν ότι οι πολιτικές και οι διαδικασίες γνωστοποίησης των εν λόγω δεδομένων δημοσιοποιούνται.

## Τμήμα II

### Δικαιοδοσία και καταχώριση

#### Άρθρο 24

#### *Δικαιοδοσία και εδαφικότητα*

- 1α. Οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας θεωρείται ότι υπάγονται στη δικαιοδοσία του κράτους μέλους στο οποίο παρέχουν τις υπηρεσίες τους. Οι οντότητες των σημείων 1 έως 7 και 10 του παραρτήματος I, οι πάροχοι υπηρεσιών εμπιστοσύνης και οι πάροχοι σημείων ανταλλαγής κίνησης διαδικτύου του σημείου 8 του παραρτήματος I, και οι οντότητες των σημείων 1 έως 5 του παραρτήματος II θεωρείται ότι υπάγονται στη δικαιοδοσία του κράτους μέλους στην επικράτεια του οποίου είναι εγκατεστημένοι.**
1. Οι πάροχοι υπηρεσιών DNS, τα μητρώα ονομάτων TLD[...] **και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD**, οι πάροχοι υπηρεσιών νεφοϋπολογιστικής, οι πάροχοι υπηρεσιών κέντρου δεδομένων, [...] οι πάροχοι δικτύων διανομής περιεχομένου, **οι πάροχοι υπηρεσιών διαχείρισης, και οι πάροχοι υπηρεσιών διαχείρισης ασφάλειας** που αναφέρονται στο παράρτημα I σημείο 8 **και σημείο 8α**, καθώς και οι πάροχοι ψηφιακών υπηρεσιών που αναφέρονται στο παράρτημα II σημείο 6 θεωρείται ότι υπάγονται στη δικαιοδοσία του κράτους μέλους στο οποίο έχουν την κύρια εγκατάστασή τους στην Ένωση.
2. Για τους σκοπούς της παρούσας οδηγίας, οι οντότητες που αναφέρονται στην παράγραφο 1 θεωρείται ότι έχουν την κύρια εγκατάστασή τους στην Ένωση στο κράτος μέλος όπου λαμβάνονται **κυρίως οι αποφάσεις σχετικά με τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας**. Εάν **δεν μπορεί να προσδιορισθεί ο τόπος στον οποίο λαμβάνονται κυρίως οι εν λόγω αποφάσεις** ή οι αποφάσεις αυτές δεν λαμβάνονται σε κάποια εγκατάσταση στην Ένωση, η κύρια εγκατάσταση θεωρείται ότι βρίσκεται στο κράτος μέλος στο οποίο οι οντότητες έχουν την εγκατάσταση με τον μεγαλύτερο αριθμό εργαζομένων στην Ένωση. **Όταν οι υπηρεσίες παρέχονται από όμιλο επιχειρήσεων, η κύρια εγκατάσταση θεωρείται ως η κύρια εγκατάσταση του ομίλου επιχειρήσεων.**

3. Εάν μια οντότητα που αναφέρεται στην παράγραφο 1 δεν είναι εγκατεστημένη στην Ένωση, αλλά παρέχει υπηρεσίες εντός της Ένωσης, ορίζει εκπρόσωπο στην Ένωση. Ο εκπρόσωπος είναι εγκατεστημένος σε ένα από τα κράτη μέλη στα οποία προσφέρονται οι υπηρεσίες. Μια τέτοια οντότητα θεωρείται ότι υπόκειται στη δικαιοδοσία του κράτους μέλους στο οποίο είναι εγκατεστημένος ο εκπρόσωπος. Εάν δεν έχει οριστεί εκπρόσωπος εντός της Ένωσης δυνάμει του παρόντος άρθρου, κάθε κράτος μέλος στο οποίο η οντότητα παρέχει υπηρεσίες μπορεί να κινήσει νομικές διαδικασίες κατά της οντότητας για μη συμμόρφωση με τις υποχρεώσεις που απορρέουν από την παρούσα οδηγία.
4. Ο ορισμός εκπροσώπου από οντότητα που αναφέρεται στην παράγραφο 1 δεν θίγει τις νομικές ενέργειες οι οποίες μπορούν να αναληφθούν κατά της ίδιας της οντότητας.
- 4α. Τα κράτη μέλη που έχουν λάβει αίτημα αμοιβαίας συνδρομής σε σχέση με τις οντότητες που αναφέρονται στην παράγραφο 1, μπορούν, εντός των ορίων του αιτήματος, να λαμβάνουν κατάλληλα μέτρα εποπτείας και επιβολής σε σχέση με την οικεία οντότητα η οποία παρέχει υπηρεσίες ή διαθέτει το σύστημα δικτύου και πληροφοριών στην επικράτειά τους.**

#### *Άρθρο 25*

#### *Μητρώο ορισμένων οντοτήτων ψηφιακών υποδομών και παρόχων ψηφιακών υπηρεσιών*

1. [...] Τα κράτη μέλη διασφαλίζουν ότι οι [...] οντότητες του άρθρου 24 παράγραφος 1 των οποίων η κύρια εγκατάσταση βρίσκεται στην επικράτειά τους ή, αν δεν είναι εγκατεστημένες στην Ένωση, των οποίων ο εντεταλμένος εκπρόσωπος στην Ένωση είναι εγκατεστημένος στην επικράτειά τους, υποχρεούνται να [...] υποβάλλουν τις ακόλουθες πληροφορίες στις αρμόδιες αρχές [...] το [αργότερο έως 12 μήνες από την έναρξη ισχύος της οδηγίας]:

- α) την επωνυμία της οντότητας·
- αα) το είδος της οντότητας σύμφωνα με τα παραρτήματα Ι και ΙΙ της παρούσας οδηγίας·**
- β) τη διεύθυνση της κύριας εγκατάστασής της και των άλλων νόμιμων εγκαταστάσεών της στην Ένωση ή, εάν δεν είναι εγκατεστημένη στην Ένωση, του εκπροσώπου της που έχει οριστεί σύμφωνα με το άρθρο 24 παράγραφος 3·
- γ) επικαιροποιημένα στοιχεία επικοινωνίας, συμπεριλαμβανομένων των διευθύνσεων ηλεκτρονικού ταχυδρομείου και των αριθμών τηλεφώνου των οντοτήτων, **καθώς και των εκπροσώπων τους·**
- δ) **τα κράτη μέλη στα οποία η οντότητα παρέχει την υπηρεσία.**

**Κατά περίπτωση, οι πληροφορίες αυτές υποβάλλονται μέσω του εθνικού μηχανισμού[...] αυτοκοινοποίησης που αναφέρεται στο άρθρο 2α.**

2. **Τα κράτη μέλη διασφαλίζουν ότι οι[...] οντότητες που αναφέρονται στην παράγραφο 1[...] κοινοποιούν επίσης** τυχόν αλλαγές στα στοιχεία που υπέβαλαν σύμφωνα με την παράγραφο 1 χωρίς καθυστέρηση και, σε κάθε περίπτωση, εντός τριών μηνών από την ημερομηνία πραγματοποίησης της αλλαγής.
3. [...] **Τα ενιαία σημεία επαφής των κρατών μελών διαβιβάζουν τις πληροφορίες που αναφέρονται στις παραγράφους 1 και 2 [...] στον [...] ENISA. [...]**

3α. Με βάση τις πληροφορίες που λαμβάνονται σύμφωνα με την παράγραφο 3 του παρόντος άρθρου, ο ENISA δημιουργεί και διατηρεί μητρώο με τις οντότητες που αναφέρονται στην παράγραφο 1. Κατόπιν αιτήματος των κρατών μελών, ο ENISA επιτρέπει την πρόσβαση των σχετικών αρμόδιων αρχών στο μητρώο, διασφαλίζοντας παράλληλα, κατά περίπτωση, τις αναγκαίες εγγυήσεις για την προστασία του απορρήτου των πληροφοριών.

4. [...]

## ΚΕΦΑΛΑΙΟ V

### *Ανταλλαγή πληροφοριών*

#### *Άρθρο 26*

##### *Ρυθμίσεις για την ανταλλαγή πληροφοριών στον τομέα της κυβερνοασφάλειας*

1. [...] Τα κράτη μέλη διασφαλίζουν ότι οι βασικές και σημαντικές οντότητες μπορούν να ανταλλάσσουν μεταξύ τους, **σε εθελοντική βάση**, σχετικές πληροφορίες για την κυβερνοασφάλεια, μεταξύ άλλων πληροφορίες για κυβερνοαπειλές, **παρ' ολίγον περιστατικά**, τρωτά σημεία, δείκτες έκθεσης σε κίνδυνο, τακτικές, τεχνικές και διαδικασίες, προειδοποιήσεις για την κυβερνοασφάλεια και εργαλεία παραμετροποίησης, στον βαθμό που η εν λόγω ανταλλαγή πληροφοριών:
  - α) αποσκοπεί στην πρόληψη, τον εντοπισμό, την αντιμετώπιση ή τον μετριασμό περιστατικών

