ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Πρόταση

# ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

## σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και με την τροποποίηση του κανονισμού (ΕΕ) 2019/1020

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

# ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ

## 1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ

- **Αιτιολόγηση και στόχοι της πρότασης**

Τα προϊόντα υλισμικού και λογισμικού δέχονται όλο και περισσότερο επιτυχείς κυβερνοεπιθέσεις: ως αποτέλεσμα το εκτιμώμενο ετήσιο κόστος του κυβερνοεγκλήματος το 2021 ανήλθε σε 5,5 τρισ. EUR. Τα προϊόντα αυτά πάσχουν από δύο σημαντικά προβλήματα που αυξάνουν το κόστος για τους χρήστες και την κοινωνία: 1) χαμηλό επίπεδο κυβερνοασφάλειας, το οποίο αντικατοπτρίζεται από τα εκτεταμένα τρωτά σημεία και την ελλιπή και ασυνεπή παροχή ενημερώσεων ασφάλειας για την αντιμετώπισή τους, και 2) ελλιπής κατανόηση και πρόσβαση των χρηστών σε πληροφορίες, γεγονός που τους εμποδίζει να επιλέγουν προϊόντα με επαρκείς ιδιότητες κυβερνοασφάλειας ή να τα χρησιμοποιούν με ασφαλή τρόπο. Σε ένα συνδεδεμένο περιβάλλον, ένα συμβάν κυβερνοασφάλειας σε ένα προϊόν μπορεί να επηρεάσει έναν ολόκληρο οργανισμό ή μια ολόκληρη εφοδιαστική αλυσίδα, ενώ μάλιστα συχνά εξαπλώνεται και εκτός των συνόρων της εσωτερικής αγοράς μέσα σε λίγα μόλις λεπτά. Αυτό μπορεί να οδηγήσει σε σοβαρή διαταραχή των οικονομικών και κοινωνικών δραστηριοτήτων ή ακόμη και να αποτελέσει απειλή για τη ζωή.

Η κυβερνοασφάλεια προϊόντων με ψηφιακά στοιχεία έχει ισχυρή διασυνοριακή διάσταση, καθώς τα προϊόντα που κατασκευάζονται σε μία χώρα συχνά χρησιμοποιούνται σε ολόκληρη την εσωτερική αγορά. Επιπλέον, τα συμβάντα που αρχικά πλήττουν μία μόνο οντότητα ή ένα μόνο κράτος μέλος συχνά εξαπλώνονται εντός λίγων λεπτών σε ολόκληρη την εσωτερική αγορά.

Ενώ η ισχύουσα νομοθεσία για την εσωτερική αγορά εφαρμόζεται σε ορισμένα προϊόντα με ψηφιακά στοιχεία, τα περισσότερα προϊόντα υλισμικού και λογισμικού δεν καλύπτονται επί του παρόντος από ενωσιακή νομοθεσία που αφορά ζητήματα κυβερνοασφάλειας. Ειδικότερα, το ισχύον νομικό πλαίσιο της ΕΕ δεν εξετάζει το ζήτημα της κυβερνοασφάλειας του μη ενσωματωμένου λογισμικού, ακόμη και αν οι κυβερνοεπιθέσεις στοχεύουν όλο και περισσότερο τα τρωτά σημεία των προϊόντων αυτών, με αποτέλεσμα να προκαλείται σημαντικό κοινωνικό και οικονομικό κόστος. Υπάρχουν πολυάριθμα παραδείγματα αξιοσημείωτων κυβερνοεπιθέσεων που οφείλονται στην ελλιπή ασφάλεια των προϊόντων, όπως το λυτρισμικό WannaCry, το οποίο εκμεταλλεύτηκε ένα τρωτό σημείο των Windows που επηρέασε 200 000 υπολογιστές σε 150 χώρες το 2017 και προκάλεσε ζημία ύψους δισεκατομμυρίων δολαρίων ΗΠΑ, η επίθεση στην αλυσίδα εφοδιασμού Kaseya VSA, η οποία χρησιμοποίησε το λογισμικό διαχείρισης δικτύου της Kaseya για να επιτεθεί σε περισσότερες από 1 000 εταιρείες και ανάγκασε μια αλυσίδα σούπερ μάρκετ να κλείσει τα συνολικά 500 καταστήματά της σε ολόκληρη τη Σουηδία, ή πολυάριθμα συμβάντα παραβίασης τραπεζικών εφαρμογών για αφαίρεση χρημάτων από ανυποψίαστους καταναλωτές.

Προσδιορίστηκαν δύο κύριοι στόχοι που αποσκοπούν στη διασφάλιση της ορθής λειτουργίας της εσωτερικής αγοράς: 1) να δημιουργηθούν συνθήκες για την ανάπτυξη ασφαλών προϊόντων με ψηφιακά στοιχεία μέσω της διασφάλισης ότι στην αγορά διατίθενται προϊόντα υλισμικού και λογισμικού με λιγότερα τρωτά σημεία και να διασφαλιστεί ότι οι κατασκευαστές λαμβάνουν σοβαρά υπόψη το ζήτημα της ασφάλειας καθ' όλη τη διάρκεια του κύκλου ζωής των προϊόντων· και 2) να δημιουργηθούν συνθήκες που επιτρέπουν στους χρήστες να λαμβάνουν υπόψη την κυβερνοασφάλεια κατά την επιλογή και τη χρήση προϊόντων με ψηφιακά στοιχεία. Καθορίστηκαν τέσσερις ειδικοί στόχοι: i) να διασφαλιστεί ότι οι κατασκευαστές βελτιώνουν την ασφάλεια των προϊόντων με ψηφιακά στοιχεία ήδη από

το στάδιο σχεδιασμού και ανάπτυξης και καθ' όλη τη διάρκεια του κύκλου ζωής· ii) να διασφαλιστεί ένα συνεκτικό πλαίσιο κυβερνοασφάλειας, το οποίο θα διευκολύνει τη συμμόρφωση των κατασκευαστών υλισμικού και λογισμικού· iii) να ενισχυθεί η διαφάνεια των ιδιοτήτων ασφάλειας των προϊόντων με ψηφιακά στοιχεία και iv) να παρέχονται στις επιχειρήσεις και στους καταναλωτές η δυνατότητα να χρησιμοποιούν με ασφάλεια τα προϊόντα με ψηφιακά στοιχεία.

Ο ισχυρός διασυνοριακός χαρακτήρας της κυβερνοασφάλειας και ο αυξανόμενος αριθμός των συμβάντων, με δευτερογενείς επιπτώσεις σε διασυνοριακό επίπεδο, καθώς και σε τομείς και προϊόντα, σημαίνουν ότι οι στόχοι δεν μπορούν να επιτευχθούν αποτελεσματικά μόνο από τα κράτη μέλη. Δεδομένου του παγκόσμιου χαρακτήρα των αγορών προϊόντων με ψηφιακά στοιχεία, τα κράτη μέλη αντιμετωπίζουν τους ίδιους κινδύνους για το ίδιο προϊόν με ψηφιακά στοιχεία στην επικράτειά τους. Το κατακερματισμένο πλαίσιο δυνητικά αποκλινόντων εθνικών κανόνων που αναδύεται, ενέχει τον κίνδυνο να παρεμποδίσει την ύπαρξη μιας ανοικτής και ανταγωνιστικής ενιαίας αγοράς για προϊόντα με ψηφιακά στοιχεία. Ως εκ τούτου, η κοινή δράση σε επίπεδο ΕΕ είναι αναγκαία για την αύξηση του επιπέδου εμπιστοσύνης μεταξύ των χρηστών και της ελκυστικότητας των ενωσιακών προϊόντων με ψηφιακά στοιχεία. Θα ωφελήσει επίσης την εσωτερική αγορά, καθώς θα παρέχει ασφάλεια δικαίου και θα εξασφαλίσει ισότιμους όρους ανταγωνισμού για τους πωλητές προϊόντων με ψηφιακά στοιχεία, όπως επισημαίνεται επίσης στην τελική έκθεση της Διάσκεψης για το Μέλλον της Ευρώπης, στην οποία οι πολίτες ζητούν να ενισχυθεί ο ρόλος της ΕΕ στην αντιμετώπιση των απειλών κατά της κυβερνοασφάλειας.

- **Αλληλεπίδραση με τις ισχύουσες διατάξεις στον τομέα πολιτικής**

Το πλαίσιο της ΕΕ περιλαμβάνει διάφορες οριζόντιες νομοθετικές πράξεις που καλύπτουν ορισμένες πτυχές που συνδέονται με την κυβερνοασφάλεια από διάφορες οπτικές γωνίες (προϊόντα, υπηρεσίες, διαχείριση κρίσεων και εγκλήματα). Το 2013 άρχισε να ισχύει η οδηγία για τις επιθέσεις κατά συστημάτων πληροφοριών[1], με σκοπό την εναρμόνιση της ποινικοποίησης και των κυρώσεων για σειρά αδικημάτων που στρέφονται κατά των συστημάτων πληροφοριών. Τον Αύγουστο του 2016, άρχισε να ισχύει η οδηγία (ΕΕ) 2016/1148 για την ασφάλεια συστημάτων δικτύου και πληροφοριών (οδηγία NIS)[2] ως η πρώτη νομοθετική πράξη σε επίπεδο ΕΕ για την κυβερνοασφάλεια. Η αναθεώρησή της, η οποία κατέληξε στην οδηγία [οδηγία XXX/XXXX (NIS2)], αυξάνει το κοινό επίπεδο φιλοδοξίας της ΕΕ. Το 2019 άρχισε να ισχύει η πράξη της ΕΕ για την κυβερνοασφάλεια[3], με στόχο την ενίσχυση της ασφάλειας των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ με τη θέσπιση ενός εθελοντικού ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας[4].

---

1 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).

2 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 της 19.7.2016, σ. 1).

3 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).

4 Η πράξη για την κυβερνοασφάλεια επιτρέπει την ανάπτυξη ειδικών συστημάτων πιστοποίησης. Κάθε σύστημα περιλαμβάνει παραπομπές σε σχετικά πρότυπα, τεχνικές προδιαγραφές ή άλλες απαιτήσεις

Η κυβερνοασφάλεια ολόκληρης της αλυσίδας εφοδιασμού εξασφαλίζεται μόνο εφόσον όλα τα στοιχεία της είναι κυβερνοασφαλή. Ωστόσο, η προαναφερθείσα νομοθεσία της ΕΕ παρουσιάζει σημαντικά κενά εν προκειμένω, καθώς δεν καλύπτει τις υποχρεωτικές απαιτήσεις για την ασφάλεια των προϊόντων με ψηφιακά στοιχεία.

Ενώ η προτεινόμενη πράξη για την κυβερνοανθεκτικότητα καλύπτει προϊόντα με ψηφιακά στοιχεία που διατίθενται στην αγορά, η οδηγία [οδηγία XXX/XXX (NIS2)] αποσκοπεί στη διασφάλιση υψηλού επιπέδου κυβερνοασφάλειας των υπηρεσιών που παρέχονται από βασικές και σημαντικές οντότητες. Η οδηγία [οδηγία XXX/XXXX (NIS2)] απαιτεί από τα κράτη μέλη να διασφαλίζουν ότι οι βασικές και σημαντικές οντότητες που εμπίπτουν στο πεδίο εφαρμογής της, όπως οι πάροχοι υγειονομικής περίθαλψης ή οι πάροχοι υπηρεσιών υπολογιστικού νέφους και οι φορείς δημόσιας διοίκησης, λαμβάνουν κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα κυβερνοασφάλειας. Μεταξύ άλλων, περιλαμβάνεται η απαίτηση να διασφαλίζεται η ασφάλεια κατά την αγορά, την ανάπτυξη και τη συντήρηση συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένων του χειρισμού και της γνωστοποίησης τρωτών σημείων. Η οδηγία [οδηγία XXX/XXXX (NIS2)] απαιτεί από την Επιτροπή να εκδίδει εκτελεστικές πράξεις για τον καθορισμό των τεχνικών και μεθοδολογικών απαιτήσεων των εν λόγω μέτρων εντός 21 μηνών από την ημερομηνία έναρξης ισχύος της παρούσας οδηγίας για ορισμένους τύπους οντοτήτων, όπως οι πάροχοι υπηρεσιών υπολογιστικού νέφους. Για όλες τις άλλες οντότητες, η Επιτροπή μπορεί να εκδώσει εκτελεστική πράξη για τον καθορισμό των τεχνικών και μεθοδολογικών απαιτήσεων, καθώς και των απαιτήσεων ανά τομέα. Το πλαίσιο αυτό θα διασφαλίσει ότι τεχνικές προδιαγραφές και μέτρα παρόμοια με τις βασικές απαιτήσεις κυβερνοασφάλειας της πράξης για την κυβερνοανθεκτικότητα εφαρμόζονται επίσης για τον σχεδιασμό, την ανάπτυξη και τον χειρισμό των τρωτών σημείων του λογισμικού που παρέχεται ως υπηρεσία (λογισμικό ως υπηρεσία). Για παράδειγμα, αυτό θα μπορούσε να αποτελέσει μέσο για τη διασφάλιση υψηλού επιπέδου κυβερνοασφάλειας σε περιπτώσεις όπως τα συστήματα ηλεκτρονικών μητρώων υγείας, μεταξύ άλλων όταν παραδίδονται ως λογισμικό ως υπηρεσία (SaaS) ή αναπτύσσονται σε μονάδες υγείας (εσωτερικά), σύμφωνα με τον προτεινόμενο [κανονισμό για τον ευρωπαϊκό χώρο δεδομένων για την υγεία].

- **Αλληλεπίδραση με άλλες πολιτικές της Ένωσης**

Όπως ορίζεται στην ανακοίνωση της Επιτροπής με τίτλο «Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης»[5], η ΕΕ είναι κρίσιμο να αξιοποιήσει όλα τα οφέλη της ψηφιακής εποχής και να ενισχύσει τη βιομηχανική ικανότητά της και την ικανότητά της για καινοτομία, εντός ασφαλών και δεοντολογικών ορίων. Η ευρωπαϊκή στρατηγική για τα δεδομένα καθορίζει τέσσερις πυλώνες —προστασία δεδομένων, θεμελιώδη δικαιώματα, ασφάλεια και κυβερνοασφάλεια— ως βασικές προϋποθέσεις για μια κοινωνία που βασίζεται στη χρήση δεδομένων.

Το ισχύον πλαίσιο της ΕΕ[6] για τα προϊόντα που ενδεχομένως έχουν και ψηφιακά στοιχεία περιλαμβάνει πολλές νομοθετικές πράξεις, συμπεριλαμβανομένης της νομοθεσίας της ΕΕ για συγκεκριμένα προϊόντα που καλύπτουν πτυχές σχετικές με την ασφάλεια και της γενικής νομοθεσίας περί ευθύνης λόγω ελαττωματικών προϊόντων. Η πρόταση συνάδει με το ισχύον

---

κυβερνοασφάλειας που ορίζονται στο σύστημα. Η απόφαση για την ανάπτυξη πιστοποίησης της κυβερνοασφάλειας λαμβάνεται βάσει κινδύνου.

5 Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών «Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης» [COM(2020) 67 final της 19ης Φεβρουαρίου 2020].

6 Κυρίως νομοθεσία του νέου νομοθετικού πλαισίου (ΝΝΠ).

κανονιστικό πλαίσιο της ΕΕ για τα προϊόντα, καθώς και με πρόσφατες νομοθετικές προτάσεις, όπως η πρόταση κανονισμού της Επιτροπής [κανονισμός για την τεχνητή νοημοσύνη (ΤΝ)][7].

Ο προτεινόμενος κανονισμός θα εφαρμόζεται σε όλο τον ραδιοεξοπλισμό που εμπίπτει στο πεδίο εφαρμογής του κατ' εξουσιοδότηση κανονισμού (ΕΕ) 2022/30 της Επιτροπής. Επιπλέον, οι απαιτήσεις που ορίζονται στον παρόντα κανονισμό περιλαμβάνουν όλα τα στοιχεία των ουσιωδών απαιτήσεων που αναφέρονται στο άρθρο 3 παράγραφος 3 στοιχεία δ), ε) και στ) της οδηγίας 2014/53/ΕΕ, συμπεριλαμβανομένων των κύριων στοιχείων που καθορίζονται στην [εκτελεστική απόφαση XXX/2022 της Επιτροπής σχετικά με αίτημα τυποποίησης προς τους ευρωπαϊκούς οργανισμούς τυποποίησης] που εκδίδεται βάσει του εν λόγω κατ' εξουσιοδότηση κανονισμού. Προκειμένου να αποφευχθούν ρυθμιστικές επικαλύψεις, προβλέπεται ότι η Επιτροπή θα καταργήσει ή θα τροποποιήσει τον κατ' εξουσιοδότηση κανονισμό όσον αφορά τον ραδιοεξοπλισμό που καλύπτεται από τον προτεινόμενο κανονισμό, έτσι ώστε ο τελευταίος να εφαρμοστεί σε αυτόν, μόλις τεθεί σε εφαρμογή.

Επιπλέον, προκειμένου να αποφευχθεί η αλληλεπικάλυψη των εργασιών, προβλέπεται ότι η Επιτροπή και οι ευρωπαϊκοί οργανισμοί τυποποίησης θα λάβουν υπόψη τις εργασίες τυποποίησης που πραγματοποιήθηκαν στο πλαίσιο της εκτελεστικής απόφασης C(2022)5637 της Επιτροπής σχετικά με αίτημα τυποποίησης για τον κατ' εξουσιοδότηση κανονισμό 2022/30 της Επιτροπής κατά την κατάρτιση και την ανάπτυξη εναρμονισμένων προτύπων για τη διευκόλυνση της εφαρμογής του κανονισμού.

## 2. ΝΟΜΙΚΗ ΒΑΣΗ, ΕΠΙΚΟΥΡΙΚΟΤΗΤΑ ΚΑΙ ΑΝΑΛΟΓΙΚΟΤΗΤΑ

### • Νομική βάση

Η νομική βάση της παρούσας πρότασης είναι το άρθρο 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), το οποίο προβλέπει την έκδοση μέτρων για τη διασφάλιση της εγκαθίδρυσης και της λειτουργίας της εσωτερικής αγοράς. Σκοπός της πρότασης είναι η εναρμόνιση των απαιτήσεων κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία σε όλα τα κράτη μέλη και η άρση των εμποδίων στην ελεύθερη κυκλοφορία των εμπορευμάτων.

Το άρθρο 114 της ΣΛΕΕ μπορεί να χρησιμοποιηθεί ως νομική βάση για την πρόληψη της εμφάνισης των εμποδίων που προκύπτουν από αποκλίνουσες εθνικές νομοθεσίες και προσεγγίσεις σχετικά με τον τρόπο αντιμετώπισης της έλλειψης ασφάλειας δικαίου και των νομοθετικών κενών στα υφιστάμενα νομικά πλαίσια[8]. Επιπλέον, το Δικαστήριο έχει αναγνωρίσει ότι η ανομοιογενής εφαρμογή των τεχνικών απαιτήσεων θα μπορούσε να αποτελέσει βάσιμο λόγο για την εφαρμογή του άρθρου 114 της ΣΛΕΕ[9].

---

[7] Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (πράξη για την τεχνητή νοημοσύνη) και για την τροποποίηση ορισμένων νομοθετικών πράξεων της Ένωσης [COM(2021) 206 final της 21ης Απριλίου 2021].

[8] Απόφαση του Δικαστηρίου (τμήμα μείζονος συνθέσεως) της 3ης Δεκεμβρίου 2019, Τσεχική Δημοκρατία κατά Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της Ευρωπαϊκής Ένωσης, υπόθεση C-482/17, σκέψη 35.

[9] Απόφαση του Δικαστηρίου (τμήμα μείζονος συνθέσεως) της 2ας Μαΐου 2006, Ηνωμένο Βασίλειο της Μεγάλης Βρετανίας και της Βόρειας Ιρλανδίας κατά Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της Ευρωπαϊκής Ένωσης, υπόθεση C-217/04, σκέψεις 62-63.

Το ισχύον νομοθετικό πλαίσιο της ΕΕ για τα προϊόντα με ψηφιακά στοιχεία βασίζεται στο άρθρο 114 της ΣΛΕΕ και περιλαμβάνει πολλές νομοθετικές πράξεις, μεταξύ άλλων για συγκεκριμένα προϊόντα και πτυχές σχετικές με την ασφάλεια ή τη γενική νομοθεσία περί ευθύνης λόγω ελαττωματικών προϊόντων. Ωστόσο, καλύπτει μόνο ορισμένες πτυχές που συνδέονται με την κυβερνοασφάλεια των υλικών ψηφιακών προϊόντων και, κατά περίπτωση, του ενσωματωμένου λογισμικού στα εν λόγω προϊόντα. Σε εθνικό επίπεδο, τα κράτη μέλη αρχίζουν να λαμβάνουν εθνικά μέτρα που απαιτούν από τους πωλητές ψηφιακών προϊόντων να ενισχύσουν την κυβερνοασφάλειά τους[10]. Ταυτόχρονα, η κυβερνοασφάλεια των ψηφιακών προϊόντων έχει ιδιαίτερα ισχυρή διασυνοριακή διάσταση, καθώς τα προϊόντα που κατασκευάζονται σε μία χώρα συχνά χρησιμοποιούνται από οργανισμούς και καταναλωτές σε ολόκληρη την εσωτερική αγορά. Συμβάντα που αρχικά αφορούν μία μόνο οντότητα ή ένα κράτος μέλος συχνά διαδίδονται εντός λίγων λεπτών σε οργανισμούς, τομείς και διάφορα κράτη μέλη.

Οι διάφορες πράξεις και πρωτοβουλίες που έχουν δρομολογηθεί μέχρι στιγμής σε ενωσιακό και εθνικό επίπεδο αντιμετωπίζουν εν μέρει μόνο τα προβλήματα που εντοπίστηκαν και ενέχουν τον κίνδυνο να δημιουργηθεί ένα νομοθετικό συνονθύλευμα εντός της εσωτερικής αγοράς, να αυξηθεί η ανασφάλεια δικαίου τόσο για τους πωλητές όσο και για τους χρήστες των εν λόγω προϊόντων και να προστεθεί περιττός φόρτος για τις εταιρείες όσον αφορά τη συμμόρφωσή τους με σειρά απαιτήσεων για παρόμοιους τύπους προϊόντων.

Ο προτεινόμενος κανονισμός θα εναρμονίσει και θα εξορθολογίσει το κανονιστικό τοπίο στην ΕΕ με τη θέσπιση απαιτήσεων κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και την αποφυγή επικαλυπτόμενων απαιτήσεων που απορρέουν από τις διαφορετικές νομοθετικές πράξεις. Κατ' αυτό τον τρόπο, θα ενισχυθεί η ασφάλεια δικαίου για τους φορείς και τους χρήστες σε ολόκληρη την Ένωση, ενώ παράλληλα θα βελτιωθεί η εναρμόνιση της ευρωπαϊκής ενιαίας αγοράς, με αποτέλεσμα να δημιουργηθούν πιο βιώσιμες συνθήκες για τους φορείς που επιθυμούν να εισέλθουν στην αγορά της ΕΕ.

- **Επικουρικότητα (σε περίπτωση μη αποκλειστικής αρμοδιότητας)**

Ο ισχυρός διασυνοριακός χαρακτήρας της κυβερνοασφάλειας εν γένει, καθώς και ο αυξανόμενος αριθμός των κινδύνων και των συμβάντων, τα οποία έχουν δευτερογενείς επιπτώσεις σε διασυνοριακό επίπεδο, καθώς και σε τομείς και προϊόντα, σημαίνουν ότι οι στόχοι της παρούσας παρέμβασης δεν μπορούν να επιτευχθούν αποτελεσματικά μόνο από τα κράτη μέλη. Οι προσεγγίσεις σε εθνικό επίπεδο για την αντιμετώπιση των προβλημάτων, και ιδίως οι προσεγγίσεις που εισάγουν υποχρεωτικές απαιτήσεις, θα δημιουργήσουν μεγαλύτερη ανασφάλεια δικαίου και περισσότερα νομικά εμπόδια. Θα μπορούσαν να προκληθούν εμπόδια στην απρόσκοπτη επέκταση των εταιρειών σε άλλα κράτη μέλη, γεγονός που θα στερούσε από τους χρήστες τα οφέλη των προϊόντων τους.

Ως εκ τούτου, η κοινή δράση σε επίπεδο ΕΕ είναι αναγκαία για την εδραίωση υψηλού επιπέδου εμπιστοσύνης μεταξύ των χρηστών, ώστε να ενισχυθεί η ελκυστικότητα των ενωσιακών προϊόντων με ψηφιακά στοιχεία. Μπορεί επίσης να ωφελήσει την ψηφιακή ενιαία αγορά και την εσωτερική αγορά εν γένει, παρέχοντας ασφάλεια δικαίου και επιτυγχάνοντας ισότιμους όρους ανταγωνισμού για τους κατασκευαστές προϊόντων με ψηφιακά στοιχεία.

[10] Για παράδειγμα, το 2019 η Φινλανδία δημιούργησε ένα σύστημα επισήμανσης για συσκευές IoT, όπως έξυπνες τηλεοράσεις, έξυπνα τηλέφωνα και παιχνίδια με βάση τα πρότυπα του ETSI. Η Γερμανία πρόσφατα θέσπισε ετικέτα ασφάλειας των καταναλωτών για ευρυζωνικούς δρομολογητές, έξυπνες τηλεοράσεις, φωτογραφικές μηχανές, ηχεία, παιχνίδια, καθώς και για ρομπότ καθαρισμού και κηπουρικής.

Τέλος, στα συμπεράσματα του Συμβουλίου της 23ης Μαΐου 2022 σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο, η Επιτροπή καλείται να προτείνει, έως το τέλος του 2022, κοινές απαιτήσεις κυβερνοασφάλειας για τις συνδεδεμένες συσκευές.

- **Αναλογικότητα**

Όσον αφορά την αναλογικότητα του προτεινόμενου κανονισμού, τα μέτρα στις επιλογές πολιτικής που εξετάστηκαν δεν θα υπερέβαιναν τα αναγκαία για την επίτευξη των γενικών και ειδικών στόχων και δεν θα συνεπάγονταν δυσανάλογο κόστος. Ειδικότερα, η εξεταζόμενη παρέμβαση θα διασφαλίσει ότι τα προϊόντα με ψηφιακά στοιχεία θα είναι εξασφαλισμένα καθ' όλη τη διάρκεια του κύκλου ζωής τους και αναλογικά προς τους κινδύνους που ενέχουν μέσω τεχνολογικά ουδέτερων απαιτήσεων που προσανατολίζονται στους στόχους, παραμένουν εύλογες και εν γένει ανταποκρίνονται στο συμφέρον των εμπλεκόμενων οντοτήτων.

Οι βασικές απαιτήσεις κυβερνοασφάλειας στην πρόταση βασίζονται σε ευρέως χρησιμοποιούμενα πρότυπα, ενώ η διαδικασία τυποποίησης που θα ακολουθήσει θα λαμβάνει υπόψη τις τεχνικές ιδιαιτερότητες των προϊόντων. Αυτό σημαίνει ότι, εφόσον απαιτείται για δεδομένο επίπεδο κινδύνου, οι διαδικασίες ασφάλειας θα προσαρμόζονται. Επιπλέον, οι προβλεπόμενοι οριζόντιοι κανόνες θα προβλέπουν μόνο αξιολόγηση από τρίτους για τα κρίσιμα προϊόντα. Στο πλαίσιο αυτό, θα περιλαμβάνεται μόνο ένα μικρό μερίδιο της αγοράς για προϊόντα με ψηφιακά στοιχεία. Ο αντίκτυπος στις ΜΜΕ θα εξαρτηθεί από την παρουσία τους στην αγορά αυτών των συγκεκριμένων κατηγοριών προϊόντων.

Όσον αφορά την αναλογικότητα του κόστους για την αξιολόγηση της συμμόρφωσης, οι κοινοποιημένοι οργανισμοί που διενεργούν τις αξιολογήσεις από τρίτους θα λαμβάνουν υπόψη το μέγεθος της επιχείρησης για τον καθορισμό της αμοιβής τους. Θα προβλεφθεί επίσης εύλογη μεταβατική περίοδος 24 μηνών για την προετοιμασία της εφαρμογής, ώστε οι σχετικές αγορές να έχουν χρόνο για να προετοιμαστούν, ενώ παράλληλα θα παρέχονται σαφείς κατευθύνσεις για επενδύσεις στην έρευνα και ανάπτυξη. Το πιθανό κόστος συμμόρφωσης για τις επιχειρήσεις θα αντισταθμίζεται από τα οφέλη που θα προκύψουν από το υψηλότερο επίπεδο ασφάλειας των προϊόντων με ψηφιακά στοιχεία και, κατ' επέκταση, από την αύξηση της εμπιστοσύνης των χρηστών στα εν λόγω προϊόντα.

- **Επιλογή της νομικής πράξης**

Μια ρυθμιστική παρέμβαση θα συνεπαγόταν την έκδοση κανονισμού και όχι οδηγίας. Αυτό οφείλεται στο γεγονός ότι, για το συγκεκριμένο είδος νομοθεσίας για τα προϊόντα, ένας κανονισμός θα αντιμετώπιζε αποτελεσματικότερα τα προβλήματα που εντοπίζονται και θα ανταποκρινόταν στους διατυπωμένους στόχους, δεδομένου ότι πρόκειται για παρέμβαση που θέτει τους όρους για τη διάθεση μιας πολύ ευρείας κατηγορίας προϊόντων στην εσωτερική αγορά. Η διαδικασία μεταφοράς μιας οδηγίας στο εθνικό δίκαιο για μια τέτοια παρέμβαση θα μπορούσε να αφήνει υπερβολικά περιθώρια διακριτικής ευχέρειας σε εθνικό επίπεδο, με αποτέλεσμα ενδεχομένως την έλλειψη ομοιομορφίας ορισμένων βασικών απαιτήσεων κυβερνοασφάλειας, ανασφάλεια δικαίου, περαιτέρω κατακερματισμό ή ακόμη και καταστάσεις που εισάγουν διακρίσεις σε διασυνοριακό επίπεδο, αν ληφθεί μάλιστα υπόψη το γεγονός ότι τα προϊόντα που καλύπτονται θα μπορούσαν να είναι πολλαπλών σκοπών ή χρήσεων και ότι οι κατασκευαστές μπορούν να παράγουν πολλαπλές κατηγορίες τέτοιων προϊόντων.

## 3. ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΩΝ ΕΚ ΤΩΝ ΥΣΤΕΡΩΝ ΑΞΙΟΛΟΓΗΣΕΩΝ, ΤΩΝ ΔΙΑΒΟΥΛΕΥΣΕΩΝ ΜΕ ΤΑ ΕΝΔΙΑΦΕΡΟΜΕΝΑ ΜΕΡΗ ΚΑΙ ΤΩΝ ΕΚΤΙΜΗΣΕΩΝ ΕΠΙΠΤΩΣΕΩΝ

- **Διαβουλεύσεις με τα ενδιαφερόμενα μέρη**

Η Επιτροπή έχει προβεί σε διαβουλεύσεις με ένα ευρύ φάσμα ενδιαφερομένων μερών. Τα κράτη μέλη και τα ενδιαφερόμενα μέρη κλήθηκαν να συμμετάσχουν στην ανοικτή δημόσια διαβούλευση και στις έρευνες και τα εργαστήρια που διοργανώθηκαν στο πλαίσιο μελέτης που εκπονήθηκε από κοινοπραξία για την υποστήριξη των προπαρασκευαστικών εργασιών της Επιτροπής για την εκτίμηση επιπτώσεων: Wavestone, Κέντρο Μελετών Ευρωπαϊκής Πολιτικής (CEPS) και ICF. Τα ενδιαφερόμενα μέρη που συμμετείχαν στη διαβούλευση περιλάμβαναν εθνικές αρχές εποπτείας της αγοράς, όργανα της Ένωσης που ασχολούνται με την κυβερνοασφάλεια, κατασκευαστές υλισμικού και λογισμικού, εισαγωγείς και διανομείς υλισμικού και λογισμικού, εμπορικές ενώσεις, οργανώσεις καταναλωτών και χρήστες προϊόντων με ψηφιακά στοιχεία και πολίτες, ερευνητές και πανεπιστήμια, κοινοποιημένους οργανισμούς και οργανισμούς διαπίστευσης, καθώς και επαγγελματίες του κλάδου της κυβερνοασφάλειας.

Οι δραστηριότητες διαβούλευσης περιλάμβαναν:

- Μια πρώτη μελέτη που εκπονήθηκε από κοινοπραξία αποτελούμενη από τις ICF, Wavestone, Carsa και CEPS, η οποία δημοσιεύθηκε τον Δεκέμβριο του 2021[11]. Η μελέτη εντόπισε διάφορες αδυναμίες της αγοράς και αξιολόγησε πιθανές ρυθμιστικές παρεμβάσεις.
- Ανοικτή δημόσια διαβούλευση που απευθυνόταν σε πολίτες, ενδιαφερόμενα μέρη και εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας. Υποβλήθηκαν 176 απαντήσεις. Οι απαντήσεις αυτές συνέβαλαν στη συλλογή ποικίλων απόψεων και εμπειριών από όλες τις ομάδες ενδιαφερομένων.
- Στα εργαστήρια που διοργανώθηκαν στο πλαίσιο της μελέτης για την υποστήριξη των προπαρασκευαστικών εργασιών της Επιτροπής για μια πράξη για την κυβερνοανθεκτικότητα συμμετείχαν περίπου 100 εκπρόσωποι και από τα 27 κράτη μέλη, οι οποίοι εκπροσωπούσαν διάφορα ενδιαφερόμενα μέρη.
- Πραγματοποιήθηκαν συνεντεύξεις με εμπειρογνώμονες, με σκοπό τη βαθύτερη κατανόηση των σημερινών προκλήσεων στον τομέα της κυβερνοασφάλειας όσον αφορά τα προϊόντα με ψηφιακά στοιχεία, καθώς και για να συζητηθούν επιλογές πολιτικής για μια πιθανή ρυθμιστική παρέμβαση.
- Πραγματοποιήθηκαν διμερείς συζητήσεις με τις εθνικές αρχές κυβερνοασφάλειας, τον ιδιωτικό τομέα και οργανώσεις καταναλωτών.
- Πραγματοποιήθηκαν στοχευμένες επαφές με βασικούς ενδιαφερόμενους φορείς των ΜΜΕ.

- **Συλλογή και χρήση εμπειρογνωσίας**

Οι δραστηριότητες διαβούλευσης αποσκοπούσαν στη συγκέντρωση στοιχείων σχετικά με τα πέντε κύρια κριτήρια αξιολόγησης με βάση τις κατευθυντήριες γραμμές της ΕΕ για τη

[11] Μελέτη σχετικά με την ανάγκη των απαιτήσεων κυβερνοασφάλειας για προϊόντα ΤΠΕ — αριθ. 2020-0715, τελική έκθεση μελέτης, διαθέσιμη στη διεύθυνση https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.

βελτίωση της νομοθεσίας (αποτελεσματικότητα, αποδοτικότητα, συνάφεια, συνοχή, ενωσιακή προστιθέμενη αξία), καθώς και τις πιθανές επιπτώσεις των πιθανών επιλογών για το μέλλον. Ο ανάδοχος δεν προσέγγισε απλώς τα ενδιαφερόμενα μέρη που θα επηρεαστούν άμεσα από τον προτεινόμενο κανονισμό, αλλά παράλληλα έχει πραγματοποιήσει διαβουλεύσεις με ευρύ φάσμα εμπειρογνωμόνων στον τομέα της κυβερνοασφάλειας.

- **Εκτίμηση επιπτώσεων**

Η Επιτροπή διενήργησε εκτίμηση των επιπτώσεων για την παρούσα πρόταση, η οποία εξετάστηκε από την επιτροπή ρυθμιστικού ελέγχου της Επιτροπής. Στις 6 Ιουλίου 2022 πραγματοποιήθηκε συνεδρίαση με την επιτροπή ρυθμιστικού ελέγχου, σε συνέχεια της οποίας εκδόθηκε θετική γνώμη. Η εκτίμηση επιπτώσεων προσαρμόστηκε ώστε να ληφθούν υπόψη οι συστάσεις και οι παρατηρήσεις της επιτροπής ρυθμιστικού ελέγχου.

Η Επιτροπή εξέτασε διάφορες επιλογές πολιτικής για την επίτευξη του γενικού στόχου της πρότασης:

- Προσέγγιση μη δεσμευτικού δικαίου και προαιρετικά μέτρα (επιλογή 1): Στην επιλογή αυτή, δεν θα υπάρχει υποχρεωτική ρυθμιστική παρέμβαση. Αντ' αυτού, η Επιτροπή θα εκδίδει ανακοινώσεις, κατευθυντήριες γραμμές, συστάσεις και ενδεχομένως κώδικες δεοντολογίας για να ενθαρρύνει τη λήψη προαιρετικών μέτρων. Θα εξακολουθήσουν να θεσπίζονται εθνικά συστήματα, προαιρετικά ή υποχρεωτικά, για την αντιστάθμιση της έλλειψης οριζόντιων κανόνων της ΕΕ.
- Ad hoc ρυθμιστική παρέμβαση για την κυβερνοασφάλεια υλικών προϊόντων με ψηφιακά στοιχεία και αντίστοιχο ενσωματωμένο λογισμικό (επιλογή 2): Η επιλογή αυτή θα περιορίζεται στην προσθήκη και/ή στην τροποποίηση των απαιτήσεων κυβερνοασφάλειας της ήδη υφιστάμενης νομοθεσίας ή στη θέσπιση νέας νομοθεσίας όταν εμφανίζονται νέοι κίνδυνοι, μεταξύ άλλων δυνητικά σε μη ενσωματωμένο λογισμικό.

Οι επιλογές 3 και 4 συνεπάγονται οριζόντια ρυθμιστική παρέμβαση που ποικίλλει ως προς το πεδίο εφαρμογής, σε μεγάλο βαθμό σύμφωνα με το νέο νομοθετικό πλαίσιο (ΝΝΠ). Το πλαίσιο αυτό καθορίζει τις βασικές απαιτήσεις ως προϋπόθεση για τη διάθεση ορισμένων προϊόντων στην εσωτερική αγορά. Το ΝΝΠ προβλέπει επίσης κατά κανόνα την αξιολόγηση της συμμόρφωσης, τη διαδικασία που διεξάγεται από τον κατασκευαστή για να αποδείξει αν πληρούνται οι ειδικές απαιτήσεις που αφορούν ένα προϊόν.

- Μικτή προσέγγιση, συμπεριλαμβανομένων οριζόντιων υποχρεωτικών κανόνων για την κυβερνοασφάλεια υλικών προϊόντων με ψηφιακά στοιχεία και αντίστοιχου ενσωματωμένου λογισμικού και κλιμακωτή προσέγγιση για μη ενσωματωμένο λογισμικό (επιλογή 3): Η επιλογή αυτή συνεπάγεται την έκδοση κανονισμού για τη θέσπιση οριζόντιων απαιτήσεων κυβερνοασφάλειας για όλα τα υλικά προϊόντα με ψηφιακά στοιχεία και το λογισμικό που είναι ενσωματωμένο σε αυτά, ως προϋπόθεση για τη διάθεση στην αγορά, και θα περιλαμβάνει δύο επιμέρους επιλογές με και χωρίς υποχρεωτική αξιολόγηση από τρίτους (3i και 3ii). Το μη ενσωματωμένο λογισμικό δεν θα αποτελεί αντικείμενο κανονιστικής ρύθμισης.
- Οριζόντια ρυθμιστική παρέμβαση με την οποία θεσπίζονται απαιτήσεις κυβερνοασφάλειας για ευρύ φάσμα υλικών και άυλων προϊόντων με ψηφιακά στοιχεία, συμπεριλαμβανομένου του μη ενσωματωμένου λογισμικού (επιλογή 4): Η επιλογή αυτή είναι όμοια με την επιλογή 3, εκτός από το πεδίο

εφαρμογής. Η επιλογή 4 περιλαμβάνει μη ενσωματωμένο λογισμικό [με δύο επιμέρους επιλογές που περιλαμβάνουν, αντίστοιχα, μόνο κρίσιμο λογισμικό (4α) ή το σύνολο του λογισμικού (4β)] στο πεδίο εφαρμογής ενός πιθανού κανονισμού. Για κάθε επιμέρους επιλογή, θα εξετάζονται οι ίδιες επιμέρους επιλογές που σχετίζονται με την αξιολόγηση της συμμόρφωσης όπως και για την επιλογή 3.

Η επιλογή 4 (με επιμέρους επιλογές που καλύπτουν όλο το λογισμικό και περιλαμβάνουν υποχρεωτική αξιολόγηση από τρίτους για κρίσιμα προϊόντα) αναδείχθηκε ως η προτιμώμενη επιλογή με βάση την αξιολόγηση της αποτελεσματικότητας σε σχέση με τους ειδικούς στόχους και της αποδοτικότητας του κόστους έναντι των οφελών. Η επιλογή αυτή θα διασφάλιζε τον καθορισμό ειδικών οριζόντιων απαιτήσεων κυβερνοασφάλειας για όλα τα προϊόντα με ψηφιακά στοιχεία που διατίθενται ή καθίστανται διαθέσιμα στην εσωτερική αγορά, και θα ήταν η μόνη επιλογή που θα κάλυπτε ολόκληρη την ψηφιακή αλυσίδα εφοδιασμού. Το μη ενσωματωμένο λογισμικό, το οποίο συχνά είναι εκτεθειμένο σε τρωτά σημεία, θα καλύπτεται επίσης από σχετική ρυθμιστική παρέμβαση, ώστε να διασφαλιστεί μια συνεκτική προσέγγιση για όλα τα προϊόντα με ψηφιακά στοιχεία, με σαφές μερίδιο ευθυνών μεταξύ των διαφόρων οικονομικών φορέων.

Αυτή η επιλογή πολιτικής προσφέρει επίσης προστιθέμενη αξία καλύπτοντας πτυχές του καθήκοντος επιμέλειας και ολόκληρου του κύκλου ζωής μετά τη διάθεση των προϊόντων με ψηφιακά στοιχεία στην αγορά, ώστε να διασφαλίζεται, μεταξύ άλλων, η κατάλληλη πληροφόρηση σχετικά με την υποστήριξη της ασφάλειας και η παροχή ενημερώσεων ασφαλείας. Αυτή η επιλογή πολιτικής θα μπορούσε επίσης να συμπληρώσει αποτελεσματικότερα την πρόσφατη αναθεώρηση του πλαισίου NIS, διασφαλίζοντας τις προϋποθέσεις για την ενίσχυση της ασφάλειας της αλυσίδας εφοδιασμού.

Η προτιμώμενη επιλογή θα αποφέρει σημαντικά οφέλη στα διάφορα ενδιαφερόμενα μέρη. Όσον αφορά τις επιχειρήσεις, θα αποτρέψει την ύπαρξη αποκλινόντων κανόνων ασφάλειας για προϊόντα με ψηφιακά στοιχεία και θα μειώσει το κόστος συμμόρφωσης όσον αφορά τη σχετική νομοθεσία για την κυβερνοασφάλεια. Με τον τρόπο αυτόν, θα μειωθεί ο αριθμός των κυβερνοσυμβάντων, το κόστος διαχείρισης συμβάντων και η ζημία στη φήμη τους. Όσον αφορά ολόκληρη την ΕΕ, εκτιμάται ότι η πρωτοβουλία θα μπορούσε να οδηγήσει σε μείωση του κόστους από συμβάντα που πλήττουν τις επιχειρήσεις κατά περίπου 180 έως 290 δισ. EUR ετησίως. Θα οδηγήσει σε αύξηση του κύκλου εργασιών λόγω της χρήσης προϊόντων με ψηφιακά στοιχεία. Θα βελτιώσει την παγκόσμια φήμη των εταιρειών, με αποτέλεσμα την αύξηση της ζήτησης και εκτός της ΕΕ. Για τους χρήστες, η προτιμώμενη επιλογή θα ενισχύσει τη διαφάνεια των ιδιοτήτων ασφάλειας και θα διευκολύνει τη χρήση προϊόντων με ψηφιακά στοιχεία. Οι καταναλωτές και οι πολίτες θα ωφεληθούν επίσης από την καλύτερη προστασία των θεμελιωδών δικαιωμάτων τους, όπως η προστασία της ιδιωτικής ζωής και των δεδομένων.

Όταν τους ζητήθηκε να βαθμολογήσουν την αποτελεσματικότητα των παρεμβάσεων πολιτικής, οι συμμετέχοντες στη δημόσια διαβούλευση συμφώνησαν ότι η επιλογή 4 θα ήταν το αποτελεσματικότερο μέτρο (4,08 σε κλίμακα από το 1 έως το 5). Σε αυτούς περιλαμβάνονται οι οργανώσεις καταναλωτών (5,00), οι συμμετέχοντες που αυτοπροσδιορίζονται ως χρήστες (4,22), οι κοινοποιημένοι οργανισμοί (4,17), οι αρχές εποπτείας της αγοράς (5,00) και οι κατασκευαστές προϊόντων με ψηφιακά στοιχεία (3,85), συμπεριλαμβανομένων επιχειρήσεων μικρού και μεσαίου μεγέθους (4,05).

- **Καταλληλότητα και απλούστευση του κανονιστικού πλαισίου**

Η παρούσα πρόταση καθορίζει τις απαιτήσεις που θα ισχύουν για τους κατασκευαστές λογισμικού και υλισμικού. Είναι αναγκαίο να διασφαλιστεί η ασφάλεια δικαίου και να αποφευχθεί ο περαιτέρω κατακερματισμός της αγοράς όσον αφορά τις απαιτήσεις που ισχύουν για τα προϊόντα σχετικά με την κυβερνοασφάλεια στην εσωτερική αγορά, κάτι που έχει αποδειχθεί από την ευρεία υποστήριξη διαφόρων ενδιαφερόμενων μερών για μια οριζόντια παρέμβαση. Η πρόταση θα ελαχιστοποιήσει τον κανονιστικό φόρτο τον οποίο συνεπάγονται για τους κατασκευαστές οι διάφορες πράξεις για την ασφάλεια των προϊόντων. Η εναρμόνιση με το ΝΝΠ σημαίνει καλύτερη λειτουργία της παρέμβασης και της επιβολής της. Η πρόταση εξορθολογίζει τη διαδικασία των μεθόδων διασφάλισης, με τη συμμετοχή των κατασκευαστών και των κρατών μελών πριν από την κοινοποίηση προς την Επιτροπή. Πολλοί από τους κατασκευαστές που εμπίπτουν στο πεδίο εφαρμογής της πρότασης είναι ήδη εξοικειωμένοι με τις εργασίες του ΝΝΠ, γεγονός που θα συμβάλει στην κατανόηση και την εφαρμογή του. Όσον αφορά τους καταναλωτές και τις επιχειρήσεις, η πρόταση θα προωθήσει την εμπιστοσύνη στα προϊόντα με ψηφιακά στοιχεία.

- **Θεμελιώδη δικαιώματα**

Όλες οι επιλογές πολιτικής αναμένεται να ενισχύσουν σε ορισμένο βαθμό την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών, όπως η ιδιωτική ζωή, η προστασία των δεδομένων προσωπικού χαρακτήρα, η επιχειρηματική ελευθερία και η προστασία της ιδιοκτησίας ή της προσωπικής αξιοπρέπειας και ακεραιότητας. Ειδικότερα, η προτιμώμενη επιλογή πολιτικής 4, η οποία αποτελείται από οριζόντιες ρυθμιστικές παρεμβάσεις και ευρύ πλαίσιο πολιτικής, θα ήταν η πλέον αποτελεσματική από την άποψη αυτή, καθώς είναι πιθανότερο να συμβάλει στη μείωση του αριθμού και της σοβαρότητας των συμβάντων, συμπεριλαμβανομένων των παραβιάσεων δεδομένων προσωπικού χαρακτήρα. Θα αυξήσει επίσης την ασφάλεια δικαίου και θα εξασφαλίσει ισότιμους όρους ανταγωνισμού για τους οικονομικούς φορείς, θα αυξήσει την εμπιστοσύνη μεταξύ των χρηστών και την ελκυστικότητα των ενωσιακών προϊόντων με ψηφιακά στοιχεία στο σύνολό τους, προστατεύοντας έτσι την ιδιοκτησία και βελτιώνοντας τις συνθήκες άσκησης επιχειρηματικών δραστηριοτήτων από τους οικονομικούς φορείς.

Οι οριζόντιες απαιτήσεις κυβερνοασφάλειας θα συμβάλουν στην ασφάλεια των δεδομένων προσωπικού χαρακτήρα μέσω της προστασίας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών στα προϊόντα με ψηφιακά στοιχεία. Η συμμόρφωση με τις εν λόγω απαιτήσεις θα διευκολύνει τη συμμόρφωση με την απαίτηση ασφάλειας της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα βάσει του κανονισμού (ΕΕ) 2016/679 (Γενικός Κανονισμός για την Προστασία Δεδομένων — ΓΚΠΔ)[12]. Η πρόταση θα ενισχύσει τη διαφάνεια και την ενημέρωση των χρηστών, συμπεριλαμβανομένων εκείνων που ενδέχεται να διαθέτουν λιγότερες δεξιότητες στον τομέα της κυβερνοασφάλειας. Οι χρήστες θα είναι επίσης καλύτερα ενημερωμένοι σχετικά με τους κινδύνους, τις ικανότητες και τους περιορισμούς των προϊόντων με ψηφιακά στοιχεία, γεγονός που θα τους βοηθήσει περισσότερο να λάβουν τα αναγκαία μέτρα πρόληψης και άμβλυνσης για τον περιορισμό των υπολειπόμενων κινδύνων.

