ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ **ΤΟ ΣΥΜΒΟΥΛΙΟ**

Βρυξέλλες, 25 Σεπτεμβρίου 2024
(OR. en)

2022/0272 (COD) **PE-CONS 100/23**

CYBER 328
JAI 1731
DATAPROTECT 391
TELECOM 409
MI 1168
CSC 579
CSCI 215
CODEC 2601

ΝΟΜΟΘΕΤΙΚΕΣ ΚΑΙ ΑΛΛΕΣ ΠΡΑΞΕΙΣ

Θέμα:	ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 168/2013 και (ΕΕ) 2019/1020 και της οδηγίας (ΕΕ) 2020/1828 (κανονισμός για την κυβερνοανθεκτικότητα)

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2024/…
ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της …

σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 168/2013 και (ΕΕ) 2019/1020 και της οδηγίας (ΕΕ) 2020/1828 (κανονισμός για την κυβερνοανθεκτικότητα)

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

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

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

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

Αφού ζήτησαν τη γνώμη της Επιτροπής των Περιφερειών

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία[2],

---

1 ΕΕ C 100 της 16.3.2023, σ. 101.

2 Θέση του Ευρωπαϊκού Κοινοβουλίου της 12ης Μαρτίου 2024 (δεν έχει ακόμη δημοσιευτεί στην Επίσημη Εφημερίδα) και απόφαση του Συμβουλίου της ….

Εκτιμώντας τα ακόλουθα:

(1) Η κυβερνοασφάλεια είναι μία από τις βασικές προκλήσεις για την Ένωση. Ο αριθμός και η ποικιλία των συνδεδεμένων συσκευών θα αυξηθούν εκθετικά τα επόμενα έτη. Οι κυβερνοεπιθέσεις αποτελούν ζήτημα δημόσιου συμφέροντος, καθώς έχουν κρίσιμο αντίκτυπο όχι μόνο στην οικονομία της Ένωσης, αλλά και στη δημοκρατία καθώς και την ασφάλεια και την υγεία των καταναλωτών. Είναι επομένως αναγκαίο να ενισχυθεί η προσέγγιση της Ένωσης όσον αφορά την κυβερνοασφάλεια, να αντιμετωπιστεί σε επίπεδο Ένωσης το θέμα της κυβερνοανθεκτικότητας και 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 τις εκτεταμένες ευπάθειες 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 καθορισμό των οριακών συνθηκών για την ανάπτυξη ασφαλών προϊόντων με ψηφιακά στοιχεία διασφαλίζοντας ότι στην αγορά τίθενται σε κυκλοφορία προϊόντα υλισμικού και λογισμικού με λιγότερες ευπάθειες 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, για παράδειγμα με τη βελτίωση της διαφάνειας όσον αφορά την περίοδο υποστήριξης για προϊόντα με ψηφιακά στοιχεία που διατίθενται στην αγορά.

(3) Το ισχύον σχετικό ενωσιακό δίκαιο περιλαμβάνει διάφορα σύνολα οριζόντιων κανόνων που καλύπτουν ορισμένες πτυχές που συνδέονται με την κυβερνοασφάλεια από διαφορετικές οπτικές γωνίες, συμπεριλαμβανομένων μέτρων για τη βελτίωση της ασφάλειας της ψηφιακής αλυσίδας εφοδιασμού. Ωστόσο, το υφιστάμενο ενωσιακό δίκαιο σχετικά με την κυβερνοασφάλεια, συμπεριλαμβανομένων του κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[3] και της οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[4], δεν καλύπτει άμεσα τις υποχρεωτικές απαιτήσεις για την ασφάλεια των προϊόντων με ψηφιακά στοιχεία.

---

[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] Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) (ΕΕ L 333 της 27.12.2022, σ. 80).

(4) Ενώ το υφιστάμενο ενωσιακό δίκαιο 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 επιχειρήσεις και τους οργανισμούς όσον αφορά τη συμμόρφωσή τους με σειρά απαιτήσεων και υποχρεώσεων για παρόμοιους τύπους προϊόντων. Η κυβερνοασφάλεια των εν λόγω προϊόντων έχει ιδιαίτερα ισχυρή διασυνοριακή διάσταση, καθώς τα προϊόντα με ψηφιακά στοιχεία που κατασκευάζονται σε ένα κράτος μέλος ή τρίτη 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, ώστε να διασφαλιστεί εναρμονισμένο κανονιστικό πλαίσιο και ασφάλεια δικαίου για τους χρήστες, τους οργανισμούς και τις επιχειρήσεις, συμπεριλαμβανομένων των πολύ μικρών και των μικρών και μεσαίων επιχειρήσεων, όπως ορίζονται στο παράρτημα της σύστασης 2003/361/ΕΚ της Επιτροπής[5]. Το κανονιστικό τοπίο της Ένωσης θα πρέπει να εναρμονιστεί, με τη θέσπιση οριζόντιων απαιτήσεων κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία. Επιπλέον, θα πρέπει να διασφαλιστεί σε ολόκληρη την Ένωση η ασφάλεια δικαίου για τους οικονομικούς φορείς και τους χρήστες, καθώς και η καλύτερη εναρμόνιση της εσωτερικής αγοράς και η αναλογικότητα για τις πολύ μικρές και τις μικρές και μεσαίες επιχειρήσεις, ώστε να δημιουργηθούν πιο βιώσιμες συνθήκες για τους οικονομικούς φορείς που επιδιώκουν να εισέλθουν στην εν λόγω αγορά.

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

(5) Όσον αφορά τις πολύ μικρές και τις μικρές και μεσαίες επιχειρήσεις, κατά τον καθορισμό της κατηγορίας στην οποία εμπίπτει μια επιχείρηση, οι διατάξεις του παραρτήματος της σύστασης 2003/361/ΕΚ της Επιτροπής θα πρέπει να εφαρμόζονται στο σύνολό τους. Κατά συνέπεια, κατά τον υπολογισμό του αριθμού των απασχολουμένων και των οικονομικών ανώτατων ορίων βάσει των οποίων καθορίζονται οι κατηγορίες επιχειρήσεων, θα πρέπει επίσης να εφαρμόζονται οι διατάξεις του άρθρου 6 του παραρτήματος της σύστασης 2003/361/ΕΚ της Επιτροπής για τον καθορισμό των δεδομένων μιας επιχείρησης λαμβανομένων υπόψη συγκεκριμένων τύπων επιχειρήσεων, όπως οι συνεργαζόμενες επιχειρήσεις ή οι συνδεδεμένες επιχειρήσεις.

(6) Η Επιτροπή θα πρέπει να παρέχει καθοδήγηση προκειμένου να βοηθήσει τους οικονομικούς φορείς, ιδίως τις πολύ μικρές και τις μικρές και μεσαίες επιχειρήσεις, στην εφαρμογή του παρόντος κανονισμού. Η εν λόγω καθοδήγηση θα πρέπει να καλύπτει, μεταξύ άλλων, το πεδίο εφαρμογής του παρόντος κανονισμού, ιδίως σε σχέση με την εξ αποστάσεως επεξεργασία δεδομένων και τις συνέπειές της για τους φορείς ανάπτυξης ελεύθερου λογισμικού ανοικτού κώδικα, την εφαρμογή των κριτηρίων που χρησιμοποιούνται για τον καθορισμό των περιόδων υποστήριξης για προϊόντα με ψηφιακά στοιχεία, την αλληλεπίδραση μεταξύ του παρόντος κανονισμού και άλλων νομοθετικών πράξεων της Ένωσης και την έννοια της ουσιαστικής τροποποίησης.