- β) ενισχύει το επίπεδο κυβερνοασφάλειας, ιδίως μέσω της ευαισθητοποίησης σε σχέση με τις κυβερνοαπειλές, του περιορισμού ή της παρεμπόδισης της ικανότητας διάδοσης των εν λόγω απειλών, της στήριξης μιας σειράς αμυντικών ικανοτήτων, της αποκατάστασης και γνωστοποίησης τρωτών σημείων, των τεχνικών ανίχνευσης απειλών, των στρατηγικών μετριασμού ή των σταδίων αντίδρασης και ανάκαμψης.
2. Τα κράτη μέλη διασφαλίζουν ότι η ανταλλαγή πληροφοριών πραγματοποιείται στο πλαίσιο [...] κοινοτήτων βασικών και σημαντικών οντοτήτων. Η ανταλλαγή αυτή πραγματοποιείται βάσει ρυθμίσεων ανταλλαγής πληροφοριών όσον αφορά τον δυνητικά ευαίσθητο χαρακτήρα των ανταλλασσόμενων πληροφοριών [...].
3. Τα κράτη μέλη [...] **μπορούν να** θεσπίζουν κανόνες που προσδιορίζουν τη διαδικασία, τα επιχειρησιακά στοιχεία (συμπεριλαμβανομένης της χρήσης ειδικών πλατφορμών ΤΠΕ), το περιεχόμενο και τους όρους των ρυθμίσεων ανταλλαγής πληροφοριών που αναφέρονται στην παράγραφο 2. Οι εν λόγω κανόνες [...] **μπορούν να** καθορίζουν επίσης τις λεπτομέρειες της συμμετοχής των δημόσιων αρχών στις εν λόγω ρυθμίσεις, καθώς και τα επιχειρησιακά στοιχεία, συμπεριλαμβανομένης της χρήσης ειδικών πλατφορμών ΤΠ. Τα κράτη μέλη παρέχουν στήριξη για την εφαρμογή των εν λόγω ρυθμίσεων σύμφωνα με τις πολιτικές τους που αναφέρονται στο άρθρο 5 παράγραφος 2 στοιχείο ζ).
4. Οι βασικές και σημαντικές οντότητες γνωστοποιούν στις αρμόδιες αρχές τη συμμετοχή τους στις ρυθμίσεις ανταλλαγής πληροφοριών που αναφέρονται στην παράγραφο 2, μόλις προσχωρήσουν στις εν λόγω ρυθμίσεις ή, ανάλογα με την περίπτωση, την ανάκληση της συμμετοχής τους στις ρυθμίσεις αυτές, μόλις τεθεί σε ισχύ η απόσυρση.
5. [...] Ο ENISA στηρίζει τη θέσπιση ρυθμίσεων για την ανταλλαγή πληροφοριών στον τομέα της κυβερνοασφάλειας που αναφέρονται στην παράγραφο 2, παρέχοντας βέλτιστες πρακτικές και καθοδήγηση.

*Εθελούσια κοινοποίηση των σχετικών πληροφοριών*

- 1. Με την επιφύλαξη του άρθρου 20, τα κράτη μέλη διασφαλίζουν ότι βασικές και σημαντικές οντότητες μπορούν να κοινοποιούν, σε εθελοντική βάση, στις αρμόδιες αρχές ή στις CSIRT τυχόν σχετικά περιστατικά, κυβερνοαπειλές ή παρ' ολίγον περιστατικά.**
- Τα κράτη μέλη διασφαλίζουν ότι, με την επιφύλαξη του άρθρου 3, οι οντότητες που δεν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας μπορούν να υποβάλλουν κοινοποιήσεις, σε εθελοντική βάση, για σημαντικά περιστατικά, κυβερνοαπειλές ή παρ' ολίγον περιστατικά. Κατά την επεξεργασία των κοινοποιήσεων, τα κράτη μέλη ενεργούν σύμφωνα με τη διαδικασία που προβλέπεται στο άρθρο 20. Τα κράτη μέλη μπορούν να δίνουν προτεραιότητα στην επεξεργασία των υποχρεωτικών έναντι των εθελούσιων κοινοποιήσεων. **Με την επιφύλαξη της διερεύνησης, του εντοπισμού και της δίωξης ποινικών αδικημάτων, η[...] εθελούσια αναφορά δεν συνεπάγεται την επιβολή στην αναφέρουσα οντότητα πρόσθετων υποχρεώσεων τις οποίες δεν θα υπείχε αν δεν προέβαινε στην κοινοποίηση.**
- 3. Οι εθελούσιες κοινοποιήσεις υποβάλλονται σε επεξεργασία μόνον εφόσον η επεξεργασία αυτή δεν συνιστά δυσανάλογη ή περιττή επιβάρυνση για το οικείο κράτος μέλος.**



# ΚΕΦΑΛΑΙΟ VI

## *Εποπτεία και επιβολή*

### *Άρθρο 28*

#### ***Γενικές πτυχές που αφορούν την εποπτεία και την επιβολή***

1. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές παρακολουθούν αποτελεσματικά και λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν τη συμμόρφωση με την παρούσα οδηγία [...], ιδίως με τις υποχρεώσεις που ορίζονται στα άρθρα 18, [...] 20 και 23. **Τα κράτη μέλη μπορούν να επιτρέπουν στις αρμόδιες αρχές να δίνουν προτεραιότητα στην εποπτεία, η οποία βασίζεται σε μια προσέγγιση με βάση τον κίνδυνο.**
2. Κατά την αντιμετώπιση περιστατικών κυβερνοασφάλειας, οι αρμόδιες αρχές συνεργάζονται στενά με τις αρχές προστασίας δεδομένων, **με τις αρμόδιες αρχές που έχουν οριστεί σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων], με εποπτικούς φορείς που έχουν οριστεί σύμφωνα με τον κανονισμό (ΕΕ) 910/2014 και με άλλες αρμόδιες αρχές που έχουν οριστεί σύμφωνα με τομεακές νομοθετικές πράξεις της Ένωσης . [...]**
3. **Με την επιφύλαξη των εθνικών νομοθετικών και θεσμικών πλαισίων, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές, κατά την εποπτεία της συμμόρφωσης των φορέων δημόσιας διοίκησης με την παρούσα οδηγία και την επιβολή ενδεχόμενων κυρώσεων σε περιπτώσεις μη συμμόρφωσης, διαθέτουν τις κατάλληλες εξουσίες για την εκτέλεση των εν λόγω καθηκόντων με επιχειρησιακή ανεξαρτησία έναντι των εποπτευόμενων οντοτήτων. Τα κράτη μέλη μπορούν να αποφασίζουν την επιβολή κατάλληλων, αναλογικών και αποτελεσματικών μέτρων εποπτείας και επιβολής σε σχέση με τις εν λόγω οντότητες σύμφωνα με τα εθνικά πλαίσια και την εθνική έννομη τάξη.**

**Εποπτεία και επιβολή όσον αφορά τις βασικές οντότητες**

1. Τα κράτη μέλη διασφαλίζουν ότι τα μέτρα εποπτείας ή επιβολής που επιβάλλονται σε βασικές οντότητες σε σχέση με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία είναι αποτελεσματικά, αναλογικά και αποτρεπτικά, λαμβάνοντας υπόψη τις περιστάσεις κάθε μεμονωμένης περίπτωσης.
2. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές, κατά την άσκηση των εποπτικών τους καθηκόντων σε σχέση με βασικές οντότητες, **ακολουθούν μια προσέγγιση με βάση τον κίνδυνο και έχουν την εξουσία να υποβάλλουν τις εν λόγω οντότητες κατ' ελάχιστον σε διαδικασίες που αφορούν:**
  - α) επιτόπιες επιθεωρήσεις και εποπτεία εκτός των εγκαταστάσεων, συμπεριλαμβανομένων δειγματοληπτικών ελέγχων·
  - β) τακτικούς ελέγχους **ασφάλειας**·
  - γ) στοχευμένους ελέγχους ασφάλειας με βάση εκτιμήσεις κινδύνου ή διαθέσιμες πληροφορίες σχετικά με τον κίνδυνο·
  - δ) σαρώσεις ασφάλειας που βασίζονται σε αντικειμενικά, αμερόληπτα, δίκαια και διαφανή κριτήρια αξιολόγησης κινδύνου, **όπου απαιτείται για τεχνικούς λόγους, με τη συνεργασία του ενδιαφερόμενου φορέα**·
  - ε) αιτήματα παροχής πληροφοριών που είναι αναγκαίες για την αξιολόγηση των μέτρων κυβερνοασφάλειας που λαμβάνει η οντότητα, συμπεριλαμβανομένων τεκμηριωμένων πολιτικών κυβερνοασφάλειας[...].
  - στ) αιτήματα πρόσβασης σε δεδομένα, έγγραφα ή πληροφορίες που απαιτούνται για την εκτέλεση των εποπτικών καθηκόντων τους·
  - ζ) αιτήματα για αποδεικτικά στοιχεία που αφορούν την εφαρμογή των πολιτικών κυβερνοασφάλειας, όπως τα αποτελέσματα των ελέγχων ασφάλειας που διενεργούνται από εξουσιοδοτημένο επιθεωρητή και τα αντίστοιχα υποκείμενα αποδεικτικά στοιχεία.

- 2α. Κατά την άσκηση των εποπτικών εξουσιών τους που προβλέπονται στην παράγραφο 2 του παρόντος άρθρου, οι αρμόδιες αρχές μπορούν να θεσπίζουν εποπτικές μεθόδους που επιτρέπουν την ιεράρχηση των καθηκόντων αυτών ακολουθώντας μια προσέγγιση με βάση τον κίνδυνο.
3. Κατά την άσκηση των εξουσιών τους δυνάμει της παραγράφου 2 στοιχεία ε) έως ζ), οι αρμόδιες αρχές δηλώνουν τον σκοπό του αιτήματος και προσδιορίζουν τις ζητούμενες πληροφορίες.
4. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές, κατά την άσκηση των εξουσιών τους επιβολής σε σχέση με βασικές οντότητες, δύνανται **τουλάχιστον**:
- α) να εκδίδουν προειδοποιήσεις σχετικά με τη μη συμμόρφωση των οντοτήτων με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία·
  - β) να εκδίδουν δεσμευτικές οδηγίες ή διαταγή προς τις εν λόγω οντότητες να αποκαταστήσουν τις διαπιστωθείσες ελλείψεις ή τις παραβάσεις των υποχρεώσεων που ορίζονται στην παρούσα οδηγία·
  - γ) να διατάσσουν τις εν λόγω οντότητες να παύσουν συμπεριφορά που δεν συμμορφώνεται προς τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία και να απόσχουν από την επανάληψη της εν λόγω συμπεριφοράς·
  - δ) να διατάσσουν τις εν λόγω οντότητες να προβούν σε συμμόρφωση των μέτρων διαχείρισης κινδύνου και/ή των υποχρεώσεων αναφοράς περιστατικών προς τις υποχρεώσεις που ορίζονται στα άρθρα 18 και 20 με συγκεκριμένο τρόπο και εντός καθορισμένης προθεσμίας·
  - ε) να διατάσσουν τις εν λόγω οντότητες να ενημερώνουν το φυσικό ή νομικό πρόσωπο (ή πρόσωπα), στα οποία παρέχουν υπηρεσίες ή δραστηριότητες που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή, **για τη φύση της απειλής, καθώς και για τυχόν μέτρα προστασίας ή αποκατάστασης που μπορούν να ληφθούν από το εν λόγω φυσικό ή νομικό πρόσωπο (ή πρόσωπα) για την αντιμετώπιση της εν λόγω απειλής·**
  - στ) να διατάσσουν τις εν λόγω οντότητες να εφαρμόσουν τις συστάσεις που διατυπώθηκαν κατόπιν ελέγχου ασφάλειας εντός εύλογης προθεσμίας·
  - ζ) [...]