[12] 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).

## 4. ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ

Προκειμένου ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) να εκπληρώσει τα καθήκοντα που του ανατίθενται δυνάμει του παρόντος κανονισμού, θα πρέπει να ανακατανείμει πόρους της τάξης των περίπου 4,5 ΙΠΑ. Η Επιτροπή θα πρέπει να διαθέσει 7 ΙΠΑ για την εκπλήρωση των υποχρεώσεών της όσον αφορά την επιβολή δυνάμει του παρόντος κανονισμού.

*Λεπτομερής επισκόπηση του σχετικού κόστους παρέχεται στο «δημοσιονομικό δελτίο» που συνοδεύει την παρούσα πρόταση.*

## 5. ΛΟΙΠΑ ΣΤΟΙΧΕΙΑ

- **Σχέδια εφαρμογής και ρυθμίσεις παρακολούθησης, αξιολόγησης και υποβολής εκθέσεων**

Η Επιτροπή θα παρακολουθεί την υλοποίηση, την εφαρμογή και τη συμμόρφωση με τις νέες αυτές διατάξεις με σκοπό την αξιολόγηση της αποτελεσματικότητάς τους. Δυνάμει του κανονισμού, η Επιτροπή θα κληθεί να προβεί σε αξιολόγηση και επανεξέταση και να υποβάλει σχετική δημόσια έκθεση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο εντός 36 μηνών από την ημερομηνία εφαρμογής και στη συνέχεια ανά τετραετία.

- **Αναλυτική επεξήγηση των επιμέρους διατάξεων της πρότασης**

Γενικές διατάξεις (Κεφάλαιο Ι)

Ο παρών προτεινόμενος κανονισμός θεσπίζει α) κανόνες για τη διάθεση προϊόντων με ψηφιακά στοιχεία στην αγορά, ώστε να διασφαλίζεται η κυβερνοασφάλεια των εν λόγω προϊόντων· β) ουσιώδεις απαιτήσεις για τον σχεδιασμό, την ανάπτυξη και την παραγωγή προϊόντων με ψηφιακά στοιχεία και υποχρεώσεις για τους οικονομικούς φορείς σε σχέση με τα εν λόγω προϊόντα όσον αφορά την κυβερνοασφάλεια· γ) ουσιώδεις απαιτήσεις για τις διαδικασίες χειρισμού τρωτών σημείων που εφαρμόζουν οι κατασκευαστές με σκοπό τη διασφάλιση της κυβερνοασφάλειας προϊόντων με ψηφιακά στοιχεία καθ' όλη τη διάρκεια του κύκλου ζωής, καθώς και υποχρεώσεις για τους οικονομικούς φορείς σε σχέση με τις εν λόγω διαδικασίες· δ) κανόνες για την εποπτεία της αγοράς και την επιβολή των προαναφερθέντων κανόνων και απαιτήσεων.

Ο προτεινόμενος κανονισμός θα εφαρμόζεται σε όλα τα προϊόντα με ψηφιακά στοιχεία των οποίων η προβλεπόμενη και ευλόγως προβλέψιμη χρήση περιλαμβάνει άμεση ή έμμεση λογική ή φυσική σύνδεση δεδομένων με συσκευή ή δίκτυο.

Ο προτεινόμενος κανονισμός δεν θα εφαρμόζεται σε προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού (ΕΕ) 2017/745 [ιατροτεχνολογικά προϊόντα για ανθρώπινη χρήση και εξαρτήματα τέτοιων τεχνολογικών προϊόντων] και του κανονισμού (ΕΕ) 2017/746 [in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα για ανθρώπινη χρήση και εξαρτήματα τέτοιων τεχνολογικών προϊόντων], δεδομένου ότι και οι δύο κανονισμοί περιέχουν απαιτήσεις σχετικά με τα ιατροτεχνολογικά προϊόντα, μεταξύ άλλων σχετικά με το λογισμικό και τις γενικές υποχρεώσεις των κατασκευαστών, που καλύπτουν ολόκληρο τον κύκλο ζωής των προϊόντων, καθώς και τις διαδικασίες αξιολόγησης της συμμόρφωσης. Ο παρών κανονισμός δεν θα εφαρμόζεται σε προϊόντα με ψηφιακά στοιχεία που έχουν πιστοποιηθεί σύμφωνα με τον κανονισμό 2018/1139 [υψηλό ομοιόμορφο επίπεδο ασφάλειας της πολιτικής αεροπορίας], ούτε σε προϊόντα στα οποία εφαρμόζεται ο κανονισμός (ΕΕ) 2019/2144 [για τις απαιτήσεις έγκρισης τύπου των μηχανοκίνητων οχημάτων και των

ρυμουλκουμένων τους και των συστημάτων, κατασκευαστικών στοιχείων και χωριστών τεχνικών μονάδων που προορίζονται για τα οχήματα αυτά].

Τα κρίσιμα προϊόντα με ψηφιακά στοιχεία υπόκεινται σε ειδικές διαδικασίες αξιολόγησης της συμμόρφωσης και υποδιαιρούνται στην κατηγορία Ι και την κατηγορία ΙΙ, όπως ορίζεται στο παράρτημα ΙΙΙ, όπου αντικατοπτρίζεται το επίπεδο κινδύνου για την κυβερνοασφάλεια, με την κατηγορία ΙΙ να αντιπροσωπεύει μεγαλύτερο κίνδυνο. Ένα προϊόν με ψηφιακά στοιχεία θεωρείται κρίσιμο και, ως εκ τούτου, περιλαμβάνεται στο παράρτημα ΙΙΙ, δεδομένου ότι λαμβάνονται υπόψη οι επιπτώσεις των δυνητικών τρωτών σημείων που περιλαμβάνονται στο προϊόν με ψηφιακά στοιχεία όσον αφορά την κυβερνοασφάλεια. Κατά τον προσδιορισμό του κινδύνου για την κυβερνοασφάλεια λαμβάνονται, μεταξύ άλλων, υπόψη η λειτουργικότητα του προϊόντος με ψηφιακά στοιχεία όσον αφορά την κυβερνοασφάλεια, καθώς και η προβλεπόμενη χρήση σε ευαίσθητα περιβάλλοντα, όπως ένα βιομηχανικό περιβάλλον.

Ανατίθεται επίσης στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις για τη συμπλήρωση του παρόντος κανονισμού με τον προσδιορισμό κατηγοριών εξαιρετικά κρίσιμων προϊόντων με ψηφιακά στοιχεία για τα οποία οι κατασκευαστές υποχρεούνται να λάβουν ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας στο πλαίσιο ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας για να αποδείξουν τη συμμόρφωση με τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα Ι, ή μέρη αυτών. Κατά τον καθορισμό των εν λόγω κατηγοριών εξαιρετικά κρίσιμων προϊόντων με ψηφιακά στοιχεία, η Επιτροπή λαμβάνει υπόψη το επίπεδο κινδύνου κυβερνοασφάλειας που σχετίζεται με την κατηγορία προϊόντων με ψηφιακά στοιχεία, υπό το πρίσμα ενός ή περισσότερων από τα κριτήρια που λαμβάνονται υπόψη για την καταχώριση κρίσιμων προϊόντων με ψηφιακά στοιχεία στο παράρτημα ΙΙΙ, καθώς και ενόψει της αξιολόγησης του αν η εν λόγω κατηγορία προϊόντων χρησιμοποιείται από βασικές οντότητες του τύπου που αναφέρεται στο παράρτημα [παράρτημα Ι] της οδηγίας [οδηγία XXX/XXXX (NIS2)] ή στην οποία οι εν λόγω οντότητες βασίζονται, ή η οποία θα έχει δυνητική μελλοντική σημασία για τις δραστηριότητες των εν λόγω οντοτήτων· ή αφορά την ανθεκτικότητα της συνολικής αλυσίδας εφοδιασμού προϊόντων με ψηφιακά στοιχεία έναντι συμβάντων που προκαλούν διαταραχές.

Υποχρεώσεις των οικονομικών φορέων (Κεφάλαιο ΙΙ)

Η πρόταση περιλαμβάνει υποχρεώσεις για τους κατασκευαστές, τους εισαγωγείς και τους διανομείς με βάση τις διατάξεις αναφοράς που προβλέπονται στην απόφαση 768/2008/ΕΚ. Οι ουσιώδεις απαιτήσεις και υποχρεώσεις κυβερνοασφάλειας ορίζουν ότι όλα τα προϊόντα με ψηφιακά στοιχεία καθίστανται διαθέσιμα στην αγορά μόνον εάν, εφόσον παρέχονται δεόντως, εγκαθίστανται, συντηρούνται και χρησιμοποιούνται ορθά για τον προβλεπόμενο σκοπό ή υπό εύλογα προβλέψιμες συνθήκες, πληρούν τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό.

Οι ουσιώδεις απαιτήσεις και υποχρεώσεις θα υποχρεώνουν τους κατασκευαστές να λαμβάνουν υπόψη την κυβερνοασφάλεια στον σχεδιασμό, την ανάπτυξη και την παραγωγή των προϊόντων με ψηφιακά στοιχεία, να επιδεικνύουν δέουσα επιμέλεια όσον αφορά τις πτυχές ασφάλειας κατά τον σχεδιασμό και την ανάπτυξη των προϊόντων τους, να λειτουργούν με διαφάνεια όσον αφορά τις πτυχές κυβερνοασφάλειας που πρέπει να γνωστοποιούνται στους πελάτες, να διασφαλίζουν την υποστήριξη της ασφάλειας (ενημερώσεις) με αναλογικό τρόπο και να συμμορφώνονται με τις απαιτήσεις διαχείρισης τρωτών σημείων.

Θα καθοριστούν υποχρεώσεις για τους οικονομικούς φορείς, αρχής γενομένης από τους κατασκευαστές, έως τους διανομείς και τους εισαγωγείς, σε σχέση με τη διάθεση προϊόντων με ψηφιακά στοιχεία στην αγορά, οι οποίες θα είναι κατάλληλες για τον ρόλο και τις ευθύνες τους στην αλυσίδα εφοδιασμού.

Συμμόρφωση του προϊόντος με ψηφιακά στοιχεία (Κεφάλαιο III)

Το προϊόν με ψηφιακά στοιχεία το οποίο πληροί εναρμονισμένα πρότυπα ή μέρη εναρμονισμένων προτύπων τα στοιχεία αναφοράς των οποίων έχουν δημοσιευτεί στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, τεκμαίρεται ότι συμμορφώνεται προς τις ουσιώδεις απαιτήσεις του παρόντος προτεινόμενου κανονισμού. Όταν δεν υπάρχουν εναρμονισμένα πρότυπα ή αυτά είναι ανεπαρκή ή όταν υπάρχουν αδικαιολόγητες καθυστερήσεις στη διαδικασία τυποποίησης ή όταν το αίτημα της Επιτροπής δεν έχει γίνει δεκτό από τους ευρωπαϊκούς οργανισμούς τυποποίησης, η Επιτροπή μπορεί, μέσω εκτελεστικών πράξεων, να θεσπίσει κοινές προδιαγραφές.

Επιπλέον, τα προϊόντα με ψηφιακά στοιχεία που έχουν πιστοποιηθεί ή για τα οποία έχει εκδοθεί δήλωση συμμόρφωσης ΕΕ ή πιστοποιητικό στο πλαίσιο ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας σύμφωνα με τον κανονισμό (ΕΕ) 2019/881, και για τα οποία η Επιτροπή διευκρίνισε μέσω εκτελεστικής πράξης ότι μπορεί να παράσχει τεκμήριο συμμόρφωσης για τον παρόντα κανονισμό, τεκμαίρεται ότι συμμορφώνονται προς τις ουσιώδεις απαιτήσεις του παρόντος κανονισμού, ή μέρη αυτών, εφόσον η δήλωση συμμόρφωσης ΕΕ ή το πιστοποιητικό κυβερνοασφάλειας, ή μέρη αυτών, καλύπτουν τις εν λόγω απαιτήσεις.

Επιπλέον, προκειμένου να αποφευχθεί ο περιττός διοικητικός φόρτος για τους κατασκευαστές, κατά περίπτωση, η Επιτροπή θα πρέπει να διευκρινίζει αν ένα πιστοποιητικό κυβερνοασφάλειας που εκδίδεται στο πλαίσιο ενός τέτοιου ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας καταργεί την υποχρέωση των κατασκευαστών να διενεργούν αξιολόγηση της συμμόρφωσης από τρίτους, όπως προβλέπεται στον παρόντα κανονισμό για τις αντίστοιχες απαιτήσεις.

Ο κατασκευαστής διενεργεί αξιολόγηση της συμμόρφωσης του προϊόντος με ψηφιακά στοιχεία και των διαδικασιών χειρισμού τρωτών σημείων που εφαρμόζει για να αποδείξει τη συμμόρφωση με τις ουσιώδεις απαιτήσεις που καθορίζονται στο παράρτημα I ακολουθώντας μία από τις διαδικασίες που καθορίζονται στο παράρτημα VI. Οι κατασκευαστές κρίσιμων προϊόντων των κατηγοριών I και II χρησιμοποιούν τις αντίστοιχες ενότητες που απαιτούνται για τη συμμόρφωση. Οι κατασκευαστές κρίσιμων προϊόντων της κατηγορίας II πρέπει να εμπλέκουν τρίτο μέρος στην αξιολόγηση της συμμόρφωσής τους.

Κοινοποίηση των οργανισμών αξιολόγησης της συμμόρφωσης (Κεφάλαιο IV)

Η ορθή λειτουργία των κοινοποιημένων οργανισμών είναι καίριας σημασίας για τη διασφάλιση υψηλού επιπέδου προστασίας της κυβερνοασφάλειας και για την εμπιστοσύνη όλων των ενδιαφερομένων μερών στο σύστημα νέας προσέγγισης. Ως εκ τούτου, σύμφωνα με την απόφαση 768/2008/ΕΚ, η πρόταση ορίζει απαιτήσεις για τις εθνικές αρχές που είναι αρμόδιες για τους οργανισμούς αξιολόγησης της συμμόρφωσης (κοινοποιημένοι οργανισμοί). Αφήνει την τελική ευθύνη για τον καθορισμό και την παρακολούθηση των κοινοποιημένων οργανισμών στα κράτη μέλη. Τα κράτη μέλη ορίζουν κοινοποιούσα αρχή η οποία είναι υπεύθυνη για τον καθορισμό και τη διεξαγωγή των αναγκαίων διαδικασιών αξιολόγησης και κοινοποίησης των οργανισμών αξιολόγησης της συμμόρφωσης και για την παρακολούθηση των κοινοποιημένων οργανισμών.

Εποπτεία της αγοράς και επιβολή (Κεφάλαιο V)

Σύμφωνα με τον κανονισμό (ΕΕ) 2019/1020, οι εθνικές αρχές εποπτείας της αγοράς διενεργούν εποπτεία της αγοράς στην επικράτεια του εν λόγω κράτους μέλους. Τα κράτη μέλη μπορούν να επιλέξουν να ορίσουν οποιαδήποτε υφιστάμενη ή νέα αρχή που θα ενεργεί ως αρχή εποπτείας της αγοράς, συμπεριλαμβανομένων των εθνικών αρμόδιων αρχών που ορίζονται στο άρθρο [άρθρο X] της οδηγίας [οδηγία XXX/XXXX (NIS2)] ή των

εντεταλμένων εθνικών αρχών πιστοποίησης της κυβερνοασφάλειας που αναφέρονται στο άρθρο 58 του κανονισμού (ΕΕ) 2019/881. Οι οικονομικοί φορείς καλούνται να συνεργαστούν πλήρως με τις αρχές εποπτείας της αγοράς και άλλες αρμόδιες αρχές.

Αρμοδιότητες κατ' εξουσιοδότηση και διαδικασίες επιτροπής (Κεφάλαιο VI)

Προκειμένου να διασφαλιστεί ότι το κανονιστικό πλαίσιο μπορεί να προσαρμοστεί όπου απαιτείται, ανατίθεται στην Επιτροπή η εξουσία έκδοσης πράξεων σύμφωνα με το άρθρο 290 ΣΛΕΕ για την επικαιροποίηση του καταλόγου των κρίσιμων προϊόντων των κατηγοριών I και II και για τον προσδιορισμό των ορισμών των εν λόγω προϊόντων· προσδιορισμός του αν απαιτείται περιορισμός ή αποκλεισμός για προϊόντα με ψηφιακά στοιχεία που καλύπτονται από άλλους ενωσιακούς κανόνες που καθορίζουν απαιτήσεις που επιτυγχάνουν το ίδιο επίπεδο προστασίας με τον παρόντα κανονισμό· την επιβολή της πιστοποίησης ορισμένων εξαιρετικά κρίσιμων προϊόντων με ψηφιακά στοιχεία βάσει των κριτηρίων που καθορίζονται στον παρόντα κανονισμό· τον προσδιορισμό του ελάχιστου περιεχομένου της δήλωσης συμμόρφωσης ΕΕ και τη συμπλήρωση των στοιχείων που πρέπει να περιλαμβάνονται στον τεχνικό φάκελο.

Ανατίθεται επίσης στην Επιτροπή η αρμοδιότητα έκδοσης εκτελεστικών πράξεων για τους εξής σκοπούς: τον προσδιορισμό του μορφοτύπου ή των στοιχείων των υποχρεώσεων υποβολής εκθέσεων και του καταλόγου υλικών του λογισμικού· τον προσδιορισμό των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας που μπορούν να χρησιμοποιηθούν για την απόδειξη της συμμόρφωσης προς τις ουσιώδεις απαιτήσεις ή μέρη αυτών, όπως ορίζονται στον παρόντα κανονισμό· τη θέσπιση κοινών προδιαγραφών· τον καθορισμό τεχνικών προδιαγραφών για την τοποθέτηση της σήμανσης CE· τη θέσπιση διορθωτικών ή περιοριστικών μέτρων σε επίπεδο Ένωσης σε εξαιρετικές περιστάσεις που δικαιολογούν άμεση παρέμβαση για τη διατήρηση της εύρυθμης λειτουργίας της εσωτερικής αγοράς.

Εμπιστευτικότητα και κυρώσεις (Κεφάλαιο VII)

Όλα τα μέρη που εφαρμόζουν τον παρόντα κανονισμό τηρούν την εμπιστευτικότητα των πληροφοριών και των δεδομένων που λαμβάνουν κατά την εκτέλεση των καθηκόντων και των δραστηριοτήτων τους.

Προκειμένου να διασφαλιστεί η αποτελεσματική επιβολή των υποχρεώσεων που ορίζονται στον παρόντα κανονισμό, κάθε αρχή εποπτείας της αγοράς θα πρέπει να έχει την εξουσία να επιβάλλει ή να ζητεί την επιβολή διοικητικών προστίμων. Στο ίδιο πνεύμα, ο παρών κανονισμός καθορίζει ανώτατα επίπεδα διοικητικών προστίμων που θα πρέπει να προβλέπονται στην εθνική νομοθεσία σε περίπτωση μη συμμόρφωσης με τις υποχρεώσεις που ορίζονται στον παρόντα κανονισμό.

Μεταβατικές και τελικές διατάξεις (Κεφάλαιο VIII)

Για να δοθεί στους κατασκευαστές, τους κοινοποιημένους οργανισμούς και τα κράτη μέλη η δυνατότητα να προσαρμοστούν στις νέες απαιτήσεις, ο προτεινόμενος κανονισμός θα τεθεί σε εφαρμογή [24 μήνες] μετά την έναρξη ισχύος του, με εξαίρεση την υποχρέωση υποβολής εκθέσεων από τους κατασκευαστές, η οποία θα εφαρμοστεί από [12 μήνες] μετά την ημερομηνία έναρξης ισχύος.

2022/0272 (COD)

Πρόταση

# ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

## σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και με την τροποποίηση του κανονισμού (ΕΕ) 2019/1020

(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 τις προτάσεις της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής[1],

Έχοντας υπόψη τη γνώμη της Επιτροπής των Περιφερειών[2],

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία,

Εκτιμώντας τα ακόλουθα:

(1) Είναι αναγκαίο να βελτιωθεί η λειτουργία της εσωτερικής αγοράς με τη θέσπιση ενιαίου νομικού πλαισίου για τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας για τη διάθεση προϊόντων με ψηφιακά στοιχεία στην αγορά της Ένωσης. Πρέπει να αντιμετωπιστούν δύο σημαντικά προβλήματα που αυξάνουν το κόστος για τους χρήστες και την κοινωνία: αφενός, το χαμηλό επίπεδο κυβερνοασφάλειας των προϊόντων με ψηφιακά στοιχεία, το οποίο αντικατοπτρίζεται από τα εκτεταμένα τρωτά σημεία και την ελλιπή και ασυνεπή παροχή ενημερώσεων ασφάλειας για την αντιμετώπισή τους, και αφετέρου, η ελλιπής κατανόηση και πρόσβαση των χρηστών σε πληροφορίες, γεγονός που τους εμποδίζει να επιλέγουν προϊόντα με επαρκείς ιδιότητες κυβερνοασφάλειας ή να τα χρησιμοποιούν με ασφαλή τρόπο.

(2) Ο παρών κανονισμός αποσκοπεί στον καθορισμός των οριακών συνθηκών για την ανάπτυξη ασφαλών προϊόντων με ψηφιακά στοιχεία διασφαλίζοντας ότι στην αγορά διατίθενται προϊόντα υλισμικού και λογισμικού με λιγότερα τρωτά σημεία και ότι οι κατασκευαστές λαμβάνουν σοβαρά υπόψη το ζήτημα της ασφάλειας καθ' όλη τη διάρκεια του κύκλου ζωής των προϊόντων. Αποσκοπεί επίσης στη δημιουργία συνθηκών που επιτρέπουν στους χρήστες να λαμβάνουν υπόψη την κυβερνοασφάλεια κατά την επιλογή και τη χρήση προϊόντων με ψηφιακά στοιχεία.

(3) Η σχετική ενωσιακή νομοθεσία που ισχύει επί του παρόντος περιλαμβάνει διάφορα σύνολα οριζόντιων κανόνων που καλύπτουν ορισμένες πτυχές που συνδέονται με την

[1] ΕΕ C της , σ. .
[2] ΕΕ C της , σ. .

κυβερνοασφάλεια από διαφορετικές οπτικές γωνίες, συμπεριλαμβανομένων μέτρων για τη βελτίωση της ασφάλειας της ψηφιακής αλυσίδας εφοδιασμού. Ωστόσο, η υφιστάμενη ενωσιακή νομοθεσία σχετικά με την κυβερνοασφάλεια, συμπεριλαμβανομένων της [οδηγίας XXX/XXXX (NIS2)] και του κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[3] δεν καλύπτει άμεσα τις υποχρεωτικές απαιτήσεις για την ασφάλεια των προϊόντων με ψηφιακά στοιχεία.

(4) Ενώ η υφιστάμενη νομοθεσία της Ένωσης εφαρμόζεται σε ορισμένα προϊόντα με ψηφιακά στοιχεία, δεν υπάρχει οριζόντιο κανονιστικό πλαίσιο της Ένωσης που να θεσπίζει ολοκληρωμένες απαιτήσεις κυβερνοασφάλειας για όλα τα προϊόντα με ψηφιακά στοιχεία. Οι διάφορες πράξεις και πρωτοβουλίες που έχουν δρομολογηθεί μέχρι στιγμής σε ενωσιακό και εθνικό επίπεδο αντιμετωπίζουν εν μέρει μόνο τα προβλήματα και τους κινδύνους που εντοπίζονται όσον αφορά την κυβερνοασφάλεια, με αποτέλεσμα να δημιουργείται ένα νομοθετικό συνονθύλευμα εντός της εσωτερικής αγοράς, να αυξάνεται η ανασφάλεια δικαίου τόσο για τους κατασκευαστές όσο και για τους χρήστες των εν λόγω προϊόντων και να προστίθεται περιττός φόρτος για τις εταιρείες όσον αφορά τη συμμόρφωσή τους με σειρά απαιτήσεων για παρόμοιους τύπους προϊόντων. Η κυβερνοασφάλεια των εν λόγω προϊόντων έχει ιδιαίτερα ισχυρή διασυνοριακή διάσταση, καθώς τα προϊόντα που κατασκευάζονται σε μία χώρα συχνά χρησιμοποιούνται από οργανισμούς και καταναλωτές σε ολόκληρη την εσωτερική αγορά. Για τον λόγο αυτόν, καθίσταται αναγκαία η κανονιστική ρύθμιση του τομέα σε επίπεδο Ένωσης. Το κανονιστικό τοπίο της Ένωσης θα πρέπει να εναρμονιστεί, με τη θέσπιση απαιτήσεων κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία. Επιπλέον, θα πρέπει να διασφαλιστεί βεβαιότητα για τους φορείς εκμετάλλευσης και τους χρήστες σε ολόκληρη την Ένωση, καθώς και καλύτερη εναρμόνιση της ενιαίας αγοράς, ώστε να δημιουργηθούν πιο βιώσιμες συνθήκες για τους φορείς εκμετάλλευσης που επιδιώκουν να εισέλθουν στην αγορά της Ένωσης.

(5) Σε επίπεδο Ένωσης, στο πλαίσιο διαφόρων προγραμματικών και πολιτικών εγγράφων, όπως η στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία[4], τα συμπεράσματα του Συμβουλίου της 2ας Δεκεμβρίου 2020 και της 23ης Μαΐου 2022 ή το ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 10ης Ιουνίου 2021[5], έχει ζητηθεί η θέσπιση ειδικών ενωσιακών απαιτήσεων κυβερνοασφάλειας για ψηφιακά ή συνδεδεμένα προϊόντα, ενώ αρκετές χώρες ανά τον κόσμο θεσπίζουν μέτρα για την αντιμετώπιση του ζητήματος αυτού με δική τους πρωτοβουλία. Στην τελική έκθεση της Διάσκεψης για το μέλλον της Ευρώπης[6], οι πολίτες ζήτησαν «ενίσχυση του ρόλου της ΕΕ στην αντιμετώπιση των κυβερνοαπειλών».

(6) Για να αυξηθεί το συνολικό επίπεδο κυβερνοασφάλειας όλων των προϊόντων με ψηφιακά στοιχεία που διατίθενται στην εσωτερική αγορά, είναι αναγκαίο να

---

3 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).

4 JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=JOIN:2020:18:FIN.

5 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EL.html.

6 *Διάσκεψη για το μέλλον της Ευρώπης, Έκθεση επί του τελικού αποτελέσματος*, Μάιος 2022, πρόταση 28 σημείο 2. Η διάσκεψη πραγματοποιήθηκε από τον Απρίλιο του 2021 έως τον Μάιο του 2022. Ήταν μια μοναδική άσκηση της διαβουλευτικής δημοκρατίας με πρωτοβουλία των πολιτών σε πανευρωπαϊκό επίπεδο, με τη συμμετοχή χιλιάδων Ευρωπαίων πολιτών, καθώς και πολιτικών παραγόντων, κοινωνικών εταίρων, εκπροσώπων της κοινωνίας των πολιτών και βασικών ενδιαφερόμενων φορέων.

θεσπιστούν προσανατολισμένες σε στόχους και τεχνολογικά ουδέτερες ουσιώδεις απαιτήσεις κυβερνοασφάλειας για τα εν λόγω προϊόντα, οι οποίες θα εφαρμόζονται οριζόντια.

(7) Υπό ορισμένες προϋποθέσεις, όλα τα προϊόντα με ψηφιακά στοιχεία που είναι ενσωματωμένα σε ευρύτερο ηλεκτρονικό σύστημα πληροφοριών ή συνδεδεμένα με αυτό μπορούν να χρησιμεύσουν ως φορέας επίθεσης από κακόβουλους παράγοντες. Ως εκ τούτου, ακόμη και το υλισμικό και το λογισμικό που θεωρούνται λιγότερο κρίσιμα μπορούν να διευκολύνουν την αρχική διατάραξη της λειτουργίας μιας συσκευής ή ενός δικτύου, επιτρέποντας στους κακόβουλους παράγοντες να αποκτήσουν προνομιακή πρόσβαση σε ένα σύστημα ή να μετακινηθούν πλαγίως μεταξύ των συστημάτων. Ως εκ τούτου, οι κατασκευαστές θα πρέπει να διασφαλίζουν ότι όλα τα συνδέσιμα προϊόντα με ψηφιακά στοιχεία σχεδιάζονται και αναπτύσσονται σύμφωνα με τις ουσιώδεις απαιτήσεις που ορίζονται στον παρόντα κανονισμό. Μεταξύ αυτών περιλαμβάνονται τόσο προϊόντα που μπορούν να συνδεθούν υλικά μέσω διεπαφών υλισμικού όσο και προϊόντα που συνδέονται λογικά, όπως μέσω υποδοχών δικτύου, σωλήνων, αρχείων, διεπαφών προγραμματισμού εφαρμογών ή οποιουδήποτε άλλου είδους διεπαφής λογισμικού. Δεδομένου ότι οι απειλές για την κυβερνοασφάλεια μπορούν να διαδοθούν μέσω διαφόρων προϊόντων με ψηφιακά στοιχεία πριν από την επίτευξη συγκεκριμένου στόχου, για παράδειγμα με την αλυσιδωτή προσέγγιση εκμετάλλευσης πολλαπλών τρωτών σημείων, οι κατασκευαστές θα πρέπει επίσης να διασφαλίζουν την κυβερνοασφάλεια των προϊόντων που συνδέονται μόνο έμμεσα με άλλες συσκευές ή δίκτυα.

(8) Με τον καθορισμό απαιτήσεων κυβερνοασφάλειας για τη διάθεση προϊόντων με ψηφιακά στοιχεία στην αγορά, θα ενισχυθεί η κυβερνοασφάλεια των εν λόγω προϊόντων τόσο για τους καταναλωτές όσο και για τις επιχειρήσεις. Μεταξύ αυτών περιλαμβάνονται επίσης απαιτήσεις για την κυκλοφορία καταναλωτικών προϊόντων με ψηφιακά στοιχεία που προορίζονται για ευάλωτους καταναλωτές, όπως παιχνίδια και συσκευές ενδοεπικοινωνίας για βρέφη.

(9) Ο παρών κανονισμός διασφαλίζει υψηλό επίπεδο κυβερνοασφάλειας προϊόντων με ψηφιακά στοιχεία. Δεν ρυθμίζει υπηρεσίες, όπως το λογισμικό ως υπηρεσία (SaaS), εκτός από τις λύσεις εξ αποστάσεως επεξεργασίας δεδομένων που αφορούν προϊόν με ψηφιακά στοιχεία, οι οποίες νοούνται ως κάθε εξ αποστάσεως επεξεργασία δεδομένων για την οποία το λογισμικό έχει σχεδιαστεί και αναπτυχθεί από τον κατασκευαστή του οικείου προϊόντος ή υπό την ευθύνη του εν λόγω κατασκευαστή, και η απουσία των οποίων θα εμπόδιζε ένα τέτοιο προϊόν με ψηφιακά στοιχεία να εκτελέσει κάποια από τις λειτουργίες του. Η [οδηγία XXX/XXXX (NIS2)] θεσπίζει απαιτήσεις κυβερνοασφάλειας και αναφοράς συμβάντων για βασικές και σημαντικές οντότητες, όπως οι υποδομές ζωτικής σημασίας, με σκοπό την ενίσχυση της ανθεκτικότητας των υπηρεσιών τις οποίες παρέχουν. Η [οδηγία XXX/XXXX (NIS2)] εφαρμόζεται στις υπηρεσίες υπολογιστικού νέφους και στα μοντέλα υπηρεσιών υπολογιστικού νέφους, όπως το SaaS. Όλες οι οντότητες που παρέχουν υπηρεσίες υπολογιστικού νέφους στην Ένωση και οι οποίες πληρούν ή υπερβαίνουν το κατώτατο όριο για τις μεσαίες επιχειρήσεις εμπίπτουν στο πεδίο εφαρμογής της εν λόγω οδηγίας.

(10) Προκειμένου να μην παρεμποδιστεί η καινοτομία ή η έρευνα, το δωρεάν λογισμικό ανοικτού κώδικα που αναπτύσσεται ή παρέχεται εκτός του πλαισίου εμπορικής δραστηριότητας δεν θα πρέπει να καλύπτεται από τον παρόντα κανονισμό. Αυτό ισχύει ιδίως για το λογισμικό, συμπεριλαμβανομένων του πηγαίου κώδικα και των τροποποιημένων εκδόσεών του, το οποίο κοινοποιείται σε όλους και είναι δυνατή η

ελεύθερη πρόσβαση, χρήση, τροποποίηση και αναδιανομή του. Στο πλαίσιο του λογισμικού, μια δραστηριότητα θα μπορούσε να χαρακτηριστεί εμπορική όχι μόνο από τη χρέωση ενός προϊόντος, αλλά και από τη χρέωση των υπηρεσιών τεχνικής υποστήριξης, από την παροχή πλατφόρμας λογισμικού μέσω της οποίας ο κατασκευαστής παρέχει άλλες υπηρεσίες έναντι χρηματικού αντιτίμου, ή από τη χρήση δεδομένων προσωπικού χαρακτήρα για άλλους λόγους, και όχι αποκλειστικά για τη βελτίωση της ασφάλειας, της συμβατότητας ή της διαλειτουργικότητας του λογισμικού.

(11) Το ασφαλές διαδίκτυο είναι απαραίτητο για τη λειτουργία των υποδομών ζωτικής σημασίας και για την κοινωνία στο σύνολό της. Η [οδηγία XXX/XXXX (NIS2)] αποσκοπεί στη διασφάλιση υψηλού επιπέδου κυβερνοασφάλειας των υπηρεσιών που παρέχονται από βασικές και σημαντικές οντότητες, συμπεριλαμβανομένων των παρόχων ψηφιακών υποδομών που υποστηρίζουν βασικές λειτουργίες του ανοικτού διαδικτύου, διασφαλίζουν την πρόσβαση στο διαδίκτυο και τις υπηρεσίες διαδικτύου. Ως εκ τούτου, είναι σημαντικό τα προϊόντα με ψηφιακά στοιχεία που είναι απαραίτητα ώστε οι πάροχοι ψηφιακών υποδομών να μπορούν να διασφαλίσουν τη λειτουργία του διαδικτύου να αναπτύσσονται με ασφαλή τρόπο και να συμμορφώνονται με τα καθιερωμένα πρότυπα ασφάλειας του διαδικτύου. Ο παρών κανονισμός, ο οποίος εφαρμόζεται σε όλα τα συνδέσιμα προϊόντα υλισμικού και λογισμικού, αποσκοπεί επίσης στη διευκόλυνση της συμμόρφωσης των παρόχων ψηφιακών υποδομών με τις απαιτήσεις της [οδηγίας XXX/XXXX (NIS2)] για την αλυσίδα εφοδιασμού, διασφαλίζοντας ότι τα προϊόντα με ψηφιακά στοιχεία που χρησιμοποιούν για την παροχή των υπηρεσιών τους αναπτύσσονται με ασφαλή τρόπο και ότι έχουν πρόσβαση σε έγκαιρες ενημερώσεις ασφαλείας για τα εν λόγω προϊόντα.

(12) Ο κανονισμός (ΕΕ) 2017/745 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[7] θεσπίζει κανόνες σχετικά με τα ιατροτεχνολογικά προϊόντα και ο κανονισμός (ΕΕ) 2017/746 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[8] θεσπίζει κανόνες σχετικά με τα in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα. Και οι δύο κανονισμοί αντιμετωπίζουν τους κινδύνους για την κυβερνοασφάλεια και ακολουθούν συγκεκριμένες προσεγγίσεις που επίσης εξετάζονται στον παρόντα κανονισμό. Ειδικότερα, οι κανονισμοί (ΕΕ) 2017/745 και (ΕΕ) 2017/746 καθορίζουν τις ουσιώδεις απαιτήσεις για τα ιατροτεχνολογικά προϊόντα που λειτουργούν μέσω ηλεκτρονικού συστήματος ή αποτελούν τα ίδια λογισμικό. Οι εν λόγω κανονισμοί καλύπτουν επίσης ορισμένα μη ενσωματωμένα λογισμικά και την προσέγγιση που συνδέεται με τον κύκλο ζωής του προϊόντος. Οι απαιτήσεις αυτές υποχρεώνουν τους κατασκευαστές να αναπτύσσουν και να κατασκευάζουν τα προϊόντα τους εφαρμόζοντας αρχές διαχείρισης κινδύνου και καθορίζοντας απαιτήσεις σχετικά με τα μέτρα ασφάλειας ΤΠ, καθώς και τις αντίστοιχες διαδικασίες αξιολόγησης της συμμόρφωσης. Επιπλέον, από τον Δεκέμβριο του 2019 έχουν θεσπιστεί ειδικές κατευθυντήριες γραμμές σχετικά με την κυβερνοασφάλεια για τα ιατροτεχνολογικά προϊόντα, οι οποίες παρέχουν στους κατασκευαστές ιατροτεχνολογικών προϊόντων, συμπεριλαμβανομένων των in vitro διαγνωστικών ιατροτεχνολογικών προϊόντων,

---

[7] 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).

[8] 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).

καθοδήγηση σχετικά με τον τρόπο εκπλήρωσης όλων των σχετικών ουσιωδών απαιτήσεων του παραρτήματος I των εν λόγω κανονισμών όσον αφορά την κυβερνοασφάλεια[9]. Ως εκ τούτου, τα προϊόντα με ψηφιακά στοιχεία στα οποία εφαρμόζεται οποιοσδήποτε από τους εν λόγω κανονισμούς δεν θα πρέπει να εμπίπτουν στον παρόντα κανονισμό.

(13) Ο κανονισμός (ΕΕ) 2019/2144 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[10] θεσπίζει απαιτήσεις για την έγκριση τύπου οχημάτων, καθώς και των συστημάτων και των κατασκευαστικών στοιχείων τους, θεσπίζει ορισμένες απαιτήσεις κυβερνοασφάλειας, μεταξύ άλλων σχετικά με τη λειτουργία πιστοποιημένου συστήματος διαχείρισης της κυβερνοασφάλειας, τις ενημερώσεις λογισμικού, καλύπτει τις πολιτικές και τις διαδικασίες των οργανισμών για τους κυβερνοκινδύνους που σχετίζονται με ολόκληρο τον κύκλο ζωής των οχημάτων, του εξοπλισμού και των υπηρεσιών σύμφωνα με τους ισχύοντες κανονισμούς των Ηνωμένων Εθνών για τις τεχνικές προδιαγραφές και την κυβερνοασφάλεια[11], και προβλέπει ειδικές διαδικασίες αξιολόγησης της συμμόρφωσης. Στον τομέα των αερομεταφορών, ο κύριος στόχος του κανονισμού (ΕΕ) 2018/1139 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[12] είναι η εγκαθίδρυση και διατήρηση υψηλού και ομοιόμορφου επιπέδου ασφαλείας της πολιτικής αεροπορίας στην Ένωση. Δημιουργεί ένα πλαίσιο για τις ουσιώδεις απαιτήσεις όσον αφορά την αξιοπλοΐα αεροναυτικών προϊόντων, εξαρτημάτων, εξοπλισμού, συμπεριλαμβανομένου του λογισμικού, που λαμβάνουν υπόψη τις υποχρεώσεις προστασίας από απειλές κατά της ασφάλειας των πληροφοριών. Ως εκ τούτου, τα προϊόντα με ψηφιακά στοιχεία στα οποία εφαρμόζεται ο κανονισμός (ΕΕ) 2019/2144 και τα προϊόντα που έχουν πιστοποιηθεί σύμφωνα με τον κανονισμό (ΕΕ) 2018/1139 δεν υπόκεινται στις ουσιώδεις απαιτήσεις και τις διαδικασίες αξιολόγησης της συμμόρφωσης που καθορίζονται στον παρόντα κανονισμό. Η διαδικασία πιστοποίησης βάσει του κανονισμού (ΕΕ) 2018/1139 διασφαλίζει το επίπεδο ασφάλειας που επιδιώκει ο παρών κανονισμός.

---

9 MDCG 2019-16, έγγραφο που εγκρίθηκε από το Συντονιστικό Όργανο Ιατροτεχνολογικών Προϊόντων (ΣΟΙΠ), το οποίο συστάθηκε με το άρθρο 103 του κανονισμού (ΕΕ) 2017/745.

10 Κανονισμός (ΕΕ) 2019/2144 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Νοεμβρίου 2019, για τις απαιτήσεις έγκρισης τύπου των μηχανοκίνητων οχημάτων και των ρυμουλκουμένων τους και των συστημάτων, κατασκευαστικών στοιχείων και χωριστών τεχνικών μονάδων που προορίζονται για τα οχήματα αυτά όσον αφορά τη γενική τους ασφάλεια και την προστασία των επιβατών των οχημάτων και του ευάλωτου χρήστη της οδού, για την τροποποίηση του κανονισμού (ΕΕ) 2018/858 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και την κατάργηση των κανονισμών (ΕΚ) αριθ. 78/2009, (ΕΚ) αριθ. 79/2009 και (ΕΚ) αριθ. 661/2009 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και των κανονισμών (ΕΚ) αριθ. 631/2009, (ΕΕ) αριθ. 406/2010, (ΕΕ) αριθ. 672/2010, (ΕΕ) αριθ. 1003/2010, (ΕΕ) αριθ. 1005/2010, (ΕΕ) αριθ. 1008/2010, (ΕΕ) αριθ. 1009/2010, (ΕΕ) αριθ. 19/2011, (ΕΕ) αριθ. 109/2011, (ΕΕ) αριθ. 458/2011, (ΕΕ) αριθ. 65/2012, (ΕΕ) αριθ. 130/2012, (ΕΕ) αριθ. 347/2012, (ΕΕ) αριθ. 351/2012, (ΕΕ) αριθ. 1230/2012 και (ΕΕ) 2015/166 της Επιτροπής (ΕΕ L 325 της 16.12.2019, σ. 1).

11 Κανονισμός του ΟΗΕ αριθ. 155 — Ενιαίες διατάξεις σχετικά με την έγκριση οχημάτων όσον αφορά την κυβερνοασφάλεια και το σύστημα διαχείρισης της κυβερνοασφάλειας [2021/387].

12 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 Ασφάλεια της Αεροπορίας, 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) Ο παρών κανονισμός θεσπίζει οριζόντιους κανόνες κυβερνοασφάλειας που δεν αφορούν συγκεκριμένα τομείς ή ορισμένα προϊόντα με ψηφιακά στοιχεία. Ωστόσο, θα μπορούσαν να θεσπιστούν ειδικοί ενωσιακοί κανόνες για συγκεκριμένους τομείς ή συγκεκριμένα προϊόντα, οι οποίοι θα καθορίζουν απαιτήσεις για την αντιμετώπιση του συνόλου ή μέρους των κινδύνων που καλύπτονται από τις ουσιώδεις απαιτήσεις που ορίζονται στον παρόντα κανονισμό. Στις περιπτώσεις αυτές, η εφαρμογή του παρόντος κανονισμού σε προϊόντα με ψηφιακά στοιχεία που καλύπτονται από άλλους ενωσιακούς κανόνες οι οποίοι καθορίζουν απαιτήσεις για την αντιμετώπιση του συνόλου ή μέρους των κινδύνων που καλύπτονται από τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα Ι του παρόντος κανονισμού μπορεί να περιοριστεί ή να αποκλειστεί, όταν ο εν λόγω περιορισμός ή αποκλεισμός συνάδει με το συνολικό κανονιστικό πλαίσιο που ισχύει για τα εν λόγω προϊόντα και όταν οι τομεακοί κανόνες επιτυγχάνουν το ίδιο επίπεδο προστασίας με εκείνο που προβλέπεται στον παρόντα κανονισμό. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις για την τροποποίηση του παρόντος κανονισμού με τον προσδιορισμό των εν λόγω προϊόντων και κανόνων. Για την υφιστάμενη νομοθεσία της Ένωσης όπου θα πρέπει να εφαρμόζονται τέτοιοι περιορισμοί ή εξαιρέσεις, ο παρών κανονισμός περιέχει ειδικές διατάξεις για την αποσαφήνιση της σχέσης του με την εν λόγω ενωσιακή νομοθεσία.

(15) Ο κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2022/30 ορίζει ότι οι ουσιώδεις απαιτήσεις που ορίζονται στο άρθρο 3 παράγραφος 3 στοιχείο δ) (βλάβη στο δίκτυο και κατάχρηση των πόρων του δικτύου), στοιχείο ε) (δεδομένα προσωπικού χαρακτήρα και ιδιωτικότητα) και στοιχείο στ) (απάτη) της οδηγίας 2014/53/ΕΕ εφαρμόζονται σε ορισμένους τύπους ραδιοεξοπλισμού. Η [εκτελεστική απόφαση XXX/2022 της Επιτροπής σχετικά με αίτημα τυποποίησης προς τους ευρωπαϊκούς οργανισμούς τυποποίησης] καθορίζει απαιτήσεις για την ανάπτυξη ειδικών προτύπων, προσδιορίζοντας περαιτέρω τον τρόπο με τον οποίο θα πρέπει να εξεταστούν αυτές οι τρεις ουσιώδεις απαιτήσεις. Οι ουσιώδεις απαιτήσεις που καθορίζονται στον παρόντα κανονισμό περιλαμβάνουν όλα τα στοιχεία των ουσιωδών απαιτήσεων που αναφέρονται στο άρθρο 3 παράγραφος 3 στοιχεία δ), ε) και στ) της οδηγίας 2014/53/ΕΕ. Επιπλέον, οι ουσιώδεις απαιτήσεις που ορίζονται στον παρόντα κανονισμό συνάδουν με τους στόχους των απαιτήσεων για συγκεκριμένα πρότυπα που περιλαμβάνονται στο εν λόγω αίτημα τυποποίησης. Ως εκ τούτου, εάν η Επιτροπή καταργήσει ή τροποποιήσει τον κατ' εξουσιοδότηση κανονισμό (ΕΕ) 2022/30 με συνέπεια αυτός να παύσει να εφαρμόζεται σε ορισμένα προϊόντα που υπόκεινται στον παρόντα κανονισμό, η Επιτροπή και οι ευρωπαϊκοί οργανισμοί τυποποίησης θα λάβουν υπόψη τις εργασίες τυποποίησης που πραγματοποιήθηκαν στο πλαίσιο της εκτελεστικής απόφασης C(2022)5637 της Επιτροπής σχετικά με αίτημα τυποποίησης για τον κατ' εξουσιοδότηση κανονισμό 2022/30 της Επιτροπής κατά την κατάρτιση και την ανάπτυξη εναρμονισμένων προτύπων για τη διευκόλυνση της εφαρμογής του παρόντος κανονισμού.

(16) Η οδηγία 85/374/ΕΟΚ[13] συμπληρώνει τον παρόντα κανονισμό. Η εν λόγω οδηγία θεσπίζει κανόνες περί ευθύνης λόγω ελαττωματικών προϊόντων, ώστε οι ζημιωθέντες να μπορούν να διεκδικήσουν αποζημίωση όταν η ζημία προκλήθηκε από ελαττωματικά προϊόντα. Καθιερώνει την αρχή ότι ο κατασκευαστής ενός προϊόντος

[13] Οδηγία 85/374/ΕΟΚ του Συμβουλίου, της 25ης Ιουλίου 1985, για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών σε θέματα ευθύνης λόγω ελαττωματικών προϊόντων (ΕΕ L 210 της 7.8.1985, σ. 85).

ευθύνεται για τις ζημίες που προκαλούνται από την έλλειψη ασφάλειας του προϊόντος του, ανεξαρτήτως υπαιτιότητας (αντικειμενική ευθύνη). Όταν η εν λόγω έλλειψη ασφάλειας συνίσταται σε έλλειψη ενημερώσεων ασφαλείας μετά τη διάθεση του προϊόντος στην αγορά, με αποτέλεσμα την πρόκληση ζημίας, θα μπορούσε να θεμελιωθεί η ευθύνη του κατασκευαστή. Οι υποχρεώσεις των κατασκευαστών που αφορούν την παροχή των εν λόγω ενημερώσεων ασφαλείας θα πρέπει να καθοριστούν στον παρόντα κανονισμό.

(17) Ο παρών κανονισμός δεν θα πρέπει να θίγει τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[14], μεταξύ άλλων τις διατάξεις για τη θέσπιση μηχανισμών πιστοποίησης προστασίας των δεδομένων και σφραγίδων και σημάτων προστασίας των δεδομένων, προκειμένου να αποδεικνύεται η συμμόρφωση με τον εν λόγω κανονισμό των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Οι πράξεις αυτές θα μπορούσαν να ενσωματωθούν σε ένα προϊόν με ψηφιακά στοιχεία. Η προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, καθώς και η κυβερνοασφάλεια γενικότερα, αποτελούν βασικά στοιχεία του κανονισμού (ΕΕ) 2016/679. Με την προστασία των καταναλωτών και των οργανισμών από κινδύνους για την κυβερνοασφάλεια, οι ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό θα συμβάλουν επίσης στην ενίσχυση της προστασίας των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής των ατόμων. Θα πρέπει να εξεταστεί το ενδεχόμενο ανάπτυξης συνεργειών, τόσο όσον αφορά την τυποποίηση όσο και την πιστοποίηση σε πτυχές κυβερνοασφάλειας μέσω της συνεργασίας μεταξύ της Επιτροπής, των ευρωπαϊκών οργανισμών τυποποίησης, του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ) που συστάθηκε με τον κανονισμό (ΕΕ) 2016/679 και των εθνικών εποπτικών αρχών προστασίας δεδομένων. Θα πρέπει επίσης να δημιουργηθούν συνέργειες μεταξύ του παρόντος κανονισμού και της ενωσιακής νομοθεσίας για την προστασία των δεδομένων στον τομέα της εποπτείας της αγοράς και της επιβολής. Για τον σκοπό αυτόν, οι εθνικές αρχές εποπτείας της αγοράς που ορίζονται βάσει του παρόντος κανονισμού θα πρέπει να συνεργάζονται με τις αρχές που εποπτεύουν τη νομοθεσία της Ένωσης για την προστασία των δεδομένων. Οι τελευταίες θα πρέπει επίσης να έχουν πρόσβαση σε πληροφορίες σχετικές με την εκτέλεση των καθηκόντων τους.