(7) Σε επίπεδο Ένωσης, στο πλαίσιο διαφόρων προγραμματικών και πολιτικών εγγράφων, όπως η κοινή ανακοίνωση της Επιτροπής και του Ύπατου Εκπροσώπου της Ένωσης για Θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας, της 16ης Δεκεμβρίου 2020, με τίτλο «Η στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία», τα συμπεράσματα του Συμβουλίου της 2ας Δεκεμβρίου 2020 σχετικά με την κυβερνοασφάλεια των συνδεδεμένων συσκευών και της 23ης Μαΐου 2022 σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο και το ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 10ης Ιουνίου 2021 σχετικά με τη στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία[6], έχει ζητηθεί η θέσπιση ειδικών ενωσιακών απαιτήσεων κυβερνοασφάλειας για ψηφιακά ή συνδεδεμένα προϊόντα, ενώ αρκετές τρίτες χώρες θεσπίζουν μέτρα για την αντιμετώπιση του ζητήματος αυτού με δική τους πρωτοβουλία. Στην τελική έκθεση της Διάσκεψης για το μέλλον της Ευρώπης, οι πολίτες ζήτησαν «ενίσχυση του ρόλου της ΕΕ στην αντιμετώπιση των κυβερνοαπειλών». Προκειμένου η Ένωση να διαδραματίσει ηγετικό διεθνή ρόλο στον τομέα της κυβερνοασφάλειας, είναι σημαντικό να θεσπιστεί ένα φιλόδοξο κανονιστικό πλαίσιο.

(8) Για να αυξηθεί το συνολικό επίπεδο κυβερνοασφάλειας όλων των προϊόντων με ψηφιακά στοιχεία που διατίθενται στην εσωτερική αγορά, είναι αναγκαίο να θεσπιστούν προσανατολισμένες σε στόχους και τεχνολογικά ουδέτερες ουσιώδεις απαιτήσεις κυβερνοασφάλειας για τα εν λόγω προϊόντα, οι οποίες θα εφαρμόζονται οριζόντια.

[6] ΕΕ C 67 της 8.2.2022, σ. 81.

(9) 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. Κατά συνέπεια, οι κατασκευαστές θα πρέπει να διασφαλίζουν ότι όλα τα προϊόντα με ψηφιακά στοιχεία σχεδιάζονται και αναπτύσσονται σύμφωνα με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό. Η εν λόγω υποχρέωση αφορά τόσο προϊόντα που μπορούν να συνδεθούν φυσικά 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 κυβερνοαπειλές μπορούν να διαδοθούν μέσω διαφόρων προϊόντων με ψηφιακά στοιχεία πριν από την επίτευξη συγκεκριμένου στόχου, για παράδειγμα με την αλυσιδωτή προσέγγιση εκμετάλλευσης πολλαπλών ευπαθειών, οι κατασκευαστές θα πρέπει επίσης να διασφαλίζουν την κυβερνοασφάλεια των προϊόντων με ψηφιακά στοιχεία που συνδέονται μόνο έμμεσα με άλλες συσκευές ή δίκτυα.

(10) Με τον καθορισμό απαιτήσεων κυβερνοασφάλειας για τη θέση σε κυκλοφορία στην αγορά προϊόντων με ψηφιακά στοιχεία, επιδιώκεται η ενίσχυση της κυβερνοασφάλειας των εν λόγω προϊόντων τόσο για τους καταναλωτές όσο και για τις επιχειρήσεις. Με τις εν λόγω απαιτήσεις θα διασφαλίζεται επίσης η συνεκτίμηση της κυβερνοασφάλειας στο σύνολο των αλυσίδων εφοδιασμού, ώστε να καταστούν ασφαλέστερα τα τελικά προϊόντα με ψηφιακά στοιχεία και τα δομοστοιχεία τους. Μεταξύ αυτών περιλαμβάνονται επίσης απαιτήσεις για τη θέση σε κυκλοφορία στην αγορά καταναλωτικών προϊόντων με ψηφιακά στοιχεία που προορίζονται για ευάλωτους καταναλωτές, όπως παιχνίδια και συστήματα ενδοεπικοινωνίας για βρέφη. Τα καταναλωτικά προϊόντα με ψηφιακά στοιχεία που κατηγοριοποιούνται στον παρόντα κανονισμό ως σημαντικά προϊόντα με ψηφιακά στοιχεία παρουσιάζουν υψηλότερο κίνδυνο για την κυβερνοασφάλεια, καθώς επιτελούν λειτουργία που ενέχει σημαντικό κίνδυνο δυσμενών επιπτώσεων όσον αφορά την ένταση και την ικανότητά της να βλάψει την υγεία, την ασφάλεια ή την προστασία των χρηστών των εν λόγω προϊόντων, και θα πρέπει να υποβάλλονται σε αυστηρότερη διαδικασία αξιολόγησης της συμμόρφωσης. Αυτό ισχύει για προϊόντα όπως έξυπνα οικιακά προϊόντα με λειτουργίες ασφαλείας, συμπεριλαμβανομένων έξυπνων κλειδαριών θυρών, συστημάτων ενδοεπικοινωνίας για βρέφη και συστημάτων συναγερμού, συνδεδεμένων παιχνιδιών και ατομικών φορετών συσκευών υγείας. Επιπλέον, οι αυστηρότερες διαδικασίες αξιολόγησης της συμμόρφωσης στις οποίες πρέπει να υποβάλλονται άλλα προϊόντα με ψηφιακά στοιχεία που έχουν κατηγοριοποιηθεί στον παρόντα κανονισμό ως σημαντικά ή κρίσιμα προϊόντα με ψηφιακά στοιχεία, θα συμβάλουν στην πρόληψη δυνητικών αρνητικών επιπτώσεων στους καταναλωτές από την εκμετάλλευση των ευπαθειών.

(11) Με τον παρόντα κανονισμό επιδιώκεται η διασφάλιση υψηλού επιπέδου κυβερνοασφάλειας των προϊόντων με ψηφιακά στοιχεία και των ενσωματωμένων λύσεών τους για την εξ αποστάσεως επεξεργασία δεδομένων. Οι εν λόγω λύσεις εξ αποστάσεως επεξεργασίας δεδομένων θα πρέπει να ορίζονται ως η εξ αποστάσεως επεξεργασία δεδομένων για την οποία το λογισμικό σχεδιάζεται και αναπτύσσεται από τον κατασκευαστή ή για λογαριασμό του κατασκευαστή του οικείου προϊόντος με ψηφιακά στοιχεία, και η απουσία της οποίας θα εμπόδιζε το προϊόν με ψηφιακά στοιχεία να εκτελέσει μία από τις λειτουργίες του. Με την προσέγγιση αυτή διασφαλίζεται ότι τα εν λόγω προϊόντα προστατεύονται επαρκώς στο σύνολό τους από τους κατασκευαστές τους, ανεξάρτητα από το αν τα δεδομένα υποβάλλονται σε επεξεργασία ή αποθηκεύονται τοπικά στη συσκευή του χρήστη ή εξ αποστάσεως από τον κατασκευαστή. Ταυτόχρονα, η εξ αποστάσεως επεξεργασία ή αποθήκευση εμπίπτει στο πεδίο εφαρμογής του παρόντος κανονισμού μόνο στον βαθμό που αυτή είναι αναγκαία για την εκτέλεση των λειτουργιών ενός προϊόντος με ψηφιακά στοιχεία. Η εν λόγω εξ αποστάσεως επεξεργασία ή αποθήκευση περιλαμβάνει την περίπτωση κατά την οποία μια εφαρμογή για φορητές συσκευές απαιτεί πρόσβαση σε διεπαφή προγραμματισμού εφαρμογών ή σε βάση δεδομένων που παρέχεται μέσω υπηρεσίας που έχει αναπτύξει ο κατασκευαστής. Στην περίπτωση αυτή, η υπηρεσία εμπίπτει στο πεδίο εφαρμογής του παρόντος κανονισμού ως λύση εξ αποστάσεως επεξεργασίας δεδομένων. Κατά συνέπεια, οι απαιτήσεις σχετικά με τις λύσεις εξ αποστάσεως επεξεργασίας δεδομένων που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού δεν συνεπάγονται τεχνικά, επιχειρησιακά ή οργανωτικά μέτρα που αποσκοπούν στη διαχείριση των κινδύνων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών του κατασκευαστή στο σύνολό τους.