η) να διατάσσουν τις εν λόγω οντότητες να δημοσιοποιούν πτυχές της μη συμμόρφωσης με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία με συγκεκριμένο τρόπο, **εφόσον η δημοσιοποίηση αυτή δεν οδηγεί σε επιζήμια έκθεση της αντίστοιχης οντότητας**

θ) [...]

ι) να επιβάλλουν ή να ζητούν από τα αρμόδια όργανα ή δικαστήρια να επιβάλουν, σύμφωνα με την εθνική νομοθεσία, διοικητικό πρόστιμο δυνάμει του άρθρου 31 επιπλέον ή αντί των μέτρων που αναφέρονται στα στοιχεία α) έως θ) της παρούσας παραγράφου, ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης.

5. Σε περίπτωση που τα μέτρα επιβολής που θεσπίζονται σύμφωνα με την παράγραφο 4 στοιχεία α) έως δ) και στ) αποδειχθούν αναποτελεσματικά, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές έχουν την εξουσία να ορίσουν προθεσμία εντός της οποίας η βασική οντότητα καλείται να λάβει τα αναγκαία μέτρα για την αποκατάσταση των ελλείψεων ή τη συμμόρφωση με τις απαιτήσεις των εν λόγω αρχών. Εάν τα ζητούμενα μέτρα δεν ληφθούν εντός της ταχθείσας προθεσμίας, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές έχουν την εξουσία:

α) να αναστείλουν ή να ζητήσουν από φορέα πιστοποίησης ή εξουσιοδότησης **ή από δικαστήρια, σύμφωνα με την εθνική νομοθεσία**, να αναστείλουν πιστοποίηση ή εξουσιοδότηση που αφορά μέρος ή το σύνολο των υπηρεσιών ή δραστηριοτήτων που παρέχονται από βασική οντότητα·

β) να επιβάλουν ή να ζητήσουν από τα αρμόδια όργανα ή δικαστήρια να επιβάλουν, σύμφωνα με την εθνική νομοθεσία, προσωρινή απαγόρευση κατά οποιουδήποτε προσώπου ασκεί διευθυντικά καθήκοντα σε επίπεδο γενικού διευθυντή ή νομικού εκπροσώπου στην εν λόγω βασική οντότητα, καθώς και οποιουδήποτε άλλου φυσικού προσώπου θεωρείται υπαίτιο για την παράβαση, να ασκούν διευθυντικά καθήκοντα στην εν λόγω οντότητα.

Οι κυρώσεις αυτές επιβάλλονται μόνο έως ότου η οντότητα λάβει τα αναγκαία μέτρα για την αποκατάσταση των ελλείψεων ή τη συμμόρφωση με τις απαιτήσεις της αρμόδιας αρχής για τις οποίες επιβλήθηκαν οι εν λόγω κυρώσεις.

**Οι κυρώσεις που προβλέπονται στην παρούσα παράγραφο δεν εφαρμόζονται σε φορείς της δημόσιας διοίκησης που υπάγονται στο πεδίο εφαρμογής της παρούσας οδηγίας.**

6. Τα κράτη μέλη διασφαλίζουν ότι κάθε φυσικό πρόσωπο που είναι υπεύθυνο ή ενεργεί ως αντιπρόσωπος βασικής οντότητας με βάση την εξουσία εκπροσώπησής της, την αρμοδιότητα να λαμβάνει αποφάσεις εξ ονόματός της ή να ασκεί τον έλεγχό της, έχει τις εξουσίες να διασφαλίζει τη συμμόρφωσή της με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία. Τα κράτη μέλη μεριμνούν ώστε τα εν λόγω φυσικά πρόσωπα να μπορούν να θεωρηθούν υπεύθυνα για παράβαση των καθηκόντων τους όσον αφορά την τήρηση των υποχρεώσεων που ορίζονται στην παρούσα οδηγία. **Όσον αφορά τους φορείς δημόσιας διοίκησης, η παρούσα διάταξη εφαρμόζεται με την επιφύλαξη της νομοθεσίας των κρατών μελών όσον αφορά την ευθύνη των δημοσίων υπαλλήλων και των εκλεγμένων και διορισμένων αξιωματούχων.**
7. Κατά τη λήψη μέτρων επιβολής ή την επιβολή κυρώσεων σύμφωνα με τις παραγράφους 4 και 5, οι αρμόδιες αρχές συμμορφώνονται με τα δικαιώματα της υπεράσπισης και λαμβάνουν υπόψη τις περιστάσεις κάθε μεμονωμένης περίπτωσης και, κατ' ελάχιστον, λαμβάνουν δεόντως υπόψη:
  - α) τη σοβαρότητα της παράβασης και τη σημασία των διατάξεων που παραβιάστηκαν. Στις παραβάσεις που θα πρέπει να θεωρούνται σοβαρές συγκαταλέγονται: επανειλημμένες παραβιάσεις, παράλειψη κοινοποίησης ή αποκατάστασης περιστατικών με αποτέλεσμα τη σημαντική διατάραξη, αδυναμία αποκατάστασης ελλείψεων σύμφωνα με δεσμευτικές οδηγίες των αρμόδιων αρχών, παρεμπόδιση των ελέγχων ή των δραστηριοτήτων παρακολούθησης που διατάσσονται από την αρμόδια αρχή μετά τη διαπίστωση παράβασης, παροχή ψευδών ή χονδροειδώς διαστρεβλωμένων πληροφοριών σε σχέση με τις απαιτήσεις διαχείρισης κινδύνου ή τις υποχρεώσεις αναφοράς περιστατικών που ορίζονται στα άρθρα 18 και 20.

- β) η διάρκεια της παράβασης, συμπεριλαμβανομένου του στοιχείου των επανειλημμένων παραβάσεων·
  - γ) η πραγματική ζημία που προκλήθηκε ή οι απώλειες που προέκυψαν ή οι δυνητικές ζημιές ή απώλειες που θα μπορούσαν να έχουν προκληθεί, στον βαθμό που μπορούν να προσδιοριστούν. Κατά την αξιολόγηση αυτής της πτυχής, λαμβάνονται υπόψη, μεταξύ άλλων, οι πραγματικές ή δυνητικές χρηματοοικονομικές ή οικονομικές απώλειες, οι επιπτώσεις σε άλλες υπηρεσίες, ο αριθμός των χρηστών που επηρεάζονται ή ενδέχεται να επηρεαστούν·
  - δ) το αν η παράβαση διαπράχθηκε εκ προθέσεως ή εξ αμελείας·
  - ε) μέτρα που λαμβάνει η οντότητα για την πρόληψη ή τον μετριασμό της ζημίας ή/και των απωλειών·
  - στ) η τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης·
  - ζ) ο βαθμός συνεργασίας του υπαίτιου φυσικού ή νομικού προσώπου (ή προσώπων) με τις αρμόδιες αρχές.
8. Οι αρμόδιες αρχές αιτιολογούν λεπτομερώς τις αποφάσεις τους όσον αφορά την επιβολή. Πριν από τη λήψη των εν λόγω αποφάσεων, οι αρμόδιες αρχές κοινοποιούν στις ενδιαφερόμενες οντότητες τα προκαταρκτικά πορίσματά τους και παρέχουν εύλογο χρονικό διάστημα στις εν λόγω οντότητες για να υποβάλουν τις παρατηρήσεις τους, **πλην των περιπτώσεων επικείμενου κινδύνου.**

9. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους **δυνάμει της παρούσας οδηγίας** ενημερώνουν τις σχετικές αρμόδιες αρχές **μέσα στο ίδιο** κράτος μέλος που έχουν οριστεί σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων] κατά την άσκηση των εξουσιών τους εποπτείας και επιβολής με σκοπό τη διασφάλιση της συμμόρφωσης βασικής οντότητας που έχει χαρακτηριστεί κρίσιμη [ή ισοδύναμη με κρίσιμη οντότητα], δυνάμει της οδηγίας (ΕΕ) XXXX/XXXX [οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων], προς τις υποχρεώσεις που απορρέουν από την παρούσα οδηγία. **Κατά περίπτωση, [...]** οι αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) XXXX/XXXX [οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων][...] **μπορούν να ζητούν** από τις αρμόδιες αρχές **δυνάμει της παρούσας οδηγίας** [...] **να** ασκούν τις εξουσίες τους εποπτείας και επιβολής σε βασική οντότητα υπαγόμενη στο πεδίο εφαρμογής της παρούσας οδηγίας που έχει επίσης χαρακτηριστεί κρίσιμη [ή εξομοιώνεται με κρίσιμη] **δυνάμει της οδηγίας (ΕΕ) XXXX/XXXX [οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων].**
10. Τα κράτη μέλη διασφαλίζουν ότι οι δυνάμει της παρούσας οδηγίας αρμόδιες αρχές τους ενημερώνουν το φόρουμ εποπτείας σύμφωνα με το άρθρο 29 παράγραφος 1 του κανονισμού (ΕΕ) XXXX/XXXX [DORA] κατά την άσκηση των εξουσιών τους εποπτείας και επιβολής που έχουν ως στόχο να διασφαλίσουν ότι η βασική οντότητα που έχει οριστεί ως κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 28 του κανονισμού (ΕΕ) XXXX/XXXX [DORA] συμμορφώνεται προς τις υποχρεώσεις που απορρέουν από την παρούσα οδηγία.
- 10α. Τα κράτη μέλη διασφαλίζουν ότι οι δυνάμει της παρούσας οδηγίας αρμόδιες αρχές τους ενημερώνουν τις σχετικές αρμόδιες αρχές που έχουν οριστεί σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014 κατά την άσκηση των εξουσιών τους εποπτείας και επιβολής που έχουν ως στόχο να διασφαλίσουν ότι η οντότητα που έχει οριστεί ως πάροχος υπηρεσιών εμπιστοσύνης σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014 συμμορφώνεται προς τις υποχρεώσεις που απορρέουν από την παρούσα οδηγία.