(18) Στον βαθμό που τα προϊόντα τους εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού, οι εκδότες ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας, όπως αναφέρονται στο άρθρο [άρθρο 6α παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 910/2014, όπως τροποποιήθηκε με την πρόταση κανονισμού για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 όσον αφορά τη θέσπιση πλαισίου για την ευρωπαϊκή ψηφιακή ταυτότητα], θα πρέπει να συμμορφώνονται τόσο με τις οριζόντιες ουσιώδεις απαιτήσεις που θεσπίζονται με τον παρόντα κανονισμό όσο και με τις ειδικές απαιτήσεις ασφάλειας που θεσπίζονται με το άρθρο [άρθρο 6α του κανονισμού (ΕΕ) αριθ. 910/2014, όπως τροποποιήθηκε με την πρόταση κανονισμού για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 όσον αφορά τη θέσπιση

[14] 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).

πλαισίου για την ευρωπαϊκή ψηφιακή ταυτότητα]. Προκειμένου να διευκολυνθεί η συμμόρφωση, οι εκδότες πορτοφολιών θα πρέπει να είναι σε θέση να αποδεικνύουν τη συμμόρφωση των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας με τις απαιτήσεις που ορίζονται αντίστοιχα και στις δύο πράξεις, πιστοποιώντας τα προϊόντα τους στο πλαίσιο ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας που θεσπίστηκε με τον κανονισμό (ΕΕ) 2019/881 και για τα οποία η Επιτροπή καθόρισε μέσω εκτελεστικής πράξης τεκμήριο συμμόρφωσης για τον παρόντα κανονισμό, στον βαθμό που το πιστοποιητικό ή μέρη αυτού καλύπτουν τις εν λόγω απαιτήσεις.

(19) Ορισμένα καθήκοντα που προβλέπονται στον παρόντα κανονισμό θα πρέπει να εκτελούνται από τον ENISA, σύμφωνα με το άρθρο 3 παράγραφος 2 του κανονισμού (ΕΕ) 2019/881. Ειδικότερα, ο ENISA θα πρέπει να λαμβάνει κοινοποιήσεις από τους κατασκευαστές σχετικά με τρωτά σημεία που περιέχονται σε προϊόντα με ψηφιακά στοιχεία και αποτελούν αντικείμενο ενεργού εκμετάλλευσης, καθώς και σχετικά με συμβάντα που έχουν αντίκτυπο στην ασφάλεια των εν λόγω προϊόντων. Ο ENISA θα πρέπει επίσης να διαβιβάζει τις κοινοποιήσεις αυτές στις σχετικές ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια των υπολογιστών (CSIRT) ή, αντίστοιχα, στα σχετικά ενιαία σημεία επαφής των κρατών μελών που ορίζονται σύμφωνα με το άρθρο [άρθρο X] της οδηγίας [οδηγία XXX/XXXX (NIS2)], και να ενημερώνει τις αρμόδιες αρχές εποπτείας της αγοράς σχετικά με το κοινοποιηθέν τρωτό σημείο. Με βάση τις πληροφορίες που συγκεντρώνει, ο ENISA θα πρέπει να καταρτίζει διετή τεχνική έκθεση σχετικά με τις αναδυόμενες τάσεις όσον αφορά τους κινδύνους για την κυβερνοασφάλεια σε προϊόντα με ψηφιακά στοιχεία και να την υποβάλλει στην ομάδα συνεργασίας που αναφέρεται στην οδηγία [οδηγία XXX/XXXX (NIS2)]. Επιπλέον, λαμβάνοντας υπόψη την εμπειρογνωμοσύνη και την εντολή του, ο ENISA θα πρέπει να είναι σε θέση να υποστηρίζει τη διαδικασία εφαρμογής του παρόντος κανονισμού. Ειδικότερα, θα πρέπει να είναι σε θέση να προτείνει κοινές δραστηριότητες που θα διεξάγονται από τις αρχές εποπτείας της αγοράς βάσει ενδείξεων ή πληροφοριών σχετικά με πιθανή μη συμμόρφωση προϊόντων με ψηφιακά στοιχεία προς τον παρόντα κανονισμό σε διάφορα κράτη μέλη, ή να εντοπίζει κατηγορίες προϊόντων για τα οποία θα πρέπει να οργανώνονται ταυτόχρονες συντονισμένες δράσεις ελέγχου. Σε εξαιρετικές περιστάσεις, κατόπιν αιτήματος της Επιτροπής, ο ENISA θα πρέπει να είναι σε θέση να διενεργεί αξιολογήσεις όσον αφορά συγκεκριμένα προϊόντα με ψηφιακά στοιχεία που παρουσιάζουν σημαντικό κίνδυνο για την κυβερνοασφάλεια, εφόσον απαιτείται άμεση παρέμβαση για τη διατήρηση της εύρυθμης λειτουργίας της εσωτερικής αγοράς.

(20) Τα προϊόντα με ψηφιακά στοιχεία θα πρέπει να φέρουν τη σήμανση CE ώστε να δηλώνεται η συμμόρφωσή τους με τον παρόντα κανονισμό και να μπορούν να κυκλοφορούν ελεύθερα εντός της εσωτερικής αγοράς. Τα κράτη μέλη δεν θα πρέπει να δημιουργούν αδικαιολόγητα εμπόδια στην κυκλοφορία προϊόντων με ψηφιακά στοιχεία που συμμορφώνονται με τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό και φέρουν τη σήμανση CE.

(21) Προκειμένου να διασφαλιστεί ότι οι κατασκευαστές μπορούν να διαθέτουν λογισμικό για σκοπούς διεξαγωγής δοκιμών προτού υποβάλουν τα προϊόντα τους σε αξιολόγηση της συμμόρφωσης, τα κράτη μέλη δεν θα πρέπει να εμποδίζουν τη διαθεσιμότητα ημιτελούς λογισμικού, όπως οι εκδόσεις «άλφα», οι εκδόσεις «βήτα» ή υποψήφιες εκδόσεις, εφόσον η έκδοση διατίθεται μόνο για το χρονικό διάστημα που απαιτείται για τη δοκιμή της και τη συλλογή παρατηρήσεων. Οι κατασκευαστές θα πρέπει να διασφαλίζουν ότι το λογισμικό που διατίθεται υπό τις συνθήκες αυτές κυκλοφορεί μόνο κατόπιν εκτίμησης κινδύνου και ότι συμμορφώνεται, στο μέτρο του δυνατού, με

τις απαιτήσεις ασφάλειας που αφορούν τις ιδιότητες των προϊόντων με ψηφιακά στοιχεία, όπως αυτές επιβάλλονται από τον παρόντα κανονισμό. Οι κατασκευαστές θα πρέπει επίσης να εφαρμόζουν τις απαιτήσεις χειρισμού τρωτών σημείων στο μέτρο του δυνατού. Οι κατασκευαστές δεν θα πρέπει να υποχρεώνουν τους χρήστες να πραγματοποιούν αναβάθμιση σε εκδόσεις που διατίθενται μόνο για σκοπούς διεξαγωγής δοκιμής.

(22) Προκειμένου να διασφαλιστεί ότι τα προϊόντα με ψηφιακά στοιχεία, όταν διατίθενται στην αγορά, δεν ενέχουν κινδύνους για την κυβερνοασφάλεια σε πρόσωπα και οργανισμούς, θα πρέπει να καθοριστούν ουσιώδεις απαιτήσεις για τα εν λόγω προϊόντα. Όταν τα προϊόντα τροποποιούνται μεταγενέστερα, με φυσικά ή ψηφιακά μέσα, κατά τρόπο που δεν προβλέπεται από τον κατασκευαστή και που μπορεί να συνεπάγεται ότι δεν πληρούν πλέον τις σχετικές ουσιώδεις απαιτήσεις, η τροποποίηση θα πρέπει να θεωρείται ουσιαστική. Για παράδειγμα, οι ενημερώσεις ή επισκευές λογισμικού θα μπορούσαν να εξομοιωθούν με τις εργασίες συντήρησης, υπό τον όρο ότι δεν τροποποιούν προϊόν που ήδη διατίθεται στην αγορά κατά τρόπο που να επηρεάζει τη συμμόρφωση του τελευταίου με τις ισχύουσες απαιτήσεις, ή που να μπορεί να αλλάξει η προβλεπόμενη χρήση για την οποία έχει αξιολογηθεί το προϊόν. Όπως και στην περίπτωση των υλικών επισκευών ή τροποποιήσεων, ένα προϊόν με ψηφιακά στοιχεία θα πρέπει να θεωρείται ότι έχει τροποποιηθεί ουσιαστικά με αλλαγή λογισμικού όταν η ενημέρωση λογισμικού τροποποιεί τις αρχικές προβλεπόμενες λειτουργίες, τον τύπο ή τις επιδόσεις του προϊόντος και οι αλλαγές αυτές δεν είχαν προβλεφθεί στην αρχική εκτίμηση κινδύνου, ή η φύση του κινδύνου έχει αλλάξει ή το επίπεδο κινδύνου έχει αυξηθεί λόγω της ενημέρωσης του λογισμικού.

(23) Σύμφωνα με την κοινώς καθιερωμένη έννοια της ουσιαστικής τροποποίησης όσον αφορά τα προϊόντα που ρυθμίζονται από την ενωσιακή νομοθεσία εναρμόνισης, όταν επέρχεται ουσιαστική τροποποίηση που ενδέχεται να επηρεάσει τη συμμόρφωση ενός προϊόντος με τον παρόντα κανονισμό ή όταν αλλάζει ο επιδιωκόμενος σκοπός του εν λόγω προϊόντος, είναι σκόπιμο να επαληθεύεται η συμμόρφωση του προϊόντος με ψηφιακά στοιχεία και, κατά περίπτωση, να υποβάλλεται σε νέα αξιολόγηση της συμμόρφωσης. Κατά περίπτωση, εάν ο κατασκευαστής προβεί σε αξιολόγηση της συμμόρφωσης με τη συμμετοχή τρίτου, οι αλλαγές που ενδέχεται να οδηγήσουν σε ουσιαστικές τροποποιήσεις θα πρέπει να κοινοποιούνται στο τρίτο μέρος.

(24) Η ανακατασκευή, συντήρηση και επισκευή ενός προϊόντος με ψηφιακά στοιχεία, όπως ορίζεται στον κανονισμό [κανονισμός για τον οικολογικό σχεδιασμό], δεν συνεπάγεται κατ’ ανάγκη ουσιαστική τροποποίηση του προϊόντος, για παράδειγμα εάν η προβλεπόμενη χρήση και οι λειτουργίες δεν αλλάξουν και το επίπεδο κινδύνου παραμένει αμετάβλητο. Ωστόσο, η αναβάθμιση ενός προϊόντος από τον κατασκευαστή ενδέχεται να οδηγήσει σε αλλαγές στον σχεδιασμό και την ανάπτυξη του προϊόντος και, ως εκ τούτου, ενδέχεται να επηρεάσει την προβλεπόμενη χρήση και τη συμμόρφωση του προϊόντος με τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό.

(25) Τα προϊόντα με ψηφιακά στοιχεία θα πρέπει να θεωρούνται κρίσιμα εάν ο αρνητικός αντίκτυπος της εκμετάλλευσης πιθανών τρωτών σημείων κυβερνοασφάλειας του προϊόντος μπορεί να είναι σοβαρός λόγω, μεταξύ άλλων, της λειτουργικότητας που σχετίζεται με την κυβερνοασφάλεια ή της προβλεπόμενης χρήσης. Ειδικότερα, τα τρωτά σημεία σε προϊόντα με ψηφιακά στοιχεία που έχουν λειτουργία η οποία σχετίζεται με την κυβερνοασφάλεια, όπως τα ασφαλή στοιχεία, μπορούν να οδηγήσουν στη διάδοση προβλημάτων ασφάλειας σε ολόκληρη την αλυσίδα εφοδιασμού. Η σοβαρότητα του αντικτύπου ενός συμβάντος κυβερνοασφάλειας

μπορεί επίσης να αυξηθεί όταν λαμβάνεται υπόψη η προβλεπόμενη χρήση του προϊόντος, όπως σε βιομηχανικό περιβάλλον ή στο πλαίσιο βασικής οντότητας του τύπου που αναφέρεται στο παράρτημα [παράρτημα Ι] της οδηγίας [οδηγία XXX/XXXX (NIS2)], ή για την εκτέλεση κρίσιμων ή ευαίσθητων λειτουργιών, όπως η επεξεργασία δεδομένων προσωπικού χαρακτήρα.

(26) Τα κρίσιμα προϊόντα με ψηφιακά στοιχεία θα πρέπει να υπόκεινται σε αυστηρότερες διαδικασίες αξιολόγησης της συμμόρφωσης, ενώ παράλληλα θα πρέπει να διατηρείται μια αναλογική προσέγγιση. Για τον σκοπό αυτό, τα κρίσιμα προϊόντα με ψηφιακά στοιχεία θα πρέπει να χωρίζονται σε δύο κατηγορίες, οι οποίες θα αντικατοπτρίζουν το επίπεδο κινδύνου που συνδέεται με αυτές τις κατηγορίες προϊόντων όσον αφορά την κυβερνοασφάλεια. Ένα δυνητικό κυβερνοσυμβάν το οποίο αφορά προϊόντα της κατηγορίας ΙΙ μπορεί να έχει μεγαλύτερες αρνητικές επιπτώσεις από ένα συμβάν που αφορά προϊόντα της κατηγορίας Ι, για παράδειγμα λόγω της φύσης της λειτουργίας τους όσον αφορά την κυβερνοασφάλεια ή της προβλεπόμενης χρήσης τους σε ευαίσθητα περιβάλλοντα, και, ως εκ τούτου, θα πρέπει να υποβάλλεται σε αυστηρότερη διαδικασία αξιολόγησης της συμμόρφωσης.

(27) Οι κατηγορίες κρίσιμων προϊόντων με ψηφιακά στοιχεία που αναφέρονται στο παράρτημα ΙΙΙ του παρόντος κανονισμού θα πρέπει να νοούνται ως τα προϊόντα που έχουν τη βασική λειτουργικότητα του τύπου που παρατίθεται στο παράρτημα ΙΙΙ του παρόντος κανονισμού. Για παράδειγμα, το παράρτημα ΙΙΙ του παρόντος κανονισμού περιλαμβάνει τα προϊόντα που ορίζονται από τη βασική τους λειτουργικότητα ως μικροεπεξεργαστές γενικής χρήσης στην κατηγορία ΙΙ. Ως εκ τούτου, οι μικροεπεξεργαστές γενικής χρήσης υπόκεινται σε υποχρεωτική αξιολόγηση της συμμόρφωσης από τρίτους. Αυτό δεν ισχύει για άλλα προϊόντα που δεν αναφέρονται ρητά στο παράρτημα ΙΙΙ του παρόντος κανονισμού, στα οποία μπορεί να ενσωματωθεί μικροεπεξεργαστής γενικής χρήσης. Η Επιτροπή θα πρέπει να εκδώσει κατ' εξουσιοδότηση πράξεις [εντός 12 μηνών από την έναρξη ισχύος του παρόντος κανονισμού] για τον καθορισμό των ορισμών των κατηγοριών προϊόντων που εμπίπτουν στην κατηγορία Ι και την κατηγορία ΙΙ, όπως ορίζονται στο παράρτημα ΙΙΙ.

(28) Ο παρών κανονισμός αντιμετωπίζει τους κινδύνους για την κυβερνοασφάλεια με στοχευμένο τρόπο. Ωστόσο, τα προϊόντα με ψηφιακά στοιχεία ενδέχεται να εγκυμονούν άλλους κινδύνους για την ασφάλεια, οι οποίοι δεν σχετίζονται με την κυβερνοασφάλεια. Οι κίνδυνοι αυτοί θα πρέπει να εξακολουθήσουν να ρυθμίζονται από άλλη σχετική ενωσιακή νομοθεσία για τα προϊόντα. Εάν δεν εφαρμόζεται άλλη ενωσιακή νομοθεσία εναρμόνισης, θα πρέπει να υπόκεινται στον κανονισμό [κανονισμός για τη γενική ασφάλεια των προϊόντων]. Ως εκ τούτου, λόγω του στοχευμένου χαρακτήρα του παρόντος κανονισμού, κατά παρέκκλιση από το άρθρο 2 παράγραφος 1 τρίτο εδάφιο στοιχείο β) του κανονισμού [κανονισμός για τη γενική ασφάλεια των προϊόντων], το κεφάλαιο ΙΙΙ τμήμα 1, τα κεφάλαια V και VII και τα κεφάλαια IX έως XI του κανονισμού [κανονισμός για τη γενική ασφάλεια των προϊόντων] θα πρέπει να εφαρμόζονται σε προϊόντα με ψηφιακά στοιχεία όσον αφορά τους κινδύνους ασφάλειας που δεν καλύπτονται από τον παρόντα κανονισμό, εάν τα εν λόγω προϊόντα δεν υπόκεινται σε ειδικές απαιτήσεις που επιβάλλονται από άλλη ενωσιακή νομοθεσία εναρμόνισης κατά την έννοια του [άρθρου 3 σημείο 25 του κανονισμού για τη γενική ασφάλεια των προϊόντων].

(29) Τα προϊόντα με ψηφιακά στοιχεία που ταξινομούνται ως συστήματα ΤΝ υψηλού κινδύνου σύμφωνα με το άρθρο 6 του κανονισμού[15] [κανονισμός για την ΤΝ] και τα οποία εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού θα πρέπει να συμμορφώνονται με τις ουσιώδεις απαιτήσεις που ορίζονται στον παρόντα κανονισμό. Όταν τα εν λόγω συστήματα ΤΝ υψηλού κινδύνου πληρούν τις ουσιώδεις απαιτήσεις του παρόντος κανονισμού, θα πρέπει να θεωρείται ότι συμμορφώνονται με τις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο άρθρο [άρθρο 15] του κανονισμού [κανονισμός για την ΤΝ], στον βαθμό που οι εν λόγω απαιτήσεις καλύπτονται από τη δήλωση συμμόρφωσης ΕΕ ή μέρη αυτής, όπως εκδίδεται δυνάμει του παρόντος κανονισμού. Όσον αφορά τις διαδικασίες αξιολόγησης της συμμόρφωσης που αφορούν τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας ενός προϊόντος με ψηφιακά στοιχεία που καλύπτεται από τον παρόντα κανονισμό και ταξινομείται ως σύστημα ΤΝ υψηλού κινδύνου, κατά κανόνα θα πρέπει να εφαρμόζονται οι σχετικές διατάξεις του άρθρου 43 του κανονισμού [κανονισμός για την ΤΝ] αντί των αντίστοιχων διατάξεων του παρόντος κανονισμού. Ωστόσο, ο κανόνας αυτός δεν θα πρέπει να έχει ως αποτέλεσμα τη μείωση του αναγκαίου επιπέδου διασφάλισης για τα κρίσιμα προϊόντα με ψηφιακά στοιχεία που καλύπτονται από τον παρόντα κανονισμό. Ως εκ τούτου, κατά παρέκκλιση από τον εν λόγω κανόνα, τα συστήματα ΤΝ υψηλού κινδύνου που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού [κανονισμός για την ΤΝ] και χαρακτηρίζονται επίσης ως κρίσιμα προϊόντα με ψηφιακά στοιχεία σύμφωνα με τον παρόντα κανονισμό και στα οποία εφαρμόζεται η διαδικασία αξιολόγησης της συμμόρφωσης με βάση τον εσωτερικό έλεγχο που αναφέρεται στο παράρτημα VI του κανονισμού [κανονισμός για την ΤΝ], θα πρέπει να υπόκεινται στις διατάξεις του παρόντος κανονισμού σχετικά με την αξιολόγηση της συμμόρφωσης, όσον αφορά τις ουσιώδεις απαιτήσεις του παρόντος κανονισμού. Στην περίπτωση αυτή, για όλες τις άλλες πτυχές που καλύπτονται από τον κανονισμό [κανονισμός για την ΤΝ] θα πρέπει να εφαρμόζονται οι αντίστοιχες διατάξεις για την αξιολόγηση της συμμόρφωσης με βάση τον εσωτερικό έλεγχο, όπως ορίζεται στο παράρτημα VI του κανονισμού [κανονισμός για την ΤΝ].

(30) Τα μηχανολογικά προϊόντα που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού [πρόταση κανονισμού για τα μηχανήματα] και τα οποία είναι προϊόντα με ψηφιακά στοιχεία κατά την έννοια του παρόντος κανονισμού και για τα οποία έχει εκδοθεί δήλωση συμμόρφωσης βάσει του παρόντος κανονισμού, θα πρέπει να θεωρείται ότι συμμορφώνονται με τις ουσιώδεις απαιτήσεις υγείας και ασφάλειας που ορίζονται στο [παράρτημα ΙΙΙ τμήματα 1.1.9 και 1.2.1] του κανονισμού [πρόταση κανονισμού για τα μηχανήματα], όσον αφορά την προστασία από τη διαφθορά, καθώς και την ασφάλεια και την αξιοπιστία των συστημάτων ελέγχου, εφόσον η συμμόρφωση με τις εν λόγω απαιτήσεις αποδεικνύεται από τη δήλωση συμμόρφωσης ΕΕ που εκδίδεται δυνάμει του παρόντος κανονισμού.

(31) Ο κανονισμός [πρόταση κανονισμού για τον ευρωπαϊκό χώρο δεδομένων για την υγεία] συμπληρώνει τις ουσιώδεις απαιτήσεις που ορίζονται στον παρόντα κανονισμό. Ως εκ τούτου, τα συστήματα ηλεκτρονικών μητρώων υγείας (συστήματα ΗΜΥ) που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού [πρόταση κανονισμού για τον ευρωπαϊκό χώρο δεδομένων για την υγεία], τα οποία είναι προϊόντα με ψηφιακά στοιχεία κατά την έννοια του παρόντος κανονισμού, θα πρέπει επίσης να συμμορφώνονται με τις ουσιώδεις απαιτήσεις που ορίζονται στον παρόντα κανονισμό. Οι κατασκευαστές τους θα πρέπει να αποδεικνύουν τη συμμόρφωση, όπως απαιτείται

[15] Κανονισμός [κανονισμός για την ΤΝ].

από τον κανονισμό [πρόταση κανονισμού για τον ευρωπαϊκό χώρο δεδομένων για την υγεία]. Για τη διευκόλυνση της συμμόρφωσης, οι κατασκευαστές μπορούν να καταρτίζουν ενιαίο τεχνικό φάκελο που περιέχει τα στοιχεία που απαιτούνται και από τις δύο νομικές πράξεις. Δεδομένου ότι ο παρών κανονισμός δεν καλύπτει το SaaS καθαυτό, τα συστήματα ΗΜΥ που προσφέρονται μέσω του μοντέλου αδειοδότησης και παράδοσης SaaS δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού. Ομοίως, τα συστήματα ΗΜΥ που αναπτύσσονται και χρησιμοποιούνται εσωτερικά δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού, καθώς δεν διατίθενται στην αγορά.

(32) Προκειμένου να διασφαλιστεί ότι τα προϊόντα με ψηφιακά στοιχεία είναι ασφαλή τόσο κατά τη διάθεσή τους στην αγορά όσο και καθ' όλη τη διάρκεια του κύκλου ζωής τους, είναι αναγκαίο να καθοριστούν ουσιώδεις απαιτήσεις για τον χειρισμό τρωτών σημείων, καθώς και ουσιώδεις απαιτήσεις κυβερνοασφάλειας σχετικά με τις ιδιότητες των προϊόντων με ψηφιακά στοιχεία. Ενώ οι κατασκευαστές θα πρέπει να συμμορφώνονται με όλες τις ουσιώδεις απαιτήσεις που σχετίζονται με τον χειρισμό τρωτών σημείων και να διασφαλίζουν ότι όλα τα προϊόντα τους παραδίδονται χωρίς γνωστά εκμεταλλεύσιμα τρωτά σημεία, θα πρέπει να προσδιορίζουν ποιες άλλες ουσιώδεις απαιτήσεις που σχετίζονται με τις ιδιότητες του προϊόντος είναι συναφείς για τον συγκεκριμένο τύπο προϊόντος. Για τον σκοπό αυτόν, οι κατασκευαστές θα πρέπει να διενεργούν αξιολόγηση των κινδύνων κυβερνοασφάλειας που συνδέονται με ένα προϊόν με ψηφιακά στοιχεία, προκειμένου να εντοπίζουν τους σχετικούς κινδύνους και τις σχετικές ουσιώδεις απαιτήσεις και να εφαρμόζουν κατάλληλα εναρμονισμένα πρότυπα ή κοινές προδιαγραφές.

(33) Προκειμένου να βελτιωθεί η ασφάλεια των προϊόντων με ψηφιακά στοιχεία που διατίθενται στην εσωτερική αγορά, είναι αναγκαίο να καθοριστούν ουσιώδεις απαιτήσεις. Οι εν λόγω ουσιώδεις απαιτήσεις δεν θα πρέπει να θίγουν τις συντονισμένες από την ΕΕ εκτιμήσεις κινδύνου για τις αλυσίδες εφοδιασμού κρίσιμης σημασίας που θεσπίζονται με το [άρθρο Χ] της οδηγίας [οδηγία XXX/XXXX (NIS2)][16], οι οποίες λαμβάνουν υπόψη τόσο τεχνικούς όσο και, κατά περίπτωση, μη τεχνικούς παράγοντες κινδύνου, όπως η αθέμιτη επιρροή τρίτης χώρας στους προμηθευτές. Επιπλέον, δεν θα πρέπει να θίγονται τα προνόμια των κρατών μελών να καθορίζουν πρόσθετες απαιτήσεις που λαμβάνουν υπόψη μη τεχνικούς παράγοντες, με σκοπό την εξασφάλιση υψηλού επιπέδου ανθεκτικότητας, συμπεριλαμβανομένων εκείνων που ορίζονται στη σύσταση (ΕΕ) 2019/534, στη συντονισμένη σε επίπεδο Ένωσης εκτίμηση κινδύνου για την ασφάλεια των δικτύων 5G και στην εργαλειοθήκη της ΕΕ για την κυβερνοασφάλεια των δικτύων 5G που συμφωνήθηκε από την ομάδα συνεργασίας NIS, όπως αναφέρεται στην [οδηγία XXX/XXXX (NIS2)].

(34) Για να διασφαλιστεί ότι οι εθνικές CSIRT και τα ενιαία σημεία επαφής που ορίζονται σύμφωνα με το άρθρο [άρθρο Χ] της οδηγίας [οδηγία XX/XXXX (NIS2)] διαθέτουν τις πληροφορίες που απαιτούνται για την εκπλήρωση των καθηκόντων τους και την αύξηση του συνολικού επιπέδου κυβερνοασφάλειας των βασικών και σημαντικών οντοτήτων, καθώς και για να διασφαλιστεί η αποτελεσματική λειτουργία των αρχών εποπτείας της αγοράς, οι κατασκευαστές προϊόντων με ψηφιακά στοιχεία θα πρέπει να κοινοποιούν στον ENISA τα τρωτά σημεία που αποτελούν αντικείμενο ενεργού εκμετάλλευσης. Δεδομένου ότι τα περισσότερα προϊόντα με ψηφιακά στοιχεία

[16] Οδηγία XXX του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της [ημερομηνία], [σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (ΕΕ L XX, ημερομηνία, σ. Χ)].

διατίθενται σε ολόκληρη την εσωτερική αγορά, οποιαδήποτε εκμετάλλευση τρωτού σημείου σε προϊόν με ψηφιακά στοιχεία θα πρέπει να θεωρείται απειλή για τη λειτουργία της εσωτερικής αγοράς. Οι κατασκευαστές θα πρέπει επίσης να εξετάζουν το ενδεχόμενο γνωστοποίησης επιδιορθωμένων τρωτών σημείων στην ευρωπαϊκή βάση δεδομένων τρωτών σημείων που δημιουργήθηκε δυνάμει της οδηγίας [οδηγία XX/XXXX (NIS2)] και τελεί υπό τη διαχείριση του ENISA ή στο πλαίσιο οποιασδήποτε άλλης προσβάσιμης στο κοινό βάσης δεδομένων τρωτών σημείων.

(35) Οι κατασκευαστές θα πρέπει επίσης να αναφέρουν στον ENISA κάθε συμβάν που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία. Παρά τις υποχρεώσεις αναφοράς συμβάντων που προβλέπονται στην οδηγία [οδηγία XXX/XXXX (NIS2)] για βασικές και σημαντικές οντότητες, είναι ζωτικής σημασίας για τον ENISA, τα ενιαία σημεία επαφής που ορίζονται από τα κράτη μέλη σύμφωνα με το άρθρο [άρθρο X] της οδηγίας [οδηγία XXX/XXXX (NIS2)] και τις αρχές εποπτείας της αγοράς να λαμβάνουν πληροφορίες από τους κατασκευαστές προϊόντων με ψηφιακά στοιχεία που τους επιτρέπουν να αξιολογούν την ασφάλεια των εν λόγω προϊόντων. Προκειμένου να διασφαλιστεί ότι οι χρήστες μπορούν να αντιδρούν γρήγορα σε συμβάντα που έχουν αντίκτυπο στην ασφάλεια των προϊόντων τους με ψηφιακά στοιχεία, οι κατασκευαστές θα πρέπει επίσης να ενημερώνουν τους χρήστες τους για κάθε σχετικό συμβάν και, κατά περίπτωση, για τυχόν διορθωτικά μέτρα που μπορούν να εφαρμόσουν οι χρήστες για τον μετριασμό των επιπτώσεων του συμβάντος, για παράδειγμα δημοσιεύοντας σχετικές πληροφορίες στους δικτυακούς τόπους τους ή, όταν ο κατασκευαστής είναι σε θέση να επικοινωνήσει με τους χρήστες και, όταν δικαιολογείται από τους κινδύνους, επικοινωνώντας απευθείας με τους χρήστες.

(36) Οι κατασκευαστές προϊόντων με ψηφιακά στοιχεία θα πρέπει να εφαρμόζουν συντονισμένες πολιτικές γνωστοποίησης τρωτών σημείων για τη διευκόλυνση της αναφοράς τρωτών σημείων από άτομα ή οντότητες. Η συντονισμένη πολιτική γνωστοποίησης τρωτών σημείων θα πρέπει να προσδιορίζει μια διαρθρωμένη διαδικασία μέσω της οποίας τα τρωτά σημεία αναφέρονται σε κατασκευαστή κατά τρόπο που να επιτρέπει στον κατασκευαστή να διαγνώσει και να διορθώσει τα εν λόγω τρωτά σημεία πριν να αποκαλυφθούν σε τρίτα μέρη ή στο ευρύ κοινό λεπτομερείς πληροφορίες σχετικά με τα τρωτά σημεία. Δεδομένου ότι οι πληροφορίες σχετικά με εκμεταλλεύσιμα τρωτά σημεία ευρέως χρησιμοποιούμενων προϊόντων με ψηφιακά στοιχεία μπορούν να πωλούνται σε υψηλές τιμές στη μαύρη αγορά, οι κατασκευαστές των εν λόγω προϊόντων θα πρέπει να είναι σε θέση να χρησιμοποιούν προγράμματα, στο πλαίσιο των συντονισμένων πολιτικών τους για τη γνωστοποίηση τρωτών σημείων, με τα οποία θα παρέχουν κίνητρα για την αναφορά των τρωτών σημείων, διασφαλίζοντας ότι τα άτομα ή οι οντότητες λαμβάνουν αναγνώριση και αποζημίωση για τις προσπάθειές τους (προγράμματα ανεύρεσης τρωτών σημείων γνωστά ως «bug bounty»).

(37) Προκειμένου να διευκολυνθεί η ανάλυση τρωτότητας, οι κατασκευαστές θα πρέπει να εντοπίζουν και να τεκμηριώνουν τις συνιστώσες που περιέχονται στα προϊόντα με ψηφιακά στοιχεία, μεταξύ άλλων με την κατάρτιση καταλόγου υλικών του λογισμικού. Ο κατάλογος υλικών του λογισμικού μπορεί να παρέχει σε όσους κατασκευάζουν, αγοράζουν και χειρίζονται λογισμικό πληροφορίες που βελτιώνουν την κατανόηση της αλυσίδας εφοδιασμού, γεγονός που έχει πολλαπλά οφέλη, αλλά κυρίως βοηθά τους κατασκευαστές και τους χρήστες να εντοπίζουν γνωστά νεοεμφανιζόμενα τρωτά σημεία και κινδύνους. Είναι ιδιαίτερα σημαντικό για τους κατασκευαστές να διασφαλίζουν ότι τα προϊόντα τους δεν περιέχουν ευάλωτες συνιστώσες που έχουν αναπτυχθεί από τρίτους.

(38) Προκειμένου να διευκολυνθεί η αξιολόγηση της συμμόρφωσης προς τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό, θα πρέπει να υπάρχει τεκμήριο συμμόρφωσης για προϊόντα με ψηφιακά στοιχεία που συμμορφώνονται με εναρμονισμένα πρότυπα, τα οποία μετουσιώνουν τις ουσιώδεις απαιτήσεις του παρόντος κανονισμού σε λεπτομερείς τεχνικές προδιαγραφές και τα οποία εγκρίνονται σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[17]. Ο κανονισμός (ΕΕ) αριθ. 1025/2012 προβλέπει διαδικασία διατύπωσης αντιρρήσεων σε εναρμονισμένα πρότυπα όταν τα εν λόγω πρότυπα δεν ικανοποιούν πλήρως τις απαιτήσεις του παρόντος κανονισμού.

(39) Ο κανονισμός (ΕΕ) 2019/881 θεσπίζει εθελοντικό ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας για προϊόντα, διαδικασίες και υπηρεσίες ΤΠΕ. Τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας μπορούν να καλύπτουν προϊόντα με ψηφιακά στοιχεία που καλύπτονται από τον παρόντα κανονισμό. Ο παρών κανονισμός θα πρέπει να δημιουργήσει συνέργειες με τον κανονισμό (ΕΕ) 2019/881. Προκειμένου να διευκολυνθεί η αξιολόγηση της συμμόρφωσης με τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό, τα προϊόντα με ψηφιακά στοιχεία που έχουν πιστοποιηθεί ή για τα οποία έχει εκδοθεί δήλωση συμμόρφωσης στο πλαίσιο συστήματος κυβερνοασφάλειας σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 και τα οποία έχουν προσδιοριστεί από την Επιτροπή σε εκτελεστική πράξη, τεκμαίρεται ότι συμμορφώνονται με τις ουσιώδεις απαιτήσεις του παρόντος κανονισμού, εφόσον το πιστοποιητικό κυβερνοασφάλειας ή η δήλωση συμμόρφωσης ή μέρη αυτών καλύπτουν τις εν λόγω απαιτήσεις. Η ανάγκη για νέα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία θα πρέπει να αξιολογηθεί υπό το πρίσμα του παρόντος κανονισμού. Τα εν λόγω μελλοντικά ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας που καλύπτουν προϊόντα με ψηφιακά στοιχεία θα πρέπει να λαμβάνουν υπόψη τις ουσιώδεις απαιτήσεις που ορίζονται στον παρόντα κανονισμό και να διευκολύνουν τη συμμόρφωση με τον παρόντα κανονισμό. Η Επιτροπή θα πρέπει να εξουσιοδοτηθεί να καθορίζει, μέσω εκτελεστικών πράξεων, τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας που μπορούν να χρησιμοποιηθούν για την απόδειξη της συμμόρφωσης με τις ουσιώδεις απαιτήσεις που ορίζονται στον παρόντα κανονισμό. Επιπλέον, προκειμένου να αποφευχθεί ο περιττός διοικητικός φόρτος για τους κατασκευαστές, κατά περίπτωση, η Επιτροπή θα πρέπει να διευκρινίζει αν ένα πιστοποιητικό κυβερνοασφάλειας που εκδίδεται στο πλαίσιο των εν λόγω ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας καταργεί την υποχρέωση των κατασκευαστών να διενεργούν αξιολόγηση της συμμόρφωσης από τρίτους, όπως προβλέπεται στον παρόντα κανονισμό για τις αντίστοιχες απαιτήσεις.

(40) Κατά την έναρξη ισχύος της εκτελεστικής πράξης που θεσπίζει τον [εκτελεστικό κανονισμό (ΕΕ) αριθ. …/… της Επιτροπής, της XXX, σχετικά με το ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων] (EUCC), ο οποίος αφορά προϊόντα υλισμικού που καλύπτονται από τον παρόντα κανονισμό, όπως μονάδες ασφάλειας υλισμικού και μικροεπεξεργαστές, η Επιτροπή μπορεί να

[17] 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).

προσδιορίζει, μέσω εκτελεστικής πράξης, τον τρόπο με τον οποίο ο EUCC παρέχει τεκμήριο συμμόρφωσης με τις ουσιώδεις απαιτήσεις που αναφέρονται στο παράρτημα Ι του παρόντος κανονισμού ή με μέρη αυτών. Επιπλέον, η εν λόγω εκτελεστική πράξη μπορεί να προσδιορίζει τον τρόπο με τον οποίο ένα πιστοποιητικό που εκδίδεται βάσει του EUCC καταργεί την υποχρέωση των κατασκευαστών να διενεργούν αξιολόγηση από τρίτο μέρος, όπως προβλέπεται από τον παρόντα κανονισμό για τις αντίστοιχες απαιτήσεις.

(41) Όταν δεν εγκρίνονται εναρμονισμένα πρότυπα ή όταν τα εναρμονισμένα πρότυπα δεν ανταποκρίνονται επαρκώς στις ουσιώδεις απαιτήσεις του παρόντος κανονισμού, η Επιτροπή θα πρέπει να είναι σε θέση να θεσπίζει κοινές προδιαγραφές μέσω εκτελεστικών πράξεων. Οι λόγοι για τη θέσπιση των εν λόγω κοινών προδιαγραφών, αντί να βασίζονται σε εναρμονισμένα πρότυπα, μπορεί να περιλαμβάνουν απόρριψη του αιτήματος τυποποίησης από οποιονδήποτε από τους ευρωπαϊκούς οργανισμούς τυποποίησης, αδικαιολόγητες καθυστερήσεις στην κατάρτιση κατάλληλων εναρμονισμένων προτύπων ή έλλειψη συμμόρφωσης των προτύπων που έχουν θεσπιστεί με τις απαιτήσεις του παρόντος κανονισμού ή με αίτημα της Επιτροπής. Προκειμένου να διευκολυνθεί η αξιολόγηση της συμμόρφωσης με τις ουσιώδεις απαιτήσεις που καθορίζονται στον παρόντα κανονισμό, θα πρέπει να υπάρχει τεκμήριο συμμόρφωσης για προϊόντα με ψηφιακά στοιχεία που συμμορφώνονται με τις κοινές προδιαγραφές που θεσπίζει η Επιτροπή σύμφωνα με τον παρόντα κανονισμό με σκοπό τη διατύπωση λεπτομερών τεχνικών προδιαγραφών των εν λόγω απαιτήσεων.

(42) Οι κατασκευαστές θα πρέπει να καταρτίζουν δήλωση συμμόρφωσης ΕΕ με την οποία να παρέχουν τις πληροφορίες που απαιτούνται δυνάμει του παρόντος κανονισμού σχετικά με τη συμμόρφωση των προϊόντων με ψηφιακά στοιχεία προς τις ουσιώδεις απαιτήσεις του παρόντος κανονισμού και, κατά περίπτωση, άλλης συναφούς ενωσιακής νομοθεσίας εναρμόνισης από την οποία καλύπτεται το προϊόν. Ενδέχεται να απαιτείται από τους κατασκευαστές να συντάσσουν δήλωση συμμόρφωσης ΕΕ και από άλλη νομοθεσία της Ένωσης. Για να εξασφαλιστεί η αποτελεσματική πρόσβαση σε πληροφορίες για σκοπούς εποπτείας της αγοράς, θα πρέπει να συντάσσεται ενιαία δήλωση συμμόρφωσης ΕΕ όσον αφορά τη συμμόρφωση με όλες τις συναφείς πράξεις της Ένωσης. Για τη μείωση της διοικητικής επιβάρυνσης των οικονομικών φορέων, θα πρέπει να υπάρχει η δυνατότητα η εν λόγω ενιαία δήλωση συμμόρφωσης ΕΕ να είναι φάκελος που περιλαμβάνει τις σχετικές επιμέρους δηλώσεις συμμόρφωσης.

(43) Η σήμανση CE, που δηλώνει τη συμμόρφωση του προϊόντος, είναι η ορατή συνέπεια ολόκληρης διαδικασίας η οποία συμπεριλαμβάνει την αξιολόγηση της συμμόρφωσης υπό ευρεία έννοια. Οι γενικές αρχές που διέπουν τη σήμανση CE ορίζονται στον κανονισμό (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[18]. Οι κανόνες για την τοποθέτηση της σήμανσης CE επί προϊόντων με ψηφιακά στοιχεία θα πρέπει να οριστούν στον παρόντα κανονισμό. Η σήμανση «CE» θα πρέπει να είναι η μόνη σήμανση η οποία εγγυάται τη συμμόρφωση των προϊόντων με ψηφιακά στοιχεία προς τις απαιτήσεις του παρόντος κανονισμού.

(44) Για να δοθεί η δυνατότητα στους οικονομικούς φορείς να αποδείξουν τη συμμόρφωση προς τις ουσιώδεις απαιτήσεις που ορίζονται στον παρόντα κανονισμό, και για να

[18] Κανονισμός (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Ιουλίου 2008, για τον καθορισμό των απαιτήσεων διαπίστευσης και για την κατάργηση του κανονισμού (ΕΟΚ) αριθ. 339/93 (ΕΕ L 218 της 13.8.2008, σ. 30).

μπορέσουν οι αρμόδιες αρχές να εξασφαλίσουν ότι τα προϊόντα με ψηφιακά στοιχεία που είναι διαθέσιμα στην αγορά συμμορφώνονται προς αυτές τις απαιτήσεις, είναι απαραίτητο να προβλεφθούν διαδικασίες αξιολόγησης της συμμόρφωσης. Η απόφαση αριθ. 768/2008/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[19] θεσπίζει ενότητες για τις διαδικασίες αξιολόγησης της συμμόρφωσης κατ' αναλογία προς το επίπεδο κινδύνου και το επίπεδο ασφάλειας που απαιτείται. Προκειμένου να διασφαλιστεί η διατομεακή συνοχή και να αποφευχθούν ad hoc παραλλαγές, οι διαδικασίες αξιολόγησης της συμμόρφωσης που είναι κατάλληλες για την επαλήθευση της συμμόρφωσης των προϊόντων με ψηφιακά στοιχεία προς τις ουσιώδεις απαιτήσεις που ορίζονται στον παρόντα κανονισμό έχουν βασιστεί στις εν λόγω ενότητες. Οι διαδικασίες αξιολόγησης της συμμόρφωσης θα πρέπει να εξετάζουν και να επαληθεύουν τις απαιτήσεις που αφορούν τόσο το προϊόν όσο και τη διαδικασία και οι οποίες καλύπτουν ολόκληρο τον κύκλο ζωής των προϊόντων με ψηφιακά στοιχεία, συμπεριλαμβανομένου του προγραμματισμού, του σχεδιασμού, της ανάπτυξης ή της παραγωγής, της δοκιμής και της συντήρησης του προϊόντος.

(45) Κατά γενικό κανόνα, η αξιολόγηση της συμμόρφωσης των προϊόντων με ψηφιακά στοιχεία θα πρέπει να διενεργείται από τον κατασκευαστή με δική του ευθύνη, σύμφωνα με τη διαδικασία που βασίζεται στην ενότητα Α της απόφασης 768/2008/ΕΚ. Ο κατασκευαστής θα πρέπει να διατηρεί την ευελιξία να επιλέγει αυστηρότερη διαδικασία αξιολόγησης της συμμόρφωσης με τη συμμετοχή τρίτου. Εάν το προϊόν ταξινομείται ως κρίσιμο προϊόν της κατηγορίας Ι, απαιτείται πρόσθετη διασφάλιση για να αποδειχθεί η συμμόρφωση με τις ουσιώδεις απαιτήσεις που ορίζονται στον παρόντα κανονισμό. Ο κατασκευαστής θα πρέπει να εφαρμόζει εναρμονισμένα πρότυπα, κοινές προδιαγραφές ή συστήματα πιστοποίησης της κυβερνοασφάλειας βάσει του κανονισμού (ΕΕ) 2019/881, τα οποία έχουν προσδιοριστεί από την Επιτροπή με εκτελεστική πράξη, εάν επιθυμεί να διενεργήσει την αξιολόγηση της συμμόρφωσης με δική του ευθύνη (ενότητα Α). Εάν ο κατασκευαστής δεν εφαρμόζει τα εν λόγω εναρμονισμένα πρότυπα, τις κοινές προδιαγραφές ή τα συστήματα πιστοποίησης της κυβερνοασφάλειας, θα πρέπει να υποβάλλεται σε αξιολόγηση της συμμόρφωσης με τη συμμετοχή τρίτου. Εάν ληφθεί υπόψη ο διοικητικός φόρτος για τους κατασκευαστές και το γεγονός ότι η κυβερνοασφάλεια διαδραματίζει σημαντικό ρόλο στη φάση σχεδιασμού και ανάπτυξης υλικών και άυλων προϊόντων με ψηφιακά στοιχεία, οι διαδικασίες αξιολόγησης της συμμόρφωσης που βασίζονται αντίστοιχα στις ενότητες Β+Γ ή Η της απόφασης 768/2008/ΕΚ έχουν επιλεγεί ως οι πλέον κατάλληλες για την αξιολόγηση της συμμόρφωσης κρίσιμων προϊόντων με ψηφιακά στοιχεία με αναλογικό και αποτελεσματικό τρόπο. Ο κατασκευαστής που διενεργεί την αξιολόγηση της συμμόρφωσης από τρίτους μπορεί να επιλέξει τη διαδικασία που ταιριάζει καλύτερα στη διαδικασία σχεδιασμού και παραγωγής του. Δεδομένου του ακόμη μεγαλύτερου κινδύνου κυβερνοασφάλειας που συνδέεται με τη χρήση προϊόντων που ταξινομούνται ως κρίσιμα προϊόντα της κατηγορίας ΙΙ, η αξιολόγηση της συμμόρφωσης θα πρέπει πάντα να περιλαμβάνει τρίτους.

(46) Ενώ η δημιουργία υλικών προϊόντων με ψηφιακά στοιχεία απαιτεί συνήθως από τους κατασκευαστές να καταβάλλουν σημαντικές προσπάθειες καθ' όλη τη διάρκεια των φάσεων σχεδιασμού, ανάπτυξης και παραγωγής, η δημιουργία προϊόντων με ψηφιακά

[19] Απόφαση αριθ. 768/2008/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Ιουλίου 2008, για κοινό πλαίσιο εμπορίας των προϊόντων και για την κατάργηση της απόφασης 93/465/ΕΟΚ του Συμβουλίου (ΕΕ L 218 της 13.8.2008, σ. 82).

στοιχεία με τη μορφή λογισμικού επικεντρώνεται σχεδόν αποκλειστικά στον σχεδιασμό και την ανάπτυξη, ενώ η φάση της παραγωγής διαδραματίζει ρόλο ήσσονος σημασίας. Ωστόσο, σε πολλές περιπτώσεις, τα προϊόντα λογισμικού πρέπει πρώτα να μεταγλωττιστούν, να αναπτυχθούν, να συσκευαστούν, να διατεθούν για τηλεφόρτωση ή να αντιγραφούν σε υλικά μέσα προτού διατεθούν στην αγορά. Οι δραστηριότητες αυτές θα πρέπει να θεωρούνται δραστηριότητες που ισοδυναμούν με παραγωγή κατά την εφαρμογή των σχετικών ενοτήτων αξιολόγησης της συμμόρφωσης για την επαλήθευση της συμμόρφωσης του προϊόντος με τις ουσιώδεις απαιτήσεις του παρόντος κανονισμού σε όλα τα στάδια σχεδιασμού, ανάπτυξης και παραγωγής.

(47) Για τη διενέργεια αξιολόγησης της συμμόρφωσης από τρίτους φορείς, όσον αφορά τα προϊόντα με ψηφιακά στοιχεία, οι φορείς αξιολόγησης της συμμόρφωσης θα πρέπει να κοινοποιούνται από τις εθνικές αρχές κοινοποίησης προς την Επιτροπή και τα άλλα κράτη μέλη, υπό την προϋπόθεση ότι συμμορφώνονται με ένα σύνολο απαιτήσεων, ιδίως όσον αφορά την ανεξαρτησία, την επάρκεια και την απουσία συγκρούσεων συμφερόντων.