(12) Οι λύσεις υπολογιστικού νέφους αποτελούν λύσεις εξ αποστάσεως επεξεργασίας δεδομένων κατά την έννοια του παρόντος κανονισμού μόνον εφόσον πληρούν τον ορισμό που προβλέπεται στον παρόντα κανονισμό. Για παράδειγμα, οι λειτουργίες με δυνατότητα υπολογιστικού νέφους που παρέχονται από κατασκευαστή έξυπνων οικιακών συσκευών και οι οποίες επιτρέπουν στους χρήστες να ελέγχουν τη συσκευή εξ αποστάσεως, εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού. Από την άλλη πλευρά, οι ιστότοποι που δεν υποστηρίζουν τη λειτουργικότητα προϊόντος με ψηφιακά στοιχεία ή οι υπηρεσίες υπολογιστικού νέφους που σχεδιάζονται και αναπτύσσονται εκτός της ευθύνης του κατασκευαστή προϊόντος με ψηφιακά στοιχεία, δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού. Η οδηγία (ΕΕ) 2022/2555 εφαρμόζεται στις υπηρεσίες υπολογιστικού νέφους και στα μοντέλα υπηρεσιών υπολογιστικού νέφους, όπως το λογισμικό ως υπηρεσία (SaaS), η πλατφόρμα ως υπηρεσία (PaaS) ή η υποδομή ως υπηρεσία (IaaS). Οι οντότητες που παρέχουν υπηρεσίες υπολογιστικού νέφους στην Ένωση και οι οποίες χαρακτηρίζονται ως μεσαίες επιχειρήσεις σύμφωνα με το άρθρο 2 του παραρτήματος της σύστασης 2003/361/ΕΚ της Επιτροπής, ή υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις που προβλέπονται στην παράγραφο 1 του εν λόγω άρθρου, εμπίπτουν στο πεδίο εφαρμογής της εν λόγω οδηγίας.

(13) Σύμφωνα με τον στόχο του παρόντος κανονισμού να αρθούν τα εμπόδια για την ελεύθερη κυκλοφορία προϊόντων με ψηφιακά στοιχεία, τα κράτη μέλη δεν θα πρέπει εμποδίζουν, όσον αφορά τα ζητήματα που καλύπτονται από τον παρόντα κανονισμό, τη διάθεση στην αγορά προϊόντων με ψηφιακά στοιχεία που συμμορφώνονται με τον παρόντα κανονισμό. Κατά συνέπεια, σε σχέση με τα ζητήματα που αποτελούν αντικείμενο εναρμόνισης στο πλαίσιο του παρόντος κανονισμού, τα κράτη μέλη δεν μπορούν να επιβάλλουν πρόσθετες απαιτήσεις κυβερνοασφάλειας για τη διάθεση στην αγορά προϊόντων με ψηφιακά στοιχεία. Κάθε οντότητα, είτε δημόσια είτε ιδιωτική, μπορεί, ωστόσο, να θεσπίζει πρόσθετες απαιτήσεις πέραν εκείνων που ορίζονται στον παρόντα κανονισμό για την προμήθεια ή τη χρήση προϊόντων με ψηφιακά στοιχεία για τους συγκεκριμένους σκοπούς της και, επομένως, μπορεί να επιλέγει να χρησιμοποιεί προϊόντα με ψηφιακά στοιχεία που πληρούν αυστηρότερες ή πιο συγκεκριμένες απαιτήσεις κυβερνοασφάλειας από εκείνες που ισχύουν για τη διάθεση στην αγορά δυνάμει του παρόντος κανονισμού. Με την επιφύλαξη των οδηγιών 2014/24/ΕΕ[7] και 2014/25/ΕΕ[8] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, κατά την προμήθεια προϊόντων με ψηφιακά στοιχεία, τα οποία πρέπει να συμμορφώνονται με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό, συμπεριλαμβανομένων εκείνων που αφορούν τον χειρισμό ευπαθειών, τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι οι εν λόγω απαιτήσεις λαμβάνονται υπόψη κατά τη διαδικασία προμήθειας και ότι λαμβάνεται επίσης υπόψη η ικανότητα των κατασκευαστών να εφαρμόζουν μέτρα κυβερνοασφάλειας και να διαχειρίζονται κυβερνοαπειλές με αποτελεσματικό τρόπο.

---

7 Οδηγία 2014/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Φεβρουαρίου 2014, σχετικά με τις διαδικασίες σύναψης δημοσίων συμβάσεων και την κατάργηση της οδηγίας 2004/18/ΕΚ (ΕΕ L 94 της 28.3.2014, σ. 65).

8 Οδηγία 2014/25/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Φεβρουαρίου 2014, σχετικά με τις προμήθειες φορέων που δραστηριοποιούνται στους τομείς του ύδατος, της ενέργειας, των μεταφορών και των ταχυδρομικών υπηρεσιών και την κατάργηση της οδηγίας 2004/17/ΕΚ (ΕΕ L 94 της 28.3.2014, σ. 243).

Επιπλέον, με την οδηγία (ΕΕ) 2022/2555 καθορίζονται μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας για τις βασικές και σημαντικές οντότητες όπως αναφέρονται στο άρθρο 3 της εν λόγω οδηγίας, τα οποία θα μπορούσαν να περιλαμβάνουν μέτρα ασφάλειας της αλυσίδας εφοδιασμού που απαιτούν τη χρήση από τις εν λόγω οντότητες προϊόντων με ψηφιακά στοιχεία που πληρούν αυστηρότερες απαιτήσεις κυβερνοασφάλειας από εκείνες που ορίζονται στον παρόντα κανονισμό. Κατά συνέπεια, σύμφωνα με την οδηγία (ΕΕ) 2022/2555 και σύμφωνα με την αρχή της ελάχιστης εναρμόνισης, τα κράτη μέλη μπορούν να επιβάλλουν πρόσθετες απαιτήσεις κυβερνοασφάλειας για τη χρήση προϊόντων ΤΠΕ από βασικές ή σημαντικές οντότητες δυνάμει της εν λόγω οδηγίας, προκειμένου να διασφαλιστεί υψηλότερο επίπεδο κυβερνοασφάλειας, υπό την προϋπόθεση ότι οι εν λόγω απαιτήσεις συνάδουν με τις υποχρεώσεις των κρατών μελών που ορίζονται στο ενωσιακό δίκαιο. Τα θέματα που δεν καλύπτονται από τον παρόντα κανονισμό μπορούν να περιλαμβάνουν μη τεχνικούς παράγοντες που σχετίζονται με προϊόντα με ψηφιακά στοιχεία και τους κατασκευαστές τους. Επομένως, τα κράτη μέλη μπορούν να θεσπίζουν εθνικά μέτρα, συμπεριλαμβανομένων περιορισμών για τα προϊόντα με ψηφιακά στοιχεία ή τους προμηθευτές των εν λόγω προϊόντων, που λαμβάνουν υπόψη μη τεχνικούς παράγοντες. Τα εθνικά μέτρα που αφορούν τέτοιους παράγοντες οφείλουν να συμμορφώνονται με το ενωσιακό δίκαιο.

(14) Ο παρών κανονισμός δεν θα πρέπει να θίγει την ευθύνη των κρατών μελών να διαφυλάσσουν την εθνική ασφάλεια, σύμφωνα με το ενωσιακό δίκαιο. Τα κράτη μέλη θα πρέπει να μπορούν να θεσπίζουν πρόσθετα μέτρα για προϊόντα με ψηφιακά στοιχεία που αγοράζονται ή χρησιμοποιούνται για σκοπούς εθνικής ασφάλειας ή άμυνας, υπό την προϋπόθεση ότι τα εν λόγω μέτρα συνάδουν με τις υποχρεώσεις των κρατών μελών που ορίζονται στο ενωσιακό δίκαιο.