## Άρθρο 30

### Εποπτεία και επιβολή όσον αφορά σημαντικές οντότητες

1. Όταν τους υποβάλλονται αποδεικτικά στοιχεία ή ενδείξεις ή πληροφορίες ότι μια σημαντική οντότητα **φέρεται ότι** δεν συμμορφώνεται με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία, και ιδίως στα άρθρα 18 και 20, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές αναλαμβάνουν δράση, όπου απαιτείται, μέσω εκ των υστέρων εποπτικών μέτρων.
2. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές, κατά την άσκηση των εποπτικών τους καθηκόντων σε σχέση με σημαντικές οντότητες, **ακολουθούν μια προσέγγιση με βάση τον κίνδυνο και έχουν την εξουσία να υποβάλλουν τις εν λόγω οντότητες κατ' ελάχιστον σε διαδικασίες που αφορούν:**
  - α) επιτόπιες επιθεωρήσεις και εκ των υστέρων εποπτεία εκτός των εγκαταστάσεων·
  - β) στοχευμένους ελέγχους ασφάλειας με βάση εκτιμήσεις κινδύνου ή διαθέσιμες πληροφορίες σχετικά με τον κίνδυνο·
  - γ) σαρώσεις ασφάλειας που βασίζονται σε αντικειμενικά, **αμερόληπτα**, δίκαια και διαφανή κριτήρια αξιολόγησης κινδύνου, **όπου απαιτείται για τεχνικούς λόγους, με τη συνεργασία του ενδιαφερόμενου φορέα·**
  - δ) αιτήματα για τυχόν πληροφορίες που είναι αναγκαίες για την εκ των υστέρων αξιολόγηση των μέτρων κυβερνοασφάλειας[...];
  - ε) αιτήματα πρόσβασης σε δεδομένα, έγγραφα ή/και πληροφορίες που απαιτούνται για την εκτέλεση των εποπτικών καθηκόντων·
  - εα) **αιτήματα για αποδεικτικά στοιχεία που αφορούν την εφαρμογή των πολιτικών κυβερνοασφάλειας, όπως τα αποτελέσματα των ελέγχων ασφάλειας που διενεργούνται από εξουσιοδοτημένο επιθεωρητή και τα αντίστοιχα υποκείμενα αποδεικτικά στοιχεία.**



- 2α. Κατά την άσκηση των εποπτικών εξουσιών τους που προβλέπονται στην παράγραφο 2 του παρόντος άρθρου, οι αρμόδιες αρχές μπορούν να θεσπίζουν εποπτικές μεθόδους που επιτρέπουν την ιεράρχηση των καθηκόντων αυτών ακολουθώντας μια προσέγγιση με βάση τον κίνδυνο.**
3. Κατά την άσκηση των εξουσιών τους δυνάμει της παραγράφου 2 στοιχεία δ) έως εα), οι αρμόδιες αρχές δηλώνουν τον σκοπό του αιτήματος και προσδιορίζουν τις ζητούμενες πληροφορίες.
4. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές, κατά την άσκηση των εξουσιών τους επιβολής σε σχέση με σημαντικές οντότητες, δύνανται **τουλάχιστον**:
- α) να εκδίδουν προειδοποιήσεις σχετικά με τη μη συμμόρφωση των οντοτήτων με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία·
  - β) να εκδίδουν δεσμευτικές οδηγίες ή διαταγή προς τις εν λόγω οντότητες να αποκαταστήσουν τις διαπιστωθείσες ελλείψεις ή την παράβαση των υποχρεώσεων που ορίζονται στην παρούσα οδηγία·
  - γ) να διατάσσουν τις εν λόγω οντότητες να παύσουν τη συμπεριφορά που δεν συμμορφώνεται προς τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία και να απόσχουν από την επανάληψη της εν λόγω συμπεριφοράς·
  - δ) να διατάσσουν τις εν λόγω οντότητες να προβούν σε συμμόρφωση των μέτρων διαχείρισης κινδύνου ή των υποχρεώσεων αναφοράς περιστατικών προς τις υποχρεώσεις που ορίζονται στα άρθρα 18 και 20 με συγκεκριμένο τρόπο και εντός καθορισμένης προθεσμίας·
  - ε) να διατάσσουν τις εν λόγω οντότητες να ενημερώνουν το φυσικό ή νομικό πρόσωπο (ή πρόσωπα), στα οποία παρέχουν υπηρεσίες ή δραστηριότητες που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή, **για τη φύση της απειλής, καθώς και για τυχόν μέτρα προστασίας ή αποκατάστασης που μπορούν να ληφθούν από το εν λόγω φυσικό ή νομικό πρόσωπο (ή πρόσωπα) για την αντιμετώπιση της εν λόγω απειλής·**
  - στ) να διατάσσουν τις εν λόγω οντότητες να εφαρμόσουν τις συστάσεις που διατυπώθηκαν κατόπιν ελέγχου ασφάλειας εντός εύλογης προθεσμίας·

- ζ) να διατάσσουν τις εν λόγω οντότητες να δημοσιοποιούν πτυχές της μη συμμόρφωσης με τις υποχρεώσεις τους που ορίζονται στην παρούσα οδηγία με συγκεκριμένο τρόπο, **εφόσον η δημοσιοποίηση αυτή δεν οδηγεί σε επιζήμια έκθεση της αντίστοιχης οντότητας**
- η) [...]
- θ) να επιβάλλουν ή να ζητούν από τα αρμόδια όργανα ή δικαστήρια να επιβάλουν, σύμφωνα με την εθνική νομοθεσία, διοικητικό πρόστιμο δυνάμει του άρθρου 31 επιπλέον ή αντί των μέτρων που αναφέρονται στα στοιχεία α) έως η) της παρούσας παραγράφου, ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης.
5. Το άρθρο 29 παράγραφοι 6 έως 8 εφαρμόζεται επίσης στα μέτρα εποπτείας και επιβολής που προβλέπονται στο παρόν άρθρο για [...] σημαντικές οντότητες [...].

#### *Άρθρο 31*

##### ***Γενικοί όροι για την επιβολή διοικητικών προστίμων σε βασικές και σε σημαντικές οντότητες***

1. Τα κράτη μέλη διασφαλίζουν ότι η επιβολή διοικητικών προστίμων σε βασικές και σε σημαντικές οντότητες σύμφωνα με το παρόν άρθρο για παραβάσεις των υποχρεώσεων που ορίζονται στην παρούσα οδηγία είναι, σε κάθε μεμονωμένη περίπτωση, αποτελεσματική, αναλογική και αποτρεπτική.
2. Τα διοικητικά πρόστιμα, ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης, επιβάλλονται επιπρόσθετα ή αντί των μέτρων που αναφέρονται στο άρθρο 29 παράγραφος 4 στοιχεία α) έως θ), στο άρθρο 29 παράγραφος 5 και στο άρθρο 30 παράγραφος 4 στοιχεία α) έως η).
3. Όταν αποφασίζεται η ενδεχόμενη επιβολή διοικητικού προστίμου και το ύψος του σε κάθε μεμονωμένη περίπτωση, λαμβάνονται δεόντως υπόψη, κατ' ελάχιστον, τα στοιχεία που προβλέπονται στο άρθρο 29 παράγραφος 7.

4. Τα κράτη μέλη διασφαλίζουν ότι οι παραβάσεις **από τις βασικές οντότητες** των υποχρεώσεων που προβλέπονται στο άρθρο 18 ή στο άρθρο 20 υπόκεινται, σύμφωνα με τις παραγράφους 2 και 3 του παρόντος άρθρου, σε διοικητικά πρόστιμα ύψους κατ' ανώτατο όριο τουλάχιστον 4 [...] 000 000 EUR ή, **σε περίπτωση νομικού προσώπου**, [...] 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκει η βασική [...] οντότητα κατά το προηγούμενο οικονομικό έτος, ανάλογα με το ποιο ποσό είναι υψηλότερο.
- 4α. Τα κράτη μέλη διασφαλίζουν ότι οι παραβάσεις από τις σημαντικές οντότητες των υποχρεώσεων που προβλέπονται στο άρθρο 18 ή στο άρθρο 20 υπόκεινται, σύμφωνα με τις παραγράφους 2 και 3 του παρόντος άρθρου, σε διοικητικά πρόστιμα ύψους κατ' ανώτατο όριο τουλάχιστον 2 000 000 EUR ή, σε περίπτωση νομικού προσώπου, 1 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκει η σημαντική οντότητα κατά το προηγούμενο οικονομικό έτος, ανάλογα με το ποιο ποσό είναι υψηλότερο.**
5. Τα κράτη μέλη μπορούν να προβλέψουν τη δυνατότητα άσκησης εξουσίας επιβολής περιοδικών χρηματικών ποινών προκειμένου να υποχρεώσουν βασική ή σημαντική οντότητα να παύσει μια παράβαση σύμφωνα με προηγούμενη απόφαση της αρμόδιας αρχής.
6. Με την επιφύλαξη των εξουσιών των αρμόδιων αρχών σύμφωνα με τα άρθρα 29 και 30, κάθε κράτος μέλος δύναται να καθορίζει τους κανόνες σχετικά με το εάν και σε ποιο βαθμό μπορούν να επιβάλλονται διοικητικά πρόστιμα σε φορείς της δημόσιας διοίκησης που αναφέρονται στο άρθρο 4 παράγραφος 23, με την επιφύλαξη των υποχρεώσεων που προβλέπονται στην παρούσα οδηγία.

6α. Όταν το νομικό σύστημα του κράτους μέλους δεν προβλέπει επιβολή διοικητικών προστίμων, τα κράτη μέλη διασφαλίζουν ότι το παρόν άρθρο μπορεί να εφαρμόζεται κατά τρόπο ώστε η διαδικασία επιβολής να κινείται από την αρμόδια αρχή και να επιβάλλεται από τα αρμόδια εθνικά δικαστήρια, με την ταυτόχρονη διασφάλιση ότι τα εν λόγω μέτρα επανόρθωσης είναι αποτελεσματικά και έχουν ισοδύναμο αποτέλεσμα με τα διοικητικά πρόστιμα που επιβάλλονται από τις αρμόδιες αρχές. Σε κάθε περίπτωση, τα πρόστιμα που επιβάλλονται είναι αποτελεσματικά, αναλογικά και αποτρεπτικά. Τα εν λόγω κράτη μέλη κοινοποιούν στην Επιτροπή τις διατάξεις των νόμων τους που θεσπίζουν σύμφωνα με την παρούσα παράγραφο, έως τις [...] και, χωρίς καθυστέρηση, κάθε επακολουθούντα τροποποιητικό νόμο ή τροποποίησή τους.