(48) Για να διασφαλιστεί ομοιόμορφο επίπεδο ποιότητας κατά την αξιολόγηση της συμμόρφωσης των προϊόντων με ψηφιακά στοιχεία, πρέπει επίσης να καθοριστούν απαιτήσεις για τις κοινοποιούσες αρχές και τους άλλους φορείς που συμμετέχουν στην αξιολόγηση, την κοινοποίηση και την παρακολούθηση των κοινοποιημένων οργανισμών. Το σύστημα που θεσπίζεται με τον παρόντα κανονισμό θα πρέπει να συμπληρώνεται με το σύστημα διαπίστευσης που προβλέπεται στον κανονισμό (ΕΚ) αριθ. 765/2008. Επειδή η διαπίστευση είναι βασικό μέσο για να επαληθευτεί η επάρκεια των οργανισμών αξιολόγησης της συμμόρφωσης, θα πρέπει επίσης να χρησιμοποιείται για τον σκοπό της κοινοποίησης.

(49) Η διαφανής διαπίστευση που προβλέπεται από τον κανονισμό (ΕΚ) αριθ. 765/2008 και εξασφαλίζει το αναγκαίο επίπεδο εμπιστοσύνης στα πιστοποιητικά συμμόρφωσης θα πρέπει να θεωρείται από τις εθνικές δημόσιες αρχές σε ολόκληρη την Ένωση ως το προτιμώμενο μέσο απόδειξης της τεχνικής επάρκειας των οργανισμών αξιολόγησης της συμμόρφωσης. Ωστόσο, οι εθνικές αρχές μπορούν να θεωρούν ότι διαθέτουν τα κατάλληλα μέσα για να διενεργούν οι ίδιες αυτή την αξιολόγηση. Στις περιπτώσεις αυτές, για να εξασφαλίζεται το κατάλληλο επίπεδο αξιοπιστίας των αξιολογήσεων από άλλες εθνικές αρχές, οι εθνικές αρχές θα πρέπει να προσκομίζουν στην Επιτροπή και στα άλλα κράτη μέλη τα αναγκαία αποδεικτικά έγγραφα ότι οι οργανισμοί αξιολόγησης της συμμόρφωσης που έχουν αξιολογηθεί πληρούν τις σχετικές κανονιστικές απαιτήσεις.

(50) Οι οργανισμοί αξιολόγησης της συμμόρφωσης συχνά αναθέτουν υπεργολαβικά σε τρίτους ή σε θυγατρική τους μέρη των δραστηριοτήτων τους που συνδέονται με την αξιολόγηση της συμμόρφωσης. Προκειμένου να διασφαλίζεται το απαιτούμενο επίπεδο προστασίας για τα προϊόντα με ψηφιακά στοιχεία που διατίθενται στην αγορά, είναι αναγκαίο οι εν λόγω υπεργολάβοι και θυγατρικές να πληρούν τις ίδιες απαιτήσεις που ισχύουν για τους κοινοποιημένους οργανισμούς όσον αφορά την εκτέλεση των καθηκόντων αξιολόγησης της συμμόρφωσης.

(51) Η κοινοποίηση ενός οργανισμού αξιολόγησης της συμμόρφωσης θα πρέπει να αποστέλλεται από την κοινοποιούσα αρχή στην Επιτροπή και στα άλλα κράτη μέλη μέσω του συστήματος πληροφόρησης των κοινοποιημένων και διαπιστευμένων οργανισμών νέας προσέγγισης (NANDO). Το NANDO είναι το ηλεκτρονικό εργαλείο

κοινοποίησης που ανέπτυξε και διαχειρίζεται η Επιτροπή και στο οποίο διατίθεται κατάλογος όλων των κοινοποιημένων οργανισμών.

(52) Επειδή οι κοινοποιημένοι οργανισμοί μπορούν να προσφέρουν τις υπηρεσίες τους σε όλη την Ένωση, ενδείκνυται να δίνεται στα άλλα κράτη μέλη και στην Επιτροπή η δυνατότητα να προβάλουν ένσταση σχετικά με κοινοποιημένο οργανισμό. Συνεπώς, είναι σημαντικό να προβλεφθεί χρονικό διάστημα κατά το οποίο θα μπορούν να αποσαφηνίζονται τυχόν αμφιβολίες ή ανησυχίες ως προς την επάρκεια των οργανισμών αξιολόγησης της συμμόρφωσης, προτού αυτοί αρχίσουν να λειτουργούν ως κοινοποιημένοι οργανισμοί.

(53) Για λόγους ανταγωνιστικότητας έχει ζωτική σημασία να εφαρμόζουν οι κοινοποιημένοι οργανισμοί τις διαδικασίες αξιολόγησης της συμμόρφωσης χωρίς περιττή επιβάρυνση για τους οικονομικούς φορείς. Για τον ίδιο λόγο, και για να εξασφαλιστεί η ίση μεταχείριση των οικονομικών φορέων, θα πρέπει να εξασφαλίζεται η συνέπεια στην τεχνική εφαρμογή των διαδικασιών αξιολόγησης της συμμόρφωσης. Αυτό αναμένεται να επιτευχθεί καλύτερα με τον συντονισμό και τη συνεργασία των κοινοποιημένων οργανισμών.

(54) Η εποπτεία της αγοράς αποτελεί βασικό εργαλείο για τη διασφάλιση της ορθής και ομοιόμορφης εφαρμογής της νομοθεσίας της Ένωσης. Ως εκ τούτου, είναι σκόπιμο να θεσπιστεί νομικό πλαίσιο εντός του οποίου θα είναι δυνατό να διεξάγεται με κατάλληλο τρόπο η εποπτεία της αγοράς. Οι κανόνες για την εποπτεία της ενωσιακής αγοράς και τον έλεγχο των προϊόντων που εισέρχονται σε αυτή, όπως προβλέπονται στον κανονισμό (ΕΕ) 2019/1020 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[20], εφαρμόζονται στα προϊόντα με ψηφιακά στοιχεία που καλύπτονται από τον παρόντα κανονισμό.

(55) Σύμφωνα με τον κανονισμό (ΕΕ) 2019/1020, οι αρχές εποπτείας της αγοράς διενεργούν εποπτεία της αγοράς στην επικράτεια του εν λόγω κράτους μέλους. Ο παρών κανονισμός δεν θα πρέπει να εμποδίζει τα κράτη μέλη να επιλέγουν τις αρμόδιες αρχές που θα εκτελούν αυτά τα καθήκοντα. Κάθε κράτος μέλος θα πρέπει να ορίζει μία ή περισσότερες αρχές εποπτείας της αγοράς στο έδαφός του. Τα κράτη μέλη μπορούν να επιλέξουν να ορίσουν οποιαδήποτε υφιστάμενη ή νέα αρχή που θα ενεργεί ως αρχή εποπτείας της αγοράς, συμπεριλαμβανομένων των εθνικών αρμόδιων αρχών που ορίζονται στο άρθρο [άρθρο X] της οδηγίας [οδηγία XXX/XXXX (NIS2)] ή των εντεταλμένων εθνικών αρχών πιστοποίησης της κυβερνοασφάλειας που αναφέρονται στο άρθρο 58 του κανονισμού (ΕΕ) 2019/881. Οι οικονομικοί φορείς θα πρέπει να συνεργάζονται πλήρως με τις αρχές εποπτείας της αγοράς και άλλες αρμόδιες αρχές. Κάθε κράτος μέλος θα πρέπει να ενημερώνει την Επιτροπή και τα υπόλοιπα κράτη μέλη για τις οικείες αρχές εποπτείας της αγοράς και για το πεδίο αρμοδιοτήτων καθεμίας από αυτές τις αρχές, ενώ παράλληλα θα πρέπει να διασφαλίζει τους αναγκαίους πόρους και τις δεξιότητες για την εκτέλεση των καθηκόντων εποπτείας που σχετίζονται με τον παρόντα κανονισμό. Σύμφωνα με το άρθρο 10 παράγραφοι 2 και 3 του κανονισμού (ΕΕ) 2019/1020, κάθε κράτος μέλος θα πρέπει να ορίσει ένα ενιαίο γραφείο σύνδεσης το οποίο θα πρέπει να είναι αρμόδιο, μεταξύ άλλων, για την εκπροσώπηση της συντονισμένης θέσης των αρχών εποπτείας

[20] Κανονισμός (ΕΕ) 2019/1020 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Ιουνίου 2019, για την εποπτεία της αγοράς και τη συμμόρφωση των προϊόντων και για την κατάργηση της οδηγίας 2004/42/ΕΚ και των κανονισμών (ΕΚ) αριθ. 765/2008 και (ΕΕ) αριθ. 305/2011 (ΕΕ L 169 της 25.6.2019, σ. 1).

της αγοράς και για τη συνδρομή στη συνεργασία μεταξύ των αρχών εποπτείας της αγοράς στα διάφορα κράτη μέλη.

(56) Θα πρέπει να συσταθεί ειδική ομάδα διοικητικής συνεργασίας (ADCO) για την ομοιόμορφη εφαρμογή του παρόντος κανονισμού, σύμφωνα με το άρθρο 30 παράγραφος 2 του κανονισμού (ΕΕ) 2019/1020. Η ADCO θα πρέπει να αποτελείται από εκπροσώπους των καθορισμένων αρχών εποπτείας της αγοράς και, κατά περίπτωση, εκπροσώπους των ενιαίων γραφείων σύνδεσης. Η Επιτροπή θα πρέπει να στηρίζει και να ενθαρρύνει τη συνεργασία μεταξύ των αρχών εποπτείας της αγοράς μέσω του Ενωσιακού Δικτύου Συμμόρφωσης των Προϊόντων, το οποίο έχει συσταθεί βάσει του άρθρου 29 του κανονισμού (ΕΕ) 2019/1020 και απαρτίζεται από εκπροσώπους από κάθε κράτος μέλος, συμπεριλαμβανομένου ενός εκπροσώπου κάθε ενιαίου γραφείου σύνδεσης που αναφέρεται στο άρθρο 10 του κανονισμού (ΕΕ) 2019/1020 και ενός προαιρετικού εθνικού εμπειρογνώμονα, των προέδρων των ADCO και εκπροσώπων της Επιτροπής. Η Επιτροπή θα πρέπει να συμμετέχει στις συνεδριάσεις του Δικτύου, των υποομάδων του και της αντίστοιχης ADCO. Θα πρέπει επίσης να συνδράμει το Δίκτυο, μέσω μιας εκτελεστικής γραμματείας που παρέχει τεχνική και υλικοτεχνική υποστήριξη.

(57) Προκειμένου να διασφαλιστεί η λήψη έγκαιρων, αναλογικών και αποτελεσματικών μέτρων όσον αφορά τα προϊόντα με ψηφιακά στοιχεία που παρουσιάζουν σημαντικό κίνδυνο για την κυβερνοασφάλεια, θα πρέπει να προβλεφθεί ενωσιακή διαδικασία διασφάλισης στο πλαίσιο της οποίας τα ενδιαφερόμενα μέρη θα ενημερώνονται για τα μέτρα που πρόκειται να ληφθούν όσον αφορά τα εν λόγω προϊόντα. Θα πρέπει επίσης να παρέχεται η δυνατότητα στις αρχές που είναι αρμόδιες για την εποπτεία της αγοράς, σε συνεργασία με τους σχετικούς οικονομικούς φορείς, να ενεργούν σε πρωιμότερο στάδιο, εφόσον αυτό είναι αναγκαίο. Όταν τα κράτη μέλη και η Επιτροπή συμφωνούν ως προς την αιτιολόγηση ενός μέτρου που λαμβάνεται από κράτος μέλος, δεν θα πρέπει να απαιτείται περαιτέρω ανάμειξη της Επιτροπής, εκτός αν η μη συμμόρφωση μπορεί να αποδοθεί σε ελλείψεις εναρμονισμένου προτύπου.

(58) Σε ορισμένες περιπτώσεις, ένα προϊόν με ψηφιακά στοιχεία που συμμορφώνεται με τον παρόντα κανονισμό μπορεί, ωστόσο, να εγκυμονεί σημαντικό κίνδυνο για την κυβερνοασφάλεια ή να ενέχει κίνδυνο για την υγεία ή την ασφάλεια των προσώπων, τη συμμόρφωση με τις υποχρεώσεις που απορρέουν από το ενωσιακό ή το εθνικό δίκαιο για την προστασία των θεμελιωδών δικαιωμάτων, τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα ή την εμπιστευτικότητα των υπηρεσιών που προσφέρονται με τη χρήση ηλεκτρονικού συστήματος πληροφοριών από βασικές οντότητες του τύπου που αναφέρεται στο [παράρτημα I της οδηγίας XXX/XXXX (NIS2)] ή σε άλλες πτυχές προστασίας του δημόσιου συμφέροντος. Ως εκ τούτου, είναι αναγκαίο να θεσπιστούν κανόνες που να διασφαλίζουν τον μετριασμό των εν λόγω κινδύνων. Ως εκ τούτου, οι αρχές εποπτείας της αγοράς θα πρέπει να λαμβάνουν μέτρα προκειμένου να απαιτούν από τον οικονομικό φορέα να διασφαλίσει ότι το προϊόν δεν παρουσιάζει πλέον τον εν λόγω κίνδυνο, να το ανακαλέσει ή να το αποσύρει, ανάλογα με τον κίνδυνο. Μόλις η αρχή εποπτείας της αγοράς προβεί σε περιορισμό ή απαγόρευση της ελεύθερης κυκλοφορίας ενός προϊόντος με τον τρόπο αυτόν, το κράτος μέλος θα πρέπει να κοινοποιεί χωρίς καθυστέρηση στην Επιτροπή και στα άλλα κράτη μέλη τα προσωρινά μέτρα, επισημαίνοντας τους λόγους και την αιτιολόγηση της απόφασης. Όταν η αρχή εποπτείας της αγοράς λαμβάνει τέτοια μέτρα σε σχέση με προϊόντα που παρουσιάζουν κίνδυνο, η Επιτροπή θα πρέπει να ξεκινά χωρίς καθυστέρηση διαβουλεύσεις με τα κράτη μέλη και τον σχετικό οικονομικό φορέα ή τους σχετικούς οικονομικούς φορείς και να αξιολογεί το εθνικό μέτρο. Βάσει

των αποτελεσμάτων της εν λόγω αξιολόγησης, η Επιτροπή θα πρέπει να αποφασίζει εάν το εθνικό μέτρο είναι δικαιολογημένο ή όχι. Η Επιτροπή θα πρέπει να απευθύνει την απόφασή της σε όλα τα κράτη μέλη και την ανακοινώνει αμέσως σε αυτά και στον/στους σχετικό/-ούς οικονομικό/-ούς φορέα/-είς. Εάν το μέτρο θεωρηθεί δικαιολογημένο, η Επιτροπή μπορεί επίσης να εξετάσει το ενδεχόμενο έκδοσης προτάσεων για την αναθεώρηση της αντίστοιχης ενωσιακής νομοθεσίας.

(59) Για προϊόντα με ψηφιακά στοιχεία που παρουσιάζουν σημαντικό κίνδυνο για την κυβερνοασφάλεια, και όταν υπάρχουν λόγοι να πιστεύεται ότι αυτά δεν συμμορφώνονται με τον παρόντα κανονισμό, ή για προϊόντα που συμμορφώνονται με τον παρόντα κανονισμό, αλλά παρουσιάζουν άλλους σημαντικούς κινδύνους, όπως κινδύνους για την υγεία ή την ασφάλεια των προσώπων, θεμελιώδη δικαιώματα ή την παροχή υπηρεσιών από βασικές οντότητες του τύπου που αναφέρεται στο [παράρτημα Ι της οδηγίας XXX/XXXX (NIS2)], η Επιτροπή μπορεί να ζητήσει από τον ENISA να διενεργήσει αξιολόγηση. Με βάση την εν λόγω αξιολόγηση, η Επιτροπή μπορεί να θεσπίσει, μέσω εκτελεστικών πράξεων, διορθωτικά ή περιοριστικά μέτρα σε επίπεδο Ένωσης, συμπεριλαμβανομένης της εντολής απόσυρσης από την αγορά ή της ανάκλησης των αντίστοιχων προϊόντων, εντός εύλογου χρονικού διαστήματος, ανάλογου προς τη φύση του κινδύνου. Η Επιτροπή μπορεί να κάνει χρήση της παρέμβασης αυτής μόνο σε εξαιρετικές περιστάσεις που αιτιολογούν άμεση παρέμβαση για τη διατήρηση της εύρυθμης λειτουργίας της εσωτερικής αγοράς, και μόνον εφόσον δεν έχουν ληφθεί αποτελεσματικά μέτρα από τις αρχές εποπτείας για την αντιμετώπιση της κατάστασης. Τέτοιες εξαιρετικές περιστάσεις μπορεί να είναι καταστάσεις έκτακτης ανάγκης, όταν, για παράδειγμα, ένα μη συμμορφούμενο προϊόν διατίθεται ευρέως από τον κατασκευαστή σε διάφορα κράτη μέλη, χρησιμοποιείται επίσης σε βασικούς τομείς από οντότητες που εμπίπτουν στο πεδίο εφαρμογής της [οδηγίας XXX/XXXX (NIS2)], ενώ περιέχει γνωστά τρωτά σημεία τα οποία εκμεταλλεύονται κακόβουλοι παράγοντες και για τα οποία ο κατασκευαστής δεν παρέχει διαθέσιμα λογισμικά επιδιόρθωσης. Η Επιτροπή μπορεί να παρεμβαίνει σε αυτές τις καταστάσεις έκτακτης ανάγκης μόνο για όσο διαρκούν οι εξαιρετικές περιστάσεις και εάν η μη συμμόρφωση με τον παρόντα κανονισμό ή οι σημαντικοί κίνδυνοι που παρουσιάζονται εξακολουθούν να υφίστανται.

(60) Σε περιπτώσεις που υπάρχουν ενδείξεις μη συμμόρφωσης με τον παρόντα κανονισμό σε διάφορα κράτη μέλη, οι αρχές εποπτείας της αγοράς θα πρέπει να είναι σε θέση να διεξάγουν κοινές δραστηριότητες με άλλες αρχές, με σκοπό την επαλήθευση της συμμόρφωσης και τον εντοπισμό των κινδύνων για την κυβερνοασφάλεια που ενέχουν τα προϊόντα με ψηφιακά στοιχεία.

(61) Οι ταυτόχρονες συντονισμένες δράσεις ελέγχου (στο εξής: σαρώσεις) είναι συγκεκριμένες δράσεις επιβολής από τις αρχές εποπτείας της αγοράς, οι οποίες μπορούν να ενισχύσουν περαιτέρω την ασφάλεια των προϊόντων. Πιο συγκεκριμένα, οι σαρώσεις θα πρέπει να διεξάγονται σε περιπτώσεις κατά τις οποίες τάσεις της αγοράς, καταγγελίες καταναλωτών ή άλλες ενδείξεις υποδεικνύουν ότι ορισμένες κατηγορίες προϊόντων διαπιστώνεται συχνά ότι παρουσιάζουν σοβαρούς κινδύνους για την κυβερνοασφάλεια. Ο ENISA θα πρέπει να υποβάλλει στις αρχές εποπτείας της αγοράς προτάσεις για κατηγορίες προϊόντων για τις οποίες θα μπορούσαν να οργανωθούν σαρώσεις, με βάση, μεταξύ άλλων, τις κοινοποιήσεις τρωτών σημείων των προϊόντων και συμβάντων τις οποίες λαμβάνει.

(62) Προκειμένου να διασφαλιστεί ότι το κανονιστικό πλαίσιο μπορεί να προσαρμοστεί όπου απαιτείται, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων σύμφωνα με το άρθρο 290 της Συνθήκης όσον αφορά επικαιροποιήσεις του

καταλόγου των κρίσιμων προϊόντων στο παράρτημα ΙΙΙ και τον προσδιορισμό των ορισμών των εν λόγω κατηγοριών προϊόντων. Θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων σύμφωνα με το εν λόγω άρθρο για τον προσδιορισμό των προϊόντων με ψηφιακά στοιχεία που καλύπτονται από άλλους ενωσιακούς κανόνες οι οποίοι επιτυγχάνουν το ίδιο επίπεδο προστασίας με τον παρόντα κανονισμό, όπου θα προσδιορίζεται κατά πόσον θα ήταν αναγκαίος ο περιορισμός ή η εξαίρεση από το πεδίο εφαρμογής του παρόντος κανονισμού, καθώς και το πεδίο εφαρμογής του εν λόγω περιορισμού, κατά περίπτωση. Θα πρέπει επίσης να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων σύμφωνα με το εν λόγω άρθρο όσον αφορά τη δυνητική εντολή πιστοποίησης ορισμένων εξαιρετικά κρίσιμων προϊόντων με ψηφιακά στοιχεία με βάση τα κριτήρια κρισιμότητας που καθορίζονται στον παρόντα κανονισμό, καθώς και τον προσδιορισμό του ελάχιστου περιεχομένου της δήλωσης συμμόρφωσης ΕΕ και τη συμπλήρωση των στοιχείων που πρέπει να περιλαμβάνονται στον τεχνικό φάκελο. Είναι ιδιαίτερα σημαντικό η Επιτροπή να διεξάγει, κατά τις προπαρασκευαστικές της εργασίες, τις κατάλληλες διαβουλεύσεις, μεταξύ άλλων σε επίπεδο εμπειρογνωμόνων, και οι διαβουλεύσεις αυτές να πραγματοποιούνται σύμφωνα με τις αρχές που ορίζονται στη διοργανική συμφωνία της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου[21]. Πιο συγκεκριμένα, προκειμένου να εξασφαλιστεί η ίση συμμετοχή στην προετοιμασία των κατ' εξουσιοδότηση πράξεων, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο λαμβάνουν όλα τα έγγραφα κατά τον ίδιο χρόνο με τους εμπειρογνώμονες των κρατών μελών, και οι εμπειρογνώμονές τους έχουν συστηματικά πρόσβαση στις συνεδριάσεις των ομάδων εμπειρογνωμόνων της Επιτροπής που ασχολούνται με την προετοιμασία κατ' εξουσιοδότηση πράξεων.

(63) Προκειμένου να διασφαλιστούν ενιαίες προϋποθέσεις για την εφαρμογή του παρόντος κανονισμού, θα πρέπει να ανατεθούν στην Επιτροπή εκτελεστικές αρμοδιότητες, με τους εξής σκοπούς: τον προσδιορισμό του μορφοτύπου και των στοιχείων του καταλόγου υλικών του λογισμικού, τον περαιτέρω προσδιορισμό του είδους των πληροφοριών, του μορφοτύπου και της διαδικασίας των κοινοποιήσεων σχετικά με τρωτά σημεία που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και συμβάντα που υποβάλλονται στον ENISA από τους κατασκευαστές, τον προσδιορισμό των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας που εγκρίνονται σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 και μπορούν να χρησιμοποιηθούν για την απόδειξη της συμμόρφωσης με τις ουσιώδεις απαιτήσεις ή μέρη αυτών, όπως ορίζεται στο παράρτημα Ι του παρόντος κανονισμού, τη θέσπιση κοινών προδιαγραφών όσον αφορά τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα Ι, τον καθορισμό τεχνικών προδιαγραφών για εικονογράμματα ή άλλα σήματα που σχετίζονται με την ασφάλεια των προϊόντων με ψηφιακά στοιχεία, καθώς και μηχανισμών για την προώθηση της χρήσης τους, τη λήψη αποφάσεων σχετικά με διορθωτικά ή περιοριστικά μέτρα σε επίπεδο Ένωσης σε εξαιρετικές περιστάσεις που αιτιολογούν άμεση παρέμβαση για τη διατήρηση της εύρυθμης λειτουργίας της εσωτερικής αγοράς. Οι εν λόγω αρμοδιότητες θα πρέπει να ασκούνται σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 182/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[22].

---

21 ΕΕ L 123 της 12.5.2016, σ. 1.

22 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).

(64) Για να διασφαλιστεί η αξιόπιστη και εποικοδομητική συνεργασία των αρχών εποπτείας της αγοράς σε ενωσιακό και εθνικό επίπεδο, όλα τα μέρη που συμμετέχουν στην εφαρμογή του παρόντος κανονισμού θα πρέπει να τηρούν την εμπιστευτικότητα των πληροφοριών και των δεδομένων που λαμβάνονται κατά την εκτέλεση των καθηκόντων τους.

(65) Προκειμένου να διασφαλιστεί η αποτελεσματική επιβολή των υποχρεώσεων που ορίζονται στον παρόντα κανονισμό, κάθε αρχή εποπτείας της αγοράς θα πρέπει να έχει την εξουσία να επιβάλλει ή να ζητεί την επιβολή διοικητικών προστίμων. Ως εκ τούτου, θα πρέπει να καθοριστούν ανώτατα επίπεδα διοικητικών προστίμων που θα προβλέπονται στην εθνική νομοθεσία σε περίπτωση μη συμμόρφωσης με τις υποχρεώσεις που ορίζονται στον παρόντα κανονισμό. Κατά τη λήψη απόφασης σχετικά με το ύψος του διοικητικού προστίμου σε κάθε μεμονωμένη περίπτωση, θα πρέπει να λαμβάνονται υπόψη όλες οι σχετικές περιστάσεις της συγκεκριμένης περίπτωσης και, κατ' ελάχιστον, εκείνες που καθορίζονται ρητά στον παρόντα κανονισμό, συμπεριλαμβανομένου του κατά πόσον έχουν ήδη επιβληθεί διοικητικά πρόστιμα από άλλες αρχές εποπτείας της αγοράς στην ίδια επιχείρηση για παρόμοιες παραβάσεις. Οι περιστάσεις αυτές μπορεί να είναι επιβαρυντικές, σε περιπτώσεις κατά τις οποίες η παράβαση από την ίδια επιχείρηση συνεχίζεται στο έδαφος άλλων κρατών μελών, πέραν εκείνου όπου έχει ήδη επιβληθεί διοικητικό πρόστιμο, ή ελαφρυντικές, ώστε να διασφαλίζεται ότι οποιοδήποτε άλλο διοικητικό πρόστιμο που λαμβάνεται υπόψη από άλλη αρχή εποπτείας της αγοράς για τον ίδιο οικονομικό φορέα ή για τον ίδιο τύπο παράβασης θα πρέπει ήδη να λαμβάνει υπόψη, μαζί με άλλες σχετικές ειδικές περιστάσεις, την ποινή και το ύψος της ποινής που επιβάλλεται σε άλλα κράτη μέλη. Σε όλες αυτές τις περιπτώσεις, το σωρευτικό διοικητικό πρόστιμο που θα μπορούσε να επιβληθεί από τις αρχές εποπτείας της αγοράς διαφόρων κρατών μελών στον ίδιο οικονομικό φορέα για τον ίδιο τύπο παράβασης θα πρέπει να διασφαλίζει την τήρηση της αρχής της αναλογικότητας.

(66) Σε περίπτωση που τα διοικητικά πρόστιμα επιβάλλονται σε πρόσωπα που δεν είναι επιχειρήσεις, η αρμόδια 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.

(67) Η ΕΕ, στο πλαίσιο των σχέσεών της με τις τρίτες χώρες, επιδιώκει να προωθήσει το διεθνές εμπόριο των ρυθμιζόμενων προϊόντων. Μπορεί να εφαρμοστεί ευρύ φάσμα μέτρων για τη διευκόλυνση του εμπορίου, συμπεριλαμβανομένων διαφόρων νομικών πράξεων, όπως οι διμερείς (διακυβερνητικές) συμφωνίες αμοιβαίας αναγνώρισης (ΣΑΑ) για την αξιολόγηση της συμμόρφωσης και τη σήμανση των ρυθμιζόμενων προϊόντων. Οι ΣΑΑ συνάπτονται μεταξύ της Ένωσης και των τρίτων χωρών που διαθέτουν συγκρίσιμο επίπεδο τεχνικής ανάπτυξης και ακολουθούν συμβατή προσέγγιση όσον αφορά την αξιολόγηση της συμμόρφωσης. Οι εν λόγω συμφωνίες βασίζονται στην αμοιβαία αποδοχή των πιστοποιητικών, των σημάτων συμμόρφωσης και των εκθέσεων δοκιμών που εκδίδουν οι οργανισμοί αξιολόγησης της συμμόρφωσης του ενός μέρους σύμφωνα με τη νομοθεσία του άλλου μέρους. Επί του παρόντος, υπάρχουν ΣΑΑ για αρκετές χώρες. Οι συμφωνίες αφορούν συγκεκριμένους τομείς που ενδέχεται να διαφέρουν από χώρα σε χώρα. Για την περαιτέρω διευκόλυνση του εμπορίου και καθώς αναγνωρίζεται ότι οι αλυσίδες εφοδιασμού προϊόντων με ψηφιακά στοιχεία είναι παγκόσμιες, μπορούν να συνάπτονται ΣΑΑ σχετικά με την αξιολόγηση της συμμόρφωσης για προϊόντα που ρυθμίζονται βάσει

του παρόντος κανονισμού από την Ένωση σύμφωνα με το άρθρο 218 της ΣΛΕΕ. Η συνεργασία με τις χώρες εταίρους είναι επίσης σημαντική, προκειμένου να ενισχυθεί η κυβερνοανθεκτικότητα σε παγκόσμιο επίπεδο, καθώς μακροπρόθεσμα αυτό θα συμβάλει σε ένα ενισχυμένο πλαίσιο κυβερνοασφάλειας τόσο εντός όσο και εκτός της ΕΕ.

(68) Η Επιτροπή θα πρέπει να επανεξετάζει περιοδικά τον παρόντα κανονισμό, σε διαβούλευση με τα ενδιαφερόμενα μέρη, ιδίως προκειμένου να εξακριβώνεται αν απαιτείται τροποποίησή του υπό το πρίσμα της μεταβολής συνθηκών στην κοινωνία, την πολιτική, την τεχνολογία ή τις αγορές.

(69) Θα πρέπει να δοθεί επαρκής χρόνος στους οικονομικούς φορείς ώστε να προσαρμοστούν στις απαιτήσεις του παρόντος κανονισμού. Ο παρών κανονισμός θα πρέπει να εφαρμοστεί [24 μήνες] από την έναρξη ισχύος του, με εξαίρεση τις υποχρεώσεις υποβολής εκθέσεων σχετικά με τρωτά σημεία που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και συμβάντα, οι οποίες θα πρέπει να εφαρμοστούν [12 μήνες] από την έναρξη ισχύος του παρόντος κανονισμού.

(70) Δεδομένου ότι ο στόχος του παρόντος κανονισμού δεν μπορεί να επιτευχθεί επαρκώς από τα κράτη μέλη και συνεπώς, λόγω των επιπτώσεων της δράσης, μπορεί όμως να επιτευχθεί καλύτερα σε επίπεδο Ένωσης, η Ένωση δύναται να θεσπίζει μέτρα σύμφωνα με την αρχή της επικουρικότητας, όπως ορίζεται στο άρθρο 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Σύμφωνα με την αρχή της αναλογικότητας, όπως ορίζεται στο ίδιο άρθρο, ο παρών κανονισμός δεν υπερβαίνει τα αναγκαία για την επίτευξη του στόχου αυτού.

(71) Ζητήθηκε, σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου, η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων και του Συμβουλίου[23], ο οποίος γνωμοδότησε στις […],

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

## ΚΕΦΑΛΑΙΟ Ι

## ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

### *Άρθρο 1*

### *Αντικείμενο*

Ο παρών κανονισμός καθορίζει:

α) κανόνες για τη διάθεση προϊόντων με ψηφιακά στοιχεία στην αγορά, ώστε να διασφαλίζεται η κυβερνοασφάλεια των εν λόγω προϊόντων·

β) ουσιώδεις απαιτήσεις για τον σχεδιασμό, την ανάπτυξη και την παραγωγή προϊόντων με ψηφιακά στοιχεία και υποχρεώσεις για τους οικονομικούς φορείς σε σχέση με τα εν λόγω προϊόντα όσον αφορά την κυβερνοασφάλεια·

[23] Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39).

γ) ουσιώδεις απαιτήσεις για τις διαδικασίες χειρισμού τρωτών σημείων που εφαρμόζουν οι κατασκευαστές με σκοπό τη διασφάλιση της κυβερνοασφάλειας προϊόντων με ψηφιακά στοιχεία καθ' όλη τη διάρκεια του κύκλου ζωής, καθώς και υποχρεώσεις για τους οικονομικούς φορείς σε σχέση με τις εν λόγω διαδικασίες·

δ) κανόνες για την εποπτεία της αγοράς και την επιβολή των προαναφερθέντων κανόνων και απαιτήσεων.

*Άρθρο 2*

*Πεδίο εφαρμογής*

1. Ο παρών κανονισμός εφαρμόζεται σε προϊόντα με ψηφιακά στοιχεία των οποίων η προβλεπόμενη ή ευλόγως προβλέψιμη χρήση περιλαμβάνει άμεση ή έμμεση λογική ή φυσική σύνδεση δεδομένων με συσκευή ή δίκτυο.

2. Ο παρών κανονισμός δεν εφαρμόζεται σε προϊόντα με ψηφιακά στοιχεία στα οποία εφαρμόζονται οι ακόλουθες πράξεις της Ένωσης:

   α) ο κανονισμός (ΕΕ) 2017/745·

   β) ο κανονισμός (ΕΕ) 2017/746·

   γ) ο κανονισμός (ΕΕ) 2019/2144.

3. Ο παρών κανονισμός δεν εφαρμόζεται σε προϊόντα με ψηφιακά στοιχεία που έχουν πιστοποιηθεί σύμφωνα με τον κανονισμό (ΕΕ) 2018/1139.

4. Η εφαρμογή του παρόντος κανονισμού σε προϊόντα με ψηφιακά στοιχεία που καλύπτονται από άλλους ενωσιακούς κανόνες οι οποίοι καθορίζουν απαιτήσεις για την αντιμετώπιση του συνόλου ή μέρους των κινδύνων που καλύπτονται από τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα Ι μπορεί να περιοριστεί ή να αποκλειστεί, όταν:

   α) ο εν λόγω περιορισμός ή αποκλεισμός συνάδει με το συνολικό κανονιστικό πλαίσιο που ισχύει για τα εν λόγω προϊόντα· και

   β) οι τομεακοί κανόνες επιτυγχάνουν το ίδιο επίπεδο προστασίας με εκείνο που προβλέπεται στον παρόντα κανονισμό.

   Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 50 για την τροποποίηση του παρόντος κανονισμού, όπου θα προσδιορίζεται αν ο εν λόγω περιορισμός ή αποκλεισμός είναι αναγκαίος, τα σχετικά προϊόντα και οι κανόνες, καθώς και το πεδίο εφαρμογής του περιορισμού, κατά περίπτωση.

5. Ο παρών κανονισμός δεν εφαρμόζεται σε προϊόντα με ψηφιακά στοιχεία που αναπτύσσονται αποκλειστικά για σκοπούς εθνικής ασφάλειας ή στρατιωτικούς σκοπούς ή σε προϊόντα ειδικά σχεδιασμένα για την επεξεργασία διαβαθμισμένων πληροφοριών.

*Άρθρο 3*

*Ορισμοί*

Για τους σκοπούς του παρόντος κανονισμού, ισχύουν οι ακόλουθοι ορισμοί:

1) «προϊόν με ψηφιακά στοιχεία»: κάθε προϊόν λογισμικού ή υλισμικού και οι οικείες λύσεις εξ αποστάσεως επεξεργασίας δεδομένων, συμπεριλαμβανομένων των

συνιστωσών λογισμικού ή υλισμικού που πρόκειται να διατεθούν στην αγορά χωριστά·

2) «εξ αποστάσεως επεξεργασία δεδομένων»: κάθε εξ αποστάσεως επεξεργασία δεδομένων για την οποία το λογισμικό έχει σχεδιαστεί και αναπτυχθεί από τον κατασκευαστή ή υπό την ευθύνη του κατασκευαστή και η απουσία της οποίας θα εμπόδιζε το προϊόν με ψηφιακά στοιχεία να εκτελέσει κάποια από τις λειτουργίες του·

3) «κρίσιμο προϊόν με ψηφιακά στοιχεία»: προϊόν με ψηφιακά στοιχεία που παρουσιάζει κίνδυνο για την κυβερνοασφάλεια σύμφωνα με τα κριτήρια που ορίζονται στο άρθρο 6 παράγραφος 2 και του οποίου η βασική λειτουργικότητα ορίζεται στο παράρτημα III·

4) «εξαιρετικά κρίσιμο προϊόν με ψηφιακά στοιχεία»: προϊόν με ψηφιακά στοιχεία που παρουσιάζει κίνδυνο για την κυβερνοασφάλεια σύμφωνα με τα κριτήρια που ορίζονται στο άρθρο 6 παράγραφος 5·

5) «επιχειρησιακή τεχνολογία»: προγραμματιζόμενα ψηφιακά συστήματα ή συσκευές που αλληλεπιδρούν με το φυσικό περιβάλλον ή διαχειρίζονται συσκευές που αλληλεπιδρούν με το φυσικό περιβάλλον·

6) «λογισμικό»: το μέρος ηλεκτρονικού συστήματος πληροφοριών που αποτελείται από κώδικα υπολογιστή·

7) «υλισμικό»: φυσικό ηλεκτρονικό σύστημα πληροφοριών, ή μέρη αυτού, ικανό να επεξεργάζεται, να αποθηκεύει ή να διαβιβάζει ψηφιακά δεδομένα·

8) «συνιστώσα»: λογισμικό ή υλισμικό που προορίζεται για ενσωμάτωση σε ηλεκτρονικό σύστημα πληροφοριών·

9) «ηλεκτρονικό σύστημα πληροφοριών»: κάθε σύστημα, συμπεριλαμβανομένου ηλεκτρικού ή ηλεκτρονικού εξοπλισμού, ικανό να επεξεργάζεται, να αποθηκεύει ή να διαβιβάζει ψηφιακά δεδομένα·

10) «λογική σύνδεση»: εικονική αναπαράσταση σύνδεσης δεδομένων που υλοποιείται μέσω διεπαφής λογισμικού·

11) «φυσική σύνδεση»: κάθε σύνδεση μεταξύ ηλεκτρονικών συστημάτων πληροφοριών ή συνιστωσών που υλοποιείται με τη χρήση φυσικών μέσων, μεταξύ άλλων μέσω ηλεκτρικών ή μηχανικών διεπαφών, καλωδίων ή ραδιοκυμάτων·

12) «έμμεση σύνδεση»: σύνδεση με συσκευή ή δίκτυο, η οποία δεν πραγματοποιείται άμεσα, αλλά ως μέρος ενός ευρύτερου συστήματος που μπορεί να συνδεθεί απευθείας με την εν λόγω συσκευή ή το δίκτυο·

13) «προνόμιο»: δικαίωμα πρόσβασης που χορηγείται σε συγκεκριμένους χρήστες ή προγράμματα για την εκτέλεση λειτουργιών σχετικών με την ασφάλεια στο πλαίσιο ηλεκτρονικού συστήματος πληροφοριών·

14) «αυξημένο προνόμιο»: δικαίωμα πρόσβασης που χορηγείται σε συγκεκριμένους χρήστες ή προγράμματα για την εκτέλεση διευρυμένου συνόλου λειτουργιών σχετικών με την ασφάλεια στο πλαίσιο ηλεκτρονικού συστήματος πληροφοριών, το οποίο, σε περίπτωση κατάχρησης ή υπονόμευσης, θα μπορούσε να επιτρέψει σε κακόβουλο παράγοντα να αποκτήσει ευρύτερη πρόσβαση στους πόρους συστήματος ή οργανισμού·

15) «τελικό σημείο»: κάθε συσκευή που συνδέεται σε δίκτυο και χρησιμεύει ως σημείο εισόδου στο εν λόγω δίκτυο·

16) «δικτυακοί ή υπολογιστικοί πόροι»: λειτουργίες δεδομένων ή υλισμικού ή λογισμικού που είναι προσβάσιμες είτε τοπικά είτε μέσω δικτύου ή άλλης συνδεδεμένης συσκευής·

17) «οικονομικός φορέας»: ο κατασκευαστής, ο εξουσιοδοτημένος αντιπρόσωπος, ο εισαγωγέας, ο διανομέας ή κάθε άλλο φυσικό ή νομικό πρόσωπο που υπόκειται στις υποχρεώσεις που καθορίζονται στον παρόντα κανονισμό·

18) «κατασκευαστής»: κάθε φυσικό ή νομικό πρόσωπο που αναπτύσσει ή κατασκευάζει προϊόντα με ψηφιακά στοιχεία ή αναθέτει σε άλλους τον σχεδιασμό, την ανάπτυξη ή την κατασκευή προϊόντων με ψηφιακά στοιχεία και τα διαθέτει στην αγορά υπό την επωνυμία ή το εμπορικό σήμα του, είτε έναντι αντιτίμου είτε δωρεάν·

19) «εξουσιοδοτημένος αντιπρόσωπος»: κάθε φυσικό ή νομικό πρόσωπο, εγκατεστημένο στην Ένωση, που έχει λάβει γραπτή εντολή από τον κατασκευαστή να ενεργεί για λογαριασμό του για την εκτέλεση συγκεκριμένων καθηκόντων·

20) «εισαγωγέας»: κάθε φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ένωση που διαθέτει στην αγορά προϊόν με ψηφιακά στοιχεία το οποίο φέρει την επωνυμία ή το εμπορικό σήμα φυσικού ή νομικού προσώπου εγκατεστημένου εκτός της Ένωσης·

21) «διανομέας»: κάθε φυσικό ή νομικό πρόσωπο στην αλυσίδα εφοδιασμού, πλην του κατασκευαστή ή του εισαγωγέα, το οποίο θέτει προϊόν με ψηφιακά στοιχεία σε κυκλοφορία στην αγορά της Ένωσης, χωρίς να επηρεάζει τις ιδιότητές του·

22) «διάθεση στην αγορά»: η πρώτη φορά κατά την οποία ένα προϊόν με ψηφιακά στοιχεία καθίσταται διαθέσιμο στην αγορά της Ένωσης·

23) «διαθεσιμότητα στην αγορά»: κάθε προσφορά προϊόντος με ψηφιακά στοιχεία για διανομή ή χρήση στην ενωσιακή αγορά στο πλαίσιο εμπορικής δραστηριότητας, είτε έναντι αντιτίμου είτε δωρεάν·

24) «προβλεπόμενος σκοπός»: η χρήση για την οποία προορίζει το προϊόν με ψηφιακά στοιχεία ο κατασκευαστής, συμπεριλαμβανομένων του ειδικού πλαισίου και των όρων χρήσης, όπως προσδιορίζονται στις πληροφορίες που παρέχει ο κατασκευαστής στις οδηγίες χρήσης, σε διαφημιστικό υλικό ή στο υλικό πωλήσεων και σε δηλώσεις, καθώς και στον τεχνικό φάκελο·

25) «ευλόγως προβλέψιμη χρήση»: η χρήση που δεν είναι απαραίτητα ο επιδιωκόμενος σκοπός που παρέχεται από τον κατασκευαστή στις οδηγίες χρήσης, στο διαφημιστικό υλικό ή στο υλικό πωλήσεων και στις δηλώσεις, καθώς και στον τεχνικό φάκελο, αλλά η οποία είναι πιθανόν να προκύψει από ευλόγως προβλέψιμη ανθρώπινη συμπεριφορά ή τεχνικές εργασίες ή αλληλεπιδράσεις·

26) «ευλόγως προβλέψιμη κακή χρήση»: η χρήση προϊόντος με ψηφιακά στοιχεία κατά τρόπο που δεν συνάδει με τον επιδιωκόμενο σκοπό του, αλλά μπορεί να προκύψει από ευλόγως προβλέψιμη ανθρώπινη συμπεριφορά ή αλληλεπίδραση με άλλα συστήματα·

27) «κοινοποιούσα αρχή»: η εθνική αρχή που είναι υπεύθυνη για τον καθορισμό και τη διεξαγωγή των αναγκαίων διαδικασιών αξιολόγησης, ορισμού και κοινοποίησης των οργανισμών αξιολόγησης της συμμόρφωσης, καθώς και για την παρακολούθησή τους·

28) «αξιολόγηση της συμμόρφωσης»: η διαδικασία με την οποία επαληθεύεται κατά πόσον πληρούνται οι απαιτήσεις που ορίζονται στο παράρτημα Ι·

29) «οργανισμός αξιολόγησης της συμμόρφωσης»: οργανισμός που ορίζεται στο άρθρο 2 σημείο 13 του κανονισμού (ΕΕ) αριθ. 765/2008·

30) «κοινοποιημένος οργανισμός»: οργανισμός αξιολόγησης της συμμόρφωσης που ορίζεται σύμφωνα με το άρθρο 33 του παρόντος κανονισμό και άλλη σχετική ενωσιακή νομοθεσία εναρμόνισης·

31) «ουσιαστική τροποποίηση»: αλλαγή στο προϊόν με ψηφιακά στοιχεία μετά τη διάθεσή του στην αγορά, η οποία επηρεάζει τη συμμόρφωση του προϊόντος με ψηφιακά στοιχεία προς τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα Ι τμήμα 1 ή έχει ως αποτέλεσμα τροποποίηση της προβλεπόμενης χρήσης για την οποία έχει αξιολογηθεί το προϊόν με ψηφιακά στοιχεία·

32) «σήμανση CE»: σήμανση με την οποία ο κατασκευαστής δηλώνει ότι ένα προϊόν με ψηφιακά στοιχεία και οι διαδικασίες που εφαρμόζει ο κατασκευαστής συμμορφώνονται με τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα Ι και άλλες εφαρμοστέες νομοθετικές πράξεις της Ένωσης για την εναρμόνιση των όρων εμπορίας των προϊόντων (στο εξής: ενωσιακή νομοθεσία εναρμόνισης), οι οποίες προβλέπουν την τοποθέτηση της σήμανσης αυτής·

33) «αρχή εποπτείας της αγοράς»: η αρχή που ορίζεται στο άρθρο 3 σημείο 4 του κανονισμού (ΕΕ) 2019/1020·

34) «εναρμονισμένο πρότυπο»: εναρμονισμένο πρότυπο, όπως ορίζεται στο άρθρο 2 σημείο 1 στοιχείο γ) του κανονισμού (ΕΕ) αριθ. 1025/2012·

35) «κίνδυνος για την κυβερνοασφάλεια»: κίνδυνος, όπως ορίζεται στο άρθρο [άρθρο X] της οδηγίας [οδηγία XXX/XXXX (NIS2)]·

36) «σημαντικός κίνδυνος για την κυβερνοασφάλεια»: κίνδυνος για την κυβερνοασφάλεια ο οποίος, βάσει των τεχνικών χαρακτηριστικών του, μπορεί να θεωρηθεί ότι έχει υψηλή πιθανότητα συμβάντος που θα μπορούσε να οδηγήσει σε σοβαρό αρνητικό αντίκτυπο, μεταξύ άλλων προκαλώντας σημαντική υλική ή μη υλική ζημία ή διατάραξη·

37) «κατάλογος υλικών λογισμικού»: επίσημο αρχείο που περιέχει λεπτομέρειες και σχέσεις αλυσίδας εφοδιασμού των συνιστωσών που περιλαμβάνονται στα στοιχεία λογισμικού ενός προϊόντος με ψηφιακά στοιχεία·

38) «τρωτό σημείο»: τρωτό σημείο, όπως ορίζεται στο άρθρο [άρθρο X] της οδηγίας [οδηγία XXX/XXXX (NIS2)]·

39) «τρωτό σημείο που αποτελεί αντικείμενο ενεργού εκμετάλλευσης»: τρωτό σημείο για το οποίο υπάρχουν αξιόπιστα στοιχεία που αποδεικνύουν ότι πραγματοποιήθηκε εκτέλεση κακόβουλου κώδικα από παράγοντα σε σύστημα χωρίς την άδεια του ιδιοκτήτη του συστήματος·

40) «δεδομένα προσωπικού χαρακτήρα»: δεδομένα, όπως ορίζονται στο άρθρο 4 παράγραφος 1 του κανονισμού (ΕΕ) 2016/679.

*Άρθρο 4*

*Ελεύθερη κυκλοφορία*

1. Τα κράτη μέλη δεν εμποδίζουν, όσον αφορά τα ζητήματα που καλύπτονται από τον παρόντα κανονισμό, τη διαθεσιμότητα στην αγορά προϊόντων με ψηφιακά στοιχεία που συμμορφώνονται με τον παρόντα κανονισμό.

2. Σε εμπορικές εκθέσεις, παρουσιάσεις και επιδείξεις ή παρόμοιες εκδηλώσεις, τα κράτη μέλη δεν εμποδίζουν την παρουσίαση και τη χρήση προϊόντος με ψηφιακά στοιχεία που δεν συμμορφώνεται με τον παρόντα κανονισμό.

3. Τα κράτη μέλη δεν εμποδίζουν τη διαθεσιμότητα ημιτελούς λογισμικού που δεν συμμορφώνεται με τον παρόντα κανονισμό, υπό την προϋπόθεση ότι το λογισμικό διατίθεται μόνο για περιορισμένο χρονικό διάστημα που απαιτείται για σκοπούς διεξαγωγής δοκιμών και ότι δηλώνεται ρητά με ορατό σήμα ότι το λογισμικό δεν συμμορφώνεται με τον παρόντα κανονισμό και δεν είναι διαθέσιμο στην αγορά για άλλους σκοπούς πέραν της δοκιμής.