(15) Ο παρών κανονισμός εφαρμόζεται στους οικονομικούς φορείς μόνο σε σχέση με προϊόντα με ψηφιακά στοιχεία που διατίθενται στην αγορά και, ως εκ τούτου, παρέχονται για διανομή ή χρήση στην αγορά της Ένωσης στο πλαίσιο εμπορικής δραστηριότητας. Η προσφορά στο πλαίσιο εμπορικής δραστηριότητας θα μπορούσε να χαρακτηρίζεται όχι μόνο από τη χρέωση για ένα προϊόν με ψηφιακά στοιχεία, αλλά και από τη χρέωση για υπηρεσίες τεχνικής υποστήριξης, όταν αυτή δεν εξυπηρετεί μόνο την κάλυψη του πραγματικού κόστους, από την πρόθεση αποκόμισης οικονομικού οφέλους, για παράδειγμα με την παροχή πλατφόρμας λογισμικού μέσω της οποίας ο κατασκευαστής παρέχει άλλες υπηρεσίες έναντι οικονομικού οφέλους, από την απαίτηση, ως προϋπόθεση για τη χρήση, να επιτρέπεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα για λόγους άλλους από την αποκλειστική βελτίωση της ασφάλειας, της συμβατότητας ή της διαλειτουργικότητας του λογισμικού, ή από την αποδοχή δωρεών που υπερβαίνουν το κόστος που συνδέεται με τον σχεδιασμό, την ανάπτυξη και την παροχή προϊόντος με ψηφιακά στοιχεία. Η αποδοχή δωρεών χωρίς πρόθεση αποκόμισης κέρδους δεν θα πρέπει να θεωρείται εμπορική δραστηριότητα.

(16) Τα προϊόντα με ψηφιακά στοιχεία που παρέχονται στο πλαίσιο της παροχής υπηρεσίας για την οποία χρεώνεται τέλος αποκλειστικά για την ανάκτηση των πραγματικών δαπανών που σχετίζονται άμεσα με τη λειτουργία της εν λόγω υπηρεσίας, όπως μπορεί να συμβαίνει με ορισμένα προϊόντα με ψηφιακά στοιχεία που παρέχονται από φορείς της δημόσιας διοίκησης, δεν θα πρέπει να θεωρούνται, για τον λόγο αυτόν και μόνο, εμπορική δραστηριότητα για τους σκοπούς του παρόντος κανονισμού. Επιπλέον, τα προϊόντα με ψηφιακά στοιχεία που αναπτύσσονται ή τροποποιούνται από φορέα δημόσιας διοίκησης αποκλειστικά για δική του χρήση δεν θα πρέπει να θεωρείται ότι διατίθενται στην αγορά κατά την έννοια του παρόντος κανονισμού.

(17) Το λογισμικό και τα δεδομένα που κοινοποιούνται ανοιχτά και τα οποία οι χρήστες μπορούν ελεύθερα να ανακτούν, να χρησιμοποιούν, να τροποποιούν και να αναδιανέμουν αυτούσια ή σε τροποποιημένες εκδοχές, μπορούν να συμβάλλουν στην έρευνα και την καινοτομία στην αγορά. Για την προώθηση της ανάπτυξης και εγκατάστασης ελεύθερου λογισμικού ανοικτού κώδικα, ιδίως από πολύ μικρές επιχειρήσεις και μικρές και μεσαίες επιχειρήσεις, συμπεριλαμβανομένων νεοφυών επιχειρήσεων, ιδιωτών, μη κερδοσκοπικών οργανισμών και οργανισμών πανεπιστημιακής έρευνας, κατά την εφαρμογή του παρόντος κανονισμού σε προϊόντα με ψηφιακά στοιχεία που κατατάσσονται στο ελεύθερο λογισμικό ανοικτού κώδικα που παρέχεται προς διανομή ή χρήση στο πλαίσιο εμπορικής δραστηριότητας θα πρέπει να λαμβάνεται υπόψη η φύση των διαφόρων μοντέλων ανάπτυξης λογισμικού που διανέμεται και αναπτύσσεται βάσει αδειών ελεύθερου λογισμικού ανοικτού κώδικα.

(18) Ως ελεύθερο λογισμικό και λογισμικό ανοικτού κώδικα νοείται το λογισμικό του οποίου ο πηγαίος κώδικας διανέμεται ανοικτά και του οποίου η αδειοδότηση περιλαμβάνει όλα τα δικαιώματα που καθιστούν το λογισμικό ελεύθερα προσβάσιμο, χρησιμοποιήσιμο, τροποποιήσιμο και αναδιανεμητέο. Το ελεύθερο λογισμικό ανοικτού κώδικα αναπτύσσεται, συντηρείται και διανέμεται ανοιχτά, μεταξύ άλλων μέσω επιγραμμικών πλατφορμών. Όσον αφορά τους οικονομικούς φορείς που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού, μόνο το ελεύθερο λογισμικό ανοικτού κώδικα που διατίθεται στην αγορά και, συνεπώς, παρέχεται για διανομή ή χρήση στο πλαίσιο εμπορικής δραστηριότητας, θα πρέπει να εμπίπτει στο πεδίο εφαρμογής του παρόντος κανονισμού. Από μόνες τους οι συνθήκες υπό τις οποίες αναπτύχθηκε το προϊόν με ψηφιακά στοιχεία ή ο τρόπος με τον οποίο έχει χρηματοδοτηθεί η ανάπτυξη δεν θα πρέπει επομένως να λαμβάνονται υπόψη κατά τον προσδιορισμό του εμπορικού ή μη εμπορικού χαρακτήρα της εν λόγω δραστηριότητας. Ειδικότερα, για τους σκοπούς του παρόντος κανονισμού και σε σχέση με τους οικονομικούς φορείς που εμπίπτουν στο πεδίο εφαρμογής του, προκειμένου να διασφαλιστεί ότι υπάρχει σαφής διάκριση μεταξύ των φάσεων ανάπτυξης και παροχής, η διάθεση προϊόντων με ψηφιακά στοιχεία κατατασσόμενων στο ελεύθερο λογισμικό ανοικτού κώδικα τα οποία οι κατασκευαστές τους δεν διαθέτουν έναντι οικονομικού οφέλους δεν θα πρέπει να θεωρείται εμπορική δραστηριότητα. Επιπλέον, η προσφορά προϊόντων με ψηφιακά στοιχεία που αποτελούν δομοστοιχεία ελεύθερου λογισμικού ανοικτού κώδικα προοριζόμενα για ενσωμάτωση από άλλους κατασκευαστές στα δικά τους προϊόντα με ψηφιακά στοιχεία θα πρέπει να θεωρείται διάθεση στην αγορά μόνο εάν το δομοστοιχείο διατίθεται έναντι οικονομικού οφέλους από τον αρχικό κατασκευαστή του. Για παράδειγμα, το γεγονός ότι ένα προϊόν λογισμικού ανοικτού κώδικα με ψηφιακά στοιχεία λαμβάνει χρηματοδοτική υποστήριξη από τους κατασκευαστές ή ότι οι κατασκευαστές συνεισφέρουν στην ανάπτυξη ενός τέτοιου προϊόντος δεν θα πρέπει από μόνο του να καθορίζει ότι η δραστηριότητα έχει εμπορικό χαρακτήρα.