### *Άρθρο 32*

#### *Παραβάσεις που συνεπάγονται παραβίαση δεδομένων προσωπικού χαρακτήρα*

1. Εάν οι αρμόδιες αρχές, στο πλαίσιο εποπτείας ή επιβολής, [...] αντιληφθούν ότι η παράβαση από βασική ή σημαντική οντότητα των υποχρεώσεων που ορίζονται στα άρθρα 18 και 20 της παρούσας οδηγίας ενδέχεται να συνεπάγεται [...] παραβίαση δεδομένων προσωπικού χαρακτήρα, όπως ορίζεται στο άρθρο 4 παράγραφος 12 του κανονισμού (ΕΕ) αριθ. 2016/679, η οποία κοινοποιείται σύμφωνα με το άρθρο 33 του εν λόγω κανονισμού, ενημερώνουν, χωρίς αδικαιολόγητη καθυστέρηση, τις εποπτικές αρχές που είναι αρμόδιες σύμφωνα με τα άρθρα 55 και 56 του εν λόγω κανονισμού [...].
2. Εάν οι εποπτικές αρχές που είναι αρμόδιες σύμφωνα με τα άρθρα 55 και 56 του κανονισμού (ΕΕ) 2016/679 αποφασίσουν να ασκήσουν τις εξουσίες τους σύμφωνα με το άρθρο 58 παράγραφος 2 στοιχείο θ) του εν λόγω κανονισμού και να επιβάλουν διοικητικό πρόστιμο, οι αρμόδιες αρχές που αναφέρονται στο άρθρο 8 της παρούσας οδηγίας δεν επιβάλλουν διοικητικό πρόστιμο για [...] παράβαση του άρθρου 31 της παρούσας οδηγίας που τελείται με την ίδια πράξη. Οι αρμόδιες αρχές μπορούν, ωστόσο, να εφαρμόζουν τα μέτρα επιβολής ή να ασκούν τις εξουσίες επιβολής κυρώσεων που προβλέπονται στο άρθρο 29 παράγραφος 4 στοιχεία α) έως θ), στο άρθρο 29 παράγραφος 5 και στο άρθρο 30 παράγραφος 4 στοιχεία α) έως η) της παρούσας οδηγίας.

3. Εάν η εποπτική αρχή που είναι αρμόδια δυνάμει του κανονισμού (ΕΕ) 2016/679 είναι εγκατεστημένη σε κράτος μέλος διαφορετικό από την αρμόδια αρχή, η αρμόδια αρχή μπορεί να ενημερώσει την εποπτική αρχή που είναι εγκατεστημένη στο ίδιο κράτος μέλος.

### *Άρθρο 33*

#### **Κυρώσεις**

1. Τα κράτη μέλη καθορίζουν τους κανόνες για τις κυρώσεις οι οποίες πρέπει να επιβάλλονται σε περίπτωση παράβασης των εθνικών διατάξεων που θεσπίζονται κατ' εφαρμογή της παρούσας οδηγίας και λαμβάνουν όλα τα αναγκαία μέτρα για να εξασφαλίσουν την επιβολή τους. Οι προβλεπόμενες κυρώσεις είναι αποτελεσματικές, αναλογικές και αποτρεπτικές.
2. Τα κράτη μέλη κοινοποιούν στην Επιτροπή, έως [δύο] έτη μετά την ημερομηνία έναρξης ισχύος της παρούσας οδηγίας, τους κανόνες και τα μέτρα αυτά και την ενημερώνουν, χωρίς αδικαιολόγητη καθυστέρηση, για κάθε μεταγενέστερη τροποποίησή τους.

### *Άρθρο 34*

#### **Αμοιβαία συνδρομή**

1. Εάν μια βασική ή σημαντική οντότητα παρέχει υπηρεσίες σε περισσότερα από ένα κράτη μέλη ή [...] **παρέχει υπηρεσίες σε ένα ή περισσότερα κράτη μέλη**, αλλά τα δικτυακά και πληροφοριακά συστήματά της βρίσκονται σε ένα ή περισσότερα άλλα κράτη μέλη, οι αρμόδιες αρχές[...] των **ενδιαφερόμενων** κρατών μελών [...] συνεργάζονται και παρέχουν αμοιβαία συνδρομή, εφόσον απαιτείται. Η συνεργασία αυτή συνεπάγεται, τουλάχιστον, ότι:

- α) οι αρμόδιες αρχές που εφαρμόζουν μέτρα εποπτείας ή επιβολής σε ένα κράτος μέλος ενημερώνουν, μέσω του ενιαίου σημείου επαφής, και διαβουλεύονται με τις αρμόδιες αρχές των άλλων ενδιαφερόμενων κρατών μελών σχετικά με τα μέτρα εποπτείας και επιβολής που λαμβάνονται [...].
- β) μια αρμόδια αρχή μπορεί να ζητήσει από άλλη αρμόδια αρχή να λάβει τα μέτρα εποπτείας ή επιβολής [...].
- γ) μια αρμόδια αρχή, μόλις λάβει αιτιολογημένο αίτημα από άλλη αρμόδια αρχή, παρέχει συνδρομή στην άλλη αρμόδια αρχή **ανάλογη των πόρων που διαθέτει**, ώστε τα μέτρα εποπτείας ή επιβολής [...] να μπορούν να εφαρμοστούν με αποτελεσματικό, αποδοτικό και συνεπή τρόπο. Η εν λόγω αμοιβαία συνδρομή μπορεί να καλύπτει αιτήματα παροχής πληροφοριών και μέτρα εποπτείας, συμπεριλαμβανομένων αιτημάτων για τη διενέργεια επιτόπιων επιθεωρήσεων ή εποπτείας εκτός των εγκαταστάσεων ή στοχευμένων ελέγχων ασφάλειας. Η αρμόδια αρχή στην οποία απευθύνεται αίτημα συνδρομής δεν μπορεί να αρνηθεί το εν λόγω αίτημα, εκτός εάν, κατόπιν ανταλλαγής απόψεων με τις άλλες ενδιαφερόμενες αρχές [...], διαπιστωθεί ότι [...] η αρχή δεν είναι αρμόδια να παράσχει την αιτούμενη συνδρομή **ή δεν διαθέτει τους απαραίτητους πόρους** ή η αιτούμενη συνδρομή δεν είναι ανάλογη προς τα εποπτικά καθήκοντα της αρμόδιας αρχής [...] **ή το αίτημα αφορά πληροφορίες ή περιλαμβάνει δραστηριότητες που έρχονται σε σύγκρουση με την εθνική ασφάλεια, τη δημόσια ασφάλεια ή την άμυνα του εν λόγω κράτους μέλους.**
2. Κατά περίπτωση και με κοινή συμφωνία, αρμόδιες αρχές από διαφορετικά κράτη μέλη μπορούν να εκτελούν τις κοινές δράσεις εποπτείας [...].

## ΚΕΦΑΛΑΙΟ VII

*Μεταβατικές και τελικές διατάξεις*

*Άρθρο 35*

### ***Επανεξέταση***

Η Επιτροπή προβαίνει σε περιοδική επανεξέταση της λειτουργίας της παρούσας οδηγίας και υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο. Η έκθεση αξιολογεί ιδίως τη σημασία των τομέων, των υποτομέων, του μεγέθους και του είδους των οντοτήτων που αναφέρονται στα παραρτήματα I και II για τη λειτουργία της οικονομίας και της κοινωνίας σε σχέση με την κυβερνοασφάλεια. Για [...] **τον σκοπό της επανεξέτασης**, [...], η Επιτροπή λαμβάνει υπόψη τις εκθέσεις [...] του δικτύου CSIRT σχετικά με την πείρα που έχει αποκτηθεί [...] σε επιχειρησιακό επίπεδο. Η πρώτη έκθεση υποβάλλεται το αργότερο... [54 μήνες μετά την ημερομηνία έναρξης ισχύος της παρούσας οδηγίας].

*Άρθρο 36*

**[...]**

[...]

[...]

### *Άρθρο 37*

#### ***Διαδικασία επιτροπής***

1. Η Επιτροπή επικουρείται από επιτροπή. Πρόκειται για επιτροπή κατά την έννοια του κανονισμού (ΕΕ) αριθ. 182/2011.
2. Όταν γίνεται αναφορά στην παρούσα παράγραφο, εφαρμόζεται το άρθρο 5 του κανονισμού (ΕΕ) αριθ. 182/2011.
3. Αν η γνώμη της επιτροπής πρέπει να ληφθεί με γραπτή διαδικασία, η εν λόγω διαδικασία περατώνεται χωρίς αποτέλεσμα, εάν, εντός της προθεσμίας για την έκδοση γνώμης, το αποφασίσει ο πρόεδρος της επιτροπής ή το ζητήσει μέλος της επιτροπής.



*Άρθρο 38*

***Μεταφορά στο εθνικό δίκαιο***

1. Έως... [[...]24 μήνες μετά την ημερομηνία έναρξης ισχύος της παρούσας οδηγίας], τα κράτη μέλη θεσπίζουν και δημοσιεύουν[...] τις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις για να συμμορφωθούν προς την παρούσα οδηγία. Ενημερώνουν αμέσως την Επιτροπή σχετικά. Θέτουν τα μέτρα αυτά σε εφαρμογή από ... [μία ημέρα μετά την ημερομηνία που αναφέρεται στο πρώτο εδάφιο].
2. Οι διατάξεις αυτές, όταν θεσπίζονται από τα κράτη μέλη, περιέχουν αναφορά στην παρούσα οδηγία ή συνοδεύονται από την αναφορά αυτή κατά την επίσημη δημοσίευσή τους. Ο τρόπος της αναφοράς αποφασίζεται από τα κράτη μέλη.

*Άρθρο 39*

***Τροποποίηση του κανονισμού (ΕΚ) αριθ. 910/2014***

Το άρθρο 19[...] του κανονισμού (ΕΕ) αριθ. 910/2014 απαλείφεται από τις... [ημερομηνία λήξης της προθεσμίας μεταφοράς της παρούσας οδηγίας στο εθνικό δίκαιο].