*Άρθρο 5*

*Απαιτήσεις για προϊόντα με ψηφιακά στοιχεία*

Τα προϊόντα με ψηφιακά στοιχεία καθίστανται διαθέσιμα στην αγορά μόνον εφόσον:

1) πληρούν τις ουσιώδεις απαιτήσεις που ορίζονται στο τμήμα 1 του παραρτήματος I, υπό την προϋπόθεση ότι έχουν εγκατασταθεί, συντηρούνται και χρησιμοποιούνται ορθά για τον επιδιωκόμενο σκοπό ή υπό εύλογα προβλέψιμες συνθήκες και, κατά περίπτωση, επικαιροποιούνται, και

2) οι διαδικασίες που εφαρμόζει ο κατασκευαστής συμμορφώνονται με τις ουσιώδεις απαιτήσεις που ορίζονται στο τμήμα 2 του παραρτήματος I.

*Άρθρο 6*

*Κρίσιμα προϊόντα με ψηφιακά στοιχεία*

1. Τα προϊόντα με ψηφιακά στοιχεία που ανήκουν σε κατηγορία που περιλαμβάνεται στο παράρτημα III θεωρούνται κρίσιμα προϊόντα με ψηφιακά στοιχεία. Τα προϊόντα που έχουν τη βασική λειτουργικότητα κατηγορίας που περιλαμβάνεται στο παράρτημα III του παρόντος κανονισμού θεωρείται ότι εμπίπτουν στην εν λόγω κατηγορία. Οι κατηγορίες κρίσιμων προϊόντων με ψηφιακά στοιχεία υποδιαιρούνται στην κατηγορία I και την κατηγορία II, όπως ορίζεται στο παράρτημα III, οι οποίες αντικατοπτρίζουν το επίπεδο κινδύνου που σχετίζεται με τα εν λόγω προϊόντα όσον αφορά την κυβερνοασφάλεια.

2. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 50 για την τροποποίηση του παραρτήματος III με την προσθήκη νέας κατηγορίας στον κατάλογο κατηγοριών κρίσιμων προϊόντων με ψηφιακά στοιχεία ή με την αφαίρεση υπάρχουσας κατηγορίας από τον εν λόγω κατάλογο. Κατά την αξιολόγηση της ανάγκης τροποποίησης του καταλόγου του παραρτήματος III, η Επιτροπή λαμβάνει υπόψη το επίπεδο κινδύνου που σχετίζεται με την κατηγορία προϊόντων με ψηφιακά στοιχεία όσον αφορά την κυβερνοασφάλεια. Κατά τον καθορισμό του επιπέδου κινδύνου για την κυβερνοασφάλεια, λαμβάνονται υπόψη ένα ή περισσότερα από τα ακόλουθα κριτήρια:

   α) η λειτουργικότητα του προϊόντος με ψηφιακά στοιχεία όσον αφορά την κυβερνοασφάλεια και κατά πόσον το προϊόν με ψηφιακά στοιχεία έχει τουλάχιστον ένα από τα ακόλουθα χαρακτηριστικά:

i) έχει σχεδιαστεί για να λειτουργεί με αυξημένο προνόμιο ή να διαχειρίζεται προνόμια·

ii) έχει άμεση ή προνομιακή πρόσβαση σε δικτυακούς ή υπολογιστικούς πόρους·

iii) έχει σχεδιαστεί για τον έλεγχο της πρόσβασης σε δεδομένα ή επιχειρησιακή τεχνολογία·

iv) εκτελεί λειτουργία ζωτικής σημασίας για την εμπιστοσύνη, ιδίως λειτουργίες ασφάλειας όπως ο έλεγχος δικτύου, η ασφάλεια των τελικών σημείων και η προστασία του δικτύου.

β) η προβλεπόμενη χρήση σε ευαίσθητα περιβάλλοντα, μεταξύ άλλων σε βιομηχανικά περιβάλλοντα ή από βασικές οντότητες του τύπου που αναφέρεται στο παράρτημα [παράρτημα I] της οδηγίας [οδηγία XXX/XXXX (NIS2)]·

γ) η προβλεπόμενη χρήση για την εκτέλεση κρίσιμων ή ευαίσθητων λειτουργιών, όπως η επεξεργασία δεδομένων προσωπικού χαρακτήρα·

δ) η πιθανή έκταση των δυσμενών επιπτώσεων, ιδιαίτερα όσον αφορά την ένταση και την ικανότητά τους να επηρεάζουν πλήθος προσώπων·

ε) ο βαθμός στον οποίο η χρήση προϊόντων με ψηφιακά στοιχεία έχει ήδη προκαλέσει υλική ή μη υλική ζημία ή διατάραξη ή έχει προκαλέσει σημαντικές ανησυχίες σε σχέση με την επέλευση δυσμενών επιπτώσεων.

3. Ανατίθεται στην Επιτροπή η εξουσία να εκδώσει κατ' εξουσιοδότηση πράξη σύμφωνα με το άρθρο 50 για τη συμπλήρωση του παρόντος κανονισμού με τον προσδιορισμό των ορισμών των κατηγοριών προϊόντων της κατηγορίας I και της κατηγορίας II, όπως παρατίθενται στο παράρτημα III. Η κατ' εξουσιοδότηση πράξη εκδίδεται [εντός 12 μηνών από την έναρξη ισχύος του παρόντος κανονισμού].

4. Τα κρίσιμα προϊόντα με ψηφιακά στοιχεία υπόκεινται στις διαδικασίες αξιολόγησης της συμμόρφωσης που αναφέρονται στο άρθρο 24 παράγραφοι 2 και 3.

5. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 50 για τη συμπλήρωση του παρόντος κανονισμού με τον προσδιορισμό κατηγοριών εξαιρετικά κρίσιμων προϊόντων με ψηφιακά στοιχεία για τα οποία οι κατασκευαστές υποχρεούνται να λάβουν ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας στο πλαίσιο ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 για να αποδείξουν τη συμμόρφωση με τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα I, ή μέρη αυτών. Κατά τον καθορισμό των εν λόγω κατηγοριών εξαιρετικά κρίσιμων προϊόντων με ψηφιακά στοιχεία, η Επιτροπή λαμβάνει υπόψη το επίπεδο κινδύνου που σχετίζεται με την κατηγορία προϊόντων με ψηφιακά στοιχεία όσον αφορά την κυβερνοασφάλεια, υπό το πρίσμα ενός ή περισσότερων από τα κριτήρια που απαριθμούνται στην παράγραφο 2, καθώς και ενόψει της αξιολόγησης του κατά πόσον η εν λόγω κατηγορία προϊόντων:

α) χρησιμοποιείται από τις βασικές οντότητες του τύπου που αναφέρεται στο παράρτημα [παράρτημα I] της οδηγίας [οδηγία XXX/XXXX (NIS2)] ή στην οποία βασίζονται οι εν λόγω οντότητες, ή θα έχει δυνητική μελλοντική σημασία για τις δραστηριότητες των εν λόγω οντοτήτων· ή

β) αφορά την ανθεκτικότητα της συνολικής αλυσίδας εφοδιασμού προϊόντων με ψηφιακά στοιχεία έναντι συμβάντων που προκαλούν διαταραχές.

*Άρθρο 7*

*Γενική ασφάλεια των προϊόντων*

Κατά παρέκκλιση από το άρθρο 2 παράγραφος 1 τρίτο εδάφιο στοιχείο β) του κανονισμού [κανονισμός για τη γενική ασφάλεια των προϊόντων], όταν προϊόντα με ψηφιακά στοιχεία δεν υπόκεινται σε ειδικές απαιτήσεις που καθορίζονται σε άλλη ενωσιακή νομοθεσία εναρμόνισης κατά την έννοια του [άρθρου 3 σημείο 25 του κανονισμού για τη γενική ασφάλεια των προϊόντων], στα εν λόγω προϊόντα εφαρμόζονται το κεφάλαιο III τμήμα 1, τα κεφάλαια V και VII και τα κεφάλαια IX έως XI του κανονισμού [κανονισμός για τη γενική ασφάλεια των προϊόντων] όσον αφορά τους κινδύνους για την ασφάλεια που δεν καλύπτονται από τον παρόντα κανονισμό.

*Άρθρο 8*

*Συστήματα ΤΝ υψηλού κινδύνου*

1. Τα προϊόντα με ψηφιακά στοιχεία που ταξινομούνται ως συστήματα ΤΝ υψηλού κινδύνου σύμφωνα με το άρθρο [άρθρο 6] του κανονισμού [κανονισμός για την ΤΝ], τα οποία εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού και πληρούν τις ουσιώδεις απαιτήσεις που ορίζονται στο τμήμα 1 του παραρτήματος I του παρόντος κανονισμού, και όταν οι διαδικασίες που εφαρμόζει ο κατασκευαστής συμμορφώνονται με τις ουσιώδεις απαιτήσεις που ορίζονται στο τμήμα 2 του παραρτήματος I, θεωρείται ότι συμμορφώνονται με τις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο άρθρο [άρθρο 15] του κανονισμού [κανονισμός για την ΤΝ], με την επιφύλαξη των λοιπών απαιτήσεων σχετικά με την ακρίβεια και την ανθεκτικότητα που περιλαμβάνονται στο προαναφερθέν άρθρο, και στον βαθμό που η επίτευξη του επιπέδου προστασίας που απαιτείται από τις εν λόγω απαιτήσεις αποδεικνύεται με τη δήλωση συμμόρφωσης της ΕΕ που εκδίδεται δυνάμει του παρόντος κανονισμού.

2. Για τα προϊόντα και τις απαιτήσεις κυβερνοασφάλειας που αναφέρονται στην παράγραφο 1, εφαρμόζεται η σχετική διαδικασία αξιολόγησης της συμμόρφωσης που απαιτείται από το άρθρο [άρθρο 43] του κανονισμού [κανονισμός για την ΤΝ]. Για τους σκοπούς της εν λόγω αξιολόγησης, οι κοινοποιημένοι οργανισμοί που δικαιούνται να ελέγχουν τη συμμόρφωση των συστημάτων ΤΝ υψηλού κινδύνου δυνάμει του κανονισμού [κανονισμός για την ΤΝ] δικαιούνται επίσης να ελέγχουν τη συμμόρφωση των συστημάτων ΤΝ υψηλού κινδύνου που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού με τις απαιτήσεις που ορίζονται στο παράρτημα I του παρόντος κανονισμού, υπό την προϋπόθεση ότι η συμμόρφωση των εν λόγω κοινοποιημένων οργανισμών με τις απαιτήσεις που ορίζονται στο άρθρο 29 του παρόντος κανονισμού έχει αξιολογηθεί στο πλαίσιο της διαδικασίας κοινοποίησης δυνάμει του κανονισμού [κανονισμός για την ΤΝ].

3. Κατά παρέκκλιση από την παράγραφο 2, τα κρίσιμα προϊόντα με ψηφιακά στοιχεία που απαριθμούνται στο παράρτημα III του παρόντος κανονισμού, στα οποία πρέπει να εφαρμόζονται οι διαδικασίες αξιολόγησης της συμμόρφωσης που αναφέρονται στο άρθρο 24 παράγραφος 2 στοιχεία α) και β) και στο άρθρο 24 παράγραφος 3 στοιχεία α) και β) του παρόντος κανονισμού και τα οποία ταξινομούνται επίσης ως συστήματα ΤΝ υψηλού κινδύνου σύμφωνα με το άρθρο [άρθρο 6] του κανονισμού

[κανονισμός για την ΤΝ] και στα οποία εφαρμόζεται η διαδικασία αξιολόγησης της συμμόρφωσης με βάση τον εσωτερικό έλεγχο που αναφέρεται στο παράρτημα [παράρτημα VI] του κανονισμού [κανονισμός για την ΤΝ], υπόκεινται στις διαδικασίες αξιολόγησης της συμμόρφωσης που προβλέπονται από τον παρόντα κανονισμό, στον βαθμό που αφορούν τις ουσιώδεις απαιτήσεις του παρόντος κανονισμού.

*Άρθρο 9*

*Μηχανολογικά προϊόντα*

Τα μηχανολογικά προϊόντα που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού [πρόταση κανονισμού για τα μηχανήματα], τα οποία είναι προϊόντα με ψηφιακά στοιχεία κατά την έννοια του παρόντος κανονισμού και για τα οποία έχει εκδοθεί δήλωση συμμόρφωσης ΕΕ βάσει του παρόντος κανονισμού, θεωρείται ότι συμμορφώνονται με τις ουσιώδεις απαιτήσεις υγείας και ασφάλειας που ορίζονται στο παράρτημα [παράρτημα III τμήματα 1.1.9 και 1.2.1] του κανονισμού [πρόταση κανονισμού για τα μηχανήματα], όσον αφορά την προστασία από τη διαφθορά, καθώς και την ασφάλεια και την αξιοπιστία των συστημάτων ελέγχου, και εφόσον η επίτευξη του επιπέδου προστασίας που απαιτείται από τις εν λόγω απαιτήσεις αποδεικνύεται από τη δήλωση συμμόρφωσης ΕΕ που εκδίδεται δυνάμει του παρόντος κανονισμού.

## ΚΕΦΑΛΑΙΟ ΙΙ

## ΥΠΟΧΡΕΩΣΕΙΣ ΤΩΝ ΟΙΚΟΝΟΜΙΚΩΝ ΦΟΡΕΩΝ

*Άρθρο 10*

*Υποχρεώσεις των κατασκευαστών*

1. Κατά τη διάθεση προϊόντος με ψηφιακά στοιχεία στην αγορά, οι κατασκευαστές εξασφαλίζουν ότι αυτό έχει σχεδιαστεί, αναπτυχθεί και κατασκευαστεί σύμφωνα με τις ουσιώδεις απαιτήσεις που ορίζονται στο τμήμα 1 του παραρτήματος Ι.

2. Για τους σκοπούς της συμμόρφωσης με την υποχρέωση που ορίζεται στην παράγραφο 1, οι κατασκευαστές διενεργούν εκτίμηση των κινδύνων που σχετίζονται με προϊόν με ψηφιακά στοιχεία όσον αφορά την κυβερνοασφάλεια και λαμβάνουν υπόψη το αποτέλεσμα της εν λόγω αξιολόγησης κατά τα στάδια προγραμματισμού, σχεδιασμού, ανάπτυξης, παραγωγής, παράδοσης και συντήρησης του προϊόντος με ψηφιακά στοιχεία, με σκοπό την ελαχιστοποίηση των κινδύνων για την κυβερνοασφάλεια, την πρόληψη συμβάντων ασφάλειας και την ελαχιστοποίηση των επιπτώσεων των εν λόγω συμβάντων, μεταξύ άλλων στην υγεία και την ασφάλεια των χρηστών.

3. Κατά τη διάθεση προϊόντος με ψηφιακά στοιχεία στην αγορά, ο κατασκευαστής περιλαμβάνει εκτίμηση κινδύνου για την κυβερνοασφάλεια στον τεχνικό φάκελο, όπως ορίζεται στο άρθρο 23 και στο παράρτημα V. Για τα προϊόντα με ψηφιακά στοιχεία που αναφέρονται στο άρθρο 8 και στο άρθρο 24 παράγραφος 4, τα οποία υπόκεινται και σε άλλες πράξεις της Ένωσης, η εκτίμηση κινδύνου για την κυβερνοασφάλεια μπορεί να αποτελεί μέρος της εκτίμησης κινδύνου που απαιτείται από τις εν λόγω αντίστοιχες ενωσιακές πράξεις. Όταν ορισμένες ουσιώδεις απαιτήσεις δεν εφαρμόζονται στο προϊόν με ψηφιακά στοιχεία που διατίθεται στην αγορά, ο κατασκευαστής περιλαμβάνει σαφή αιτιολόγηση στον εν λόγω φάκελο.

4. Για τους σκοπούς της συμμόρφωσης με την υποχρέωση που ορίζεται στην παράγραφο 1, οι κατασκευαστές επιδεικνύουν τη δέουσα επιμέλεια κατά την ενσωμάτωση συνιστωσών που προέρχονται από τρίτους σε προϊόντα με ψηφιακά στοιχεία. Διασφαλίζουν ότι οι εν λόγω συνιστώσες δεν θέτουν σε κίνδυνο την ασφάλεια του προϊόντος με ψηφιακά στοιχεία.

5. Ο κατασκευαστής τεκμηριώνει συστηματικά, κατά τρόπο αναλογικό προς τη φύση και τους κινδύνους για την κυβερνοασφάλεια, τις σχετικές πτυχές κυβερνοασφάλειας που αφορούν το προϊόν με ψηφιακά στοιχεία, συμπεριλαμβανομένων των τρωτών σημείων που υποπίπτουν στην αντίληψή του και τυχόν σχετικές πληροφορίες που παρέχονται από τρίτους, και, κατά περίπτωση, επικαιροποιεί την εκτίμηση κινδύνου του προϊόντος.

6. Κατά τη διάθεση προϊόντος με ψηφιακά στοιχεία στην αγορά, και για την αναμενόμενη διάρκεια ζωής του προϊόντος ή για διάστημα πέντε ετών από τη διάθεση του προϊόντος στην αγορά, ανάλογα με το ποιο διάστημα είναι μικρότερο, οι κατασκευαστές εξασφαλίζουν ότι τα τρωτά σημεία του εν λόγω προϊόντος αντιμετωπίζονται αποτελεσματικά και σύμφωνα με τις ουσιώδεις απαιτήσεις που ορίζονται στο τμήμα 2 του παραρτήματος Ι.

   Οι κατασκευαστές διαθέτουν κατάλληλες πολιτικές και διαδικασίες, συμπεριλαμβανομένων συντονισμένων πολιτικών γνωστοποίησης τρωτών σημείων, όπως αναφέρονται στο παράρτημα Ι τμήμα 2 σημείο 5, για την επεξεργασία και την αποκατάσταση πιθανών τρωτών σημείων του προϊόντος με ψηφιακά στοιχεία που αναφέρονται από εσωτερικές ή εξωτερικές πηγές.

7. Πριν από τη διάθεση προϊόντος με ψηφιακά στοιχεία στην αγορά, οι κατασκευαστές καταρτίζουν τον τεχνικό φάκελο που αναφέρεται στο άρθρο 23.

   Διενεργούν τις επιλεγμένες διαδικασίες αξιολόγησης της συμμόρφωσης που αναφέρονται στο άρθρο 24 ή αναθέτουν τη διενέργειά τους σε τρίτους.

   Όταν η συμμόρφωση του προϊόντος με ψηφιακά στοιχεία με τις ουσιώδεις απαιτήσεις που καθορίζονται στο παράρτημα Ι τμήμα 1 και των διαδικασιών που εφαρμόζει ο κατασκευαστής με τις ουσιώδεις απαιτήσεις που ορίζονται στο τμήμα 2 του παραρτήματος Ι αποδεικνύεται με την εν λόγω διαδικασία αξιολόγησης της συμμόρφωσης, οι κατασκευαστές καταρτίζουν τη δήλωση συμμόρφωσης ΕΕ σύμφωνα με το άρθρο 20 και τοποθετούν τη σήμανση CE σύμφωνα με το άρθρο 22.

8. Οι κατασκευαστές διατηρούν τον τεχνικό φάκελο και τη δήλωση συμμόρφωσης ΕΕ, κατά περίπτωση, στη διάθεση των αρχών εποπτείας της αγοράς επί δέκα έτη από τη διάθεση του προϊόντος με ψηφιακά στοιχεία στην αγορά.

9. Οι κατασκευαστές διασφαλίζουν ότι εφαρμόζονται διαδικασίες ώστε τα προϊόντα με ψηφιακά στοιχεία που αποτελούν μέρος σειράς παραγωγής να συμμορφώνονται διαρκώς. Ο κατασκευαστής λαμβάνει δεόντως υπόψη τις αλλαγές στη διαδικασία ανάπτυξης και παραγωγής ή στον σχεδιασμό ή τα χαρακτηριστικά του προϊόντος με ψηφιακά στοιχεία, καθώς και τις αλλαγές στα εναρμονισμένα πρότυπα, στα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας ή στις κοινές προδιαγραφές που αναφέρονται στο άρθρο 19 και με βάση τις οποίες δηλώνεται η συμμόρφωση του προϊόντος με ψηφιακά στοιχεία ή με την εφαρμογή των οποίων επαληθεύεται η συμμόρφωσή του.

10. Οι κατασκευαστές διασφαλίζουν ότι τα προϊόντα με ψηφιακά στοιχεία συνοδεύονται από τις πληροφορίες και τις οδηγίες που ορίζονται στο παράρτημα ΙΙ, σε ηλεκτρονική ή έντυπη μορφή. Οι εν λόγω πληροφορίες και οδηγίες συντάσσονται σε

γλώσσα ευκόλως κατανοητή από τους χρήστες. Είναι σαφείς, κατανοητές, εύληπτες και ευανάγνωστες. Επιτρέπουν την ασφαλή εγκατάσταση, λειτουργία και χρήση των προϊόντων με ψηφιακά στοιχεία.

11. Οι κατασκευαστές είτε παρέχουν τη δήλωση συμμόρφωσης ΕΕ μαζί με το προϊόν με ψηφιακά στοιχεία είτε περιλαμβάνουν στις οδηγίες και στις πληροφορίες που ορίζονται στο παράρτημα ΙΙ τη διεύθυνση στο διαδίκτυο στην οποία είναι προσβάσιμη η δήλωση συμμόρφωσης ΕΕ.

12. Από τη διάθεση στην αγορά και για την αναμενόμενη διάρκεια ζωής του προϊόντος ή για διάστημα πέντε ετών μετά τη διάθεση προϊόντος με ψηφιακά στοιχεία στην αγορά, ανάλογα με το ποιο διάστημα είναι μικρότερο, οι κατασκευαστές που γνωρίζουν ή έχουν λόγους να πιστεύουν ότι το προϊόν με ψηφιακά στοιχεία ή οι διαδικασίες που εφαρμόζει ο κατασκευαστής δεν συμμορφώνονται με τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα Ι λαμβάνουν αμέσως τα αναγκαία διορθωτικά μέτρα για να εξασφαλίσουν τη συμμόρφωση του προϊόντος με ψηφιακά στοιχεία ή των διαδικασιών του κατασκευαστή, να αποσύρουν ή να ανακαλέσουν το προϊόν, κατά περίπτωση.

13. Οι κατασκευαστές παρέχουν στην αρχή εποπτείας της αγοράς, κατόπιν αιτιολογημένου αιτήματος της εν λόγω αρχής, σε γλώσσα ευκόλως κατανοητή από αυτήν, όλες τις πληροφορίες και την τεκμηρίωση που απαιτούνται, σε έντυπη ή ηλεκτρονική μορφή, για να αποδειχθεί η συμμόρφωση του προϊόντος με ψηφιακά στοιχεία και των διαδικασιών που εφαρμόζει ο κατασκευαστής προς τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα Ι. Συνεργάζονται με την εν λόγω αρχή, κατόπιν αιτήματός της, για τυχόν μέτρα που λαμβάνονται για την εξάλειψη των κινδύνων που ενέχει το προϊόν με ψηφιακά στοιχεία το οποίο έχουν διαθέσει στην αγορά, όσον αφορά την κυβερνοασφάλεια.

14. Ο κατασκευαστής που παύει τις δραστηριότητές του και, ως εκ τούτου, δεν είναι σε θέση να συμμορφωθεί με τις υποχρεώσεις που ορίζονται στον παρόντα κανονισμό ενημερώνει, πριν από την έναρξη ισχύος της παύσης των δραστηριοτήτων του, τις αρμόδιες αρχές εποπτείας της αγοράς σχετικά με την κατάσταση αυτή, καθώς και τους χρήστες των σχετικών προϊόντων με ψηφιακά στοιχεία που διατίθενται στην αγορά, με κάθε διαθέσιμο μέσο και στο μέτρο του δυνατού.

15. Η Επιτροπή μπορεί, με εκτελεστικές πράξεις, να καθορίζει τον μορφότυπο και τα στοιχεία του καταλόγου υλικών του λογισμικού που ορίζεται στο παράρτημα Ι τμήμα 2 σημείο 1. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 51 παράγραφος 2.

*Άρθρο 11*

*Υποχρεώσεις υποβολής εκθέσεων για τους κατασκευαστές*

1. Ο κατασκευαστής κοινοποιεί στον ENISA, χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που λαμβάνει γνώση, κάθε τρωτό σημείο που αποτελεί αντικείμενο ενεργού εκμετάλλευσης και περιέχεται στο προϊόν με ψηφιακά στοιχεία. Η κοινοποίηση περιλαμβάνει λεπτομέρειες σχετικά με το εν λόγω τρωτό σημείο και, κατά περίπτωση, τυχόν διορθωτικά μέτρα ή μέτρα άμβλυνσης που έχουν ληφθεί. Ο ENISA διαβιβάζει, χωρίς αδικαιολόγητη καθυστέρηση, εκτός εάν συντρέχουν αιτιολογημένοι λόγοι που σχετίζονται με κίνδυνο για την κυβερνοασφάλεια, την κοινοποίηση στην CSIRT που έχει οριστεί για τους σκοπούς της συντονισμένης γνωστοποίησης τρωτών σημείων σύμφωνα με

το άρθρο [άρθρο X] της οδηγίας [οδηγία XXX/XXXX (NIS2)] των οικείων κρατών μελών αμέσως μόλις τη λάβει και ενημερώνει την αρχή εποπτείας της αγοράς σχετικά με το κοινοποιηθέν τρωτό σημείο.

2. Ο κατασκευαστής κοινοποιεί στον ENISA, χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που λαμβάνει γνώση, κάθε συμβάν που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία. Ο ENISA διαβιβάζει, χωρίς αδικαιολόγητη καθυστέρηση, εκτός εάν συντρέχουν αιτιολογημένοι λόγοι που σχετίζονται με κίνδυνο για την κυβερνοασφάλεια, τις κοινοποιήσεις στο ενιαίο σημείο επαφής που έχει οριστεί σύμφωνα με το άρθρο [άρθρο X] της οδηγίας [οδηγία XXX/XXXX (NIS2)] των οικείων κρατών μελών και ενημερώνει την αρχή εποπτείας της αγοράς σχετικά με τα κοινοποιηθέντα συμβάντα. Η κοινοποίηση συμβάντων περιλαμβάνει πληροφορίες σχετικά με τη σοβαρότητα και τον αντίκτυπο του συμβάντος και, κατά περίπτωση, αναφέρει εάν ο κατασκευαστής έχει την υπόνοια ότι το συμβάν προκλήθηκε από παράνομες ή κακόβουλες ενέργειες ή αν θεωρεί ότι έχει διασυνοριακό αντίκτυπο.

3. Ο ENISA υποβάλλει στο ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (EU-CyCLONe) που συστάθηκε με το άρθρο [άρθρο X] της οδηγίας [οδηγία XXX/XXXX (NIS2)] πληροφορίες που κοινοποιούνται σύμφωνα με τις παραγράφους 1 και 2, εάν οι πληροφορίες αυτές είναι σημαντικές για τη συντονισμένη διαχείριση μεγάλης κλίμακας συμβάντων και κρίσεων κυβερνοασφάλειας σε επιχειρησιακό επίπεδο.

4. Ο κατασκευαστής ενημερώνει, χωρίς αδικαιολόγητη καθυστέρηση και αμέσως μόλις λάβει γνώση, τους χρήστες του προϊόντος με ψηφιακά στοιχεία σχετικά με το συμβάν και, εφόσον απαιτείται, σχετικά με τα διορθωτικά μέτρα που μπορεί να εφαρμόσει ο χρήστης για τον μετριασμό των επιπτώσεων του συμβάντος.

5. Η Επιτροπή μπορεί, με εκτελεστικές πράξεις, να προσδιορίσει περαιτέρω το είδος των πληροφοριών, τον μορφότυπο και τη διαδικασία κοινοποίησης που υποβάλλεται σύμφωνα με τις παραγράφους 1 και 2. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης του άρθρου 51 παράγραφος 2.

6. Ο ENISA, με βάση τις κοινοποιήσεις που λαμβάνει σύμφωνα με τις παραγράφους 1 και 2, καταρτίζει διετή τεχνική έκθεση σχετικά με τις αναδυόμενες τάσεις όσον αφορά τους κινδύνους για την κυβερνοασφάλεια σε προϊόντα με ψηφιακά στοιχεία και την υποβάλλει στην ομάδα συνεργασίας που αναφέρεται στο άρθρο [άρθρο X] της οδηγίας [οδηγία XXX/XXXX (NIS2)]. Η πρώτη τέτοια έκθεση υποβάλλεται εντός 24 μηνών από την έναρξη εφαρμογής των υποχρεώσεων που ορίζονται στις παραγράφους 1 και 2.

7. Οι κατασκευαστές, αμέσως μόλις εντοπίσουν ένα τρωτό σημείο σε κάποια συνιστώσα, μεταξύ άλλων σε συνιστώσα ανοικτού κώδικα, η οποία είναι ενσωματωμένη στο προϊόν με ψηφιακά στοιχεία, αναφέρουν το τρωτό σημείο στο πρόσωπο ή την οντότητα που έχει την ευθύνη για τη συντήρηση της συνιστώσας.

*Άρθρο 12*

*Εξουσιοδοτημένοι αντιπρόσωποι*

1. Οι κατασκευαστές μπορούν να ορίζουν, με γραπτή εντολή, εξουσιοδοτημένο αντιπρόσωπο.

2. Οι υποχρεώσεις που ορίζονται στο άρθρο 10 παράγραφοι 1 έως 7 πρώτη περίπτωση και παράγραφος 9 δεν αποτελούν μέρος της εντολής του εξουσιοδοτημένου αντιπροσώπου.

3. Ο εξουσιοδοτημένος αντιπρόσωπος ασκεί τα καθήκοντα που προσδιορίζονται στην εντολή την οποία λαμβάνει από τον κατασκευαστή. Η εντολή επιτρέπει στον εξουσιοδοτημένο αντιπρόσωπο τουλάχιστον τα ακόλουθα:

α) να τηρεί τη δήλωση συμμόρφωσης ΕΕ που αναφέρεται στο άρθρο 20 και τον τεχνικό φάκελο που αναφέρεται στο άρθρο 23 στη διάθεση των αρχών εποπτείας της αγοράς επί δέκα έτη μετά τη διάθεση του προϊόντος με ψηφιακά στοιχεία στην αγορά·

β) να παρέχει στην αρχή εποπτείας της αγοράς, κατόπιν αιτιολογημένου αιτήματος της εν λόγω αρχής, όλες τις πληροφορίες και την τεκμηρίωση που απαιτούνται για να αποδειχθεί η συμμόρφωση του προϊόντος με ψηφιακά στοιχεία·

γ) να συνεργάζεται με τις αρχές εποπτείας της αγοράς, κατόπιν αιτήματός τους, για τυχόν ενέργειες που έγιναν για την εξάλειψη των κινδύνων που ενέχουν τα προϊόντα με ψηφιακά στοιχεία που καλύπτει η εντολή του εξουσιοδοτημένου αντιπροσώπου.

*Άρθρο 13*

*Υποχρεώσεις των εισαγωγέων*

1. Οι εισαγωγείς διαθέτουν στην αγορά μόνο προϊόντα με ψηφιακά στοιχεία που συμμορφώνονται προς τις ουσιώδεις απαιτήσεις που ορίζονται στο τμήμα 1 του παραρτήματος Ι και εφόσον οι διαδικασίες που εφαρμόζει ο κατασκευαστής συμμορφώνονται προς τις ουσιώδεις απαιτήσεις που ορίζονται στο τμήμα 2 του παραρτήματος Ι.

2. Προτού διαθέσουν στην αγορά προϊόν με ψηφιακά στοιχεία, οι εισαγωγείς διασφαλίζουν τα εξής:

α) ο κατασκευαστής έχει διενεργήσει τις κατάλληλες διαδικασίες αξιολόγησης της συμμόρφωσης που αναφέρονται στο άρθρο 24·

β) ο κατασκευαστής έχει καταρτίσει τεχνικό φάκελο·

γ) το προϊόν με ψηφιακά στοιχεία φέρει τη σήμανση CE που αναφέρεται στο άρθρο 22 και συνοδεύεται από τις πληροφορίες και τις οδηγίες χρήσης που ορίζονται στο παράρτημα ΙΙ.

3. Όταν ένας εισαγωγέας θεωρεί ή έχει λόγους να πιστεύει ότι ένα προϊόν με ψηφιακά στοιχεία ή οι διαδικασίες που εφαρμόζει ο κατασκευαστής δεν συμμορφώνονται με τις ουσιώδεις απαιτήσεις που καθορίζονται στο παράρτημα Ι, ο εισαγωγέας δεν διαθέτει το προϊόν στην αγορά έως ότου το εν λόγω προϊόν ή οι διαδικασίες που εφαρμόζει ο κατασκευαστής συμμορφωθούν με τις ουσιώδεις απαιτήσεις που καθορίζονται στο παράρτημα Ι. Επιπλέον, όταν το προϊόν με ψηφιακά στοιχεία παρουσιάζει σημαντικό κίνδυνο για την κυβερνοασφάλεια, ο εισαγωγέας ενημερώνει σχετικά τον κατασκευαστή και τις αρχές εποπτείας της αγοράς.

4. Οι εισαγωγείς αναγράφουν το όνομα, την καταχωρισμένη εμπορική επωνυμία τους ή το καταχωρισμένο εμπορικό σήμα τους, την ταχυδρομική διεύθυνση και την ηλεκτρονική διεύθυνση επικοινωνίας τους στο προϊόν με ψηφιακά στοιχεία ή, όταν

αυτό δεν είναι δυνατόν, στη συσκευασία του ή σε έγγραφο που συνοδεύει το προϊόν με ψηφιακά στοιχεία. Τα στοιχεία επικοινωνίας παρέχονται σε γλώσσα κατανοητή από τους χρήστες και τις αρχές εποπτείας της αγοράς.

5. Οι εισαγωγείς εξασφαλίζουν ότι το προϊόν με ψηφιακά στοιχεία συνοδεύεται από τις οδηγίες και τις πληροφορίες που ορίζονται στο παράρτημα ΙΙ σε γλώσσα εύκολα κατανοητή από τους χρήστες.

6. Οι εισαγωγείς που γνωρίζουν ή έχουν λόγο να πιστεύουν ότι ένα προϊόν με ψηφιακά στοιχεία το οποίο έχουν διαθέσει στην αγορά ή οι διαδικασίες που εφαρμόζει ο κατασκευαστής του δεν συμμορφώνονται με τις ουσιώδεις απαιτήσεις που καθορίζονται στο παράρτημα Ι λαμβάνουν αμέσως τα αναγκαία διορθωτικά μέτρα για να εξασφαλίσουν τη συμμόρφωση του εν λόγω προϊόντος με ψηφιακά στοιχεία ή των διαδικασιών που εφαρμόζει ο κατασκευαστής του με τις ουσιώδεις απαιτήσεις που καθορίζονται στο παράρτημα Ι ή να αποσύρουν ή να ανακαλέσουν το προϊόν, κατά περίπτωση.

   Αμέσως μόλις εντοπίσουν ένα τρωτό σημείο στο προϊόν με ψηφιακά στοιχεία, οι εισαγωγείς ενημερώνουν τον κατασκευαστή χωρίς αδικαιολόγητη καθυστέρηση σχετικά με το εν λόγω τρωτό σημείο. Πέραν τούτου, όταν το προϊόν με ψηφιακά στοιχεία ενέχει σημαντικό κίνδυνο για την κυβερνοασφάλεια, οι εισαγωγείς ενημερώνουν αμέσως σχετικά με το θέμα αυτό τις αρχές εποπτείας της αγοράς των κρατών μελών στην αγορά των οποίων κατέστησαν διαθέσιμο το προϊόν με ψηφιακά στοιχεία, και παραθέτουν λεπτομέρειες, συγκεκριμένα, για τη μη συμμόρφωση και τα τυχόν διορθωτικά μέτρα που έλαβαν.

7. Οι εισαγωγείς τηρούν επί δέκα έτη από τη διάθεση του προϊόντος με ψηφιακά στοιχεία στην αγορά αντίγραφο της δήλωσης συμμόρφωσης ΕΕ στη διάθεση των αρχών εποπτείας της αγοράς και εξασφαλίζουν ότι ο τεχνικός φάκελος μπορεί να τεθεί στη διάθεση των εν λόγω αρχών, κατόπιν αιτήματός τους.

8. Οι εισαγωγείς παρέχουν στην αρχή εποπτείας της αγοράς, κατόπιν αιτιολογημένου αιτήματος της εν λόγω αρχής, όλες τις πληροφορίες και την τεκμηρίωση, σε έντυπη ή σε ηλεκτρονική μορφή, που απαιτούνται για να αποδειχθεί η συμμόρφωση του προϊόντος με ψηφιακά στοιχεία προς τις ουσιώδεις απαιτήσεις που ορίζονται στο τμήμα 1 του παραρτήματος Ι, καθώς και των διαδικασιών που εφαρμόζει ο κατασκευαστής προς τις ουσιώδεις απαιτήσεις που ορίζονται στο τμήμα 2 του παραρτήματος Ι, σε γλώσσα εύκολα κατανοητή από την εν λόγω αρχή. Συνεργάζονται με την εν λόγω αρχή, κατόπιν αιτήματος της, όσον αφορά τη λήψη μέτρων για την εξάλειψη των κινδύνων τους οποίους ενέχουν τα προϊόντα με ψηφιακά στοιχεία που έχουν διαθέσει στην αγορά όσον αφορά την κυβερνοασφάλεια.

9. Όταν ο εισαγωγέας προϊόντος με ψηφιακά στοιχεία αντιληφθεί ότι ο κατασκευαστής του εν λόγω προϊόντος έπαυσε τις δραστηριότητές του και, ως εκ τούτου, δεν είναι σε θέση να συμμορφωθεί με τις υποχρεώσεις που ορίζονται στον παρόντα κανονισμό, ενημερώνει τις αρμόδιες αρχές εποπτείας της αγοράς σχετικά με την κατάσταση αυτή, καθώς και τους χρήστες των προϊόντων με ψηφιακά στοιχεία που διατίθενται στην αγορά, με κάθε διαθέσιμο μέσο και στο μέτρο του δυνατού.

*Άρθρο 14*

*Υποχρεώσεις των διανομέων*

1. Όταν οι διανομείς καθιστούν ένα προϊόν με ψηφιακά στοιχεία διαθέσιμο στην αγορά, ενεργούν με τη δέουσα προσοχή σε σχέση με τις απαιτήσεις του παρόντος κανονισμού.

2. Προτού καταστήσουν διαθέσιμο ένα προϊόν με ψηφιακά στοιχεία στην αγορά, οι διανομείς επαληθεύουν ότι:

   α) το προϊόν με ψηφιακά στοιχεία φέρει τη σήμανση CE·

   β) ο κατασκευαστής και ο εισαγωγέας έχουν συμμορφωθεί με τις υποχρεώσεις που καθορίζονται αντίστοιχα στο άρθρο 10 παράγραφοι 10 και 11 και στο άρθρο 13 παράγραφος 4.

3. Όταν ο διανομέας θεωρεί ή έχει λόγους να πιστεύει ότι ένα προϊόν με ψηφιακά στοιχεία ή οι διαδικασίες που εφαρμόζει ο κατασκευαστής δεν συμμορφώνονται με τις ουσιώδεις απαιτήσεις που καθορίζονται στο παράρτημα I, ο διανομέας δεν διαθέτει στην αγορά το προϊόν με ψηφιακά στοιχεία έως ότου εξασφαλιστεί η συμμόρφωση του εν λόγω προϊόντος ή των διαδικασιών που εφαρμόζει ο κατασκευαστής. Επίσης, όταν το προϊόν με ψηφιακά στοιχεία ενέχει σημαντικό κίνδυνο για την κυβερνοασφάλεια, ο διανομέας ενημερώνει σχετικά τον κατασκευαστή καθώς και τις αρχές εποπτείας της αγοράς.

4. Οι διανομείς που γνωρίζουν ή έχουν λόγο να πιστεύουν ότι ένα προϊόν με ψηφιακά στοιχεία το οποίο έχουν διαθέσει στην αγορά ή οι διαδικασίες που εφαρμόζει ο κατασκευαστής του δεν συμμορφώνονται με τις ουσιώδεις απαιτήσεις που καθορίζονται στο παράρτημα I διασφαλίζουν ότι λαμβάνονται τα αναγκαία διορθωτικά μέτρα για να εξασφαλίσουν τη συμμόρφωση του εν λόγω προϊόντος με ψηφιακά στοιχεία ή των διαδικασιών που εφαρμόζει ο κατασκευαστής του, ή να αποσύρουν ή να ανακαλέσουν το προϊόν, κατά περίπτωση.

   Αμέσως μόλις εντοπίσουν ένα τρωτό σημείο στο προϊόν με ψηφιακά στοιχεία, οι διανομείς ενημερώνουν τον κατασκευαστή χωρίς αδικαιολόγητη καθυστέρηση σχετικά με το εν λόγω τρωτό σημείο. Πέραν τούτου, όταν το προϊόν με ψηφιακά στοιχεία ενέχει σημαντικό κίνδυνο για την κυβερνοασφάλεια, οι διανομείς ενημερώνουν αμέσως σχετικά με το θέμα αυτό τις αρχές εποπτείας της αγοράς των κρατών μελών στην αγορά των οποίων κατέστησαν διαθέσιμο το προϊόν με ψηφιακά στοιχεία, και παραθέτουν λεπτομέρειες, συγκεκριμένα, για τη μη συμμόρφωση και τα τυχόν διορθωτικά μέτρα που έλαβαν.

5. Οι διανομείς παρέχουν στην αρχή εποπτείας της αγοράς, κατόπιν αιτιολογημένου αιτήματος της εν λόγω αρχής, όλες τις πληροφορίες και την τεκμηρίωση, σε έντυπη ή σε ηλεκτρονική μορφή, που απαιτούνται για να αποδειχθεί η συμμόρφωση του προϊόντος με ψηφιακά στοιχεία, καθώς και των διαδικασιών που εφαρμόζει ο κατασκευαστής του προς τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα I, σε γλώσσα εύκολα κατανοητή από την εν λόγω αρχή. Συνεργάζονται με την εν λόγω αρχή, κατόπιν αιτήματος της, όσον αφορά τη λήψη μέτρων για την εξάλειψη των κινδύνων τους οποίους ενέχουν τα προϊόντα με ψηφιακά στοιχεία που έχουν καταστήσει διαθέσιμα στην αγορά όσον αφορά την κυβερνοασφάλεια.

6. Όταν ο διανομέας προϊόντος με ψηφιακά στοιχεία αντιληφθεί ότι ο κατασκευαστής του εν λόγω προϊόντος έπαυσε τις δραστηριότητές του και, ως εκ τούτου, δεν είναι σε θέση να συμμορφωθεί με τις υποχρεώσεις που ορίζονται στον παρόντα κανονισμό, ενημερώνει τις αρμόδιες αρχές εποπτείας της αγοράς σχετικά με την κατάσταση αυτή, καθώς και τους χρήστες των προϊόντων με ψηφιακά στοιχεία που διατίθενται στην αγορά, με κάθε διαθέσιμο μέσο και στο μέτρο του δυνατού.

*Άρθρο 15*

*Περιπτώσεις στις οποίες οι υποχρεώσεις των κατασκευαστών εφαρμόζονται στους εισαγωγείς και στους διανομείς*

Ένας εισαγωγέας ή διανομέας θεωρείται κατασκευαστής για τους σκοπούς του παρόντος κανονισμού και υπόκειται στις υποχρεώσεις που προβλέπονται για τον κατασκευαστή στα άρθρα 10 και 11 παράγραφοι 1, 2, 4 και 7 όταν ο εν λόγω εισαγωγέας ή διανομέας διαθέτει στην αγορά προϊόν με ψηφιακά στοιχεία υπό τη δική του επωνυμία ή το δικό του εμπορικό σήμα ή όταν τροποποιεί ουσιωδώς το προϊόν με ψηφιακά στοιχεία που έχει ήδη διατεθεί στην αγορά.

*Άρθρο 16*

*Άλλες περιπτώσεις στις οποίες εφαρμόζονται οι υποχρεώσεις των κατασκευαστών*

Φυσικό ή νομικό πρόσωπο, πέραν του κατασκευαστή, του εισαγωγέα ή του διανομέα, που πραγματοποιεί ουσιαστική τροποποίηση του προϊόντος με ψηφιακά στοιχεία θεωρείται κατασκευαστής για τους σκοπούς του παρόντος κανονισμού.

Το εν λόγω πρόσωπο υπόκειται στις υποχρεώσεις του κατασκευαστή που ορίζονται στο άρθρο 10 και στο άρθρο 11 παράγραφοι 1, 2, 4 και 7, για το μέρος του προϊόντος που επηρεάζεται από την ουσιαστική τροποποίηση ή, εάν η ουσιαστική τροποποίηση έχει αντίκτυπο στην κυβερνοασφάλεια του προϊόντος με ψηφιακά στοιχεία στο σύνολό του, για ολόκληρο το προϊόν.

*Άρθρο 17*

*Ταυτοποίηση των οικονομικών φορέων*

1. Οι οικονομικοί φορείς, κατόπιν αιτήματος και εφόσον οι πληροφορίες είναι διαθέσιμες, παρέχουν στις αρχές εποπτείας της αγοράς τις ακόλουθες πληροφορίες:

   α) όνομα και διεύθυνση κάθε οικονομικού φορέα που τους έχει προμηθεύσει προϊόν με ψηφιακά στοιχεία·

   β) όνομα και διεύθυνση κάθε οικονομικού φορέα στον οποίο έχουν προμηθεύσει προϊόν με ψηφιακά στοιχεία.

2. Οι οικονομικοί φορείς είναι σε θέση να παρέχουν τις πληροφορίες που αναφέρονται στην παράγραφο 1 επί δέκα έτη αφότου έχουν προμηθευτεί το προϊόν με ψηφιακά στοιχεία και επί δέκα έτη αφότου έχουν προμηθεύσει το προϊόν με ψηφιακά στοιχεία.

## ΚΕΦΑΛΑΙΟ ΙΙΙ

## ΣΥΜΜΟΡΦΩΣΗ ΤΟΥ ΠΡΟΪΟΝΤΟΣ ΜΕ ΨΗΦΙΑΚΑ ΣΤΟΙΧΕΙΑ

*Άρθρο 18*

*Τεκμήριο συμμόρφωσης*

1. Τα προϊόντα με ψηφιακά στοιχεία και οι διαδικασίες που εφαρμόζει ο κατασκευαστής που συμμορφώνονται με εναρμονισμένα πρότυπα ή μέρη αυτών τα στοιχεία αναφοράς των οποίων έχουν δημοσιευθεί στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* τεκμαίρεται ότι συμμορφώνονται προς τις ουσιώδεις

απαιτήσεις ασφάλειας τις οποίες αφορούν τα εν λόγω πρότυπα ή τα μέρη αυτών και οι οποίες ορίζονται στο παράρτημα I.

2. Τα προϊόντα με ψηφιακά στοιχεία και οι διαδικασίες που εφαρμόζει ο κατασκευαστής που συμμορφώνονται με τις κοινές προδιαγραφές που αναφέρονται στο άρθρο 19 τεκμαίρεται ότι συμμορφώνονται προς τις ουσιώδεις απαιτήσεις του παραρτήματος I, στον βαθμό που οι εν λόγω κοινές προδιαγραφές καλύπτουν αυτές τις απαιτήσεις.

3. Τα προϊόντα με ψηφιακά στοιχεία και οι διαδικασίες που εφαρμόζει ο κατασκευαστής για τα οποία έχει εκδοθεί δήλωση συμμόρφωσης ΕΕ ή πιστοποιητικό στο πλαίσιο ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας που έχει εγκριθεί σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 και προσδιορίζεται σύμφωνα με την παράγραφο 4 τεκμαίρεται ότι συμμορφώνονται με τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα I, εφόσον η δήλωση συμμόρφωσης ΕΕ ή το πιστοποιητικό κυβερνοασφάλειας, ή μέρη αυτών, καλύπτουν τις εν λόγω απαιτήσεις.

4. Η Επιτροπή εξουσιοδοτείται, μέσω εκτελεστικών πράξεων, να προσδιορίζει τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας που θεσπίζονται σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 και τα οποία μπορούν να χρησιμοποιηθούν για την απόδειξη της συμμόρφωσης προς τις ουσιώδεις απαιτήσεις ή μέρη αυτών, όπως ορίζεται στο παράρτημα I. Επιπλέον, κατά περίπτωση, η Επιτροπή προσδιορίζει αν ένα πιστοποιητικό κυβερνοασφάλειας που εκδίδεται στο πλαίσιο των εν λόγω συστημάτων καταργεί την υποχρέωση του κατασκευαστή να διενεργεί αξιολόγηση της συμμόρφωσης από τρίτους για τις αντίστοιχες απαιτήσεις, όπως ορίζεται στο άρθρο 24 παράγραφος 2 στοιχεία α) και β), και παράγραφος 3 στοιχεία α) και β). Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης του άρθρου 51 παράγραφος 2.