Επιπλέον, η ύπαρξη τακτικών εκδόσεων δεν θα πρέπει από μόνη της να οδηγεί στο συμπέρασμα ότι ένα προϊόν με ψηφιακά στοιχεία παρέχεται στο πλαίσιο εμπορικής δραστηριότητας. Τέλος, για τους σκοπούς του παρόντος κανονισμού, η ανάπτυξη από μη κερδοσκοπικούς οργανισμούς, προϊόντων με ψηφιακά στοιχεία κατατασσόμενα στο ελεύθερο λογισμικό ανοικτού κώδικα δεν θα πρέπει να θεωρείται εμπορική δραστηριότητα, υπό την προϋπόθεση ότι ο οργανισμός έχει συσταθεί κατά τρόπο που διασφαλίζει ότι όλα τα έσοδα μετά την κάλυψη του κόστους χρησιμοποιούνται για την επίτευξη μη κερδοσκοπικών στόχων. Ο παρών κανονισμός δεν εφαρμόζεται σε φυσικά ή νομικά πρόσωπα που συνεισφέρουν με πηγαίο κώδικα σε προϊόντα με ψηφιακά στοιχεία κατατασσόμενα στο ελεύθερο λογισμικό ανοικτού κώδικα τα οποία δεν τελούν υπό την ευθύνη τους.

(19) Λαμβανομένης υπόψη της σημασίας που έχουν για την κυβερνοασφάλεια πολλά προϊόντα με ψηφιακά στοιχεία κατατασσόμενα στο ελεύθερο λογισμικό ανοικτού κώδικα τα οποία δημοσιεύονται αλλά δεν διατίθενται στην αγορά κατά την έννοια του παρόντος κανονισμού, τα νομικά πρόσωπα που παρέχουν στήριξη σε διαρκή βάση για την ανάπτυξη τέτοιων προϊόντων προοριζόμενων για εμπορικές δραστηριότητες και διαδραματίζουν βασικό ρόλο στη διασφάλιση της βιωσιμότητας των εν λόγω προϊόντων (υποστηρικτές λογισμικού ανοικτού κώδικα), θα πρέπει να υπόκεινται σε χαλαρό και εξατομικευμένο ρυθμιστικό καθεστώς. Στους υποστηρικτές λογισμικού ανοικτού κώδικα περιλαμβάνονται ορισμένα ιδρύματα, καθώς και οντότητες που αναπτύσσουν και δημοσιεύουν ελεύθερο λογισμικό ανοικτού κώδικα σε επιχειρηματικό πλαίσιο, συμπεριλαμβανομένων μη κερδοσκοπικών οντοτήτων. Το ρυθμιστικό καθεστώς θα πρέπει να λαμβάνει υπόψη τον ειδικό χαρακτήρα τους και τη συμβατότητά τους με το είδος των επιβαλλόμενων υποχρεώσεων. Θα πρέπει να καλύπτει μόνο προϊόντα με ψηφιακά στοιχεία κατατασσόμενα στο ελεύθερο λογισμικό ανοικτού κώδικα τα οποία έχουν ως τελικό προορισμό εμπορικές δραστηριότητες, όπως ενσωμάτωση σε εμπορικές υπηρεσίες ή σε προϊόντα με ψηφιακά στοιχεία παρεχόμενα έναντι οικονομικού οφέλους. Για τους σκοπούς του εν λόγω κανονιστικού καθεστώτος, η πρόθεση ενσωμάτωσης σε προϊόντα με ψηφιακά στοιχεία παρεχόμενα έναντι οικονομικού οφέλους περιλαμβάνει περιπτώσεις στις οποίες κατασκευαστές που ενσωματώνουν ένα δομοστοιχείο στα δικά τους προϊόντα με ψηφιακά στοιχεία είτε συμβάλλουν στην ανάπτυξη του δομοστοιχείου αυτού σε τακτική βάση είτε παρέχουν τακτική χρηματοδοτική ενίσχυση για τη διασφάλιση της συνέχειας ενός προϊόντος λογισμικού. Η παροχή διαρκούς υποστήριξης για την ανάπτυξη ενός προϊόντος με ψηφιακά στοιχεία περιλαμβάνει, μεταξύ άλλων, τη φιλοξενία και τη διαχείριση πλατφορμών συνεργασίας για την ανάπτυξη λογισμικού, τη φιλοξενία πηγαίου κώδικα ή λογισμικού, τη διακυβέρνηση ή τη διαχείριση προϊόντων με ψηφιακά στοιχεία κατατασσόμενων στο ελεύθερο λογισμικό ανοικτού κώδικα, καθώς και την καθοδήγηση της ανάπτυξης των εν λόγω προϊόντων. Δεδομένου ότι το χαλαρό και εξατομικευμένο κανονιστικό καθεστώς δεν επιβάλλει σε εκείνους που δρουν ως υποστηρικτές λογισμικού ανοικτού κώδικα τις ίδιες υποχρεώσεις με εκείνους που δρουν ως κατασκευαστές δυνάμει του παρόντος κανονισμού, δεν θα πρέπει να τους επιτρέπεται να τοποθετούν τη σήμανση CE στα προϊόντα με ψηφιακά στοιχεία των οποίων την ανάπτυξη υποστηρίζουν.

(20) Η πράξη της φιλοξενίας προϊόντων με ψηφιακά στοιχεία σε ελεύθερα αποθετήρια, μεταξύ άλλων μέσων συστημάτων διαχείρισης πακέτων λογισμικού ή πλατφορμών συνεργασίας, δεν συνιστά από μόνη της διάθεση στην αγορά προϊόντος με ψηφιακά στοιχεία. Οι πάροχοι τέτοιων υπηρεσιών θα πρέπει να θεωρούνται διανομείς μόνο αν διαθέτουν στην αγορά τέτοιου είδους λογισμικό και επομένως το παρέχουν για διανομή ή χρήση στην αγορά της Ένωσης στο πλαίσιο εμπορικής δραστηριότητας.

(21) Προκειμένου να υποστηριχθεί και να διευκολυνθεί η δέουσα επιμέλεια των κατασκευαστών που ενσωματώνουν στα προϊόντα τους με ψηφιακά στοιχεία ελεύθερο λογισμικό ανοικτού κώδικα μη υποκείμενο στις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό, η Επιτροπή θα πρέπει να είναι σε θέση να θεσπίζει εθελοντικά προγράμματα πιστοποίησης ασφάλειας, είτε με κατ' εξουσιοδότηση πράξη που συμπληρώνει τον παρόντα κανονισμό είτε ζητώντας ευρωπαϊκό καθεστώς πιστοποίησης της κυβερνοασφάλειας σύμφωνα με το άρθρο 48 του κανονισμού (ΕΕ) 2019/881, το οποίο λαμβάνει υπόψη τις ιδιαιτερότητες των μοντέλων ανάπτυξης ελεύθερου λογισμικού ανοικτού κώδικα. Τα προγράμματα πιστοποίησης ασφάλειας θα πρέπει να σχεδιάζονται κατά τρόπο ώστε η διαδικασία βεβαίωσης ασφάλειας να κινείται ή να χρηματοδοτείται όχι μόνο από φυσικά ή νομικά πρόσωπα που αναπτύσσουν προϊόντα με ψηφιακά στοιχεία κατατασσόμενα στο ελεύθερο λογισμικό ανοικτού κώδικα ή συμβάλλουν στην ανάπτυξή τέτοιων προϊόντων, αλλά και από τρίτα μέρη, όπως κατασκευαστές που ενσωματώνουν τα εν λόγω προϊόντα στα δικά τους προϊόντα με ψηφιακά στοιχεία, χρήστες ή ενωσιακές και εθνικές δημόσιες διοικήσεις.