*Άρθρο 40*

***Τροποποίηση της οδηγίας (ΕΕ) 2018/1972***

Τα άρθρα 40 και 41[...] της οδηγίας 2018/1972/ΕΕ απαλείφονται από τις... [ημερομηνία λήξης της προθεσμίας μεταφοράς της παρούσας οδηγίας στο εθνικό δίκαιο].

*Άρθρο 41*

***Κατάργηση***

Η οδηγία (ΕΕ) 2016/1148 καταργείται από τις.. [ημερομηνία λήξης της προθεσμίας μεταφοράς της οδηγίας στο εθνικό δίκαιο].

Οι αναφορές στην οδηγία (ΕΕ) 2016/1148 θεωρούνται ως αναφορές στην παρούσα οδηγία και νοούνται σύμφωνα με τον πίνακα αντιστοιχίας του παραρτήματος ΙΙ[...].

*Άρθρο 42*

***Θέση σε ισχύ***

Η παρούσα οδηγία αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή της στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

*Άρθρο 43*

***Αποδέκτες***

Η παρούσα οδηγία απευθύνεται στα κράτη μέλη.

Βρυξέλλες,

*Για το Ευρωπαϊκό Κοινοβούλιο*

*Ο Πρόεδρος*

*Για το Συμβούλιο*

*Ο Πρόεδρος*

## ΠΑΡΑΡΤΗΜΑ Ι

### **ΤΟΜΕΙΣ, ΥΠΟΤΟΜΕΙΣ ΚΑΙ ΕΙΔΗ ΟΝΤΟΤΗΤΩΝ**

Τομέας	Υποτομέας	Είδος οντότητας
1. Ενέργεια	α) Ηλεκτρική ενέργεια	– Επιχειρήσεις ηλεκτρικής ενέργειας, που αναφέρονται στο άρθρο 2 σημείο 57 της οδηγίας (ΕΕ) 2019/944, οι οποίες ασκούν τη δραστηριότητα της «προμήθειας», που αναφέρεται στο άρθρο 2 σημείο 12 της εν λόγω οδηγίας <sup>(39)</sup>
		– Διαχειριστές συστήματος διανομής, που αναφέρονται στο άρθρο 2 σημείο 29 της οδηγίας (ΕΕ) 2019/944
		– Διαχειριστές συστήματος μεταφοράς, που αναφέρονται στο άρθρο 2 σημείο 35 της οδηγίας (ΕΕ) 2019/944
		– Παραγωγοί, που αναφέρονται στο άρθρο 2 σημείο 38 της οδηγίας (ΕΕ) 2019/944
		– Ορισθέντες διαχειριστές αγοράς ηλεκτρικής ενέργειας, που αναφέρονται στο άρθρο 2 σημείο 8 του κανονισμού (ΕΕ) 2019/943 <sup>(40)</sup>
		– Συμμετέχοντες στην αγορά ηλεκτρικής ενέργειας, που αναφέρονται στο άρθρο 2 σημείο 25 του κανονισμού (ΕΕ) 2019/943, οι οποίοι παρέχουν υπηρεσίες σωρευτικής εκπροσώπησης, απόκρισης ζήτησης ή αποθήκευσης ενέργειας, που αναφέρονται στο άρθρο 2 σημεία 18, 20 και 59 της οδηγίας (ΕΕ) 2019/944

<sup>39</sup> Οδηγία 2019/944 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Ιουνίου 2019, σχετικά με τους κοινούς κανόνες για την εσωτερική αγορά ηλεκτρικής ενέργειας και την τροποποίηση της οδηγίας 2012/27/ΕΕ (ΕΕ L 158 της 14.6.2019, σ. 125).

<sup>40</sup> Κανονισμός (ΕΕ) 2019/943 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την εσωτερική αγορά ηλεκτρικής ενέργειας (ΕΕ L 158 της 14.6.2019, σ. 54).

	β) Τηλεθέρμανση και τηλεψύξη	– Τηλεθέρμανση ή τηλεψύξη, που αναφέρεται στο άρθρο 2 σημείο 19 της οδηγίας (ΕΕ) 2018/2001 <sup>(41)</sup> για την προώθηση της χρήσης ενέργειας από ανανεώσιμες πηγές
	γ) Πετρέλαιο	<ul style="list-style-type: none"> <li>– Διαχειριστές αγωγών μεταφοράς πετρελαίου</li> <li>– Διαχειριστές παραγωγής πετρελαίου, εγκαταστάσεων διύλισης και επεξεργασίας, αποθήκευσης και μεταφοράς πετρελαίου</li> <li>– Κεντρικοί φορείς διατήρησης αποθεμάτων, που αναφέρονται στο άρθρο 2 στοιχείο στ) της οδηγίας 2009/119/ΕΚ του Συμβουλίου<sup>(42)</sup></li> </ul>
	δ) Αέριο	<ul style="list-style-type: none"> <li>– Επιχειρήσεις προμήθειας, που αναφέρονται στο άρθρο 2 σημείο 8 της οδηγίας (ΕΕ) 2009/73/ΕΚ <sup>(43)</sup></li> <li>– Διαχειριστές συστήματος διανομής, που αναφέρονται στο άρθρο 2 σημείο 6 της οδηγίας 2009/73/ΕΚ</li> <li>– Διαχειριστές συστήματος μεταφοράς, που αναφέρονται στο άρθρο 2 σημείο 4 της οδηγίας 2009/73/ΕΚ</li> <li>– Διαχειριστές συστήματος αποθήκευσης, που αναφέρονται στο άρθρο 2 σημείο 10 της οδηγίας 2009/73/ΕΚ</li> <li>– Διαχειριστές συστήματος ΥΦΑ, που</li> </ul>

<sup>41</sup> Οδηγία (ΕΕ) 2018/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για την προώθηση της χρήσης ενέργειας από ανανεώσιμες πηγές (ΕΕ L 328 της 21.12.2018, σ. 82).

<sup>42</sup> Οδηγία 2009/119/ΕΚ του Συμβουλίου, της 14ης Σεπτεμβρίου 2009, σχετικά με υποχρέωση διατήρησης ενός ελάχιστου επιπέδου αποθεμάτων αργού πετρελαίου ή/και προϊόντων πετρελαίου από τα κράτη μέλη (ΕΕ L 265 της 9.10.2009, σ. 9).

<sup>43</sup> Οδηγία 2009/73/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουλίου 2009, σχετικά με τους κοινούς κανόνες για την εσωτερική αγορά φυσικού αερίου και την κατάργηση της οδηγίας 2003/55/ΕΚ (ΕΕ L 211 της 14.8.2009, σ. 94).

		αναφέρονται στο άρθρο 2 σημείο 12 της οδηγίας 2009/73/EK
		– Επιχειρήσεις φυσικού αερίου, όπως ορίζονται στο άρθρο 2 σημείο 1 της οδηγίας 2009/73/EK
		– Διαχειριστές εγκαταστάσεων διύλισης και επεξεργασίας φυσικού αερίου
	ε) Υδρογόνο	Διαχειριστές παραγωγής, αποθήκευσης και μεταφοράς υδρογόνου
2. Μεταφορές	α) Εναέριες	<p>– Αερομεταφορείς, που αναφέρονται στο άρθρο 3 σημείο 4 του κανονισμού (ΕΚ) αριθ. 300/2008<sup>(44)</sup>, <b>οι οποίοι χρησιμοποιούνται για εμπορικούς σκοπούς</b></p> <p>– Φορείς διαχείρισης αερολιμένων, που αναφέρονται στο άρθρο 2 σημείο 2 της οδηγίας 2009/12/EK<sup>(45)</sup>, αερολιμένες, που αναφέρονται στο άρθρο 2 σημείο 1 της εν λόγω οδηγίας, συμπεριλαμβανομένων των κεντρικών αερολιμένων που απαριθμούνται στο παράρτημα ΙΙ τμήμα 2 του κανονισμού (ΕΕ) αριθ. 1315/2013<sup>(46)</sup>, και φορείς εκμετάλλευσης βοηθητικών εγκαταστάσεων που βρίσκονται εντός των αερολιμένων</p> <p>– Φορείς εκμετάλλευσης ελέγχου διαχείρισης κυκλοφορίας που παρέχουν υπηρεσίες ελέγχου εναέριας κυκλοφορίας,</p>

<sup>44</sup> Κανονισμός (ΕΚ) αριθ. 300/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 2008, για τη θέσπιση κοινών κανόνων στο πεδίο της ασφάλειας της πολιτικής αεροπορίας και την κατάργηση του κανονισμού (ΕΚ) αριθ. 2320/2002 (ΕΕ L 97 της 9.4.2008, σ. 72).

<sup>45</sup> Οδηγία 2009/12/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 2009, για τα αερολιμενικά τέλη (ΕΕ L 70 της 14.3.2009, σ. 11).

<sup>46</sup> Κανονισμός (ΕΚ) αριθ. 1315/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2013, περί των προσανατολισμών της Ένωσης για την ανάπτυξη του διευρωπαϊκού δικτύου μεταφορών και για την κατάργηση της απόφασης αριθ. 661/2010/ΕΕ (ΕΕ L 348 της 20.12.2013, σ. 1).