*Άρθρο 19*

*Κοινές προδιαγραφές*

Όταν δεν υπάρχουν τα εναρμονισμένα πρότυπα που αναφέρονται στο άρθρο 18 ή όταν η Επιτροπή θεωρεί ότι τα σχετικά εναρμονισμένα πρότυπα δεν επαρκούν για την ικανοποίηση των απαιτήσεων του παρόντος κανονισμού ή για τη συμμόρφωση με το αίτημα τυποποίησης της Επιτροπής, ή όταν υπάρχουν αδικαιολόγητες καθυστερήσεις στη διαδικασία τυποποίησης ή όταν το αίτημα της Επιτροπής για εναρμονισμένα πρότυπα δεν έχει γίνει δεκτό από τους ευρωπαϊκούς οργανισμούς τυποποίησης, η Επιτροπή εξουσιοδοτείται, με εκτελεστικές πράξεις, να θεσπίζει κοινές προδιαγραφές όσον αφορά τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα I. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 51 παράγραφος 2.

*Άρθρο 20*

*Δήλωση συμμόρφωσης ΕΕ*

1. Η δήλωση συμμόρφωσης ΕΕ καταρτίζεται από τους κατασκευαστές σύμφωνα με το άρθρο 10 παράγραφος 7 και αναφέρει ότι πληρούνται αποδεδειγμένα οι ισχύουσες ουσιώδεις απαιτήσεις του παραρτήματος I.

2. Η δήλωση συμμόρφωσης ΕΕ έχει τη δομή που ορίζει το παράρτημα IV και περιλαμβάνει τα στοιχεία που καθορίζονται στις σχετικές διαδικασίες αξιολόγησης

της συμμόρφωσης οι οποίες προβλέπονται στο παράρτημα VI. Η δήλωση αυτή επικαιροποιείται συνεχώς. Καθίσταται διαθέσιμη στη γλώσσα ή τις γλώσσες που απαιτεί το κράτος μέλος στην αγορά του οποίου διατίθεται ή καθίσταται διαθέσιμο το προϊόν με ψηφιακά στοιχεία.

3. Όταν ένα προϊόν με ψηφιακά στοιχεία διέπεται από περισσότερες από μία πράξεις της Ένωσης βάσει των οποίων απαιτείται δήλωση συμμόρφωσης ΕΕ, καταρτίζεται ενιαία δήλωση συμμόρφωσης ΕΕ για όλες τις εν λόγω πράξεις της Ένωσης. Η δήλωση αυτή περιέχει τα στοιχεία των οικείων πράξεων της Ένωσης, συμπεριλαμβανομένων των στοιχείων δημοσίευσής τους.

4. Με την κατάρτιση της δήλωσης συμμόρφωσης ΕΕ, ο κατασκευαστής αναλαμβάνει την ευθύνη για τη συμμόρφωση του προϊόντος.

5. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 50 για τη συμπλήρωση του παρόντος κανονισμού, με την προσθήκη στοιχείων στο ελάχιστο περιεχόμενο της δήλωσης συμμόρφωσης ΕΕ που παρατίθεται στο παράρτημα IV, ώστε να λαμβάνονται υπόψη οι τεχνολογικές εξελίξεις.

*Άρθρο 21*

*Γενικές αρχές της σήμανσης CE*

Η σήμανση CE, όπως ορίζεται στο άρθρο 3 παράγραφος 32, υπόκειται στις γενικές αρχές του άρθρου 30 του κανονισμού (ΕΚ) αριθ. 765/2008.

*Άρθρο 22*

*Κανόνες και όροι για την τοποθέτηση της σήμανσης CE*

1. Η σήμανση CE τοποθετείται στο προϊόν με ψηφιακά στοιχεία κατά τρόπο εμφανή, ευανάγνωστο και ανεξίτηλο. Όταν αυτό δεν είναι δυνατό ή δεν δικαιολογείται λόγω της φύσης της συσκευής ή του προϊόντος με ψηφιακά στοιχεία, τοποθετείται στη συσκευασία και στη δήλωση συμμόρφωσης ΕΕ που αναφέρεται στο άρθρο 20 οι οποίες συνοδεύουν το προϊόν με ψηφιακά στοιχεία. Για προϊόντα με ψηφιακά στοιχεία τα οποία έχουν τη μορφή λογισμικού, η σήμανση CE τοποθετείται είτε στη δήλωση συμμόρφωσης ΕΕ που αναφέρεται στο άρθρο 20 είτε στον ιστότοπο που συνοδεύει το προϊόν λογισμικού.

2. Λόγω της φύσης του προϊόντος με ψηφιακά στοιχεία, το ύψος της σήμανσης CE που τοποθετείται στο προϊόν μπορεί να είναι μικρότερο από 5 mm, υπό τον όρο ότι αυτή παραμένει ευδιάκριτη και ευανάγνωστη.

3. Η σήμανση CE τοποθετείται προτού το προϊόν με ψηφιακά στοιχεία διατεθεί στην αγορά. Μπορεί να συνοδεύεται από εικονόγραμμα ή άλλο σήμα που υποδεικνύει ειδικό κίνδυνο ή ειδική χρήση, όπως ορίζεται στις εκτελεστικές πράξεις που αναφέρονται στην παράγραφο 6.

4. Η σήμανση CE ακολουθείται από τον αριθμό μητρώου του κοινοποιημένου οργανισμού, όταν ο οργανισμός αυτός συμμετέχει στη διαδικασία αξιολόγησης της συμμόρφωσης με βάση την πλήρη διασφάλιση ποιότητας (βάσει της ενότητας Η) που αναφέρεται στο άρθρο 24.

Ο αριθμός μητρώου του κοινοποιημένου οργανισμού τοποθετείται είτε από τον ίδιο τον οργανισμό είτε, σύμφωνα με τις οδηγίες του, από τον κατασκευαστή ή τον εξουσιοδοτημένο αντιπρόσωπο του κατασκευαστή.

5. Τα κράτη μέλη βασίζονται σε υφιστάμενους μηχανισμούς για να εξασφαλίζουν την ορθή εφαρμογή του καθεστώτος που διέπει τη σήμανση CE και λαμβάνουν κατάλληλα μέτρα σε περίπτωση αθέμιτης χρήσης της εν λόγω σήμανσης. Όταν το προϊόν με ψηφιακά στοιχεία διέπεται από άλλη ενωσιακή νομοθεσία που επίσης προβλέπει την τοποθέτηση της σήμανσης CE, η σήμανση CE δηλώνει ότι το προϊόν πληροί επίσης τις απαιτήσεις της άλλης νομοθεσίας.

6. Η Επιτροπή μπορεί, με εκτελεστικές πράξεις, να καθορίζει τεχνικές προδιαγραφές για εικονογράμματα ή άλλα σήματα που σχετίζονται με την ασφάλεια των προϊόντων με ψηφιακά στοιχεία, καθώς και μηχανισμούς για την προώθηση της χρήσης τους. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης του άρθρου 51 παράγραφος 2.

*Άρθρο 23*

*Τεχνικός φάκελος*

1. Ο τεχνικός φάκελος περιέχει όλα τα σχετικά δεδομένα ή λεπτομέρειες σχετικά με τα μέσα που χρησιμοποιεί ο κατασκευαστής για να εξασφαλίσει ότι το προϊόν με ψηφιακά στοιχεία και οι διαδικασίες που εφαρμόζει ο κατασκευαστής συμμορφώνονται με τις ουσιώδεις απαιτήσεις που καθορίζονται στο παράρτημα I. Περιέχει τουλάχιστον τα στοιχεία που καθορίζονται στο παράρτημα V.

2. Ο τεχνικός φάκελος καταρτίζεται πριν από τη διάθεση του προϊόντος με ψηφιακά στοιχεία στην αγορά και επικαιροποιείται συνεχώς, κατά περίπτωση, κατά την αναμενόμενη διάρκεια ζωής του προϊόντος ή για διάστημα πέντε ετών μετά τη διάθεση προϊόντος με ψηφιακά στοιχεία στην αγορά, ανάλογα με το ποιο διάστημα είναι μικρότερο.

3. Για τα προϊόντα με ψηφιακά στοιχεία που αναφέρονται στο άρθρο 8 και στο άρθρο 24 παράγραφος 4, τα οποία διέπονται και από άλλες πράξεις της Ένωσης, καταρτίζεται ενιαίος τεχνικός φάκελος που περιέχει τις πληροφορίες που αναφέρονται στο παράρτημα V του παρόντος κανονισμού και τις πληροφορίες που απαιτούνται από τις εν λόγω αντίστοιχες πράξεις της Ένωσης.

4. Ο τεχνικός φάκελος και η αλληλογραφία σχετικά με τη διαδικασία αξιολόγησης της συμμόρφωσης συντάσσονται στην επίσημη γλώσσα του κράτους μέλους στο οποίο είναι εγκατεστημένος ο κοινοποιημένος οργανισμός ή σε γλώσσα αποδεκτή από τον εν λόγω οργανισμό.

5. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 50 για τη συμπλήρωση του παρόντος κανονισμού με τα στοιχεία που πρέπει να περιλαμβάνονται στον τεχνικό φάκελο του παραρτήματος V, ώστε να λαμβάνονται υπόψη οι τεχνολογικές εξελίξεις, καθώς και οι εξελίξεις που προκύπτουν κατά τη διαδικασία εφαρμογής του παρόντος κανονισμού.

*Άρθρο 24*

*Διαδικασίες αξιολόγησης της συμμόρφωσης για προϊόντα με ψηφιακά στοιχεία*

1. Ο κατασκευαστής διενεργεί αξιολόγηση της συμμόρφωσης του προϊόντος με ψηφιακά στοιχεία και των διαδικασιών που εφαρμόζει ο κατασκευαστής για να

διαπιστώσει αν πληρούνται οι ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα Ι. Ο κατασκευαστής ή ο εξουσιοδοτημένος αντιπρόσωπος του κατασκευαστή αποδεικνύει τη συμμόρφωση προς τις ουσιώδεις απαιτήσεις εφαρμόζοντας μία από τις ακόλουθες διαδικασίες:

α) τη διαδικασία εσωτερικού ελέγχου (βάσει της ενότητας Α) που ορίζεται στο παράρτημα VI· ή

β) τη διαδικασία εξέτασης τύπου ΕΕ (βάσει της ενότητας Β) που αναφέρεται στο παράρτημα VI, η οποία ακολουθείται από συμμόρφωση προς τον τύπο ΕΕ με βάση τον εσωτερικό έλεγχο παραγωγής (βάσει της ενότητας Γ) που αναφέρεται στο παράρτημα VI· ή

γ) αξιολόγηση συμμόρφωσης με βάση την πλήρη διασφάλιση ποιότητας (βάσει της ενότητας Η), που ορίζεται στο παράρτημα VI.

2. Όταν, κατά την αξιολόγηση της συμμόρφωσης του κρίσιμου προϊόντος με ψηφιακά στοιχεία της κατηγορίας Ι που ορίζεται στο παράρτημα ΙΙΙ και των διαδικασιών που εφαρμόζει ο κατασκευαστής του προς τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα Ι, ο κατασκευαστής ή ο εξουσιοδοτημένος αντιπρόσωπός του δεν έχει εφαρμόσει ή έχει εφαρμόσει μόνο εν μέρει εναρμονισμένα πρότυπα, κοινές προδιαγραφές ή ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας, όπως αναφέρονται στο άρθρο 18, ή όταν δεν υπάρχουν τα εν λόγω εναρμονισμένα πρότυπα, κοινές προδιαγραφές ή ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας, το σχετικό προϊόν με ψηφιακά στοιχεία και οι διαδικασίες που εφαρμόζει ο κατασκευαστής υποβάλλονται, όσον αφορά τις εν λόγω ουσιώδεις απαιτήσεις, σε μία από τις ακόλουθες διαδικασίες:

α) διαδικασία εξέτασης τύπου ΕΕ (βάσει της ενότητας Β) που προβλέπεται στο παράρτημα VI, η οποία ακολουθείται από συμμόρφωση προς τον τύπο ΕΕ με βάση τον εσωτερικό έλεγχο παραγωγής (βάσει της ενότητας Γ) που αναφέρεται στο παράρτημα VI· ή

β) αξιολόγηση συμμόρφωσης με βάση την πλήρη διασφάλιση ποιότητας (βάσει της ενότητας Η), που ορίζεται στο παράρτημα VI.

3. Όταν το προϊόν είναι κρίσιμο προϊόν με ψηφιακά στοιχεία της κατηγορίας ΙΙ, όπως ορίζεται στο παράρτημα ΙΙΙ, ο κατασκευαστής ή ο εξουσιοδοτημένος αντιπρόσωπός του αποδεικνύει τη συμμόρφωση προς τις ουσιώδεις απαιτήσεις που καθορίζονται στο παράρτημα Ι εφαρμόζοντας μία από τις ακόλουθες διαδικασίες:

α) τη διαδικασία εξέτασης τύπου ΕΕ (βάσει της ενότητας Β) που αναφέρεται στο παράρτημα VI, η οποία ακολουθείται από συμμόρφωση προς τον τύπο ΕΕ με βάση τον εσωτερικό έλεγχο παραγωγής (βάσει της ενότητας Γ) που αναφέρεται στο παράρτημα VI· ή

β) αξιολόγηση συμμόρφωσης με βάση την πλήρη διασφάλιση ποιότητας (βάσει της ενότητας Η), που ορίζεται στο παράρτημα VI.

4. Οι κατασκευαστές προϊόντων με ψηφιακά στοιχεία που ταξινομούνται ως συστήματα ΗΜΥ στο πλαίσιο του πεδίου εφαρμογής του κανονισμού [κανονισμός για τον ευρωπαϊκό χώρο δεδομένων για την υγεία] αποδεικνύουν τη συμμόρφωση προς τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα Ι του παρόντος κανονισμού εφαρμόζοντας τη σχετική διαδικασία αξιολόγησης της συμμόρφωσης που απαιτείται από τον κανονισμό [κεφάλαιο ΙΙΙ του κανονισμού για τον ευρωπαϊκό χώρο δεδομένων για την υγεία].

5. Οι κοινοποιημένοι οργανισμοί λαμβάνουν υπόψη τα ειδικά συμφέροντα και τις ανάγκες των μικρών και μεσαίων επιχειρήσεων (ΜΜΕ) κατά τον καθορισμό των τελών για τις διαδικασίες αξιολόγησης της συμμόρφωσης και μειώνουν τα τέλη αυτά κατ' αναλογία προς τα ειδικά συμφέροντα και τις ανάγκες τους.

## ΚΕΦΑΛΑΙΟ IV

## ΚΟΙΝΟΠΟΙΗΣΗ ΤΩΝ ΟΡΓΑΝΙΣΜΩΝ ΑΞΙΟΛΟΓΗΣΗΣ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ

*Άρθρο 25*

*Κοινοποίηση*

Τα κράτη μέλη κοινοποιούν στην Επιτροπή και στα άλλα κράτη μέλη τους οργανισμούς αξιολόγησης της συμμόρφωσης που έχουν λάβει έγκριση για τη διενέργεια αξιολογήσεων της συμμόρφωσης σύμφωνα με τον παρόντα κανονισμό.

*Άρθρο 26*

*Κοινοποιούσες αρχές*

1. Τα κράτη μέλη ορίζουν μία κοινοποιούσα αρχή η οποία είναι υπεύθυνη για τον καθορισμό και τη διεξαγωγή των αναγκαίων διαδικασιών αξιολόγησης και κοινοποίησης των οργανισμών αξιολόγησης της συμμόρφωσης και για την παρακολούθηση των κοινοποιημένων οργανισμών, συμπεριλαμβανομένης της συμμόρφωσης με τις διατάξεις του άρθρου 31.

2. Τα κράτη μέλη μπορούν να αποφασίζουν ότι η αξιολόγηση και η παρακολούθηση που αναφέρονται στην παράγραφο 1 διεξάγονται από εθνικό οργανισμό διαπίστευσης κατά την έννοια του κανονισμού (ΕΚ) αριθ. 765/2008 και σύμφωνα με τον κανονισμό αυτόν.

*Άρθρο 27*

*Απαιτήσεις σχετικά με τις κοινοποιούσες αρχές*

1. Η κοινοποιούσα αρχή συγκροτείται κατά τρόπο που δεν συνεπάγεται σύγκρουση συμφερόντων με τους οργανισμούς αξιολόγησης της συμμόρφωσης.

2. Η κοινοποιούσα αρχή οργανώνεται και λειτουργεί κατά τρόπο ώστε να διασφαλίζεται η αντικειμενικότητα και η αμεροληψία των δραστηριοτήτων της.

3. Η κοινοποιούσα αρχή οργανώνεται κατά τρόπο ώστε κάθε απόφαση που αφορά την κοινοποίηση ενός οργανισμού αξιολόγησης της συμμόρφωσης να λαμβάνεται από αρμόδια πρόσωπα που είναι άλλα από τα πρόσωπα που διεξήγαγαν την αξιολόγηση.

4. Η κοινοποιούσα αρχή δεν προσφέρει ούτε παρέχει οποιεσδήποτε δραστηριότητες που εκτελούνται από οργανισμούς αξιολόγησης της συμμόρφωσης ή οποιεσδήποτε συμβουλευτικές υπηρεσίες σε εμπορική ή ανταγωνιστική βάση.

5. Η κοινοποιούσα αρχή εξασφαλίζει την εμπιστευτικότητα των πληροφοριών που λαμβάνει.

6. Η κοινοποιούσα αρχή διαθέτει επαρκές αρμόδιο προσωπικό για την ορθή εκτέλεση των καθηκόντων της.

*Άρθρο 28*

*Υποχρέωση ενημέρωσης για τις κοινοποιούσες αρχές*

1. Τα κράτη μέλη ενημερώνουν την Επιτροπή σχετικά με τις διαδικασίες που ακολουθούν για την αξιολόγηση και την κοινοποίηση των οργανισμών αξιολόγησης της συμμόρφωσης και για την παρακολούθηση των κοινοποιημένων οργανισμών, καθώς και για τυχόν αλλαγές των διαδικασιών αυτών.

2. Η Επιτροπή δημοσιοποιεί αυτές τις πληροφορίες.

*Άρθρο 29*

*Απαιτήσεις όσον αφορά τους κοινοποιημένους οργανισμούς*

1. Για τους σκοπούς της κοινοποίησης, ο οργανισμός αξιολόγησης της συμμόρφωσης πληροί τις απαιτήσεις των παραγράφων 2 έως 12.

2. Ο οργανισμός αξιολόγησης της συμμόρφωσης ιδρύεται βάσει του εθνικού δικαίου και διαθέτει νομική προσωπικότητα.

3. Ο οργανισμός αξιολόγησης της συμμόρφωσης είναι ανεξάρτητος από τον οργανισμό ή το προϊόν που αξιολογεί.

   Ένας οργανισμός που ανήκει σε ένωση επιχειρήσεων ή επαγγελματική ομοσπονδία που εκπροσωπεί τις επιχειρήσεις οι οποίες συμμετέχουν στον σχεδιασμό, την ανάπτυξη, παραγωγή, παροχή, συναρμολόγηση, χρήση ή συντήρηση των προϊόντων με ψηφιακά στοιχεία τα οποία αξιολογεί, μπορεί να θεωρείται οργανισμός αξιολόγησης, υπό την προϋπόθεση ότι η ανεξαρτησία του και η απουσία σύγκρουσης συμφερόντων είναι αποδεδειγμένες.

4. Ο οργανισμός αξιολόγησης της συμμόρφωσης, τα διευθυντικά του στελέχη και το προσωπικό που είναι αρμόδιο για την εκτέλεση των καθηκόντων αξιολόγησης της συμμόρφωσης δεν συμπίπτουν με το σχεδιαστή, προγραμματιστή, κατασκευαστή, προμηθευτή, υπεύθυνο εγκατάστασης, αγοραστή, ιδιοκτήτη, χρήστη ή συντηρητή των προϊόντων με ψηφιακά στοιχεία που αξιολογούν ούτε με τον εξουσιοδοτημένο αντιπρόσωπο των ανωτέρω. Αυτό δεν αποκλείει τη χρήση αξιολογημένων προϊόντων που είναι αναγκαία για τις λειτουργίες του οργανισμού αξιολόγησης της συμμόρφωσης ή τη χρήση των προϊόντων για προσωπικούς σκοπούς.

   Ο οργανισμός αξιολόγησης της συμμόρφωσης, τα διευθυντικά του στελέχη και το προσωπικό που είναι αρμόδιο για την εκτέλεση των καθηκόντων αξιολόγησης της συμμόρφωσης δεν εμπλέκονται άμεσα στον σχεδιασμό, την ανάπτυξη, την παραγωγή, την εμπορία, την εγκατάσταση, τη χρήση ή τη συντήρηση των εν λόγω προϊόντων, ούτε εκπροσωπούν τα μέρη που εμπλέκονται στις δραστηριότητες αυτές. Δεν αναλαμβάνουν καμία δραστηριότητα που μπορεί να θίξει την ανεξάρτητη κρίση και την ακεραιότητά τους σε σχέση με τις δραστηριότητες αξιολόγησης της συμμόρφωσης για τις οποίες έχουν κοινοποιηθεί. Αυτό ισχύει ιδίως για τις συμβουλευτικές υπηρεσίες.

   Ο οργανισμός αξιολόγησης της συμμόρφωσης εξασφαλίζει ότι οι δραστηριότητες των θυγατρικών ή των υπεργολάβων δεν επηρεάζουν την εμπιστευτικότητα, την αντικειμενικότητα και την αμεροληψία των δραστηριοτήτων αξιολόγησης της συμμόρφωσης.

5. Ο οργανισμός αξιολόγησης της συμμόρφωσης και το προσωπικό του εκτελούν τις δραστηριότητες αξιολόγησης της συμμόρφωσης με τη μέγιστη επαγγελματική

ακεραιότητα και την απαιτούμενη τεχνική επάρκεια στον συγκεκριμένο τομέα και οφείλουν να είναι απαλλαγμένοι από κάθε πίεση και προτροπή, κυρίως οικονομική, που θα ήταν δυνατόν να επηρεάσει την κρίση τους ή τα αποτελέσματα των δραστηριοτήτων τους αυτών, ιδιαίτερα από πρόσωπα ή ομάδες προσώπων που έχουν συμφέρον από τα αποτελέσματα των ελέγχων.

6. Ο οργανισμός αξιολόγησης της συμμόρφωσης είναι σε θέση να εκτελεί όλα τα καθήκοντα τα σχετικά με την αξιολόγηση της συμμόρφωσης που του έχουν ανατεθεί βάσει των διατάξεων του παραρτήματος VI και για τα οποία έχει κοινοποιηθεί, ανεξαρτήτως του αν πρόκειται για καθήκοντα που εκτελούνται από τον ίδιο τον οργανισμό αξιολόγησης της συμμόρφωσης ή για λογαριασμό του και υπό την ευθύνη του.

Ανά πάσα στιγμή και για κάθε διαδικασία αξιολόγησης της συμμόρφωσης και για κάθε είδος ή κατηγορία προϊόντων με ψηφιακά στοιχεία για τα οποία είναι κοινοποιημένος, ο οργανισμός αξιολόγησης της συμμόρφωσης έχει στη διάθεσή του:

α) το αναγκαίο προσωπικό με τεχνικές γνώσεις και επαρκή και κατάλληλη πείρα για την εκτέλεση των καθηκόντων αξιολόγησης της συμμόρφωσης·

β) τις αναγκαίες περιγραφές των διαδικασιών σύμφωνα με τις οποίες διενεργείται η αξιολόγηση της συμμόρφωσης και εξασφαλίζεται η διαφάνεια και η δυνατότητα αναπαραγωγής αυτών των διαδικασιών. Διαθέτει την κατάλληλη πολιτική και τις διαδικασίες που εξασφαλίζουν τη διάκριση μεταξύ των καθηκόντων τα οποία εκτελεί ως κοινοποιημένος οργανισμός και οποιασδήποτε άλλης δραστηριότητας·

γ) τις αναγκαίες διαδικασίες για να ασκεί τις δραστηριότητές του λαμβάνοντας υπόψη το μέγεθος μιας επιχείρησης, τον τομέα στον οποίο δραστηριοποιείται, τη δομή της, τον βαθμό πολυπλοκότητας της τεχνολογίας του προϊόντος και τον μαζικό ή εν σειρά χαρακτήρα της παραγωγικής διαδικασίας.

Διαθέτει τα αναγκαία μέσα για την ενδεδειγμένη εκτέλεση των τεχνικών και διοικητικών καθηκόντων που συνδέονται με τις δραστηριότητες αξιολόγησης της συμμόρφωσης και έχει πρόσβαση σε όλο τον αναγκαίο εξοπλισμό ή εγκαταστάσεις.

7. Το προσωπικό που είναι αρμόδιο για τη διεξαγωγή των δραστηριοτήτων αξιολόγησης της συμμόρφωσης διαθέτει:

α) πλήρη τεχνική και επαγγελματική κατάρτιση, η οποία καλύπτει όλες τις δραστηριότητες αξιολόγησης της συμμόρφωσης για τις οποίες έχει κοινοποιηθεί ο οργανισμός αξιολόγησης της συμμόρφωσης·

β) επαρκή γνώση των απαιτήσεων των αξιολογήσεων που διενεργεί και επαρκές κύρος για την εκτέλεση των εν λόγω αξιολογήσεων·

γ) κατάλληλες γνώσεις και κατανόηση των βασικών απαιτήσεων, των εφαρμοστέων εναρμονισμένων προτύπων και των σχετικών διατάξεων της ενωσιακής νομοθεσίας εναρμόνισης και των εκτελεστικών πράξεών της·

δ) την απαιτούμενη ικανότητα να καταρτίζει τα πιστοποιητικά, τα πρακτικά και τις εκθέσεις που αποδεικνύουν τη διεξαγωγή των αξιολογήσεων.

8. Η αμεροληψία του οργανισμού αξιολόγησης της συμμόρφωσης, των διευθυντικών στελεχών του και του προσωπικού αξιολόγησης είναι εγγυημένη.

Οι αμοιβές των διευθυντικών στελεχών και του προσωπικού του οργανισμού αξιολόγησης δεν εξαρτώνται από τον αριθμό των αξιολογήσεων που διενεργούνται ή από τα αποτελέσματα των αξιολογήσεων αυτών.

9. Ο οργανισμός αξιολόγησης της συμμόρφωσης συνάπτει ασφάλεια αστικής ευθύνης, εάν η ευθύνη αυτή δεν καλύπτεται από το κράτος βάσει του εθνικού δικαίου ή εάν η αξιολόγηση της συμμόρφωσης δεν πραγματοποιείται υπό την άμεση ευθύνη του κράτους μέλους.

10. Το προσωπικό του οργανισμού αξιολόγησης της συμμόρφωσης δεσμεύεται να τηρεί το επαγγελματικό απόρρητο για κάθε πληροφορία που περιέρχεται σε γνώση του κατά την εκτέλεση των καθηκόντων του σύμφωνα με το παράρτημα VI ή οποιαδήποτε εκτελεστική διάταξη του εθνικού δικαίου, εξαιρουμένης της σχέσης με τις αρχές εποπτείας της αγοράς του κράτους μέλους στο οποίο διεξάγονται οι δραστηριότητες του οργανισμού. Τα δικαιώματα κυριότητας προστατεύονται. Ο οργανισμός αξιολόγησης της συμμόρφωσης διαθέτει τεκμηριωμένες διαδικασίες που εξασφαλίζουν τη συμμόρφωση με την παρούσα παράγραφο.

11. Οι οργανισμοί αξιολόγησης της συμμόρφωσης συμμετέχουν στις σχετικές δραστηριότητες τυποποίησης και στις δραστηριότητες της ομάδας συντονισμού των κοινοποιημένων οργανισμών, η οποία έχει συσταθεί δυνάμει του άρθρου 40, ή εξασφαλίζουν ότι το προσωπικό αξιολόγησης ενημερώνεται για τις δραστηριότητες αυτές, και εφαρμόζει ως γενικές οδηγίες τις διοικητικές αποφάσεις και τα έγγραφα που είναι το αποτέλεσμα των εργασιών της εν λόγω ομάδας.

12. Οι οργανισμοί αξιολόγησης της συμμόρφωσης λειτουργούν σύμφωνα με σειρά συνεπών, δίκαιων και εύλογων όρων και προϋποθέσεων, λαμβάνοντας ιδίως υπόψη τα συμφέροντα των ΜΜΕ σε σχέση με τις αμοιβές.

*Άρθρο 30*

*Τεκμήριο συμμόρφωσης των κοινοποιημένων οργανισμών*

Όταν ένας οργανισμός αξιολόγησης της συμμόρφωσης αποδεικνύει ότι πληροί τα κριτήρια που ορίζονται στα σχετικά εναρμονισμένα πρότυπα ή σε μέρη αυτών, τα στοιχεία αναφοράς των οποίων έχουν δημοσιευθεί στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, τότε τεκμαίρεται ότι συμμορφώνεται προς τις απαιτήσεις του άρθρου 29 εφόσον τα εφαρμοστέα εναρμονισμένα πρότυπα καλύπτουν τις απαιτήσεις αυτές.

*Άρθρο 31*

*Θυγατρικές και υπεργολάβοι κοινοποιημένων οργανισμών*

1. Όταν ο κοινοποιημένος οργανισμός αναθέτει υπεργολαβικά συγκεκριμένα καθήκοντα που συνδέονται με την αξιολόγηση της συμμόρφωσης ή προσφεύγει σε θυγατρική, εξασφαλίζει ότι ο υπεργολάβος ή η θυγατρική πληροί τις απαιτήσεις του άρθρου 29, και ενημερώνει την κοινοποιούσα αρχή.

2. Ο κοινοποιημένος οργανισμός αναλαμβάνει πλήρως την ευθύνη για τα καθήκοντα που εκτελούν οι υπεργολάβοι ή οι θυγατρικές, όπου κι αν είναι εγκατεστημένοι.

3. Οι δραστηριότητες μπορούν να ανατίθενται σε υπεργολάβο ή να διεξάγονται από θυγατρική μόνον εφόσον συμφωνήσει ο κατασκευαστής.

4. Οι κοινοποιημένοι οργανισμοί τηρούν στη διάθεση της κοινοποιούσας αρχής τα έγγραφα σχετικά με την αξιολόγηση των προσόντων του υπεργολάβου ή της

θυγατρικής και σχετικά με τις εργασίες που διεξήγαγε ο υπεργολάβος ή η θυγατρική δυνάμει του παρόντος κανονισμού.

*Άρθρο 32*

*Αίτηση κοινοποίησης*

1. Ο οργανισμός αξιολόγησης της συμμόρφωσης υποβάλλει αίτηση κοινοποίησης στην κοινοποιούσα αρχή του κράτους μέλους στο οποίο είναι εγκατεστημένος.

2. Η εν λόγω αίτηση συνοδεύεται από περιγραφή των δραστηριοτήτων αξιολόγησης της συμμόρφωσης, της διαδικασίας ή των διαδικασιών αξιολόγησης της συμμόρφωσης και του προϊόντος ή των προϊόντων για τα οποία ο οργανισμός ισχυρίζεται ότι είναι αρμόδιος, καθώς και από πιστοποιητικό διαπίστευσης, όταν αυτό υπάρχει, το οποίο έχει εκδοθεί από εθνικό οργανισμό διαπίστευσης, δια του οποίου πιστοποιείται ότι ο οργανισμός αξιολόγησης της συμμόρφωσης πληροί τις απαιτήσεις του άρθρου 29.

3. Αν ο οργανισμός αξιολόγησης της συμμόρφωσης δεν μπορεί να προσκομίσει πιστοποιητικό διαπίστευσης, τότε παρέχει στην κοινοποιούσα αρχή όλη την τεκμηρίωση που είναι αναγκαία για την επαλήθευση, αναγνώριση και τακτική παρακολούθηση της συμμόρφωσής του με τις απαιτήσεις του άρθρου 29.

*Άρθρο 33*

*Διαδικασία κοινοποίησης*

1. Οι κοινοποιούσες αρχές μπορούν να κοινοποιούν μόνο τους οργανισμούς αξιολόγησης της συμμόρφωσης που πληρούν τις απαιτήσεις του άρθρου 29.

2. Η κοινοποιούσα αρχή ενημερώνει την Επιτροπή και τα άλλα κράτη μέλη που χρησιμοποιούν το σύστημα πληροφόρησης των κοινοποιημένων και διαπιστευμένων οργανισμών νέας προσέγγισης (NANDO) που έχει αναπτύξει και διαχειρίζεται η Επιτροπή.

3. Στην κοινοποίηση περιλαμβάνονται όλα τα στοιχεία για τις δραστηριότητες αξιολόγησης της συμμόρφωσης, την ενότητα ή τις ενότητες αξιολόγησης της συμμόρφωσης και το προϊόν ή τα προϊόντα και τη σχετική βεβαίωση επάρκειας.

4. Όταν η κοινοποίηση δεν βασίζεται σε πιστοποιητικό διαπίστευσης του άρθρου 32 παράγραφος 2, η κοινοποιούσα αρχή παρέχει στην Επιτροπή και στα άλλα κράτη μέλη την τεκμηρίωση που πιστοποιεί την επάρκεια του οργανισμού αξιολόγησης της συμμόρφωσης και τις υφιστάμενες ρυθμίσεις για να εξασφαλιστεί ότι ο οργανισμός θα ελέγχεται τακτικά και θα συνεχίσει να πληροί τις απαιτήσεις του άρθρου 29.

5. Ο εν λόγω οργανισμός μπορεί να εκτελεί τις δραστηριότητες κοινοποιημένου οργανισμού μόνον εφόσον δεν έχει διατυπωθεί ένσταση από την Επιτροπή και τα άλλα κράτη μέλη εντός δύο εβδομάδων από την κοινοποίηση εάν χρησιμοποιείται πιστοποιητικό διαπίστευσης ή εντός δύο μηνών από την κοινοποίηση εάν δεν χρησιμοποιείται διαπίστευση.

   Μόνο υπό αυτές τις προϋποθέσεις θεωρείται κοινοποιημένος ο οργανισμός για τους σκοπούς του παρόντος κανονισμού.

6. Η Επιτροπή και τα άλλα κράτη μέλη ενημερώνονται για τυχόν επακόλουθες αλλαγές στην κοινοποίηση.

*Άρθρο 34*

*Αριθμοί μητρώου και κατάλογοι κοινοποιηθέντων οργανισμών*

1. Η Επιτροπή χορηγεί αριθμό μητρώου σε κάθε κοινοποιημένο οργανισμό.

   Χορηγεί έναν μοναδικό αριθμό, ακόμη και αν ο οργανισμός είναι κοινοποιημένος βάσει διαφόρων πράξεων της Ένωσης.

2. Η Επιτροπή δημοσιοποιεί τον κατάλογο των οργανισμών που κοινοποιούνται βάσει του παρόντος κανονισμού, συμπεριλαμβανομένων των αριθμών μητρώου που τους έχουν χορηγηθεί και των δραστηριοτήτων για τις οποίες έχουν κοινοποιηθεί.

   Η Επιτροπή μεριμνά για την ενημέρωση του καταλόγου αυτού.

*Άρθρο 35*

*Τροποποιήσεις κοινοποιήσεων*

1. Όταν κοινοποιούσα αρχή διαπιστώνει ή πληροφορείται ότι κοινοποιημένος οργανισμός δεν πληροί πλέον τις απαιτήσεις του άρθρου 29 ή ότι αδυνατεί να εκπληρώσει τις υποχρεώσεις του, η κοινοποιούσα αρχή περιορίζει, αναστέλλει ή ανακαλεί την κοινοποίηση, κατά περίπτωση, αναλόγως της σοβαρότητας της μη τήρησης των απαιτήσεων ή της μη εκπλήρωσης των υποχρεώσεων. Ενημερώνει αμέσως σχετικά την Επιτροπή και τα άλλα κράτη μέλη.

2. Στην περίπτωση περιορισμού, αναστολής ή ανάκλησης της κοινοποίησης ή όταν ο κοινοποιημένος οργανισμός παύσει τη δραστηριότητά του, το κοινοποιούν κράτος μέλος προβαίνει στις δέουσες ενέργειες για να εξασφαλίσει ότι τα αρχεία του οργανισμού αυτού είτε τα χειρίζεται άλλος κοινοποιημένος οργανισμός είτε τα καθιστά διαθέσιμα στις αρμόδιες αρχές κοινοποίησης και εποπτείας της αγοράς, κατόπιν αιτήματός τους.

*Άρθρο 36*

*Αμφισβήτηση της επάρκειας των κοινοποιημένων οργανισμών*

1. Η Επιτροπή ερευνά όλες τις περιπτώσεις κατά τις οποίες έχει αμφιβολίες ή περιέρχονται σε γνώση της εικασίες όσον αφορά την επάρκεια κοινοποιημένου οργανισμού ή την ικανότητα συνεχούς εκπλήρωσης από κοινοποιημένο οργανισμό των απαιτήσεων και των υποχρεώσεων που υπέχει.

2. Το κοινοποιούν κράτος μέλος παρέχει στην Επιτροπή, εάν αυτή το ζητήσει, όλες τις πληροφορίες σχετικά με την αιτιολόγηση της κοινοποίησης ή της διατήρησης της επάρκειας του εν λόγω οργανισμού.

3. Η Επιτροπή διασφαλίζει τον εμπιστευτικό χαρακτήρα όλων των ευαίσθητων πληροφοριών που λαμβάνει στο πλαίσιο των ερευνών της.

4. Όταν η Επιτροπή διαπιστώνει ότι κοινοποιημένος οργανισμός δεν πληροί ή παύει να πληροί τις απαιτήσεις κοινοποίησής του, ενημερώνει το κοινοποιούν κράτος μέλος σχετικά και ζητεί από το τελευταίο να λάβει τα αναγκαία διορθωτικά μέτρα, συμπεριλαμβανομένης της άρσης της κοινοποίησης, εφόσον είναι αναγκαίο.

*Άρθρο 37*

*Λειτουργικές υποχρεώσεις των κοινοποιημένων οργανισμών*

1. Οι κοινοποιημένοι οργανισμοί διενεργούν αξιολογήσεις συμμόρφωσης σύμφωνα με τις διαδικασίες αξιολόγησης της συμμόρφωσης που προβλέπονται στο άρθρο 24 και στο παράρτημα VI.

2. Οι αξιολογήσεις της συμμόρφωσης διενεργούνται κατά τρόπο ώστε να αποφεύγονται οι περιττές επιβαρύνσεις για τους οικονομικούς φορείς. Οι οργανισμοί αξιολόγησης της συμμόρφωσης ασκούν τις δραστηριότητές τους λαμβάνοντας δεόντως υπόψη το μέγεθος μιας επιχείρησης, τον τομέα στον οποίο δραστηριοποιείται, τη δομή της, την πολυπλοκότητα της τεχνολογίας του προϊόντος για το οποίο πρόκειται και τον μαζικό ή εν σειρά χαρακτήρα της διαδικασίας παραγωγής.

3. Οι κοινοποιημένοι οργανισμοί τηρούν τον βαθμό αυστηρότητας και το επίπεδο προστασίας που απαιτούνται για τη συμμόρφωση του προϊόντος με τις διατάξεις του παρόντος κανονισμού.

4. Όταν κοινοποιημένος οργανισμός διαπιστώσει ότι οι απαιτήσεις του παραρτήματος I ή των αντίστοιχων εναρμονισμένων προτύπων ή των κοινών προδιαγραφών που αναφέρονται στο άρθρο 19 δεν πληρούνται από τον κατασκευαστή, του ζητεί να λάβει τα ενδεδειγμένα διορθωτικά μέτρα και δεν εκδίδει πιστοποιητικό συμμόρφωσης.

5. Όταν, κατά την παρακολούθηση της συμμόρφωσης μετά την έκδοση πιστοποιητικού, κοινοποιημένος οργανισμός διαπιστώσει ότι κάποιο προϊόν δεν συμμορφώνεται πλέον με τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό, τότε απαιτεί από τον κατασκευαστή να λάβει τα απαραίτητα διορθωτικά μέτρα και αναστέλλει ή ανακαλεί το πιστοποιητικό, εφόσον απαιτείται.

6. Εάν δεν ληφθούν διορθωτικά μέτρα ή εάν αυτά δεν έχουν το απαιτούμενο αποτέλεσμα, ο κοινοποιημένος οργανισμός περιορίζει, αναστέλλει ή ανακαλεί τυχόν πιστοποιητικό, κατά περίπτωση.

*Άρθρο 38*

*Υποχρέωση ενημέρωσης για τους κοινοποιημένους οργανισμούς*

1. Οι κοινοποιημένοι οργανισμοί ενημερώνουν την κοινοποιούσα αρχή για τα εξής:

   α) άρνηση, περιορισμό, αναστολή ή ανάκληση πιστοποιητικού·

   β) καταστάσεις που επηρεάζουν το πεδίο εφαρμογής και τους όρους της κοινοποίησης·

   γ) τυχόν αίτημα παροχής πληροφοριών σχετικά με δραστηριότητες αξιολόγησης της συμμόρφωσης, το οποίο έλαβαν από τις αρχές εποπτείας της αγοράς·

   δ) κατόπιν αιτήματος, για τις δραστηριότητες αξιολόγησης της συμμόρφωσης που εκτελούν στο πλαίσιο της κοινοποίησής τους και για οποιαδήποτε άλλη δραστηριότητα, συμπεριλαμβανομένων των διασυνοριακών δραστηριοτήτων και υπεργολαβιών.

2. Οι κοινοποιημένοι οργανισμοί παρέχουν στους άλλους κοινοποιημένους δυνάμει του παρόντος κανονισμού οργανισμούς, που διεξάγουν παρόμοιες δραστηριότητες αξιολόγησης της συμμόρφωσης και καλύπτουν τα ίδια προϊόντα, τις σχετικές πληροφορίες για ζητήματα που αφορούν αρνητικά και, εάν τους ζητηθεί, θετικά αποτελέσματα αξιολόγησης της συμμόρφωσης.

*Άρθρο 39*

*Ανταλλαγή εμπειριών*

Η Επιτροπή μεριμνά για την ανταλλαγή εμπειριών μεταξύ των εθνικών αρχών των κρατών μελών που είναι αρμόδιες για την πολιτική κοινοποίησης.

*Άρθρο 40*

*Συντονισμός των κοινοποιημένων οργανισμών*

1. Η Επιτροπή διασφαλίζει ότι θεσμοθετείται κατάλληλος συντονισμός και συνεργασία μεταξύ των κοινοποιημένων οργανισμών και ότι αυτά λειτουργούν σωστά με τη μορφή διατομεακής ομάδας των κοινοποιημένων οργανισμών.

2. Τα κράτη μέλη εξασφαλίζουν ότι οι οργανισμοί τους οποίους έχουν κοινοποιήσει συμμετέχουν στις εργασίες της εν λόγω ομάδας, απευθείας ή διά διορισθέντων αντιπροσώπων.

## ΚΕΦΑΛΑΙΟ V

## ΕΠΟΠΤΕΙΑ ΤΗΣ ΑΓΟΡΑΣ ΚΑΙ ΕΠΙΒΟΛΗ ΤΗΣ ΝΟΜΟΘΕΣΙΑΣ

*Άρθρο 41*

*Εποπτεία της αγοράς και έλεγχος των προϊόντων με ψηφιακά στοιχεία στην ενωσιακή αγορά*

1. Ο κανονισμός (ΕΕ) 2019/1020 εφαρμόζεται στα προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού.

2. Κάθε κράτος μέλος ορίζει μία ή περισσότερες αρχές εποπτείας της αγοράς για τη διασφάλιση της αποτελεσματικής εφαρμογής του παρόντος κανονισμού. Τα κράτη μέλη μπορούν να ορίσουν υφιστάμενη ή νέα αρχή η οποία θα ενεργεί ως αρχή εποπτείας της αγοράς για τον παρόντα κανονισμό.

3. Κατά περίπτωση, οι αρχές εποπτείας της αγοράς συνεργάζονται με τις εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας που ορίζονται σύμφωνα με το άρθρο 58 του κανονισμού (ΕΕ) 2019/881 και ανταλλάσσουν πληροφορίες σε τακτική βάση. Όσον αφορά την εποπτεία της εφαρμογής των υποχρεώσεων υποβολής εκθέσεων σύμφωνα με το άρθρο 11 του παρόντος κανονισμού, οι ορισθείσες αρχές εποπτείας της αγοράς συνεργάζονται με τον ENISA.

4. Κατά περίπτωση, οι αρχές εποπτείας της αγοράς συνεργάζονται με άλλες αρχές εποπτείας της αγοράς που ορίζονται βάσει άλλης ενωσιακής νομοθεσίας εναρμόνισης για άλλα προϊόντα και ανταλλάσσουν πληροφορίες σε τακτική βάση.

5. Οι αρχές εποπτείας της αγοράς συνεργάζονται, κατά περίπτωση, με τις αρχές που εποπτεύουν την ενωσιακή νομοθεσία για την προστασία των δεδομένων. Η συνεργασία αυτή περιλαμβάνει την ενημέρωση των εν λόγω αρχών για κάθε εύρημα σχετικά με την εκπλήρωση των αρμοδιοτήτων τους, μεταξύ άλλων κατά την έκδοση κατευθυντήριων γραμμών και συμβουλών σύμφωνα με την παράγραφο 8 του παρόντος άρθρου, εάν οι εν λόγω κατευθυντήριες γραμμές και συμβουλές αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

   Οι αρχές που εποπτεύουν τη νομοθεσία της Ένωσης για την προστασία των δεδομένων έχουν την εξουσία να ζητούν και να έχουν πρόσβαση σε κάθε έγγραφο

που δημιουργείται ή διατηρείται δυνάμει του παρόντος κανονισμού, όταν η πρόσβαση στα εν λόγω έγγραφα είναι αναγκαία για την εκπλήρωση των καθηκόντων τους. Ενημερώνουν τις ορισθείσες αρχές εποπτείας της αγοράς του οικείου κράτους μέλους για κάθε σχετικό αίτημα.

6. Τα κράτη μέλη μεριμνούν ώστε οι ορισθείσες αρχές εποπτείας της αγοράς να διαθέτουν επαρκείς οικονομικούς και ανθρώπινους πόρους για την εκπλήρωση των καθηκόντων τους δυνάμει του παρόντος κανονισμού.

7. Η Επιτροπή διευκολύνει την ανταλλαγή εμπειριών μεταξύ των αρχών εποπτείας της αγοράς που έχουν οριστεί.

8. Οι αρχές εποπτείας της αγοράς μπορούν να παρέχουν καθοδήγηση και συμβουλές στους οικονομικούς φορείς σχετικά με την εφαρμογή του παρόντος κανονισμού, με την υποστήριξη της Επιτροπής.

9. Οι αρχές εποπτείας της αγοράς υποβάλλουν ετήσια έκθεση στην Επιτροπή για τα αποτελέσματα των σχετικών δραστηριοτήτων εποπτείας της αγοράς. Οι αρχές εποπτείας της αγοράς αναφέρουν, χωρίς καθυστέρηση, στην Επιτροπή και στις αρμόδιες εθνικές αρχές ανταγωνισμού κάθε πληροφορία που εντοπίζεται στο πλαίσιο των δραστηριοτήτων εποπτείας της αγοράς και η οποία ενδέχεται να παρουσιάζει ενδιαφέρον για την εφαρμογή των κανόνων ανταγωνισμού του ενωσιακού δικαίου περί ανταγωνισμού.

10. Για τα προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού και ταξινομούνται ως συστήματα ΤΝ υψηλού κινδύνου σύμφωνα με το άρθρο [άρθρο 6] του κανονισμού [κανονισμός για την ΤΝ], οι αρχές εποπτείας της αγοράς που ορίζονται για τους σκοπούς του κανονισμού [κανονισμός για την ΤΝ] είναι οι αρχές που είναι αρμόδιες για τις δραστηριότητες εποπτείας της αγοράς που απαιτούνται βάσει του παρόντος κανονισμού. Οι αρχές εποπτείας της αγοράς που ορίζονται σύμφωνα με τον κανονισμό [κανονισμός για την ΤΝ] συνεργάζονται, κατά περίπτωση, με τις αρχές εποπτείας της αγοράς που ορίζονται σύμφωνα με τον παρόντα κανονισμό και, όσον αφορά την εποπτεία της εκπλήρωσης των υποχρεώσεων υποβολής εκθέσεων σύμφωνα με το άρθρο 11, με τον ENISA. Οι αρχές εποπτείας της αγοράς που ορίζονται σύμφωνα με τον κανονισμό [κανονισμός για την ΤΝ] ενημερώνουν ιδίως τις αρχές εποπτείας της αγοράς που ορίζονται σύμφωνα με τον παρόντα κανονισμό για κάθε εύρημα σχετικά με την εκπλήρωση των καθηκόντων τους σε σχέση με την εφαρμογή του παρόντος κανονισμού.

11. Συγκροτείται ειδική ομάδα διοικητικής συνεργασίας (ADCO) για την ομοιόμορφη εφαρμογή του παρόντος κανονισμού, σύμφωνα με το άρθρο 30 παράγραφος 2 του κανονισμού (ΕΕ) 2019/1020. Η ADCO αποτελείται από εκπροσώπους των καθορισμένων αρχών εποπτείας της αγοράς και, κατά περίπτωση, εκπροσώπους των ενιαίων γραφείων σύνδεσης.