(22) Λαμβανομένων υπόψη των στόχων του παρόντος κανονισμού για τη δημόσια ασφάλεια στον κυβερνοχώρο και προκειμένου να βελτιωθεί η επίγνωση της κατάστασης των κρατών μελών όσον αφορά την εξάρτηση της Ένωσης από δομοστοιχεία λογισμικού και ιδίως από δυνητικά δομοστοιχεία ελεύθερου λογισμικού ανοικτού κώδικα, μια ειδική ομάδα διοικητικής συνεργασίας (ΕΟΔΚ) που συγκροτείται με τον παρόντα κανονισμό θα πρέπει να είναι σε θέση να αποφασίσει να αναλάβει από κοινού εκτίμηση της εξάρτησης της Ένωσης. Οι αρχές εποπτείας της αγοράς θα πρέπει να είναι σε θέση να ζητούν από τους κατασκευαστές κατηγοριών προϊόντων με ψηφιακά στοιχεία που καθορίζονται από την ΕΟΔΚ να υποβάλλουν τους καταλόγους υλικών λογισμικού (ΚΥΛ) που έχουν δημιουργήσει σύμφωνα με τον παρόντα κανονισμό. Προκειμένου να προστατευθεί η εμπιστευτικότητα των ΚΥΛ, οι αρχές εποπτείας της αγοράς θα πρέπει να υποβάλλουν στην ΕΟΔΚ σχετικές πληροφορίες για τις εξαρτήσεις με ανωνυμοποιημένο και συγκεντρωτικό τρόπο.

(23) Η αποτελεσματικότητα της εφαρμογής του παρόντος κανονισμού θα εξαρτηθεί επίσης από τη διαθεσιμότητα επαρκών δεξιοτήτων κυβερνοασφάλειας. Σε επίπεδο Ένωσης, διάφορα προγραμματικά και πολιτικά έγγραφα, συμπεριλαμβανομένης της ανακοίνωσης της Επιτροπής, της 18 Απριλίου 2023, σχετικά με τη γεφύρωση του χάσματος ταλέντων στον τομέα της κυβερνοασφάλειας για την τόνωση της ανταγωνιστικότητας, της ανάπτυξης και της ανθεκτικότητας της ΕΕ και των συμπερασμάτων του Συμβουλίου, της 22 Μαΐου 2023, σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα αναγνώρισαν το χάσμα δεξιοτήτων κυβερνοασφάλειας στην Ένωση και την ανάγκη αντιμετώπισης των εν λόγω προκλήσεων κατά προτεραιότητα, τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Προκειμένου να διασφαλιστεί η αποτελεσματική εφαρμογή του παρόντος κανονισμού, τα κράτη μέλη θα πρέπει να εξασφαλίζουν ότι διατίθενται επαρκείς πόροι για την κατάλληλη στελέχωση των αρχών εποπτείας της αγοράς και των οργανισμών αξιολόγησης της συμμόρφωσης για την εκτέλεση των καθηκόντων τους όπως ορίζονται στον παρόντα κανονισμό. Τα μέτρα αυτά θα πρέπει να ενισχύσουν την κινητικότητα του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας και τις συναφείς σταδιοδρομίες τους. Θα πρέπει επίσης να συμβάλουν στο να καταστεί το εργατικό δυναμικό κυβερνοασφάλειας πιο ανθεκτικό και χωρίς αποκλεισμούς, μεταξύ άλλων όσον αφορά το φύλο. Συνεπώς, τα κράτη μέλη θα πρέπει να λάβουν μέτρα για να διασφαλίσουν ότι τα καθήκοντα αυτά εκτελούνται από επαρκώς καταρτισμένους επαγγελματίες, με τις απαιτούμενες δεξιότητες κυβερνοασφάλειας. Ομοίως, οι κατασκευαστές θα πρέπει να διασφαλίζουν ότι το προσωπικό τους διαθέτει τις απαιτούμενες δεξιότητες για τη συμμόρφωση με τις υποχρεώσεις τους όπως ορίζονται στον παρόντα κανονισμό. Τα κράτη μέλη και η Επιτροπή, σύμφωνα με τα προνόμια και τις αρμοδιότητές τους και τα ειδικά καθήκοντα που τους ανατίθενται με τον παρόντα κανονισμό, θα πρέπει να λαμβάνουν μέτρα για τη στήριξη των κατασκευαστών, και ιδίως των πολύ μικρών και των μικρών και μεσαίων επιχειρήσεων, συμπεριλαμβανομένων των νεοφυών επιχειρήσεων, και σε τομείς όπως η ανάπτυξη δεξιοτήτων, για τους σκοπούς της συμμόρφωσης με τις υποχρεώσεις τους όπως ορίζονται στον παρόντα κανονισμό. Επιπλέον, δεδομένου ότι η οδηγία (ΕΕ) 2022/2555 απαιτεί από τα κράτη μέλη να εγκρίνουν πολιτικές για την προώθηση και την ανάπτυξη της κατάρτισης σχετικά με την κυβερνοασφάλεια και τις δεξιότητες κυβερνοασφάλειας στο πλαίσιο των εθνικών στρατηγικών τους για την κυβερνοασφάλεια, τα κράτη μέλη μπορούν επίσης να εξετάσουν το ενδεχόμενο, κατά την έγκριση των εν λόγω στρατηγικών, να αντιμετωπίσουν τις ανάγκες σε δεξιότητες κυβερνοασφάλειας που απορρέουν από τον παρόντα κανονισμό, συμπεριλαμβανομένων εκείνων που σχετίζονται με την επανειδίκευση και την αναβάθμιση των δεξιοτήτων.

(24) Το ασφαλές διαδίκτυο είναι απαραίτητο για τη λειτουργία των υποδομών ζωτικής σημασίας και για την κοινωνία στο σύνολό της. Η οδηγία (ΕΕ) 2022/2555 αποσκοπεί στη διασφάλιση υψηλού επιπέδου κυβερνοασφάλειας των υπηρεσιών που παρέχονται από βασικές και σημαντικές οντότητες όπως αναφέρονται στο άρθρου 3 της εν λόγω οδηγίας, συμπεριλαμβανομένων των παρόχων ψηφιακών υποδομών που υποστηρίζουν βασικές λειτουργίες του ανοικτού διαδικτύου, διασφαλίζουν την πρόσβαση στο διαδίκτυο και παρέχουν 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 (ΕΕ) 2022/2555 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.

(25) Ο κανονισμός (ΕΕ) 2017/745 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[9] θεσπίζει κανόνες σχετικά με τα ιατροτεχνολογικά προϊόντα και ο κανονισμός (ΕΕ) 2017/746 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[10] θεσπίζει κανόνες σχετικά με τα in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα. Οι εν λόγω 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 εν λόγω απαιτήσεις 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 έχει θεσπιστεί ειδική καθοδήγηση σχετικά με την κυβερνοασφάλεια για τα ιατροτεχνολογικά προϊόντα, οι οποίες παρέχουν στους κατασκευαστές ιατροτεχνολογικών προϊόντων, συμπεριλαμβανομένων των in vitro διαγνωστικών ιατροτεχνολογικών προϊόντων, καθοδήγηση σχετικά με τον τρόπο εκπλήρωσης όλων των σχετικών ουσιωδών απαιτήσεων που ορίζονται στο παράρτημα Ι των εν λόγω κανονισμών όσον αφορά την κυβερνοασφάλεια. 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.

---

9 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).

10 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).

(26) Προϊόντα με ψηφιακά στοιχεία που αναπτύσσονται ή τροποποιούνται αποκλειστικά για σκοπούς εθνικής ασφάλειας ή άμυνας, ή προϊόντα ειδικά σχεδιασμένα για την επεξεργασία διαβαθμισμένων πληροφοριών δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού. Τα κράτη μέλη ενθαρρύνονται να διασφαλίζουν για τα εν λόγω προϊόντα το ίδιο ή υψηλότερο επίπεδο προστασίας όπως και για εκείνα που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού.

(27) Ο κανονισμός (ΕΕ) 2019/2144 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[11] 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 κινδύνους κυβερνοασφάλειας 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, ιδίως τον κανονισμό του ΟΗΕ αριθ. 155 – Ενιαίες διατάξεις σχετικά με την έγκριση οχημάτων όσον αφορά την κυβερνοασφάλεια και το σύστημα διαχείρισης της κυβερνοασφάλειας, και προβλέπει ειδικές διαδικασίες αξιολόγησης της συμμόρφωσης.

---

[11] 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).