		που αναφέρονται στο άρθρο 2 σημείο 1 του κανονισμού (ΕΚ) αριθ. 549/2004 <sup>(47)</sup>
β) Σιδηροδρομικές		– Διαχειριστές υποδομών, που αναφέρονται στο άρθρο 3 σημείο 2 της οδηγίας (ΕΕ) 2012/34/ΕΕ <sup>(48)</sup>
		– Σιδηροδρομικές επιχειρήσεις, που αναφέρονται στο άρθρο 3 σημείο 1 της οδηγίας 2012/34/ΕΕ, συμπεριλαμβανομένων των φορέων εκμετάλλευσης εγκαταστάσεων για την παροχή υπηρεσιών, που αναφέρονται στο άρθρο 3 σημείο 12 της οδηγίας 2012/34/ΕΕ
γ) Πλωτές		– Εσωτερικές πλωτές, θαλάσσιες και ακτοπλοϊκές εταιρείες μεταφοράς επιβατών και εμπορευμάτων, που αναφέρονται για τις θαλάσσιες μεταφορές στο παράρτημα Ι του κανονισμού (ΕΚ) αριθ. 725/2004 <sup>(49)</sup> , μη συμπεριλαμβανομένων των μεμονωμένων σκαφών που χρησιμοποιούνται από τις εταιρείες αυτές
		– Διαχειριστικοί φορείς των λιμένων, που αναφέρονται στο άρθρο 3 σημείο 1 της οδηγίας 2005/65/ΕΚ <sup>(50)</sup> , συμπεριλαμβανομένων των λιμενικών τους εγκαταστάσεων, που αναφέρονται στο άρθρο 2 σημείο 11 του κανονισμού (ΕΚ) αριθ. 725/2004, και φορείς εκμετάλλευσης έργων και εξοπλισμού που βρίσκονται εντός των λιμένων
		– Διαχειριστές υπηρεσιών εξυπηρέτησης

<sup>47</sup> Κανονισμός (ΕΚ) αριθ. 549/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, για τη χάραξη του πλαισίου για τη δημιουργία του Ενιαίου Ευρωπαϊκού Ουρανού («κανονισμός-πλαίσιο») (ΕΕ L 96 της 31.3.2004, σ. 1).

<sup>48</sup> Οδηγία 2012/34/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Νοεμβρίου 2012, για τη δημιουργία ενιαίου ευρωπαϊκού σιδηροδρομικού χώρου (ΕΕ L 343 της 14.12.2012, σ. 32).

<sup>49</sup> Κανονισμός (ΕΚ) αριθ. 725/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 31ης Μαρτίου 2004, για τη βελτίωση της ασφάλειας στα πλοία και στις λιμενικές εγκαταστάσεις (ΕΕ L 129 της 29.4.2004, σ. 6).

<sup>50</sup> Οδηγία 2005/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Οκτωβρίου 2005, σχετικά με την ενίσχυση της ασφαλείας των λιμένων (ΕΕ L 310 της 25.11.2005, σ. 28).

		κυκλοφορίας πλοίων, που αναφέρονται στο άρθρο 3 στοιχείο ιε) της οδηγίας 2002/59/ΕΚ <sup>(51)</sup>
	δ) Οδικές	<ul style="list-style-type: none"> <li>– Οδικές αρχές, που αναφέρονται στο άρθρο 2 σημείο 12 του κατ' εξουσιοδότηση κανονισμού (ΕΕ) 2015/962 της Επιτροπής<sup>(52)</sup> που είναι υπεύθυνες για τον έλεγχο διαχείρισης της κυκλοφορίας, <b>με εξαίρεση τους δημόσιους φορείς ή τους διαχειριστές συστημάτων ευφών μεταφορών για τους οποίους η διαχείριση της κυκλοφορίας αποτελεί μόνο επομισιώδες μέρος της γενικής τους δραστηριότητας</b></li> <li>– Διαχειριστές συστημάτων ευφών μεταφορών, που αναφέρονται στο άρθρο 4 σημείο 1 της οδηγίας 2010/40/ΕΚ<sup>(53)</sup></li> </ul>
3. Τράπεζες		— Πιστωτικά ιδρύματα, που αναφέρονται στο άρθρο 4 σημείο 1 του κανονισμού (ΕΕ) αριθ. 575/2013 <sup>(54)</sup> , [πλην εκείνων που αναφέρονται στο σημείο 8 του άρθρου 2 παράγραφος 5 της οδηγίας 2013/36/ΕΕ, τα οποία εξαιρούνται δυνάμει του άρθρου 2 παράγραφος 4 του κανονισμού XX [DORA]]

<sup>51</sup> Οδηγία 2002/59/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Ιουνίου 2002, για τη δημιουργία κοινοτικού συστήματος παρακολούθησης της κυκλοφορίας των πλοίων και ενημέρωσης και την κατάργηση της οδηγίας 93/75/ΕΟΚ του Συμβουλίου (ΕΕ L 208 της 5.8.2002, σ. 10).

<sup>52</sup> Κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2015/962 της Επιτροπής, της 18ης Δεκεμβρίου 2014, για τη συμπλήρωση της οδηγίας 2010/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την παροχή σε επίπεδο Ένωσης υπηρεσιών πληροφόρησης για την κυκλοφορία σε πραγματικό χρόνο (ΕΕ L 157 της 23.6.2015, σ. 21).

<sup>53</sup> Οδηγία 2010/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Ιουλίου 2010, περί πλαισίου ανάπτυξης των Συστημάτων Ευφών Μεταφορών στον τομέα των οδικών μεταφορών και των διεπαφών με άλλους τρόπους μεταφοράς (ΕΕ L 207 της 6.8.2010, σ. 1).

<sup>54</sup> Κανονισμός (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με τις απαιτήσεις προληπτικής εποπτείας για πιστωτικά ιδρύματα και επιχειρήσεις επενδύσεων και την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 (ΕΕ L 176 της 27.6.2013, σ. 1).

4. Υποδομές χρηματοπιστωτικών αγορών	<ul style="list-style-type: none"> <li>– Διαχειριστές τόπων διαπραγμάτευσης, που αναφέρονται στο άρθρο 4 σημείο 24 της οδηγίας 2014/65/ΕΕ<sup>(55)</sup></li> </ul>
	<ul style="list-style-type: none"> <li>– Κεντρικοί αντισυμβαλλόμενοι, που αναφέρονται στο άρθρο 2 σημείο 1 του κανονισμού (ΕΕ) αριθ. 648/2012<sup>(56)</sup></li> </ul>
5. Υγεία	<ul style="list-style-type: none"> <li>— Πάροχοι υγειονομικής περίθαλψης, που αναφέρονται στο άρθρο 3 στοιχείο ζ) της οδηγίας 2011/24/ΕΕ<sup>(57)</sup></li> </ul>
	<ul style="list-style-type: none"> <li>— Εργαστήρια αναφοράς της ΕΕ που αναφέρονται στο άρθρο 15 του κανονισμού XXXX/XXXX σχετικά με σοβαρές διασυνοριακές απειλές κατά της υγείας<sup>58</sup></li> </ul>
	<ul style="list-style-type: none"> <li>— Οντότητες που πραγματοποιούν δραστηριότητες έρευνας και ανάπτυξης για φάρμακα, που αναφέρονται στο άρθρο 1 σημείο 2 της οδηγίας 2001/83/ΕΚ<sup>(59)</sup></li> <li>— Οντότητες που παρασκευάζουν βασικά φαρμακευτικά προϊόντα και φαρμακευτικά σκευάσματα που αναφέρονται στον τομέα Γ κλάδο 21 της NACE αναθ. 2</li> <li>— Οντότητες που κατασκευάζουν ιατροτεχνολογικά προϊόντα που θεωρούνται κρίσιμης σημασίας κατά τη διάρκεια κατάστασης έκτακτης ανάγκης στον τομέα της δημόσιας υγείας</li> </ul>

<sup>55</sup> Οδηγία 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και την τροποποίηση της οδηγίας 2002/92/ΕΚ και της οδηγίας 2011/61/ΕΕ (ΕΕ L 173 της 12.6.2014, σ. 349).

<sup>56</sup> Κανονισμός (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4ης Ιουλίου 2012, για τα εξωχρηματιστηριακά παράγωγα, τους κεντρικούς αντισυμβαλλομένους και τα αρχεία καταγραφής συναλλαγών (ΕΕ L 201 της 27.7.2012, σ. 1).

<sup>57</sup> Οδηγία 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Μαρτίου 2011, περί εφαρμογής των δικαιωμάτων των ασθενών στο πλαίσιο της διασυνοριακής υγειονομικής περίθαλψης (ΕΕ L 88 της 4.4.2011, σ. 45).

<sup>58</sup> [Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με σοβαρές διασυνοριακές απειλές κατά της υγείας και για την κατάργηση της απόφασης αριθ. 1082/2013/ΕΕ, η παραπομπή θα επικαιροποιηθεί μόλις εγκριθεί η πρόταση COM (2020)727 final]

<sup>59</sup> Οδηγία 2001/83/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Νοεμβρίου 2001, περί κοινοτικού κώδικος για τα φάρμακα που προορίζονται για ανθρώπινη χρήση (ΕΕ L 311 της 28.11.2001, σ. 67).



		(«κατάλογος τεχνολογικών προϊόντων κρίσιμης σημασίας κατά τη διάρκεια κατάστασης έκτακτης ανάγκης στον τομέα της δημόσιας υγείας») που αναφέρεται στο άρθρο 20 του κανονισμού XXXX <sup>60</sup>
6. Πόσιμο νερό		Προμηθευτές και διανομείς νερού ανθρώπινης κατανάλωσης που αναφέρονται στο άρθρο 2 σημείο 1 στοιχείο α) της οδηγίας 98/83/ΕΚ του Συμβουλίου <sup>(61)</sup> , αλλά εξαιρουμένων των διανομέων για τους οποίους η διανομή νερού ανθρώπινης κατανάλωσης αποτελεί μόνο <b>επουσιώδες</b> μέρος της γενικής τους δραστηριότητας διανομής λοιπών προϊόντων και αγαθών [...]
7. Λύματα		Επιχειρήσεις που συλλέγουν, διαθέτουν ή επεξεργάζονται τα αστικά λύματα, τα οικιακά λύματα και τα βιομηχανικά λύματα, που αναφέρονται στο άρθρο 2 σημεία 1 έως 3 της οδηγίας 91/271/ΕΟΚ του Συμβουλίου <sup>(62)</sup> , <b>αλλά εξαιρουμένων επιχειρήσεων για τις οποίες η συλλογή, η διάθεση ή η επεξεργασία αστικών, οικιακών και βιομηχανικών λυμάτων αποτελεί μόνο επουσιώδες μέρος της γενικής τους δραστηριότητας.</b> [...]
8. Ψηφιακές υποδομές		<p>– Πάροχοι σημείων ανταλλαγής κίνησης διαδικτύου</p> <p>– Πάροχοι υπηρεσιών συστήματος ονομάτων τομέα (DNS), <b>εξαιρουμένων των διαχειριστών των εξυπηρετητών ονομάτων ρίζας</b></p> <p>— Μητρώα ονομάτων τομέα ανώτατου επιπέδου (TLD)</p>

<sup>60</sup> [Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ενίσχυση του ρόλου του Ευρωπαϊκού Οργανισμού Φαρμάκων όσον αφορά την ετοιμότητα έναντι κρίσεων και τη διαχείριση κρίσεων για τα φάρμακα και τα ιατροτεχνολογικά προϊόντα, η παραπομπή θα επικαιροποιηθεί μόλις εγκριθεί η πρόταση COM(2020)725 final]

<sup>61</sup> Οδηγία 98/83/ΕΚ του Συμβουλίου, της 3ης Νοεμβρίου 1998, σχετικά με την ποιότητα του νερού ανθρώπινης κατανάλωσης (ΕΕ L 330 της 5.12.1998, σ. 32).