*Άρθρο 42*

*Πρόσβαση σε δεδομένα και τεκμηρίωση*

Όταν είναι αναγκαίο για την αξιολόγηση της συμμόρφωσης των προϊόντων με ψηφιακά στοιχεία και των διαδικασιών που εφαρμόζουν οι κατασκευαστές τους με τις ουσιώδεις απαιτήσεις που καθορίζονται στο παράρτημα Ι και κατόπιν αιτιολογημένου αιτήματος, οι αρχές εποπτείας της αγοράς έχουν πρόσβαση στα δεδομένα που απαιτούνται για την αξιολόγηση του σχεδιασμού, της ανάπτυξης, της παραγωγής και του χειρισμού των τρωτών

σημείων των εν λόγω προϊόντων, συμπεριλαμβανομένης της σχετικής εσωτερικής τεκμηρίωσης του αντίστοιχου οικονομικού φορέα.

*Άρθρο 43*

*Διαδικασία σε εθνικό επίπεδο σχετικά με προϊόντα με ψηφιακά στοιχεία που παρουσιάζουν σημαντικό κίνδυνο για την κυβερνοασφάλεια*

1. Όταν η αρχή εποπτείας της αγοράς ενός κράτους μέλους έχει επαρκείς λόγους να θεωρεί ότι ένα προϊόν με ψηφιακά στοιχεία, συμπεριλαμβανομένου του χειρισμού των τρωτών σημείων του, παρουσιάζει σημαντικό κίνδυνο για την κυβερνοασφάλεια, διενεργεί αξιολόγηση του οικείου προϊόντος με ψηφιακά στοιχεία όσον αφορά τη συμμόρφωσή του με όλες τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό. Οι σχετικοί οικονομικοί φορείς συνεργάζονται όπως απαιτείται με την αρχή εποπτείας της αγοράς.

   Εάν, κατά την εν λόγω αξιολόγηση, η αρχή εποπτείας της αγοράς διαπιστώσει ότι το προϊόν με ψηφιακά στοιχεία δεν συμμορφώνεται προς τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό, τότε ζητεί αμελλητί από τον σχετικό φορέα να λάβει όλα τα αναγκαία διορθωτικά μέτρα για να θέσει το προϊόν σε συμμόρφωση με τις απαιτήσεις ή να το αποσύρει από την αγορά ή να το ανακαλέσει εντός ευλόγου χρονικού διαστήματος, αναλόγου προς τη φύση του κινδύνου, το οποίο αυτή ορίζει.

   Η αρχή εποπτείας της αγοράς ενημερώνει σχετικά τον οικείο κοινοποιημένο οργανισμό. Το άρθρο 18 του κανονισμού (ΕΕ) 2019/1020 εφαρμόζεται στα αναγκαία διορθωτικά μέτρα.

2. Εάν η αρχή εποπτείας της αγοράς θεωρήσει ότι η μη συμμόρφωση δεν περιορίζεται στην εθνική της επικράτεια, ενημερώνει την Επιτροπή και τα άλλα κράτη μέλη για τα αποτελέσματα της αξιολόγησης και τα μέτρα που ζήτησε να λάβει ο φορέας εκμετάλλευσης.

3. Ο κατασκευαστής εξασφαλίζει ότι λαμβάνονται όλα τα ενδεικνυόμενα διορθωτικά μέτρα για όλα τα προϊόντα με ψηφιακά στοιχεία που έχει καταστήσει διαθέσιμα στην αγορά σε όλη την Ένωση.

4. Εάν ο κατασκευαστής προϊόντος με ψηφιακά στοιχεία δεν λάβει τα αναγκαία διορθωτικά μέτρα εντός του χρονικού διαστήματος που αναφέρεται στο δεύτερο εδάφιο της παραγράφου 1, η αρχή εποπτείας της αγοράς λαμβάνει όλα τα κατάλληλα προσωρινά μέτρα για να απαγορεύσει ή να περιορίσει τη διαθεσιμότητα του εν λόγω προϊόντος στην οικεία εθνική αγορά, να αποσύρει το προϊόν από την αγορά ή να το ανακαλέσει.

   Η εν λόγω αρχή ενημερώνει αμελλητί την Επιτροπή και τα άλλα κράτη μέλη για τα μέτρα αυτά.

5. Οι αναφερόμενες στην παράγραφο 4 πληροφορίες περιλαμβάνουν όλες τις διαθέσιμες λεπτομέρειες, ιδίως τα στοιχεία που απαιτούνται για την ταυτοποίηση των μη συμμορφούμενων προϊόντων με ψηφιακά στοιχεία, την καταγωγή του προϊόντος με ψηφιακά στοιχεία, τη φύση της τυχόν μη συμμόρφωσης και του σχετικού κινδύνου, τη φύση και τη διάρκεια των εθνικών μέτρων που ελήφθησαν καθώς και τα επιχειρήματα που προβάλλει ο σχετικός φορέας εκμετάλλευσης. Ειδικότερα, η αρχή εποπτείας της αγοράς αναφέρει αν η μη συμμόρφωση οφείλεται σε έναν ή περισσότερους από τους παρακάτω λόγους:

α) το προϊόν ή οι διαδικασίες που εφαρμόζει ο κατασκευαστής δεν πληρούν τις ουσιώδεις απαιτήσεις που καθορίζονται στο παράρτημα Ι·

β) ελλείψεις στα εναρμονισμένα πρότυπα, στα συστήματα πιστοποίησης της κυβερνοασφάλειας ή στις κοινές προδιαγραφές, όπως αναφέρονται στο άρθρο 18.

6. Οι αρχές εποπτείας της αγοράς των κρατών μελών πλην της αρχής εποπτείας της αγοράς του κράτους μέλους που κίνησε τη διαδικασία ενημερώνουν αμέσως την Επιτροπή και τα άλλα κράτη μέλη για τα μέτρα που έλαβαν και παρέχουν τυχόν άλλες πρόσθετες πληροφορίες που διαθέτουν όσον αφορά τη μη συμμόρφωση του σχετικού προϊόντος και, σε περίπτωση διαφωνίας με το κοινοποιηθέν εθνικό μέτρο, τις τυχόν αντιρρήσεις τους.

7. Εάν, εντός τριών μηνών από τη λήψη των κατά την παράγραφο 4 πληροφοριών, δεν έχει διατυπωθεί αντίρρηση από κράτος μέλος ή από την Επιτροπή σε σχέση με προσωρινό μέτρο που έχει λάβει κράτος μέλος, το μέτρο θεωρείται δικαιολογημένο. Αυτό ισχύει με την επιφύλαξη των διαδικαστικών δικαιωμάτων του ενδιαφερόμενου φορέα εκμετάλλευσης σύμφωνα με το άρθρο 18 του κανονισμού (ΕΕ) 2019/1020.

8. Οι αρχές εποπτείας της αγοράς όλων των κρατών μελών εξασφαλίζουν ότι λαμβάνονται αμελλητί τα κατάλληλα περιοριστικά μέτρα όσον αφορά το σχετικό προϊόν, όπως η άμεση απόσυρση του προϊόντος από την αγορά τους.

*Άρθρο 44*

*Διαδικασία διασφάλισης στο επίπεδο της Ένωσης*

1. Αν, εντός τριών μηνών από την παραλαβή της κοινοποίησης του άρθρου 43 παράγραφος 4, ένα κράτος μέλος διατυπώσει αντιρρήσεις για μέτρο που έλαβε άλλο κράτος μέλος ή αν η Επιτροπή κρίνει ότι το μέτρο αντιβαίνει στη νομοθεσία της Ένωσης, η Επιτροπή διαβουλεύεται αμελλητί με το οικείο κράτος μέλος και τον οικονομικό φορέα ή τους οικονομικούς φορείς και διενεργεί αξιολόγηση του εθνικού μέτρου. Βάσει των αποτελεσμάτων αυτής της αξιολόγησης, εντός εννέα μηνών από την κοινοποίηση που αναφέρεται στο άρθρο 43 παράγραφος 4 η Επιτροπή αποφασίζει αν το εθνικό μέτρο είναι δικαιολογημένο και κοινοποιεί την απόφαση αυτή στο οικείο κράτος μέλος.

2. Εάν το εθνικό μέτρο θεωρηθεί δικαιολογημένο, όλα τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν την απόσυρση του μη συμμορφούμενου προϊόντος με ψηφιακά στοιχεία από τις αγορές τους και ενημερώνουν την Επιτροπή σχετικά. Εάν το εθνικό μέτρο θεωρηθεί μη δικαιολογημένο, το οικείο κράτος μέλος ανακαλεί το μέτρο.

3. Αν το εθνικό μέτρο θεωρηθεί δικαιολογημένο και η μη συμμόρφωση του προϊόντος με ψηφιακά στοιχεία αποδοθεί σε ελλείψεις των εναρμονισμένων προτύπων, η Επιτροπή εφαρμόζει τη διαδικασία που προβλέπεται στο άρθρο 10 του κανονισμού (ΕΕ) αριθ. 1025/2012.

4. Αν το εθνικό μέτρο θεωρηθεί δικαιολογημένο και η μη συμμόρφωση του προϊόντος με ψηφιακά στοιχεία αποδοθεί σε ελλείψεις του ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας, όπως αναφέρεται στο άρθρο 18, η Επιτροπή εξετάζει αν θα τροποποιήσει ή θα καταργήσει την εκτελεστική πράξη που αναφέρεται στο άρθρο 18 παράγραφος 4, η οποία προσδιορίζει το τεκμήριο συμμόρφωσης όσον αφορά το εν λόγω σύστημα πιστοποίησης.

5. Αν το εθνικό μέτρο θεωρηθεί δικαιολογημένο και η μη συμμόρφωση του προϊόντος με ψηφιακά στοιχεία αποδοθεί σε ελλείψεις των κοινών προδιαγραφών, όπως αναφέρεται στο άρθρο 19, η Επιτροπή εξετάζει αν θα τροποποιήσει ή θα καταργήσει την εκτελεστική πράξη που αναφέρεται στο άρθρο 19 για τον καθορισμό των εν λόγω κοινών προδιαγραφών.

*Άρθρο 45*

*Διαδικασία σε ενωσιακό επίπεδο σχετικά με προϊόντα με ψηφιακά στοιχεία που παρουσιάζουν σημαντικό κίνδυνο για την κυβερνοασφάλεια*

1. Εάν η Επιτροπή έχει επαρκείς λόγους να πιστεύει, μεταξύ άλλων με βάση τις πληροφορίες που παρέχει ο ENISA, ότι ένα προϊόν με ψηφιακά στοιχεία που παρουσιάζει σημαντικό κίνδυνο για την κυβερνοασφάλεια δεν συμμορφώνεται με τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό, μπορεί να ζητήσει από τις αρμόδιες αρχές εποπτείας της αγοράς να διενεργήσουν αξιολόγηση της συμμόρφωσης και να ακολουθήσουν τις διαδικασίες που αναφέρονται στο άρθρο 43.

2. Σε εξαιρετικές περιστάσεις που δικαιολογούν άμεση παρέμβαση για τη διατήρηση της εύρυθμης λειτουργίας της εσωτερικής αγοράς και όταν η Επιτροπή έχει επαρκείς λόγους να θεωρεί ότι το προϊόν που αναφέρεται στην παράγραφο 1 εξακολουθεί να μη συμμορφώνεται με τις απαιτήσεις του παρόντος κανονισμού και δεν έχουν ληφθεί αποτελεσματικά μέτρα από τις αρμόδιες αρχές εποπτείας της αγοράς, η Επιτροπή μπορεί να ζητήσει από τον ENISA να διενεργήσει αξιολόγηση της συμμόρφωσης. Η Επιτροπή ενημερώνει σχετικά τις αρμόδιες αρχές εποπτείας της αγοράς. Οι σχετικοί οικονομικοί φορείς συνεργάζονται όπως απαιτείται με τον ENISA.

3. Με βάση την αξιολόγηση του ENISA, η Επιτροπή μπορεί να αποφασίσει ότι απαιτείται διορθωτικό ή περιοριστικό μέτρο σε επίπεδο Ένωσης. Για τον σκοπό αυτό, προβαίνει αμελλητί σε διαβουλεύσεις με τα ενδιαφερόμενα κράτη μέλη και τον σχετικό οικονομικό φορέα ή τους φορείς.

4. Με βάση τη διαβούλευση που αναφέρεται στην παράγραφο 3, η Επιτροπή μπορεί να θεσπίσει εκτελεστικές πράξεις για να αποφασίσει σχετικά με τη λήψη διορθωτικών ή περιοριστικών μέτρων σε επίπεδο Ένωσης, συμπεριλαμβανομένης της εντολής απόσυρσης από την αγορά ή της ανάκλησης, εντός εύλογου χρονικού διαστήματος, ανάλογου προς τη φύση του κινδύνου. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης του άρθρου 51 παράγραφος 2.

5. Η Επιτροπή ανακοινώνει αμέσως την απόφαση που αναφέρεται στην παράγραφο 4 στον σχετικό οικονομικό φορέα ή τους φορείς. Τα κράτη μέλη εφαρμόζουν αμελλητί τις πράξεις που αναφέρονται στην παράγραφο 4 και ενημερώνουν την Επιτροπή σχετικά.

6. Οι παράγραφοι 2 έως 5 εφαρμόζονται καθ' όλη τη διάρκεια της εξαιρετικής περίπτωσης που αιτιολογεί την παρέμβαση της Επιτροπής και για όσο διάστημα το αντίστοιχο προϊόν δεν συμμορφώνεται με τον παρόντα κανονισμό.

*Άρθρο 46*

*Συμμορφούμενα προϊόντα με ψηφιακά στοιχεία που παρουσιάζουν σημαντικό κίνδυνο για την κυβερνοασφάλεια*

1. Όταν, μετά τη διενέργεια αξιολόγησης δυνάμει του άρθρου 43, η αρχή εποπτείας της αγοράς ενός κράτους μέλους διαπιστώσει ότι, μολονότι ένα προϊόν με ψηφιακά

στοιχεία και οι διαδικασίες που εφαρμόζει ο κατασκευαστής συμμορφώνονται με τον παρόντα κανονισμό, παρουσιάζουν σημαντικό κίνδυνο για την κυβερνοασφάλεια και, επιπλέον, συνιστούν κίνδυνο για την υγεία ή την ασφάλεια των προσώπων, τη συμμόρφωση με τις υποχρεώσεις που απορρέουν από το ενωσιακό ή το εθνικό δίκαιο για την προστασία των θεμελιωδών δικαιωμάτων, τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα ή την εμπιστευτικότητα των υπηρεσιών που προσφέρονται με τη χρήση ηλεκτρονικού συστήματος πληροφοριών από βασικές οντότητες του τύπου που αναφέρεται στο [παράρτημα I της οδηγίας XXX/XXXX (NIS2)] ή για άλλες πτυχές προστασίας του δημόσιου συμφέροντος, απαιτεί από τον οικείο φορέα εκμετάλλευσης να λάβει όλα τα κατάλληλα μέτρα για να διασφαλίσει ότι το προϊόν με ψηφιακά στοιχεία και οι διαδικασίες που εφαρμόζει ο οικείος κατασκευαστής, όταν αυτό διατεθεί στην αγορά, δεν παρουσιάζει πλέον τον εν λόγω κίνδυνο, να αποσύρει το προϊόν με ψηφιακά στοιχεία από την αγορά ή να το ανακαλέσει εντός εύλογου χρονικού διαστήματος, ανάλογου προς τη φύση του κινδύνου.

2. Ο κατασκευαστής ή άλλοι σχετικοί φορείς εκμετάλλευσης διασφαλίζουν ότι λαμβάνονται διορθωτικά μέτρα όσον αφορά όλα τα σχετικά προϊόντα με ψηφιακά στοιχεία που έχουν καταστήσει διαθέσιμα στην αγορά σε ολόκληρη την Ένωση εντός του χρονοδιαγράμματος που προβλέπεται από την αρχή εποπτείας της αγοράς του κράτους μέλους που αναφέρεται στην παράγραφο 1.

3. Το κράτος μέλος ενημερώνει αμέσως την Επιτροπή και τα άλλα κράτη μέλη για τα μέτρα που λαμβάνονται σύμφωνα με την παράγραφο 1. Οι πληροφορίες αυτές περιλαμβάνουν όλα τα διαθέσιμα στοιχεία, ιδίως τα στοιχεία που είναι αναγκαία για την ταυτοποίηση των προϊόντων με ψηφιακά στοιχεία, την καταγωγή και την αλυσίδα εφοδιασμού των εν λόγω προϊόντων, τη φύση του σχετικού κινδύνου, καθώς και τη φύση και τη διάρκεια των εθνικών μέτρων που ελήφθησαν.

4. Η Επιτροπή διαβουλεύεται αμελλητί με τα κράτη μέλη και τον σχετικό οικονομικό φορέα και διενεργεί αξιολόγηση των εθνικών μέτρων που ελήφθησαν. Βάσει των αποτελεσμάτων αυτής της αξιολόγησης, η Επιτροπή αποφασίζει αν το μέτρο είναι δικαιολογημένο και, εφόσον απαιτείται, προτείνει τα δέοντα μέτρα.

5. Η Επιτροπή κοινοποιεί την απόφασή της στα κράτη μέλη.

6. Εάν η Επιτροπή έχει επαρκείς λόγους να πιστεύει, μεταξύ άλλων με βάση τις πληροφορίες που παρέχει ο ENISA, ότι ένα προϊόν με ψηφιακά στοιχεία, παρότι συμμορφώνεται με τον παρόντα κανονισμό, παρουσιάζει τους κινδύνους που αναφέρονται στην παράγραφο 1, μπορεί να ζητήσει από τη σχετική ή τις σχετικές αρχές εποπτείας της αγοράς να διενεργήσουν αξιολόγηση της συμμόρφωσης και να ακολουθήσουν τις διαδικασίες που αναφέρονται στο άρθρο 43 και στις παραγράφους 1, 2 και 3 του παρόντος άρθρου.

7. Σε εξαιρετικές περιστάσεις που δικαιολογούν άμεση παρέμβαση για τη διατήρηση της εύρυθμης λειτουργίας της εσωτερικής αγοράς και όταν η Επιτροπή έχει επαρκείς λόγους να θεωρεί ότι το προϊόν που αναφέρεται στην παράγραφο 6 εξακολουθεί να παρουσιάζει τους κινδύνους που αναφέρονται στην παράγραφο 1 και δεν έχουν ληφθεί αποτελεσματικά μέτρα από τις αρμόδιες εθνικές αρχές εποπτείας της αγοράς, η Επιτροπή μπορεί να ζητήσει από τον ENISA να διενεργήσει αξιολόγηση των κινδύνων που παρουσιάζει το προϊόν και ενημερώνει σχετικά τις αρμόδιες αρχές εποπτείας της αγοράς. Οι σχετικοί οικονομικοί φορείς συνεργάζονται όπως απαιτείται με τον ENISA.

8. Με βάση την αξιολόγηση του ENISA που αναφέρεται στην παράγραφο 7, η Επιτροπή μπορεί να κρίνει ότι απαιτείται διορθωτικό ή περιοριστικό μέτρο σε επίπεδο Ένωσης. Για τον σκοπό αυτό, προβαίνει αμελλητί σε διαβουλεύσεις με τα ενδιαφερόμενα κράτη μέλη και τον σχετικό φορέα ή τους φορείς εκμετάλλευσης.

9. Με βάση τη διαβούλευση που αναφέρεται στην παράγραφο 8, η Επιτροπή μπορεί να θεσπίσει εκτελεστικές πράξεις για να αποφασίσει σχετικά με τη λήψη διορθωτικών ή περιοριστικών μέτρων σε επίπεδο Ένωσης, συμπεριλαμβανομένης της εντολής απόσυρσης από την αγορά ή της ανάκλησης, εντός εύλογου χρονικού διαστήματος, ανάλογου προς τη φύση του κινδύνου. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης του άρθρου 51 παράγραφος 2.

10. Η Επιτροπή ανακοινώνει αμέσως την απόφαση που αναφέρεται στην παράγραφο 9 στον σχετικό οικονομικό φορέα ή τους φορείς. Τα κράτη μέλη εφαρμόζουν αμελλητί τέτοιες πράξεις και ενημερώνουν την Επιτροπή σχετικά.

11. Οι παράγραφοι 6 έως 10 εφαρμόζονται καθ' όλη τη διάρκεια της εξαιρετικής περίπτωσης που αιτιολογεί την παρέμβαση της Επιτροπής και για όσο διάστημα το αντίστοιχο προϊόν εξακολουθεί να παρουσιάζει τους κινδύνους που αναφέρονται στην παράγραφο 1.

*Άρθρο 47*

*Τυπική μη συμμόρφωση*

1. Όταν η αρχή εποπτείας της αγοράς κράτους μέλους προβεί σε μία από τις κατωτέρω διαπιστώσεις, απαιτεί από τον οικείο κατασκευαστή να θέσει τέλος στη μη συμμόρφωση:

   α) η σήμανση συμμόρφωσης έχει τοποθετηθεί κατά παράβαση των άρθρων 21 και 22·

   β) δεν έχει τοποθετηθεί η σήμανση συμμόρφωσης·

   γ) δεν έχει καταρτιστεί δήλωση συμμόρφωσης ΕΕ·

   δ) η δήλωση συμμόρφωσης ΕΕ δεν έχει καταρτιστεί ορθά·

   ε) δεν έχει τοποθετηθεί ο αριθμός μητρώου του κοινοποιημένου οργανισμού που εμπλέκεται στη διαδικασία αξιολόγησης της συμμόρφωσης, κατά περίπτωση·

   στ) ο τεχνικός φάκελος είτε δεν είναι διαθέσιμος είτε δεν είναι πλήρης·

2. Εάν η μη συμμόρφωση της παραγράφου 1 εξακολουθήσει να υφίσταται, το οικείο κράτος μέλος λαμβάνει όλα τα δέοντα μέτρα για να περιορίσει ή να απαγορεύσει τη διαθεσιμότητα του προϊόντος με ψηφιακά στοιχεία στην αγορά και να εξασφαλίσει ότι αυτό ανακαλείται ή αποσύρεται από την αγορά.

*Άρθρο 48*

*Κοινές δραστηριότητες των αρχών εποπτείας της αγοράς*

1. Οι αρχές εποπτείας της αγοράς μπορούν να συμφωνήσουν με άλλες αρμόδιες αρχές να διεξαγάγουν κοινές δραστηριότητες που αποσκοπούν στη διασφάλιση της κυβερνοασφάλειας και της προστασίας των καταναλωτών όσον αφορά συγκεκριμένα προϊόντα με ψηφιακά στοιχεία που διατίθενται ή καθίστανται διαθέσιμα στην αγορά, ιδίως προϊόντα για τα οποία διαπιστώνεται συχνά ότι ενέχουν κινδύνους για την κυβερνοασφάλεια.

2. Η Επιτροπή ή ο ENISA μπορούν να προτείνουν κοινές δραστηριότητες για τον έλεγχο της συμμόρφωσης με τον παρόντα κανονισμό, οι οποίες θα διεξάγονται από τις αρχές εποπτείας της αγοράς βάσει ενδείξεων ή πληροφοριών για πιθανή μη συμμόρφωση προϊόντων που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού σε διάφορα κράτη μέλη, προς τις απαιτήσεις που καθορίζονται από τον εν λόγω κανονισμό.

3. Οι αρχές εποπτείας της αγοράς και η Επιτροπή, κατά περίπτωση, εξασφαλίζουν ότι η συμφωνία για τη διεξαγωγή κοινών δραστηριοτήτων δεν προκαλεί αθέμιτο ανταγωνισμό μεταξύ οικονομικών φορέων, και δεν επηρεάζει αρνητικά την αντικειμενικότητα, την ανεξαρτησία και την αμεροληψία των μερών της συμφωνίας.

4. Μια αρχή εποπτείας της αγοράς μπορεί να χρησιμοποιήσει κάθε πληροφορία που προκύπτει από τις δραστηριότητες που εκτελούνται στο πλαίσιο οποιασδήποτε έρευνας την οποία αυτή διεξάγει.

5. Η οικεία αρχή εποπτείας της αγοράς και η Επιτροπή, κατά περίπτωση, δημοσιοποιούν τη συμφωνία σχετικά με τις κοινές δραστηριότητες, συμπεριλαμβανομένων των ονομάτων των εμπλεκομένων μερών.

*Άρθρο 49*

*Σαρώσεις*

1. Οι αρχές εποπτείας της αγοράς δύνανται να αποφασίσουν τη διενέργεια ταυτόχρονων, συντονισμένων δράσεων ελέγχου (στο εξής: σαρώσεις) συγκεκριμένων προϊόντων με ψηφιακά στοιχεία ή κατηγοριών αυτών, προκειμένου να ελέγξουν τη συμμόρφωσή τους ή να εντοπίσουν παραβάσεις του παρόντος κανονισμού.

2. Εκτός εάν συμφωνηθεί διαφορετικά από τις εμπλεκόμενες αρχές εποπτείας της αγοράς, τις σαρώσεις συντονίζει η Επιτροπή. Ο συντονιστής της σάρωσης δύναται, όταν αυτό αρμόζει, να δημοσιοποιεί τα συγκεντρωτικά αποτελέσματα.

3. Ο ENISA μπορεί να προσδιορίζει, κατά την εκτέλεση των καθηκόντων του, μεταξύ άλλων με βάση τις κοινοποιήσεις που λαμβάνει σύμφωνα με το άρθρο 11 παράγραφοι 1 και 2, τις κατηγορίες προϊόντων για τα οποία μπορούν να οργανωθούν σαρώσεις. Η πρόταση διενέργειας σαρώσεων υποβάλλεται στον δυνητικό συντονιστή που αναφέρεται στην παράγραφο 2 προς εξέταση από τις αρχές εποπτείας της αγοράς.

4. Όταν διενεργούν σάρωση, οι εμπλεκόμενες αρχές εποπτείας της αγοράς δύνανται να ασκούν τις εξουσίες έρευνας που καθορίζονται στα άρθρα 41 έως 47, καθώς και οποιεσδήποτε άλλες εξουσίες που τους αναθέτει το εθνικό δίκαιο.

5. Οι αρχές εποπτείας της αγοράς αρχές μπορούν να καλούν υπαλλήλους της Επιτροπής, και λοιπό βοηθητικό προσωπικό που έχει εξουσιοδοτηθεί από την Επιτροπή, να συμμετέχουν σε σαρώσεις.

## ΚΕΦΑΛΑΙΟ VI

## ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΑΡΜΟΔΙΟΤΗΤΕΣ ΚΑΙ ΔΙΑΔΙΚΑΣΙΑ ΕΠΙΤΡΟΠΗΣ

*Άρθρο 50*

*Άσκηση της εξουσιοδότησης*

1. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις υπό τους όρους του παρόντος άρθρου.

2. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις όπως προβλέπεται στο άρθρο 2 παράγραφος 4, στο άρθρο 6 παράγραφος 2, στο άρθρο 6 παράγραφος 3, στο άρθρο 6 παράγραφος 5, στο άρθρο 20 παράγραφος 5 και στο άρθρο 23 παράγραφος 5.

3. Η εξουσιοδότηση που προβλέπεται στο άρθρο 2 παράγραφος 4, στο άρθρο 6 παράγραφος 2, στο άρθρο 6 παράγραφος 3, στο άρθρο 6 παράγραφος 5, στο άρθρο 20 παράγραφος 5 και στο άρθρο 23 παράγραφος 5 μπορεί να ανακληθεί ανά πάσα στιγμή από το Ευρωπαϊκό Κοινοβούλιο ή από το Συμβούλιο. Η απόφαση ανάκλησης περατώνει την εξουσιοδότηση που προσδιορίζεται στην εν λόγω απόφαση. Αρχίζει να ισχύει την επομένη της δημοσίευσης της απόφασης στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* ή σε μεταγενέστερη ημερομηνία που ορίζεται σε αυτήν. Δεν θίγει το κύρος των κατ' εξουσιοδότηση πράξεων που ισχύουν ήδη.

4. Πριν από την έκδοση κατ' εξουσιοδότηση πράξης, η Επιτροπή διεξάγει διαβουλεύσεις με εμπειρογνώμονες που ορίζει κάθε κράτος μέλος σύμφωνα με τις αρχές της διοργανικής συμφωνίας της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου.

5. Μόλις εκδώσει κατ' εξουσιοδότηση πράξη, η Επιτροπή την κοινοποιεί ταυτόχρονα στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.

6. Κάθε κατ' εξουσιοδότηση πράξη που εκδίδεται σύμφωνα με το άρθρο 2 παράγραφος 4, το άρθρο 6 παράγραφος 2, το άρθρο 6 παράγραφος 3, το άρθρο 6 παράγραφος 5, το άρθρο 20 παράγραφος 5 και το άρθρο 23 παράγραφος 5 αρχίζει να ισχύει μόνον εφόσον δεν διατυπωθούν αντιρρήσεις είτε από το Ευρωπαϊκό Κοινοβούλιο είτε από το Συμβούλιο εντός προθεσμίας δύο μηνών από την κοινοποίηση της πράξης στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ή εάν, πριν λήξει αυτή η προθεσμία, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ενημερώσουν αμφότερα την Επιτροπή ότι δεν πρόκειται να προβάλουν αντίρρηση. Η προθεσμία αυτή παρατείνεται κατά δύο μήνες κατόπιν πρωτοβουλίας του Ευρωπαϊκού Κοινοβουλίου ή του Συμβουλίου.

*Άρθρο 51*

*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.

## ΚΕΦΑΛΑΙΟ VII

## ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΚΑΙ ΚΥΡΩΣΕΙΣ

*Άρθρο 52*

*Εμπιστευτικότητα*

1. Όλα τα μέρη που συμμετέχουν στην εφαρμογή του παρόντος κανονισμού τηρούν την εμπιστευτικότητα των πληροφοριών και των δεδομένων που λαμβάνονται κατά την εκτέλεση των καθηκόντων και των δραστηριοτήτων τους κατά τρόπο ώστε να προστατεύονται, ιδίως:

   α) τα δικαιώματα διανοητικής ιδιοκτησίας και οι εμπιστευτικές επιχειρηματικές πληροφορίες ή τα εμπορικά απόρρητα φυσικού ή νομικού προσώπου, συμπεριλαμβανομένου του πηγαίου κώδικα, με εξαίρεση τις περιπτώσεις που αναφέρονται στο άρθρο 5 της οδηγίας 2016/943 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[24].

   β) η αποτελεσματική εφαρμογή του παρόντος κανονισμού, κυρίως για τους σκοπούς επιθεωρήσεων, ερευνών ή ελέγχων·

   γ) το δημόσιο συμφέρον και τα συμφέροντα εθνικής ασφάλειας·

   δ) η ακεραιότητα των ποινικών ή διοικητικών διαδικασιών.

2. Με την επιφύλαξη της παραγράφου 1, οι πληροφορίες που ανταλλάσσονται σε εμπιστευτική βάση μεταξύ των αρχών εποπτείας της αγοράς, αφενός, και μεταξύ των αρχών εποπτείας της αγοράς και της Επιτροπής, αφετέρου, δεν δημοσιοποιούνται χωρίς την προηγούμενη σύμφωνη γνώμη της αρχής εποπτείας της αγοράς από την οποία προέρχονται.

3. Οι παράγραφοι 1 και 2 δεν θίγουν τα δικαιώματα και τις υποχρεώσεις της Επιτροπής, των κρατών μελών και των κοινοποιημένων οργανισμών για την ανταλλαγή πληροφοριών και την κοινοποίηση των προειδοποιήσεων, ούτε τις υποχρεώσεις των ενδιαφερόμενων προσώπων να παρέχουν πληροφορίες βάσει του ποινικού δικαίου των κρατών μελών.

4. Η Επιτροπή και τα κράτη μέλη μπορούν να ανταλλάσσουν, εφόσον είναι αναγκαίο, ευαίσθητες πληροφορίες με τις αρμόδιες αρχές τρίτων χωρών με τις οποίες έχουν συνάψει διμερείς ή πολυμερείς διακανονισμούς για την τήρηση της εμπιστευτικότητας οι οποίοι εγγυώνται επαρκές επίπεδο προστασίας.

*Άρθρο 53*

*Κυρώσεις*

[24] Οδηγία (ΕΕ) 2016/943 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 8ης Ιουνίου 2016, περί προστασίας της τεχνογνωσίας και των επιχειρηματικών πληροφοριών που δεν έχουν αποκαλυφθεί (εμπορικό απόρρητο) από την παράνομη απόκτηση, χρήση και αποκάλυψή τους (ΕΕ L 157 της 15.6.2016, σ. 1).

1. Τα κράτη μέλη θεσπίζουν τους κανόνες σχετικά με τις κυρώσεις που επιβάλλονται για παραβάσεις του παρόντος κανονισμού από τους οικονομικούς φορείς 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 χωρίς καθυστέρηση στην Επιτροπή τους εν λόγω κανόνες και τα εν λόγω μέτρα και την ενημερώνουν χωρίς καθυστέρηση σχετικά με κάθε μεταγενέστερη τροποποίησή τους.

3. Η μη συμμόρφωση με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I και τις υποχρεώσεις που ορίζονται στα άρθρα 10 και 11 επισύρει διοικητικά πρόστιμα ύψους έως 15 000 000 EUR ή, εάν ο παραβάτης είναι επιχείρηση, έως το 2,5 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της για το προηγούμενο οικονομικό έτος, ανάλογα με το ποιο ποσό είναι υψηλότερο.

4. Η μη συμμόρφωση με άλλες υποχρεώσεις δυνάμει του παρόντος κανονισμού επισύρει διοικητικά πρόστιμα ύψους έως 10 000 000 EUR ή, εάν ο παραβάτης είναι επιχείρηση, έως και το 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της για το προηγούμενο οικονομικό έτος, ανάλογα με το ποιο ποσό είναι υψηλότερο.

5. Η παροχή ανακριβών, ελλιπών ή παραπλανητικών πληροφοριών σε κοινοποιημένους οργανισμούς και αρχές εποπτείας της αγοράς κατά την απάντηση σε αίτημα επισύρει διοικητικά πρόστιμα ύψους έως 5 000 000 EUR ή, εάν ο παραβάτης είναι επιχείρηση, έως το 1 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της για το προηγούμενο οικονομικό έτος, ανάλογα με το ποιο ποσό είναι υψηλότερο.

6. Κατά τη λήψη απόφασης σχετικά με το ύψος του διοικητικού προστίμου σε κάθε μεμονωμένη περίπτωση, λαμβάνονται υπόψη όλες οι σχετικές περιστάσεις της συγκεκριμένης κατάστασης και λαμβάνονται δεόντως υπόψη τα ακόλουθα:

   α) η φύση, η σοβαρότητα και η διάρκεια της παράβασης και οι συνέπειές της·

   β) αν έχουν ήδη επιβληθεί διοικητικά πρόστιμα από άλλες αρχές εποπτείας της αγοράς στον ίδιο φορέα εκμετάλλευσης για παρόμοια παράβαση·

   γ) το μέγεθος και το μερίδιο αγοράς του φορέα εκμετάλλευσης που διέπραξε την παράβαση.

7. Οι αρχές εποπτείας της αγοράς που επιβάλλουν διοικητικά πρόστιμα κοινοποιούν τις πληροφορίες αυτές στις αρχές εποπτείας της αγοράς άλλων κρατών μελών μέσω του συστήματος πληροφοριών και επικοινωνίας που αναφέρεται στο άρθρο 34 του κανονισμού (ΕΕ) 2019/1020.

8. Κάθε κράτος μέλος καθορίζει τους κανόνες για το αν και σε ποιο βαθμό μπορούν να επιβάλλονται διοικητικά πρόστιμα σε δημόσιες αρχές και φορείς που έχουν συσταθεί στο εν λόγω κράτος μέλος.

9. Ανάλογα με το νομικό σύστημα των κρατών μελών, οι κανόνες για τα διοικητικά πρόστιμα μπορούν να εφαρμόζονται κατά τρόπο ώστε τα πρόστιμα να επιβάλλονται από τα αρμόδια εθνικά δικαστήρια ή από άλλους φορείς, σύμφωνα με τις αρμοδιότητες που καθορίζονται σε εθνικό επίπεδο στα εν λόγω κράτη μέλη. Η εφαρμογή των κανόνων αυτών στα εν λόγω κράτη μέλη έχει ισοδύναμο αποτέλεσμα.

10. Διοικητικά πρόστιμα μπορούν να επιβάλλονται, ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης, επιπλέον άλλων διορθωτικών ή περιοριστικών μέτρων που εφαρμόζονται από τις αρχές εποπτείας της αγοράς για την ίδια παράβαση.

## ΚΕΦΑΛΑΙΟ VIII

## ΜΕΤΑΒΑΤΙΚΕΣ ΚΑΙ ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

*Άρθρο 54*

*Τροποποίηση του κανονισμού (ΕΕ) 2019/1020*

Στο παράρτημα Ι του κανονισμού (ΕΕ) 2019/1020 προστίθεται το ακόλουθο σημείο:

«71. [Κανονισμός XXX][Πράξη για την κυβερνοανθεκτικότητα]».

*Άρθρο 55*

*Μεταβατικές διατάξεις*

1. Τα πιστοποιητικά εξέτασης τύπου ΕΕ και οι αποφάσεις έγκρισης που εκδίδονται σχετικά με τις απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία που υπόκεινται σε άλλη ενωσιακή νομοθεσία εναρμόνισης παραμένουν σε ισχύ έως [42 μήνες μετά την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], εκτός εάν λήγουν πριν από την εν λόγω ημερομηνία, ή εκτός εάν ορίζεται διαφορετικά σε άλλη ενωσιακή νομοθεσία, οπότε εξακολουθούν να ισχύουν όπως αναφέρεται στην εν λόγω ενωσιακή νομοθεσία.

2. Τα προϊόντα με ψηφιακά στοιχεία που έχουν διατεθεί στην αγορά πριν από την [ημερομηνία εφαρμογής του παρόντος κανονισμού που αναφέρεται στο άρθρο 57], υπόκεινται στις απαιτήσεις του παρόντος κανονισμού μόνον εάν, από τη συγκεκριμένη ημερομηνία, τα εν λόγω προϊόντα υπόκεινται σε ουσιαστικές τροποποιήσεις στον σχεδιασμό ή τον προβλεπόμενο σκοπό τους.

3. Κατά παρέκκλιση από την παράγραφο 2, οι υποχρεώσεις που ορίζονται στο άρθρο 11 εφαρμόζονται σε όλα τα προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού και έχουν διατεθεί στην αγορά πριν από την [ημερομηνία εφαρμογής του παρόντος κανονισμού που αναφέρεται στο άρθρο 57].

*Άρθρο 56*

*Αξιολόγηση και επανεξέταση*

Έως [36 μήνες μετά την ημερομηνία εφαρμογής του παρόντος κανονισμού] και στη συνέχεια ανά τέσσερα έτη, η Επιτροπή υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο εκθέσεις σχετικά με την αξιολόγηση και την επανεξέταση του παρόντος κανονισμού. Οι εκθέσεις δημοσιοποιούνται.

*Άρθρο 57*

*Έναρξη ισχύος και εφαρμογή*

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Εφαρμόζεται ύστερα από [24 μήνες από την έναρξη ισχύος του παρόντος κανονισμού]. Ωστόσο, το άρθρο 11 εφαρμόζεται ύστερα από [12 μήνες από την έναρξη ισχύος του παρόντος κανονισμού].

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Βρυξέλλες,

| | |
|---|---|
| *Για το Ευρωπαϊκό Κοινοβούλιο* | *Για το Συμβούλιο* |
| *Η Πρόεδρος* | *Ο Πρόεδρος* |

**ΝΟΜΟΘΕΤΙΚΟ ΔΗΜΟΣΙΟΝΟΜΙΚΟ ΔΕΛΤΙΟ**

## 1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

### 1.1. Τίτλος της πρότασης/πρωτοβουλίας

### 1.2. Σχετικοί τομείς πολιτικής

### 1.3. Η πρόταση/πρωτοβουλία αφορά:

### 1.4. Στόχοι

*1.4.1. Γενικοί στόχοι*

*1.4.2. Ειδικοί στόχοι*

*1.4.3. Αναμενόμενα αποτελέσματα και επιπτώσεις*

*1.4.4. Δείκτες επιδόσεων*

### 1.5. Αιτιολόγηση της πρότασης/πρωτοβουλίας

*1.5.1. Βραχυπρόθεσμη ή μακροπρόθεσμη κάλυψη αναγκών, συμπεριλαμβανομένου λεπτομερούς χρονοδιαγράμματος για τη σταδιακή υλοποίηση της πρωτοβουλίας*

*1.5.2. Προστιθέμενη αξία της ενωσιακής παρέμβασης (που μπορεί να προκύπτει από διάφορους παράγοντες, π.χ. οφέλη από τον συντονισμό, ασφάλεια δικαίου, μεγαλύτερη αποτελεσματικότητα ή συμπληρωματικότητα). Για τους σκοπούς του παρόντος σημείου, «προστιθέμενη αξία της ενωσιακής παρέμβασης» είναι η αξία που απορρέει από την ενωσιακή παρέμβαση και η οποία προστίθεται στην αξία που θα είχε δημιουργηθεί αν τα κράτη μέλη ενεργούσαν μεμονωμένα.*

*1.5.3. Διδάγματα από ανάλογες εμπειρίες του παρελθόντος*

*1.5.4. Συμβατότητα με το πολυετές δημοσιονομικό πλαίσιο και ενδεχόμενες συνέργειες με άλλα κατάλληλα μέσα*

*1.5.5. Αξιολόγηση των διαφόρων διαθέσιμων επιλογών χρηματοδότησης, συμπεριλαμβανομένων των δυνατοτήτων ανακατανομής*

### 1.6. Διάρκεια και δημοσιονομικές επιπτώσεις της πρότασης/πρωτοβουλίας

### 1.7. Προβλεπόμενοι τρόποι διαχείρισης

## 2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ

### 2.1. Κανόνες παρακολούθησης και υποβολής εκθέσεων

### 2.2. Συστήματα διαχείρισης και ελέγχου

*2.2.1. Αιτιολόγηση των τρόπων διαχείρισης, των μηχανισμών εκτέλεσης της χρηματοδότησης, των όρων πληρωμής και της προτεινόμενης στρατηγικής ελέγχου*

*2.2.2. Πληροφορίες σχετικά με τους κινδύνους που έχουν εντοπιστεί και τα συστήματα εσωτερικού ελέγχου που έχουν δημιουργηθεί για τον μετριασμό τους*

*2.2.3. Εκτίμηση και αιτιολόγηση της οικονομικής αποδοτικότητας των ελέγχων (λόγος του κόστους του ελέγχου προς την αξία των σχετικών κονδυλίων που αποτελούν αντικείμενο διαχείρισης) και αξιολόγηση του εκτιμώμενου επιπέδου κινδύνου σφάλματος (κατά την πληρωμή και κατά το κλείσιμο)*

### 2.3. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας

## 3. ΕΚΤΙΜΩΜΕΝΕΣ ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

### 3.1. Τομείς του πολυετούς δημοσιονομικού πλαισίου και γραμμές δαπανών του προϋπολογισμού που επηρεάζονται

### 3.2. Εκτιμώμενες δημοσιονομικές επιπτώσεις της πρότασης στις πιστώσεις

*3.2.1. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις επιχειρησιακές πιστώσεις*

*3.2.2. Εκτιμώμενο αποτέλεσμα που χρηματοδοτείται με επιχειρησιακές πιστώσεις*

*3.2.3. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις διοικητικές πιστώσεις*

*3.2.4. Συμβατότητα με το ισχύον πολυετές δημοσιονομικό πλαίσιο*

*3.2.5. Συμμετοχή τρίτων στη χρηματοδότηση*

### 3.3. Εκτιμώμενες επιπτώσεις στα έσοδα

# ΝΟΜΟΘΕΤΙΚΟ ΔΗΜΟΣΙΟΝΟΜΙΚΟ ΔΕΛΤΙΟ

## 1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

### 1.1. Τίτλος της πρότασης/πρωτοβουλίας

Πρόταση κανονισμού σχετικά με τις οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία (πράξη για την κυβερνοανθεκτικότητα)

### 1.2. Σχετικοί τομείς πολιτικής

Επικοινωνιακά Δίκτυα, Περιεχόμενο και Τεχνολογίες

### 1.3. Η πρόταση/πρωτοβουλία αφορά:

× **νέα δράση**

☐ **νέα δράση έπειτα από δοκιμαστικό σχέδιο / προπαρασκευαστική ενέργεια**[37]

☐ **την παράταση υφιστάμενης δράσης**

☐ **συγχώνευση ή αναπροσανατολισμό μίας ή περισσότερων δράσεων προς άλλη/νέα δράση**

### 1.4. Στόχοι

*1.4.1. Γενικοί στόχοι*

Η πρόταση έχει δύο κύριους στόχους, οι οποίοι αποσκοπούν στη διασφάλιση της ορθής λειτουργίας της εσωτερικής αγοράς: 1) **να δημιουργηθούν συνθήκες για την ανάπτυξη ασφαλών προϊόντων με ψηφιακά στοιχεία** μέσω της διασφάλισης ότι στην αγορά διατίθενται προϊόντα υλισμικού και λογισμικού με λιγότερα τρωτά σημεία και ότι οι κατασκευαστές λαμβάνουν σοβαρά υπόψη το ζήτημα της ασφάλειας καθ' όλη τη διάρκεια του κύκλου ζωής των προϊόντων· και 2) **να δημιουργηθούν συνθήκες που επιτρέπουν στους χρήστες να λαμβάνουν υπόψη την κυβερνοασφάλεια κατά την επιλογή και τη χρήση προϊόντων με ψηφιακά στοιχεία**.

*1.4.2. Ειδικοί στόχοι*

Για την πρόταση ορίστηκαν **τέσσερις ειδικοί στόχοι**: i) να διασφαλιστεί ότι οι κατασκευαστές βελτιώνουν την ασφάλεια των προϊόντων με ψηφιακά στοιχεία ήδη από το στάδιο σχεδιασμού και ανάπτυξης και καθ' όλη τη διάρκεια του κύκλου ζωής· ii) να διασφαλιστεί ένα συνεκτικό πλαίσιο κυβερνοασφάλειας, το οποίο θα διευκολύνει τη συμμόρφωση των κατασκευαστών υλισμικού και λογισμικού· iii) να ενισχυθεί η διαφάνεια των ιδιοτήτων ασφάλειας των προϊόντων με ψηφιακά στοιχεία και iv) να παρέχονται στις επιχειρήσεις και στους καταναλωτές η δυνατότητα να χρησιμοποιούν με ασφάλεια τα προϊόντα με ψηφιακά στοιχεία.

*Αναμενόμενα αποτελέσματα και επιπτώσεις*

*Να προσδιοριστούν τα αποτελέσματα που θα πρέπει να έχει η πρόταση/πρωτοβουλία όσον αφορά τους στοχοθετημένους δικαιούχους / τις στοχοθετημένες ομάδες.*

[37] Όπως αναφέρεται στο άρθρο 58 παράγραφος 2 στοιχείο α) ή β) του δημοσιονομικού κανονισμού.

Η πρόταση θα αποφέρει σημαντικά οφέλη στα διάφορα ενδιαφερόμενα μέρη. Όσον αφορά τις επιχειρήσεις, θα αποτρέψει την ύπαρξη αποκλινόντων κανόνων ασφάλειας για προϊόντα με ψηφιακά στοιχεία και θα μειώσει το κόστος συμμόρφωσης όσον αφορά τη σχετική νομοθεσία για την κυβερνοασφάλεια. Με τον τρόπο αυτόν, θα μειωθεί ο αριθμός των κυβερνοσυμβάντων, το κόστος διαχείρισης συμβάντων και η ζημία στη φήμη τους. Όσον αφορά ολόκληρη την ΕΕ, εκτιμάται ότι η πρωτοβουλία θα μπορούσε να οδηγήσει σε μείωση του κόστους από συμβάντα που πλήττουν τις επιχειρήσεις κατά περίπου 180 δισ. EUR έως 290 δισ. EUR ετησίως[38]. Θα οδηγήσει σε αύξηση του κύκλου εργασιών λόγω της χρήσης προϊόντων με ψηφιακά στοιχεία. Θα βελτιώσει την παγκόσμια φήμη των εταιρειών, με αποτέλεσμα την αύξηση της ζήτησης και εκτός της ΕΕ. Για τους χρήστες, η προτιμώμενη επιλογή θα ενισχύσει τη διαφάνεια των ιδιοτήτων ασφάλειας και θα διευκολύνει τη χρήση προϊόντων με ψηφιακά στοιχεία. Οι καταναλωτές και οι πολίτες θα ωφεληθούν επίσης από την καλύτερη προστασία των θεμελιωδών δικαιωμάτων τους, όπως η προστασία της ιδιωτικής ζωής και των δεδομένων.

Ταυτόχρονα, η πρόταση θα αυξήσει το κόστος συμμόρφωσης και επιβολής για τις επιχειρήσεις, τους κοινοποιημένους οργανισμούς και τις δημόσιες αρχές, συμπεριλαμβανομένων των αρχών διαπίστευσης και εποπτείας της αγοράς. Για τους κατασκευαστές λογισμικού και υλισμικού, θα προσθέσει άμεσο κόστος συμμόρφωσης για τις νέες απαιτήσεις ασφάλειας, την αξιολόγηση της συμμόρφωσης, την τεκμηρίωση και τις υποχρεώσεις υποβολής εκθέσεων, με αποτέλεσμα το συνολικό κόστος συμμόρφωσης να ανέρχεται σε περίπου 29 δισ. EUR για εκτιμώμενη τρέχουσα αξία ύψους 1 485 δισ. EUR σε κύκλο εργασιών[39]. Οι χρήστες, συμπεριλαμβανομένων των επιχειρηματικών χρηστών, οι καταναλωτές και οι πολίτες ενδέχεται να αντιμετωπίσουν αύξηση τιμών στα προϊόντα με ψηφιακά στοιχεία. Ωστόσο, οι αυξημένες τιμές θα πρέπει να εξεταστούν στο πλαίσιο των σημαντικών οφελών που περιγράφονται ανωτέρω.