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 και εξοπλισμού, συμπεριλαμβανομένου του λογισμικού, που περιλαμβάνει τις υποχρεώσεις προστασίας από απειλές κατά της ασφάλειας των πληροφοριών. Η διαδικασία πιστοποίησης βάσει του κανονισμού (ΕΕ) 2018/1139 διασφαλίζει το επίπεδο ασφάλειας που επιδιώκει ο παρών κανονισμός. 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 θα πρέπει να υπόκεινται στις ουσιώδεις απαιτήσεις κυβερονασφάλειας και τις διαδικασίες αξιολόγησης της συμμόρφωσης που καθορίζονται στον παρόντα κανονισμό.

---

[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).

(28) 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 κυβερνοασφάλειας που προβλέπονται 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 κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό 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 τουλάχιστον επίπεδο προστασίας με εκείνο που προβλέπεται στον παρόντα κανονισμό. Θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις για τη συμπλήρωση του παρόντος κανονισμού με τον προσδιορισμό των εν λόγω προϊόντων και κανόνων. Για το υφιστάμενο δίκαιο της Ένωσης όπου θα πρέπει να εφαρμόζονται τέτοιοι περιορισμοί ή εξαιρέσεις, ο παρών κανονισμός περιέχει ειδικές διατάξεις για την αποσαφήνιση της σχέσης του με το εν λόγω ενωσιακό δίκαιο.

(29) Προκειμένου να διασφαλιστεί ότι τα προϊόντα με ψηφιακά στοιχεία που διατίθενται στην αγορά μπορούν να επισκευάζονται αποτελεσματικά και ότι η ανθεκτικότητά τους παρατείνεται, θα πρέπει να προβλεφθεί εξαίρεση για τα ανταλλακτικά. Η συγκεκριμένη εξαίρεση θα πρέπει να καλύπτει τόσο ανταλλακτικά προοριζόμενα για την επισκευή παλαιών προϊόντων που έχουν καταστεί διαθέσιμα πριν από την ημερομηνία εφαρμογής του παρόντος κανονισμού όσο και ανταλλακτικά που έχουν ήδη υποβληθεί σε διαδικασία αξιολόγησης της συμμόρφωσης σύμφωνα με τον παρόντα κανονισμό.

(30) Ο κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2022/30 της Επιτροπής[13] διευκρινίζει ότι μερικές ουσιώδεις απαιτήσεις που ορίζονται στο άρθρο 3 παράγραφος 3 στοιχεία δ), ε) και στ) της οδηγίας 2014/53/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[14], που αφορά τη βλάβη δικτύου και την κατάχρηση των πόρων του δικτύου, τα δεδομένα προσωπικού χαρακτήρα και την ιδιωτικότητα, όπως επίσης την απάτη, εφαρμόζονται σε ορισμένα είδη ραδιοεξοπλισμού. Η εκτελεστική απόφαση C(2022)5637 της Επιτροπής, της 5ης Αυγούστου 2022, σχετικά με αίτημα τυποποίησης προς την Ευρωπαϊκή Επιτροπή Τυποποίησης και την Ευρωπαϊκή Επιτροπή Ηλεκτροτεχνικής Τυποποίησης καθορίζει απαιτήσεις για την ανάπτυξη ειδικών προτύπων, προσδιορίζοντας περαιτέρω τον τρόπο με τον οποίο θα πρέπει να εξεταστούν οι εν λόγω τρεις ουσιώδεις απαιτήσεις. Οι ουσιώδεις απαιτήσεις κυβερνοασφάλειας 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. Επιπλέον, οι ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στον παρόντα κανονισμό συνάδουν με τους στόχους των απαιτήσεων για συγκεκριμένα πρότυπα που περιλαμβάνονται στο εν λόγω αίτημα τυποποίησης. Ως εκ τούτου, όταν 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 κατά την κατάρτιση και την ανάπτυξη εναρμονισμένων προτύπων για τη διευκόλυνση της εφαρμογής του παρόντος κανονισμού. Κατά τη διάρκεια της μεταβατικής περιόδου για την εφαρμογή του παρόντος κανονισμού, η Επιτροπή θα πρέπει να παρέχει καθοδήγηση στους κατασκευαστές που υπάγονται στον παρόντα κανονισμό και υπάγονται επίσης στον κατ' εξουσιοδότηση κανονισμό (ΕΕ) 2022/30, ώστε να διευκολύνεται η απόδειξη της συμμόρφωσης με τους δύο κανονισμούς.

---

13 Κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2022/30 της Επιτροπής, της 29ης Οκτωβρίου 2021, για τη συμπλήρωση της οδηγίας 2014/53/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, όσον αφορά την εφαρμογή των ουσιωδών απαιτήσεων που αναφέρονται στο άρθρο 3 παράγραφος 3 στοιχεία δ), ε) κι στ) της εν λόγω οδηγίας (ΕΕ L 7 της 12.1.2022, σ. 6).

14 Οδηγία 2014/53/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Απριλίου 2014, σχετικά με την εναρμόνιση των νομοθεσιών των κρατών μελών σχετικά με τη διαθεσιμότητα ραδιοεξοπλισμού στην αγορά και την κατάργηση της οδηγίας 1999/5/ΕΚ (ΕΕ L 153 της 22.5.2014, σ. 62).

(31) Η οδηγία (ΕΕ) 2024/… του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[15+] 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 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 αφότου το προϊόν τεθεί σε κυκλοφορία 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.

---

15 Οδηγία (ΕΕ) 2024/… του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της …, για την ευθύνη λόγω ελαττωματικών προϊόντων και την κατάργηση της οδηγίας 85/374/ΕΟΚ του Συμβουλίου (ΕΕ L …).

\+ ΕΕ: να προστεθεί στο κείμενο ο αριθμός της οδηγίας που περιλαμβάνεται στο έγγραφο PE-CONS …/… (2022/0302(COD)) και να συμπληρωθούν ο αριθμός, η ημερομηνία και τα στοιχεία ΕΕ της εν λόγω οδηγίας στην υποσημείωση.

(32) Ο παρών κανονισμός δεν θα πρέπει να θίγει τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[16], μεταξύ άλλων τις διατάξεις που αφορούν 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 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. Προς το σκοπό αυτό, οι εθνικές αρχές εποπτείας της αγοράς που ορίζονται βάσει του παρόντος κανονισμού θα πρέπει να συνεργάζονται με τις αρχές που εποπτεύουν την εφαρμογή της νομοθεσίας της Ένωσης για την προστασία των δεδομένων. Οι τελευταίες θα πρέπει επίσης να έχουν πρόσβαση σε πληροφορίες σχετικές με την εκτέλεση των καθηκόντων τους.

---

16 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).

(33) Στον βαθμό που τα προϊόντα τους εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού, οι πάροχοι ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας, όπως αναφέρεται στο άρθρο 5α παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[17], θα πρέπει να συμμορφώνονται τόσο με τις οριζόντιες ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στον παρόντα κανονισμό όσο και με τις ειδικές απαιτήσεις ασφάλειας που καθορίζονται στο άρθρο 5α του κανονισμού (ΕΕ) αριθ. 910/2014. Προκειμένου να διευκολυνθεί η συμμόρφωση, οι πάροχοι πορτοφολιών θα πρέπει να είναι σε θέση να αποδεικνύουν τη συμμόρφωση των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας με τις απαιτήσεις που καθορίζονται αντίστοιχα στον παρόντα κανονισμό και στον κανονισμό (ΕΕ) αριθ. 910/2014, πιστοποιώντας τα προϊόντα τους στο πλαίσιο ευρωπαϊκού καθεστώτος πιστοποίησης της κυβερνοασφάλειας που θεσπίστηκε με τον κανονισμό (ΕΕ) 2019/881 και για τα οποία η Επιτροπή έχει καθορίσει μέσω εκτελεστικών πράξεων τεκμήριο συμμόρφωσης για τον παρόντα κανονισμό, στον βαθμό που το πιστοποιητικό ή μέρη αυτού καλύπτουν τις εν λόγω απαιτήσεις.