<sup>62</sup> Οδηγία 91/271/ΕΟΚ του Συμβουλίου, της 21ης Μαΐου 1991, για την επεξεργασία των αστικών λυμάτων (ΕΕ L 135 της 30.5.1991, σ. 40).

		<ul style="list-style-type: none"> <li>– Πάροχοι υπηρεσιών νεφροϋπολογιστικής</li> </ul>
		<ul style="list-style-type: none"> <li>– Πάροχοι υπηρεσιών κέντρου δεδομένων</li> </ul>
		<ul style="list-style-type: none"> <li>– Πάροχοι δικτύων διανομής περιεχομένου</li> </ul>
		<ul style="list-style-type: none"> <li>– Πάροχοι υπηρεσιών εμπιστοσύνης, που αναφέρονται στο άρθρο 3 σημείο 19 του κανονισμού (ΕΕ) αριθ. 910/2014<sup>(63)</sup></li> </ul>
		<ul style="list-style-type: none"> <li>– Πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών που αναφέρονται στο άρθρο 2 σημείο 8 της οδηγίας (ΕΕ) 2018/1972<sup>(64)</sup> ή πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών που αναφέρονται στο άρθρο 2 σημείο 4 της οδηγίας (ΕΕ) 2018/1972 όταν οι υπηρεσίες τους είναι δημοσίως διαθέσιμες</li> </ul>
<b>8.α Διαχείριση υπηρεσιών ΤΠΕ (B2B)</b>		<ul style="list-style-type: none"> <li>— Πάροχος υπηρεσιών διαχείρισης (MSP)</li> <li>— Πάροχος διαχείρισης υπηρεσιών ασφάλειας (MSSP)</li> </ul>

<sup>63</sup> Κανονισμός (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ (ΕΕ L 257 της 28.8.2014, σ. 73).

<sup>64</sup> Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (ΕΕ L 321 της 17.12.2018, σ. 36).

<p>9. Φορείς δημόσιας διοίκησης</p>		<p>— Φορείς δημόσιας διοίκησης εθνικών κυβερνήσεων <b>όπως ορίζονται από κράτος μέλος σύμφωνα με το εθνικό δίκαιο</b></p> <p>— [...]<sup>65</sup>[...]</p> <p>— [...]</p>
<p>10. Διάστημα</p>		<p>— Διαχειριστές επίγειων υποδομών, που ανήκουν, τελούν υπό τη διαχείριση και λειτουργούν από κράτη μέλη ή από ιδιώτες, και υποστηρίζουν την παροχή διαστημικών υπηρεσιών, με εξαίρεση τους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών που αναφέρονται στο άρθρο 2 σημείο 8 της οδηγίας (ΕΕ) 2018/1972</p>

<sup>65</sup> [...]

## ΠΑΡΑΡΤΗΜΑ ΙΙ

### ΤΟΜΕΙΣ, ΥΠΟΤΟΜΕΙΣ ΚΑΙ ΕΙΔΗ ΟΝΤΟΤΗΤΩΝ

Τομέας	Υποτομέας	Είδος οντότητας
1. Ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών		Φορείς παροχής ταχυδρομικών υπηρεσιών, που αναφέρονται στο άρθρο 2 σημείο 1[...] της οδηγίας 97/67/ΕΚ <sup>(66)</sup> , <b>συμπεριλαμβανομένων</b> [...] παρόχων υπηρεσιών ταχυμεταφορών
2. Διαχείριση αποβλήτων		Επιχειρήσεις διαχείρισης αποβλήτων, που αναφέρονται στο άρθρο 3 σημείο 9 της οδηγίας 2008/98/ΕΚ <sup>(67)</sup> , με εξαίρεση όμως τις επιχειρήσεις για τις οποίες η διαχείριση αποβλήτων δεν αποτελεί την κύρια οικονομική δραστηριότητα

<sup>66</sup> Οδηγία 97/67/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Δεκεμβρίου 1997, σχετικά με τους κοινούς κανόνες για την ανάπτυξη της εσωτερικής αγοράς κοινοτικών ταχυδρομικών υπηρεσιών και τη βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών (ΕΕ L 15 της 21.1.1998, σ. 14), **όπως τροποποιήθηκε από την οδηγία 2008/6/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Φεβρουαρίου 2008, για την τροποποίηση της οδηγίας 97/67/ΕΚ σχετικά με την πλήρη υλοποίηση της εσωτερικής αγοράς κοινοτικών ταχυδρομικών υπηρεσιών (ΕΕ L 52 της 27.2.2008, σ. 3).**

<sup>67</sup> Οδηγία 2008/98/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Νοεμβρίου 2008, για τα απόβλητα και την κατάργηση ορισμένων οδηγιών (ΕΕ L 312 της 22.11.2008, σ. 3).

3. Παρασκευή, παραγωγή και διανομή χημικών προϊόντων		Επιχειρήσεις που παρασκευάζουν[...] και διανέμουν ουσίες και [...] <b>μείγματα</b> που αναφέρονται στο άρθρο 3 σημεία [...] 9 και 14 του κανονισμού (ΕΚ) αριθ. 1907/2006 <sup>(68)</sup> και <b>επιχειρήσεις που παράγουν είδη του άρθρου 3 σημείο 3 του εν λόγω κανονισμού (ΕΚ) από ουσίες ή μείγματα.</b>
4. Παραγωγή, μεταποίηση και διανομή τροφίμων		Επιχειρήσεις τροφίμων, που αναφέρονται στο άρθρο 3 σημείο 2 του κανονισμού (ΕΚ) αριθ. 178/2002 <sup>(69)</sup> , <b>οι οποίες ασκούν δραστηριότητα χονδρικής διανομής, βιομηχανικής παραγωγής και μεταποίησης</b>
5. Κατασκευαστικός τομέας	α) Κατασκευή ιατροτεχνολογικών προϊόντων και in vitro διαγνωστικών ιατροτεχνολογικών προϊόντων	Οντότητες που κατασκευάζουν ιατροτεχνολογικά προϊόντα που αναφέρονται στο άρθρο 2 σημείο 1 του κανονισμού (ΕΕ) 2017/745 <sup>(70)</sup> , και οντότητες που κατασκευάζουν in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα που αναφέρονται στο άρθρο 2 σημείο 2 του κανονισμού (ΕΕ) 2017/746 <sup>(71)</sup> , με εξαίρεση τις οντότητες που κατασκευάζουν

<sup>68</sup> Κανονισμός (ΕΚ) αριθ. 1907/2006 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Δεκεμβρίου 2006, για την καταχώριση, την αξιολόγηση, την αδειοδότηση και τους περιορισμούς των χημικών προϊόντων (REACH) και για την ίδρυση του Ευρωπαϊκού Οργανισμού Χημικών Προϊόντων καθώς και για την τροποποίηση της οδηγίας 1999/45/ΕΚ και για κατάργηση του κανονισμού (ΕΟΚ) αριθ. 793/93 του Συμβουλίου και του κανονισμού (ΕΚ) αριθ. 1488/94 της Επιτροπής καθώς και της οδηγίας 76/769/ΕΟΚ του Συμβουλίου και των οδηγιών της Επιτροπής 91/155/ΕΟΚ, 93/67/ΕΟΚ, 93/105/ΕΚ και 2000/21/ΕΚ (ΕΕ L 396 της 30.12.2006, σ. 1).

<sup>69</sup> Κανονισμός (ΕΚ) αριθ. 178/2002 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 28ης Ιανουαρίου 2002, για τον καθορισμό των γενικών αρχών και απαιτήσεων της νομοθεσίας για τα τρόφιμα, για την ίδρυση της Ευρωπαϊκής Αρχής για την Ασφάλεια των Τροφίμων και τον καθορισμό διαδικασιών σε θέματα ασφαλείας των τροφίμων (ΕΕ L 31 της 1.2.2002, σ. 1).

<sup>70</sup> Κανονισμός (ΕΕ) 2017/745 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Απριλίου 2017, για τα ιατροτεχνολογικά προϊόντα, για την τροποποίηση της οδηγίας 2001/83/ΕΚ, του κανονισμού (ΕΚ) αριθ. 178/2002 και του κανονισμού (ΕΚ) αριθ. 1223/2009 και για την κατάργηση των οδηγιών του Συμβουλίου 90/385/ΕΟΚ και 93/42/ΕΟΚ (ΕΕ L 117 της 5.5.2017, σ. 1)

<sup>71</sup> Κανονισμός (ΕΕ) 2017/746 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Απριλίου 2017, για τα in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα και για την κατάργηση της οδηγίας 98/79/ΕΚ και της απόφασης 2010/227/ΕΕ της Επιτροπής (ΕΕ L 117 της 5.5.2017, σ. 176)

		ιατροτεχνολογικά προϊόντα που αναφέρονται στο παράρτημα 1 σημείο 5.
	β) Κατασκευή προϊόντων υπολογιστών, ηλεκτρονικών και οπτικών προϊόντων	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 26 της NACE αναθ. 2
	γ) Κατασκευή ηλεκτρολογικού εξοπλισμού	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 27 της NACE αναθ. 2
	δ) Κατασκευή μηχανημάτων και εξοπλισμού π.δ.κ.α.	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 28 της NACE αναθ. 2
	ε) Κατασκευή μηχανοκίνητων οχημάτων, ρυμουλκούμενων και ημιρυμουλκούμενων	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 29 της NACE αναθ. 2
	στ) Κατασκευή άλλου εξοπλισμού μεταφορών	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 30 της NACE αναθ. 2
6. Ψηφιακοί πάροχοι		<ul style="list-style-type: none"> <li>– Πάροχοι επιγραμμικών αγορών</li> <li>– Πάροχοι επιγραμμικών μηχανών αναζήτησης</li> <li>– Πάροχοι πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης</li> </ul>