### *1.4.3. Δείκτες επιδόσεων*

*Να προσδιοριστούν οι δείκτες για την παρακολούθηση της προόδου και των επιτευγμάτων.*

Προκειμένου να ελεγχθεί εάν οι κατασκευαστές βελτιώνουν την ασφάλεια των προϊόντων με ψηφιακά στοιχεία από το στάδιο σχεδιασμού και ανάπτυξης και καθ' όλη τη διάρκεια του κύκλου ζωής των εν λόγω προϊόντων, θα μπορούσαν να ληφθούν υπόψη διάφοροι δείκτες. Αυτοί θα μπορούσαν να είναι ο αριθμός των σημαντικών συμβάντων στην Ένωση που προκαλούνται από τρωτά σημεία, το ποσοστό των κατασκευαστών υλισμικού και λογισμικού που ακολουθούν κύκλο ζωής συστηματικής ασφαλούς ανάπτυξης, η ποιοτική ανάλυση της ασφάλειας των προϊόντων με ψηφιακά στοιχεία, η ποσοτική και ποιοτική αξιολόγηση των βάσεων δεδομένων τρωτών σημείων, η συχνότητα των ενημερώσεων ασφαλείας που διατίθενται από τους κατασκευαστές ή ο μέσος αριθμός ημερών μεταξύ της ανακάλυψης ενός τρωτού σημείου και της παροχής ενημερώσεων ασφαλείας.

[38] Βλ. [έγγραφο εργασίας των υπηρεσιών της Επιτροπής σχετικά με την έκθεση εκτίμησης επιπτώσεων που συνοδεύει τον κανονισμό σχετικά με τις οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία]

[39] Βλ. [έγγραφο εργασίας των υπηρεσιών της Επιτροπής σχετικά με την έκθεση εκτίμησης επιπτώσεων που συνοδεύει τον κανονισμό σχετικά με τις οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία]

Η απουσία στοχευμένης εθνικής νομοθεσίας για την κυβερνοασφάλεια ειδικά για κάθε προϊόν θα μπορούσε να είναι δείκτης ενός συνεκτικού πλαισίου κυβερνοασφάλειας.

Το ποσοστό των προϊόντων με ψηφιακά στοιχεία που αποστέλλονται με πληροφορίες σχετικά με τις ιδιότητες ασφάλειας θα μπορούσε να είναι δείκτης αυξημένης διαφάνειας όσον αφορά τις ιδιότητες ασφάλειας των προϊόντων με ψηφιακά στοιχεία. Επιπλέον, το ποσοστό των προϊόντων με ψηφιακά στοιχεία που διατίθενται με οδηγίες χρήστη σχετικά με την ασφαλή χρήση θα μπορούσε να χρησιμοποιηθεί ως δείκτης για το κατά πόσον οι οργανισμοί και οι καταναλωτές έχουν τη δυνατότητα να χρησιμοποιούν με ασφάλεια προϊόντα με ψηφιακά στοιχεία.

Όσον αφορά την παρακολούθηση του αντικτύπου του κανονισμού, θα εξεταστούν ορισμένοι δείκτες για τον σκοπό αυτό, οι οποίοι θα αξιολογηθούν από την Επιτροπή, κατά περίπτωση με την υποστήριξη του ENISA. Ανάλογα με τον επιχειρησιακό στόχο που πρέπει να επιτευχθεί, ορισμένοι από τους δείκτες παρακολούθησης βάσει των οποίων θα αξιολογείται η επιτυχία των οριζόντιων απαιτήσεων κυβερνοασφάλειας είναι οι εξής:

*Για την αξιολόγηση του επιπέδου κυβερνοασφάλειας προϊόντων με ψηφιακά στοιχεία:*

— Στατιστικές και ποιοτική ανάλυση σχετικά με συμβάντα που επηρεάζουν προϊόντα με ψηφιακά στοιχεία και τον τρόπο αντιμετώπισής τους. Τα στοιχεία αυτά θα μπορούσαν να συγκεντρώνονται και να αξιολογούνται από την Επιτροπή, με την υποστήριξη του ENISA.

— Αρχεία γνωστών τρωτών σημείων και αναλύσεις του τρόπου αντιμετώπισής τους. Η ανάλυση αυτή θα μπορούσε να διενεργηθεί από τον ENISA, με βάση την ευρωπαϊκή βάση δεδομένων τρωτών σημείων που δημιουργήθηκε με βάση την [οδηγία XXX/XXXX (NIS2)].

— Έρευνες μεταξύ κατασκευαστών υλισμικού και λογισμικού για την παρακολούθηση της προόδου.

*Για την αξιολόγηση του επιπέδου των πληροφοριών σχετικά με τα χαρακτηριστικά ασφαλείας, την υποστήριξη της ασφάλειας, το τέλος του κύκλου ζωής και το καθήκον επιμέλειας*: αποτελέσματα ερευνών που θα διεξαχθούν από την Επιτροπή, με την υποστήριξη του ENISA τόσο για τους χρήστες όσο και για τις επιχειρήσεις.

*Για την αξιολόγηση της υλοποίησης*, η Επιτροπή θα έχει ως στόχο να διασφαλίσει ότι οι αξιολογήσεις συμμόρφωσης διενεργούνται αποτελεσματικά. Για τον σκοπό αυτό, θα εκδοθεί αίτημα τυποποίησης και θα παρακολουθείται η εφαρμογή του. Η Επιτροπή επαληθεύει επίσης την ικανότητα των κοινοποιημένων οργανισμών και, κατά περίπτωση, των οργανισμών πιστοποίησης.

*Όσον αφορά την εφαρμογή*, μέσω των εκθέσεων των κρατών μελών, η Επιτροπή θα επαληθεύει ότι οι εθνικές πρωτοβουλίες δεν αφορούν πτυχές που καλύπτονται από τον κανονισμό.

## 1.5. Αιτιολόγηση της πρότασης/πρωτοβουλίας

*1.5.1. Βραχυπρόθεσμη ή μακροπρόθεσμη κάλυψη αναγκών, συμπεριλαμβανομένου λεπτομερούς χρονοδιαγράμματος για τη σταδιακή υλοποίηση της πρωτοβουλίας*

Ο κανονισμός θα τεθεί σε πλήρη εφαρμογή 24 μήνες μετά την έναρξη ισχύος του. Ωστόσο, θα πρέπει να υπάρχουν στοιχεία της δομής διακυβέρνησης πριν από την εν λόγω ημερομηνία. Συγκεκριμένα, τα κράτη μέλη οφείλουν να έχουν ορίσει

υφιστάμενες αρχές και/ή συστήσει νέες αρχές για την εκτέλεση των καθηκόντων που καθορίζονται στη νομοθεσία.

*1.5.2. Προστιθέμενη αξία της ενωσιακής παρέμβασης (που μπορεί να προκύπτει από διάφορους παράγοντες, π.χ. οφέλη από τον συντονισμό, ασφάλεια δικαίου, μεγαλύτερη αποτελεσματικότητα ή συμπληρωματικότητα). Για τους σκοπούς του παρόντος σημείου, «προστιθέμενη αξία της ενωσιακής παρέμβασης» είναι η αξία που απορρέει από την ενωσιακή παρέμβαση και η οποία προστίθεται στην αξία που θα είχε δημιουργηθεί αν τα κράτη μέλη ενεργούσαν μεμονωμένα.*

Ο ισχυρός διασυνοριακός χαρακτήρας της κυβερνοασφάλειας και ο αυξανόμενος αριθμός των συμβάντων, με δευτερογενείς επιπτώσεις σε διασυνοριακό επίπεδο, καθώς και σε τομείς και προϊόντα, σημαίνουν ότι οι στόχοι δεν μπορούν να επιτευχθούν αποτελεσματικά μόνο από τα κράτη μέλη. Δεδομένου του παγκόσμιου χαρακτήρα των αγορών προϊόντων με ψηφιακά στοιχεία, τα κράτη μέλη αντιμετωπίζουν τους ίδιους κινδύνους για το ίδιο προϊόν με ψηφιακά στοιχεία στην επικράτειά τους. Το κατακερματισμένο πλαίσιο δυνητικά αποκλινόντων εθνικών κανόνων που αναδύεται, ενέχει επίσης τον κίνδυνο να παρεμποδίσει την ύπαρξη μιας ανοικτής και ανταγωνιστικής ενιαίας αγοράς για προϊόντα με ψηφιακά στοιχεία. Ως εκ τούτου, η κοινή δράση σε επίπεδο ΕΕ είναι αναγκαία για την αύξηση του επιπέδου εμπιστοσύνης μεταξύ των χρηστών και της ελκυστικότητας των ενωσιακών προϊόντων με ψηφιακά στοιχεία. Μπορεί επίσης να ωφελήσει την εσωτερική αγορά, παρέχοντας ασφάλεια δικαίου και επιτυγχάνοντας ισότιμους όρους ανταγωνισμού για τους πωλητές προϊόντων με ψηφιακά στοιχεία.

*1.5.3. Διδάγματα από ανάλογες εμπειρίες του παρελθόντος*

Ο νόμος για την κυβερνοανθεκτικότητα είναι ο πρώτος κανονισμός του είδους του, ο οποίος θεσπίζει απαιτήσεις κυβερνοασφάλειας για τη διάθεση προϊόντων με ψηφιακά στοιχεία στην αγορά. Βασίζεται, ωστόσο, στον καθορισμό του νέου νομοθετικού πλαισίου και στα διδάγματα που αντλήθηκαν από τη διαδικασία εφαρμογής της υφιστάμενης ενωσιακής νομοθεσίας εναρμόνισης διαφόρων προϊόντων, ιδίως όσον αφορά την προετοιμασία για την εφαρμογή, συμπεριλαμβανομένων πτυχών όπως η κατάρτιση εναρμονισμένων προτύπων.

*1.5.4. Συμβατότητα με το πολυετές δημοσιονομικό πλαίσιο και ενδεχόμενες συνέργειες με άλλα κατάλληλα μέσα*

Ο κανονισμός σχετικά με τις οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία καθορίζει νέες απαιτήσεις κυβερνοασφάλειας για όλα τα προϊόντα με ψηφιακά στοιχεία που διατίθενται στην αγορά της ΕΕ, οι οποίες υπερβαίνουν τυχόν απαιτήσεις που προβλέπονται από την ισχύουσα νομοθεσία. Ταυτόχρονα, η πρόταση βασίζεται στον υφιστάμενο καθορισμό της νομοθεσίας για το ΝΝΠ. Ως εκ τούτου, θα βασιστεί στις υφιστάμενες δομές και διαδικασίες του ΝΝΠ, όπως η συνεργασία των κοινοποιημένων οργανισμών και η εποπτεία της αγοράς, οι ενότητες αξιολόγησης της συμμόρφωσης, και η ανάπτυξη εναρμονισμένων προτύπων. Η νέα πρόταση θα βασίζεται επίσης σε ορισμένες δομές που έχουν αναπτυχθεί σύμφωνα με άλλες νομοθετικές πράξεις για την κυβερνοασφάλεια, όπως η οδηγία 2016/1148 (οδηγία NIS), αντίστοιχα η [οδηγία XXX/XXXX (NIS2)] ή ο κανονισμός 2019/881 (πράξη για την κυβερνοασφάλεια).

*1.5.5. Αξιολόγηση των διαφόρων διαθέσιμων επιλογών χρηματοδότησης, συμπεριλαμβανομένων των δυνατοτήτων ανακατανομής*

Η διαχείριση των τομέων δράσης που ανατίθενται στον ENISA ανταποκρίνεται στην υφιστάμενη εντολή και στα γενικά καθήκοντά του. Οι εν λόγω τομείς δράσης ενδέχεται να απαιτούν ειδικά προφίλ ή νέες αναθέσεις, αλλά αυτές δεν θα είναι αξιοσημείωτες και μπορούν να απορροφηθούν από τους υφιστάμενους πόρους του ENISA και να επιλυθούν μέσω ανακατανομής ή σύνδεσης διαφόρων αναθέσεων. Για παράδειγμα, ένας από τους κύριους τομείς δράσης που έχουν ανατεθεί στον ENISA αφορά τη συλλογή και την επεξεργασία κοινοποιήσεων από τους κατασκευαστές σχετικά με τα τρωτά σημεία των προϊόντων που αποτελούν αντικείμενο εκμετάλλευσης. [Η οδηγία XXX/XXXX (NIS2)] έχει ήδη αναθέσει στον ENISA να δημιουργήσει μια ευρωπαϊκή βάση δεδομένων τρωτών σημείων στην οποία θα μπορούν να γνωστοποιούνται και να καταχωρίζονται, σε εθελοντική βάση, ευρέως γνωστά τρωτά σημεία, με σκοπό να μπορούν οι χρήστες να λαμβάνουν τα κατάλληλα μέτρα άμβλυνσης του κινδύνου. Οι πόροι που διατίθενται για τον σκοπό αυτό θα μπορούσαν επίσης να χρησιμοποιηθούν για τις νέες προαναφερθείσες αναθέσεις σχετικά με τις κοινοποιήσεις τρωτών σημείων των προϊόντων. Με τον τρόπο αυτόν, θα μπορούσε να διασφαλιστεί η αποτελεσματική χρήση των υφιστάμενων πόρων καθώς και να δημιουργηθούν οι αναγκαίες συνέργειες μεταξύ των εν λόγω αναθέσεων που θα μπορούσαν να τεκμηριώσουν καλύτερα τις αναλύσεις του ENISA σχετικά με τους κινδύνους και τις απειλές για την κυβερνοασφάλεια.

**1.6. Διάρκεια και δημοσιονομικές επιπτώσεις της πρότασης/πρωτοβουλίας**

☐ **περιορισμένη διάρκεια**

– ☐ με ισχύ από [HH/MM]EEEE έως [HH/MM]EEEE

– ☐ Δημοσιονομικές επιπτώσεις από το EEEE έως το EEEE για πιστώσεις ανάληψης υποχρεώσεων και από το EEEE έως το EEEE για πιστώσεις πληρωμών.

**απεριόριστη διάρκεια**

– Περίοδος σταδιακής εφαρμογής από το 2025.

– και στη συνέχεια πλήρης εφαρμογή.

**1.7. Προβλεπόμενοι τρόποι διαχείρισης[40]**

☐ **Άμεση διαχείριση** από την Επιτροπή

– × από τις υπηρεσίες της, συμπεριλαμβανομένου του προσωπικού της στις αντιπροσωπείες της Ένωσης

– ☐ από τους εκτελεστικούς οργανισμούς

☐ **Επιμερισμένη διαχείριση** με τα κράτη μέλη

☐ **Έμμεση διαχείριση** με ανάθεση καθηκόντων εκτέλεσης του προϋπολογισμού:

– ☐ σε τρίτες χώρες ή οργανισμούς που αυτές έχουν ορίσει

– ☐ σε διεθνείς οργανισμούς και στις οργανώσεις τους (να προσδιοριστούν)

– ☐ στην ΕΤΕπ και στο Ευρωπαϊκό Ταμείο Επενδύσεων

– ☐ στους οργανισμούς που αναφέρονται στα άρθρα 70 και 71 του δημοσιονομικού κανονισμού

– ☐ σε οργανισμούς δημοσίου δικαίου

– ☐ σε οργανισμούς που διέπονται από ιδιωτικό δίκαιο και έχουν αποστολή δημόσιας υπηρεσίας, στον βαθμό που παρέχουν επαρκείς οικονομικές εγγυήσεις

– ☐ σε οργανισμούς που διέπονται από το ιδιωτικό δίκαιο κράτους μέλους, στους οποίους έχει ανατεθεί η εκτέλεση σύμπραξης δημόσιου και ιδιωτικού τομέα και οι οποίοι παρέχουν επαρκείς οικονομικές εγγυήσεις

– ☐ σε πρόσωπα επιφορτισμένα με την εκτέλεση συγκεκριμένων δράσεων στην ΚΕΠΠΑ βάσει του τίτλου V της ΣΕΕ και τα οποία προσδιορίζονται στην αντίστοιχη βασική πράξη.

– *Αν αναφέρονται περισσότεροι του ενός τρόποι διαχείρισης, να διευκρινιστούν στο τμήμα «Παρατηρήσεις».*

Παρατηρήσεις

| |
|---|
| Ο παρών κανονισμός αναθέτει ορισμένες δράσεις στον ENISA, σύμφωνα με την υφιστάμενη εντολή του, και ιδίως το άρθρο 3 παράγραφος 2 του κανονισμού 2019/881 που ορίζει ότι ο ENISA θα πρέπει να ασκεί τα καθήκοντα που του ανατίθενται με νομικές πράξεις της Ένωσης που καθορίζουν μέτρα για την προσέγγιση νόμων, κανονισμών και διοικητικών |

[40] Οι λεπτομέρειες σχετικά με τους τρόπους διαχείρισης και οι παραπομπές στον δημοσιονομικό κανονισμό είναι διαθέσιμες στον δικτυακό τόπο BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

διατάξεων των κρατών μελών που σχετίζονται με την κυβερνοασφάλεια. Ειδικότερα, ο ENISA αναλαμβάνει το καθήκον να λαμβάνει κοινοποιήσεις από τους κατασκευαστές σχετικά με τρωτά σημεία που περιέχονται σε προϊόντα με ψηφιακά στοιχεία και αποτελούν αντικείμενο ενεργού εκμετάλλευσης, καθώς και σχετικά με συμβάντα που έχουν αντίκτυπο στην ασφάλεια αυτών των προϊόντων. Ο ENISA θα πρέπει επίσης να διαβιβάζει τις κοινοποιήσεις αυτές στις σχετικές CSIRT ή, αντίστοιχα, στο σχετικό ενιαίο σημείο των κρατών μελών που ορίζεται σύμφωνα με το άρθρο [άρθρο X] της οδηγίας [οδηγία XXX/XXXX (NIS2)], καθώς και να ενημερώνει τις αρμόδιες αρχές εποπτείας της αγοράς. Με βάση τις πληροφορίες που συγκεντρώνει, ο ENISA θα πρέπει να καταρτίζει διετή τεχνική έκθεση σχετικά με τις αναδυόμενες τάσεις όσον αφορά τους κινδύνους για την κυβερνοασφάλεια σε προϊόντα με ψηφιακά στοιχεία και να την υποβάλλει στην ομάδα συνεργασίας NIS. Επιπλέον, όσον αφορά την εμπειρογνωσία του ENISA, τις πληροφορίες που συγκεντρώνονται και τις αναλύσεις απειλών, ο ENISA μπορεί να υποστηρίζει τη διαδικασία εφαρμογής του παρόντος κανονισμού προτείνοντας κοινές δραστηριότητες που θα διεξάγονται από τις εθνικές αρχές εποπτείας της αγοράς βάσει ενδείξεων ή πληροφοριών σχετικά με πιθανή μη συμμόρφωση προϊόντων με ψηφιακά στοιχεία προς τον παρόντα κανονισμό σε διάφορα κράτη μέλη, ή να εντοπίζει κατηγορίες προϊόντων για τα οποία μπορούν να οργανώνονται ταυτόχρονες συντονισμένες δράσεις ελέγχου. Η Επιτροπή μπορεί να ζητήσει από τον ENISA να διενεργήσει αξιολογήσεις για συγκεκριμένα προϊόντα σε εξαιρετικές περιστάσεις όσον αφορά προϊόντα με ψηφιακά στοιχεία που παρουσιάζουν σημαντικό κίνδυνο για την κυβερνοασφάλεια και όταν απαιτείται άμεση παρέμβαση για τη διατήρηση της εύρυθμης λειτουργίας της εσωτερικής αγοράς.

Όλες αυτές οι εργασίες εκτιμώνται σε περίπου 4,5 ΙΠΑ από τους υφιστάμενους πόρους του ENISA, με βάση την ήδη υπάρχουσα εμπειρογνωσία και τις προπαρασκευαστικές εργασίες που πραγματοποιεί επί του παρόντος ο ENISA, μεταξύ άλλων για την υποστήριξη της επικείμενης εφαρμογής της [οδηγίας XXX/XXXX (NIS2)], για την οποία συμπληρώθηκαν οι πόροι του ENISA.

## 2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ

### 2.1. Κανόνες παρακολούθησης και υποβολής εκθέσεων

*Να προσδιοριστούν η συχνότητα και οι όροι.*

Έως 36 μήνες μετά την ημερομηνία εφαρμογής του παρόντος κανονισμού και στη συνέχεια κάθε τέσσερα έτη, η Επιτροπή θα υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο έκθεση σχετικά με την αξιολόγηση και την επανεξέτασή του. Οι εκθέσεις δημοσιοποιούνται.

### 2.2. Συστήματα διαχείρισης και ελέγχου

*2.2.1. Αιτιολόγηση των τρόπων διαχείρισης, των μηχανισμών εκτέλεσης της χρηματοδότησης, των όρων πληρωμής και της προτεινόμενης στρατηγικής ελέγχου*

Ο παρών κανονισμός θεσπίζει νέα πολιτική όσον αφορά τις εναρμονισμένες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία που διατίθενται στην εσωτερική αγορά καθ' όλη τη διάρκεια του κύκλου ζωής τους. Η νομική πράξη θα συνοδεύεται από αιτήματα της Επιτροπής προς τους ευρωπαϊκούς οργανισμούς τυποποίησης για την ανάπτυξη προτύπων.

Για την εκτέλεση των νέων αυτών καθηκόντων, είναι απαραίτητο να παρασχεθούν κατάλληλοι πόροι στις υπηρεσίες της Επιτροπής. Η επιβολή του νέου κανονισμού εκτιμάται ότι απαιτεί 7 ΙΠΑ (εκ των οποίων μία θέση END) για την κάλυψη των ακόλουθων καθηκόντων:

– κατάρτιση του αιτήματος τυποποίησης και/ή κοινών προδιαγραφών μέσω εκτελεστικών πράξεων χωρίς επιτυχή διαδικασία τυποποίησης·

– κατάρτιση κατ' εξουσιοδότηση πράξης [εντός 12 μηνών από την έναρξη ισχύος του κανονισμού] για τον προσδιορισμό των ορισμών των κρίσιμων προϊόντων με ψηφιακά στοιχεία·

– πιθανή κατάρτιση κατ' εξουσιοδότηση πράξεων για την επικαιροποίηση του καταλόγου των κρίσιμων προϊόντων των κατηγοριών I και II· προσδιορισμός του αν απαιτείται περιορισμός ή αποκλεισμός για προϊόντα με ψηφιακά στοιχεία που καλύπτονται από άλλους ενωσιακούς κανόνες που καθορίζουν απαιτήσεις που επιτυγχάνουν το ίδιο επίπεδο προστασίας με τον παρόντα κανονισμό· την επιβολή της πιστοποίησης ορισμένων εξαιρετικά κρίσιμων προϊόντων με ψηφιακά στοιχεία βάσει των κριτηρίων που καθορίζονται στον παρόντα κανονισμό· προσδιορισμός του ελάχιστου περιεχομένου της δήλωσης συμμόρφωσης ΕΕ και συμπλήρωση των στοιχείων που πρέπει να περιλαμβάνονται στον τεχνικό φάκελο·

– πιθανή κατάρτιση εκτελεστικών πράξεων σχετικά με τον μορφότυπο ή τα στοιχεία των υποχρεώσεων υποβολής εκθέσεων, τον κατάλογο υλικών λογισμικού, τις κοινές προδιαγραφές ή την τοποθέτηση της σήμανσης CE·

– ενδεχομένως προετοιμασία άμεσης παρέμβασης για την επιβολή διορθωτικών ή περιοριστικών μέτρων σε εξαιρετικές περιστάσεις για τη διατήρηση της εύρυθμης λειτουργίας της εσωτερικής αγοράς, συμπεριλαμβανομένης της κατάρτισης εκτελεστικής πράξης·

– οργάνωση και συντονισμός των κοινοποιήσεων από τα κράτη μέλη των κοινοποιημένων οργανισμών και συντονισμός των κοινοποιημένων οργανισμών·

– υποστήριξη του συντονισμού των αρχών εποπτείας της αγοράς των κρατών μελών.

*2.2.2. Πληροφορίες σχετικά με τους κινδύνους που έχουν εντοπιστεί και τα συστήματα εσωτερικού ελέγχου που έχουν δημιουργηθεί για τον μετριασμό τους*

Για να διασφαλιστεί ότι οι κοινοποιημένοι οργανισμοί και οι αρχές εποπτείας της αγοράς ανταλλάσσουν πληροφορίες και συνεργάζονται αρμονικά, η Επιτροπή είναι υπεύθυνη για τον συντονισμό τους. Για την εμπειρογνωσία σε τεχνικά ζητήματα και θέματα της αγοράς, θα συσταθεί ομάδα εμπειρογνωμόνων.

*2.2.3. Εκτίμηση και αιτιολόγηση της οικονομικής αποδοτικότητας των ελέγχων (λόγος του κόστους του ελέγχου προς την αξία των σχετικών κονδυλίων που αποτελούν αντικείμενο διαχείρισης) και αξιολόγηση του εκτιμώμενου επιπέδου κινδύνου σφάλματος (κατά την πληρωμή και κατά το κλείσιμο)*

**2.3. Για τις δαπάνες των συνεδριάσεων, δεδομένης της χαμηλής αξίας ανά συναλλαγή (π.χ. επιστροφή των εξόδων μετακίνησης αντιπροσώπου για μια συνεδρίαση), οι τυπικές διαδικασίες ελέγχου φαίνονται επαρκείς. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας**

*Να προσδιοριστούν τα ισχύοντα ή τα προβλεπόμενα μέτρα πρόληψης και προστασίας, π.χ. στη στρατηγική για την καταπολέμηση της απάτης.*

Τα ισχύοντα μέτρα πρόληψης περιπτώσεων απάτης που εφαρμόζονται στην Επιτροπή θα καλύπτουν τις πρόσθετες πιστώσεις που είναι αναγκαίες για τον παρόντα κανονισμό.

## 3. ΕΚΤΙΜΩΜΕΝΕΣ ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

### 3.1. Τομείς του πολυετούς δημοσιονομικού πλαισίου και γραμμές δαπανών του προϋπολογισμού που επηρεάζονται

- Υφιστάμενες γραμμές του προϋπολογισμού

*Σχήμα*

- Νέες γραμμές του προϋπολογισμού, των οποίων έχει ζητηθεί η δημιουργία

*Ά.Α.*

### 3.2. Εκτιμώμενες δημοσιονομικές επιπτώσεις της πρότασης στις πιστώσεις

*3.2.1. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις επιχειρησιακές πιστώσεις*

– ☑ Η πρόταση/πρωτοβουλία δεν συνεπάγεται τη χρησιμοποίηση επιχειρησιακών πιστώσεων

– ☐ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση επιχειρησιακών πιστώσεων, όπως εξηγείται κατωτέρω:

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

| **Τομέας του πολυετούς δημοσιονομικού πλαισίου** | Αριθμός | |
|---|---|---|

| ΓΔ: <…….> | | | Έτος **N**[41] | Έτος **N+1** | Έτος **N+2** | Έτος **N+3** | Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) | | | **ΣΥΝΟΛΟ** |
|---|---|---|---|---|---|---|---|---|---|---|
| • Επιχειρησιακές πιστώσεις | | | | | | | | | | |
| Γραμμή του προϋπολογισμού[42] | Αναλήψεις υποχρεώσεων | (1α) | | | | | | | | |
| | Πληρωμές | (2α) | | | | | | | | |
| Γραμμή του προϋπολογισμού | Αναλήψεις υποχρεώσεων | (1β) | | | | | | | | |
| | Πληρωμές | (2β) | | | | | | | | |
| Πιστώσεις διοικητικού χαρακτήρα χρηματοδοτούμενες από το κονδύλιο ειδικών προγραμμάτων[43] | | | | | | | | | | |
| Γραμμή του προϋπολογισμού | | (3) | | | | | | | | |
| **ΣΥΝΟΛΟ πιστώσεων** | Αναλήψεις | =1α+1 | | | | | | | | |

41 Το έτος N είναι το έτος έναρξης εφαρμογής της πρότασης/πρωτοβουλίας. Να αντικατασταθεί το «N» με το αναμενόμενο πρώτο έτος εφαρμογής (για παράδειγμα: 2021). Το ίδιο και για τα επόμενα έτη.

42 Σύμφωνα με την επίσημη ονοματολογία του προϋπολογισμού.

43 Τεχνική και/ή διοικητική βοήθεια και δαπάνες στήριξης της εφαρμογής προγραμμάτων και/ή δράσεων της ΕΕ (πρώην γραμμές «ΒΑ»), έμμεση έρευνα, άμεση έρευνα.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **για τη ΓΔ <…….>** | υποχρεώσεων | β +3 | | | | | | | | |
| | Πληρωμές | =2α+2 β +3 | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| • ΣΥΝΟΛΟ επιχειρησιακών πιστώσεων | Αναλήψεις υποχρεώσεων | (4) | | | | | | | | |
| | Πληρωμές | (5) | | | | | | | | |
| • ΣΥΝΟΛΟ πιστώσεων διοικητικού χαρακτήρα χρηματοδοτούμενων από το κονδύλιο ειδικών προγραμμάτων | | (6) | | | | | | | | |
| **ΣΥΝΟΛΟ πιστώσεων του ΤΟΜΕΑ <….>** του πολυετούς δημοσιονομικού πλαισίου | Αναλήψεις υποχρεώσεων | =4+ 6 | | | | | | | | |
| | Πληρωμές | =5+ 6 | | | | | | | | |

**<u>Αν η πρόταση/πρωτοβουλία επηρεάζει περισσότερους του ενός επιχειρησιακούς τομείς, επαναλάβετε το ανωτέρω τμήμα:</u>**

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| • ΣΥΝΟΛΟ επιχειρησιακών πιστώσεων (όλοι οι επιχειρησιακοί τομείς) | Αναλήψεις υποχρεώσεων | (4) | | | | | | | | |
| | Πληρωμές | (5) | | | | | | | | |
| ΣΥΝΟΛΟ πιστώσεων διοικητικού χαρακτήρα χρηματοδοτούμενων από το κονδύλιο ειδικών προγραμμάτων (όλοι οι επιχειρησιακοί τομείς) | | (6) | | | | | | | | |
| **ΣΥΝΟΛΟ πιστώσεων των ΤΟΜΕΩΝ 1 έως 6** του πολυετούς δημοσιονομικού πλαισίου (Ποσό αναφοράς) | Αναλήψεις υποχρεώσεων | =4+ 6 | | | | | | | | |
| | Πληρωμές | =5+ 6 | | | | | | | | |

| | | |
|---|---|---|
| **Τομέας του πολυετούς δημοσιονομικού πλαισίου** | **7** | «Διοικητικές δαπάνες» |

Αυτό το τμήμα πρέπει να συμπληρωθεί με «στοιχεία διοικητικού χαρακτήρα του προϋπολογισμού» τα οποία θα εισαχθούν, καταρχάς, στο παράρτημα του νομοθετικού δημοσιονομικού δελτίου (παράρτημα V του εσωτερικού κανονισμού), που μεταφορτώνεται στο DECIDE για διυπηρεσιακή διαβούλευση.

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

| | | Έτος **2024** | Έτος **2025** | Έτος **2026** | Έτος **2027** | **ΣΥΝΟΛΟ** |
|---|---|---|---|---|---|---|
| ΓΔ: CNECT | | | | | | |
| • Ανθρώπινοι πόροι | | 1,030 | 1,030 | 1,030 | 1,030 | **4,120** |
| • Άλλες διοικητικές δαπάνες | | **0,222** | **0,222** | **0,222** | **0,222** | **0,888** |
| **ΣΥΝΟΛΟ ΓΔ** CNECT | Πιστώσεις | **1,252** | **1,252** | **1,252** | **1,252** | **5,008** |

| | | | | | | |
|---|---|---|---|---|---|---|
| **ΣΥΝΟΛΟ πιστώσεων του ΤΟΜΕΑ 7** του πολυετούς δημοσιονομικού πλαισίου | (Σύνολο αναλήψεων υποχρεώσεων = Σύνολο πληρωμών) | **1,252** | **1,252** | **1,252** | **1,252** | **5,008** |

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

| | | Έτος **2024** | Έτος **2025** | Έτος **2026** | Έτος **2027** | **ΣΥΝΟΛΟ** |
|---|---|---|---|---|---|---|
| **ΣΥΝΟΛΟ πιστώσεων των ΤΟΜΕΩΝ 1 έως 7** του πολυετούς δημοσιονομικού πλαισίου | Αναλήψεις υποχρεώσεων | **1,252** | **1,252** | **1,252** | **1,252** | **5,008** |
| | Πληρωμές | **1,252** | **1,252** | **1,252** | **1,252** | **5,008** |

*3.2.2. Εκτιμώμενο αποτέλεσμα που χρηματοδοτείται με επιχειρησιακές πιστώσεις*

Πιστώσεις ανάληψης υποχρεώσεων σε εκατ. EUR (με τρία δεκαδικά ψηφία)

| **Να προσδιοριστούν οι στόχοι και τα αποτελέσματα** ⇩ | | | Έτος **N** | | Έτος **N+1** | | Έτος **N+2** | | Έτος **N+3** | | Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) | | | | | | **ΣΥΝΟΛΟ** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **ΑΠΟΤΕΛΕΣΜΑΤΑ** | | | | | | | | | | | | | | | | | |
| | Είδος 44 | Μέσο κόστος | Αριθ. | Κόστος | Αριθ. | Κόστος | Αριθ. | Κόστος | Αριθ. | Κόστος | Αριθ. | Κόστος | Αριθ. | Κόστος | Αριθ. | Κόστος | Συνολικός αριθ. | Συνολικό κόστος |
| ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 1[45]… | | | | | | | | | | | | | | | | | | |
| — Αποτέλεσμα | | | | | | | | | | | | | | | | | | |
| — Αποτέλεσμα | | | | | | | | | | | | | | | | | | |
| — Αποτέλεσμα | | | | | | | | | | | | | | | | | | |
| Μερικό σύνολο για τον ειδικό στόχο αριθ. 1 | | | | | | | | | | | | | | | | | | |
| ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 2 ... | | | | | | | | | | | | | | | | | | |
| — Αποτέλεσμα | | | | | | | | | | | | | | | | | | |
| Μερικό σύνολο για τον ειδικό στόχο αριθ. 2 | | | | | | | | | | | | | | | | | | |
| **ΣΥΝΟΛΑ** | | | | | | | | | | | | | | | | | | |

44 Τα αποτελέσματα είναι τα προϊόντα και οι υπηρεσίες που θα παρασχεθούν (π.χ.: αριθμός ανταλλαγών φοιτητών που θα χρηματοδοτηθούν, αριθμός χλμ. οδών που θα κατασκευαστούν κ.λπ.).

45 Όπως περιγράφεται στο σημείο 1.4.2. «Ειδικοί στόχοι…».

### *3.2.3. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις διοικητικές πιστώσεις*

– ☐ Η πρόταση/πρωτοβουλία δεν συνεπάγεται τη χρησιμοποίηση πιστώσεων διοικητικού χαρακτήρα

– ☑ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση πιστώσεων διοικητικού χαρακτήρα, όπως εξηγείται κατωτέρω:

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

| | Έτος **2024** | Έτος **2025** | Έτος **2026** | Έτος **2027** | |
|---|---|---|---|---|---|
| **ΤΟΜΕΑΣ 7 του πολυετούς δημοσιονομικού πλαισίου** | | | | | |
| Ανθρώπινοι πόροι | 1,030 | 1,030 | 1,030 | 1,030 | **4,120** |
| Άλλες διοικητικές δαπάνες | 0,222 | 0,222 | 0,222 | 0,222 | **0,888** |
| **Μερικό σύνολο του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου** | 1,252 | 1,252 | 1,252 | 1,252 | **5,008** |

| **Εκτός του ΤΟΜΕΑ 7**[46] **του πολυετούς δημοσιονομικού πλαισίου** | | | | | |
|---|---|---|---|---|---|
| Ανθρώπινοι πόροι | | | | | |
| Άλλες δαπάνες διοικητικού χαρακτήρα | | | | | |
| **Μερικό σύνολο εκτός του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου** | | | | | |

| **ΣΥΝΟΛΟ** | 1,252 | 1,252 | 1,252 | 1,252 | **5,008** |
|---|---|---|---|---|---|

Οι απαιτούμενες πιστώσεις για ανθρώπινους πόρους και άλλες δαπάνες διοικητικού χαρακτήρα θα καλυφθούν από τις πιστώσεις της ΓΔ που έχουν ήδη διατεθεί για τη διαχείριση της δράσης και/ή έχουν ανακατανεμηθεί στο εσωτερικό της ΓΔ και οι οποίες θα συμπληρωθούν, κατά περίπτωση, με πρόσθετα κονδύλια που ενδέχεται να χορηγηθούν στην αρμόδια για τη διαχείριση ΓΔ στο πλαίσιο της ετήσιας διαδικασίας κατανομής και λαμβανομένων υπόψη των υφιστάμενων δημοσιονομικών περιορισμών.

[46] Τεχνική και/ή διοικητική βοήθεια και δαπάνες στήριξης της εφαρμογής προγραμμάτων και/ή δράσεων της ΕΕ (πρώην γραμμές «ΒΑ»), έμμεση έρευνα, άμεση έρευνα.

3.2.3.1. Εκτιμώμενες ανάγκες σε ανθρώπινους πόρους

– ☐ Η πρόταση/πρωτοβουλία δεν συνεπάγεται τη χρησιμοποίηση ανθρώπινων πόρων

– ☑ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση ανθρώπινων πόρων, όπως εξηγείται κατωτέρω:

*Εκτίμηση η οποία πρέπει να εκφράζεται σε μονάδες ισοδυνάμων πλήρους απασχόλησης*

| | Έτος **2024** | Έτος **2025** | Έτος **2026** | Έτος **2027** |
|---|---|---|---|---|
| 20 01 02 01 (στην έδρα και στις αντιπροσωπείες της Επιτροπής) | 6 | 6 | 6 | 6 |
| 20 01 02 03 (στις αντιπροσωπείες της ΕΕ) | | | | |
| 01 01 01 01 (έμμεση έρευνα) | | | | |
| 01 01 01 11 (άμεση έρευνα) | | | | |
| Άλλες γραμμές του προϋπολογισμού (να προσδιοριστούν) | | | | |
| **• Εξωτερικό προσωπικό (σε μονάδα ισοδυνάμου πλήρους απασχόλησης: ΙΠΑ)**[47] | | | | |
| 20 02 01 (AC, END, INT από το συνολικό κονδύλιο) | 1 | 1 | 1 | 1 |
| 20 02 03 (AC, AL, END, INT και JPD στις αντιπροσωπείες της ΕΕ) | | | | |
| **XX** 01 xx **yy zz** [48] — στην έδρα | | | | |
| **XX** 01 xx **yy zz** [48] — στις αντιπροσωπείες της ΕΕ | | | | |
| 01 01 01 02 (AC, END, INT — έμμεση έρευνα) | | | | |
| 01 01 01 12 (AC, END, INT – άμεση έρευνα) | | | | |
| Άλλες γραμμές του προϋπολογισμού (να προσδιοριστούν) | | | | |
| **ΣΥΝΟΛΟ** | **7** | **7** | **7** | **7** |

**XX** είναι ο σχετικός τομέας πολιτικής ή ο σχετικός τίτλος του προϋπολογισμού.

Οι ανάγκες σε ανθρώπινους πόρους θα καλυφθούν από το προσωπικό της ΓΔ που έχει ήδη διατεθεί για τη διαχείριση της δράσης και/ή έχει ανακατανεμηθεί στο εσωτερικό της ΓΔ και το οποίο θα συμπληρωθεί, εάν χρειαστεί, από πρόσθετους πόρους που μπορεί να διατεθούν στην αρμόδια για τη διαχείριση ΓΔ στο πλαίσιο της ετήσιας διαδικασίας κατανομής και λαμβανομένων υπόψη των υφιστάμενων δημοσιονομικών περιορισμών.

Περιγραφή των προς εκτέλεση καθηκόντων:

| | |
|---|---|
| Μόνιμοι και έκτακτοι υπάλληλοι<br>6 ΙΠΑ x 157 000 EUR/έτος = 942 000 EUR | Όπως περιγράφεται στο σημείο 2.2.1:<br>– κατάρτιση του αιτήματος τυποποίησης και/ή κοινών προδιαγραφών μέσω εκτελεστικών πράξεων χωρίς επιτυχή διαδικασία τυποποίησης·<br>– κατάρτιση κατ' εξουσιοδότηση πράξης [εντός 12 μηνών από την έναρξη ισχύος του κανονισμού] για τον προσδιορισμό των ορισμών των κρίσιμων προϊόντων με ψηφιακά στοιχεία·<br>– πιθανή κατάρτιση κατ' εξουσιοδότηση πράξεων για την επικαιροποίηση του καταλόγου των κρίσιμων προϊόντων των κατηγοριών I και II· προσδιορισμός του αν απαιτείται περιορισμός ή αποκλεισμός για προϊόντα με ψηφιακά στοιχεία που καλύπτονται από άλλους ενωσιακούς κανόνες που καθορίζουν απαιτήσεις που επιτυγχάνουν το ίδιο επίπεδο προστασίας με τον |

[47] AC = Συμβασιούχος υπάλληλος· AL = Τοπικός υπάλληλος· END = Αποσπασμένος εθνικός εμπειρογνώμονας· INT = Προσωρινό προσωπικό· JPD = Νέος επαγγελματίας σε αντιπροσωπεία της ΕΕ.

[48] Επιμέρους ανώτατο όριο εξωτερικού προσωπικού που καλύπτεται από επιχειρησιακές πιστώσεις (πρώην γραμμές «ΒΑ»).

| | |
|---|---|
| | παρόντα κανονισμό· την επιβολή της πιστοποίησης ορισμένων εξαιρετικά κρίσιμων προϊόντων με ψηφιακά στοιχεία βάσει των κριτηρίων που καθορίζονται στον παρόντα κανονισμό· προσδιορισμός του ελάχιστου περιεχομένου της δήλωσης συμμόρφωσης ΕΕ και συμπλήρωση των στοιχείων που πρέπει να περιλαμβάνονται στον τεχνικό φάκελο·<br>– πιθανή κατάρτιση εκτελεστικών πράξεων σχετικά με τον μορφότυπο ή τα στοιχεία των υποχρεώσεων υποβολής εκθέσεων, τον κατάλογο υλικών λογισμικού, τις κοινές προδιαγραφές ή την τοποθέτηση της σήμανσης CE·<br>– ενδεχομένως προετοιμασία άμεσης παρέμβασης για την επιβολή διορθωτικών ή περιοριστικών μέτρων σε εξαιρετικές περιστάσεις για τη διατήρηση της εύρυθμης λειτουργίας της εσωτερικής αγοράς, συμπεριλαμβανομένης της κατάρτισης εκτελεστικής πράξης·<br>– οργάνωση και συντονισμός των κοινοποιήσεων από τα κράτη μέλη των κοινοποιημένων οργανισμών και συντονισμός των κοινοποιημένων οργανισμών·<br>– υποστήριξη του συντονισμού των αρχών εποπτείας της αγοράς των κρατών μελών. |
| Εξωτερικό προσωπικό<br>1 END x 88 000 EUR/έτος | Όπως περιγράφεται στο σημείο 2.2.1:<br>– κατάρτιση του αιτήματος τυποποίησης και/ή κοινών προδιαγραφών μέσω εκτελεστικών πράξεων χωρίς επιτυχή διαδικασία τυποποίησης·<br>– κατάρτιση κατ' εξουσιοδότηση πράξης [εντός 12 μηνών από την έναρξη ισχύος του κανονισμού] για τον προσδιορισμό των ορισμών των κρίσιμων προϊόντων με ψηφιακά στοιχεία·<br>– πιθανή κατάρτιση κατ' εξουσιοδότηση πράξεων για την επικαιροποίηση του καταλόγου των κρίσιμων προϊόντων των κατηγοριών I και II· προσδιορισμός του αν απαιτείται περιορισμός ή αποκλεισμός για προϊόντα με ψηφιακά στοιχεία που καλύπτονται από άλλους ενωσιακούς κανόνες που καθορίζουν απαιτήσεις που επιτυγχάνουν το ίδιο επίπεδο προστασίας με τον παρόντα κανονισμό· την επιβολή της πιστοποίησης ορισμένων εξαιρετικά κρίσιμων προϊόντων με ψηφιακά στοιχεία βάσει των κριτηρίων που καθορίζονται στον παρόντα κανονισμό· προσδιορισμός του ελάχιστου περιεχομένου της δήλωσης συμμόρφωσης ΕΕ και συμπλήρωση των στοιχείων που πρέπει να περιλαμβάνονται στον τεχνικό φάκελο·<br>– πιθανή κατάρτιση εκτελεστικών πράξεων σχετικά με τον μορφότυπο ή τα στοιχεία των υποχρεώσεων υποβολής εκθέσεων, τον κατάλογο υλικών λογισμικού, τις κοινές προδιαγραφές ή την τοποθέτηση της σήμανσης CE·<br>– ενδεχομένως προετοιμασία άμεσης παρέμβασης για την επιβολή διορθωτικών ή περιοριστικών μέτρων σε εξαιρετικές περιστάσεις για τη διατήρηση της εύρυθμης λειτουργίας της εσωτερικής αγοράς, συμπεριλαμβανομένης της κατάρτισης εκτελεστικής πράξης·<br>– οργάνωση και συντονισμός των κοινοποιήσεων από τα κράτη μέλη των κοινοποιημένων οργανισμών και συντονισμός των κοινοποιημένων οργανισμών·<br>– υποστήριξη του συντονισμού των αρχών εποπτείας της αγοράς των κρατών μελών. |

*3.2.4. Συμβατότητα με το ισχύον πολυετές δημοσιονομικό πλαίσιο*

Η πρόταση/πρωτοβουλία:

– x μπορεί να χρηματοδοτηθεί εξ ολοκλήρου με ανακατανομή εντός του οικείου τομέα του πολυετούς δημοσιονομικού πλαισίου (ΠΔΠ).

| |
|---|
| Δεν απαιτείται αναπρογραμματισμός. |

– ☐ συνεπάγεται τη χρησιμοποίηση του αδιάθετου περιθωρίου στο πλαίσιο του αντίστοιχου τομέα του ΠΔΠ και/ή τη χρήση ειδικών μηχανισμών, όπως ορίζεται στον κανονισμό για το ΠΔΠ.

| |
|---|
| — |

– ☐ συνεπάγεται την αναθεώρηση του ΠΔΠ.

| |
|---|
| — |

*3.2.5. Συμμετοχή τρίτων στη χρηματοδότηση*

Η πρόταση/πρωτοβουλία:

– x δεν προβλέπει συγχρηματοδότηση από τρίτους

– ☐ προβλέπει τη συγχρηματοδότηση από τρίτους που εκτιμάται παρακάτω:

Πιστώσεις σε εκατ. EUR (με τρία δεκαδικά ψηφία)

| | Έτος **N**[49] | Έτος **N+1** | Έτος **N+2** | Έτος **N+3** | Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) | | | Σύνολο |
|---|---|---|---|---|---|---|---|---|
| Προσδιορισμός του φορέα συγχρηματοδότησης | | | | | | | | |
| ΣΥΝΟΛΟ συγχρηματοδοτούμενων πιστώσεων | | | | | | | | |

[49] Το έτος Ν είναι το έτος έναρξης εφαρμογής της πρότασης/πρωτοβουλίας. Να αντικατασταθεί το «Ν» με το αναμενόμενο πρώτο έτος εφαρμογής (για παράδειγμα: 2021). Το ίδιο και για τα επόμενα έτη.

### 3.3. Εκτιμώμενες επιπτώσεις στα έσοδα

– ☐ Η πρόταση/πρωτοβουλία δεν έχει δημοσιονομικές επιπτώσεις στα έσοδα.

– ☐ Η πρόταση/πρωτοβουλία έχει τις δημοσιονομικές επιπτώσεις που περιγράφονται κατωτέρω:

  – ☐ στους ιδίους πόρους

  – ☐ στα λοιπά έσοδα

  – Να αναφερθεί αν τα έσοδα προορίζονται για γραμμές δαπανών ☐

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

| Γραμμή εσόδων του προϋπολογισμού: | Διαθέσιμες πιστώσεις για το τρέχον οικονομικό έτος | Επιπτώσεις της πρότασης/πρωτοβουλίας[50] | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Έτος **N** | Έτος **N+1** | Έτος **N+2** | Έτος **N+3** | Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) | | |
| Άρθρο ……. | | | | | | | | |

Ως προς τα έσοδα «για ειδικό προορισμό», να προσδιοριστούν οι γραμμές δαπανών του προϋπολογισμού που επηρεάζονται.

Άλλες παρατηρήσεις (π.χ. μέθοδος/τύπος για τον υπολογισμό των επιπτώσεων στα έσοδα ή τυχόν άλλες πληροφορίες).

[50] Όσον αφορά τους παραδοσιακούς ιδίους πόρους (δασμούς, εισφορές ζάχαρης), τα αναγραφόμενα ποσά πρέπει να είναι καθαρά ποσά, δηλ. τα ακαθάριστα ποσά μετά την αφαίρεση του 20 % για έξοδα είσπραξης.