---

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

(34) Κατά την ενσωμάτωση δομοστοιχείων προερχόμενων από τρίτους σε προϊόντα με ψηφιακά στοιχεία κατά τη φάση σχεδιασμού και ανάπτυξης, οι κατασκευαστές θα πρέπει, προκειμένου να διασφαλιστεί ότι τα προϊόντα σχεδιάζονται, αναπτύσσονται και παράγονται σύμφωνα με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό, να επιδεικνύουν τη δέουσα επιμέλεια όσον αφορά τα εν λόγω δομοστοιχεία, συμπεριλαμβανομένων στοιχείων ελεύθερου λογισμικού ανοικτού κώδικα που δεν διατεθεί στην αγορά. Το κατάλληλο επίπεδο δέουσας επιμέλειας εξαρτάται από τη φύση και το επίπεδο κινδύνου κυβερνοασφάλειας για ένα δεδομένο δομοστοιχείο και θα πρέπει, για τον σκοπό αυτό, να λαμβάνει υπόψη μία ή περισσότερες από τις ακόλουθες ενέργειες: επαλήθευση, κατά περίπτωση, του ότι ο κατασκευαστής δομοστοιχείου έχει αποδείξει τη συμμόρφωσή του με τον παρόντα κανονισμό, μεταξύ άλλων ελέγχοντας αν το δομοστοιχείο φέρει ήδη το σήμα CE· επαλήθευση του ότι ένα δομοστοιχείο λαμβάνει τακτικές ενημερώσεις ασφαλείας, για παράδειγμα με την εξέταση του ιστορικού των ενημερώσεων ασφαλείας του· επαλήθευση του ότι ένα δομοστοιχείο είναι απαλλαγμένο από ευπάθειες καταχωρημένες στην ευρωπαϊκή βάση δεδομένων ευπαθειών που δημιουργήθηκε σύμφωνα με το άρθρο 12 παράγραφος 2 της οδηγίας (ΕΕ) 2022/2555 ή σε άλλες δημόσια προσβάσιμες βάσεις δεδομένων ευπαθειών· ή διενέργεια πρόσθετων δοκιμών ασφάλειας. Οι υποχρεώσεις χειρισμού ευπαθειών που ορίζονται στον παρόντα κανονισμό, με τις οποίες πρέπει να συμμορφώνονται οι κατασκευαστές όταν θέτουν σε κυκλοφορία στην αγορά προϊόν με ψηφιακά στοιχεία και για την περίοδο υποστήριξης, ισχύουν για τα προϊόντα με ψηφιακά στοιχεία στο σύνολό τους, συμπεριλαμβανομένων όλων των ενσωματωμένων δομοστοιχείων. Όταν, κατά την άσκηση της δέουσας επιμέλειας, ο κατασκευαστής του προϊόντος με ψηφιακά στοιχεία εντοπίζει ευπάθεια σε μια συνιστώσα, μεταξύ άλλων σε δομοστοιχείο, συμπεριλαμβανομένου δομοστοιχείου ελεύθερου κώδικα ανοιχτής πηγής, θα πρέπει να ενημερώνει το πρόσωπο ή την οντότητα που κατασκευάζει ή συντηρεί το δομοστοιχείο, να αντιμετωπίζει και να αίρει την ευπάθεια και, κατά περίπτωση, να παρέχει στο πρόσωπο ή την οντότητα την εφαρμοζόμενη διόρθωση ασφάλειας.

(35) Αμέσως μετά τη μεταβατική περίοδο για την εφαρμογή του παρόντος κανονισμού, κατασκευαστές προϊόντων με ψηφιακά στοιχεία που ενσωματώνουν ένα ή περισσότερα δομοστοιχεία προερχόμενα από τρίτα μέρη τα οποία επίσης υπόκεινται στον παρόντα κανονισμό ενδέχεται να μην είναι σε θέση να επαληθεύσουν, στο πλαίσιο της υποχρέωσής του δέουσας επιμέλειας, ότι οι κατασκευαστές των εν λόγω δομοστοιχείων έχουν αποδείξει τη συμμόρφωσή τους με τον παρόντα κανονισμό ελέγχοντας, για παράδειγμα, αν τα δομοστοιχεία φέρουν ήδη τη σήμανση CE. Αυτό μπορεί να συμβαίνει όταν τα δομοστοιχεία έχουν ενσωματωθεί πριν ο παρών κανονισμός αρχίσει να εφαρμόζεται για τους κατασκευαστές των εν λόγω κατασκευαστικών στοιχείων. Στην περίπτωση αυτή, οι κατασκευαστές που ενσωματώνουν τέτοια δομοστοιχεία θα πρέπει να επιδεικνύουν δέουσα επιμέλεια με άλλα μέσα.

(36) Τα προϊόντα με ψηφιακά στοιχεία θα πρέπει να φέρουν τη σήμανση CE ώστε να δηλώνεται κατά τρόπο ορατό, ευανάγνωστο και ανεξίτηλο 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 στη θέση σε κυκλοφορία στην αγορά προϊόντων με ψηφιακά στοιχεία που συμμορφώνονται με τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό και φέρουν τη σήμανση CE. Επιπλέον, σε εμπορικές εκθέσεις και επιδείξεις ή παρόμοιες εκδηλώσεις, τα κράτη μέλη δεν θα πρέπει να εμποδίζουν την παρουσίαση ή τη χρήση προϊόντων με ψηφιακά στοιχεία που δεν συμμορφώνονται με τον παρόντα κανονισμό, συμπεριλαμβανομένων των πρωτοτύπων, υπό την προϋπόθεση ότι το προϊόν παρουσιάζεται με ευδιάκριτο σήμα που υποδεικνύει σαφώς ότι το προϊόν δεν συμμορφώνεται με τον παρόντα κανονισμό και δεν πρόκειται να διατεθεί στην αγορά έως ότου συμβεί αυτό.

(37) Προκειμένου να διασφαλιστεί ότι οι κατασκευαστές μπορούν να διαθέτουν λογισμικό για σκοπούς διεξαγωγής δοκιμών προτού υποβάλουν τα προϊόντα τους με ψηφιακά στοιχεία 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, με την προϋπόθεση ότι η ημιτελής 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 καθορίζονται στον παρόντα κανονισμό. Οι κατασκευαστές θα πρέπει επίσης να εφαρμόζουν τις απαιτήσεις χειρισμού ευπαθειών 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.

(38) Προκειμένου να διασφαλιστεί ότι τα προϊόντα με ψηφιακά στοιχεία, όταν τίθενται σε κυκλοφορία στην αγορά, δεν ενέχουν κινδύνους για την κυβερνοασφάλεια σε πρόσωπα και οργανισμούς, θα πρέπει να καθοριστούν ουσιώδεις απαιτήσεις κυβερνοασφάλειας για τα εν λόγω προϊόντα. Οι εν λόγω ουσιώδεις απαιτήσεις κυβερνοασφάλειας, συμπεριλαμβανομένων των απαιτήσεων διαχείρισης ευπαθειών, εφαρμόζονται σε κάθε μεμονωμένο προϊόν με ψηφιακά στοιχεία όταν τίθενται σε κυκλοφορία στην αγορά, ανεξάρτητα από το αν το προϊόν με ψηφιακά στοιχεία κατασκευάζεται ως μεμονωμένη μονάδα ή σε σειρά. Για παράδειγμα, για έναν τύπο προϊόντος, κάθε μεμονωμένο προϊόν με ψηφιακά στοιχεία θα πρέπει, όταν τίθεται σε κυκλοφορία στην αγορά, να έχει λάβει όλες τις διορθώσεις ή ενημερώσεις ασφαλείας που είναι διαθέσιμες για την αντιμετώπιση σχετικών ζητημάτων ασφάλειας. Όταν προϊόντα με ψηφιακά στοιχεία τροποποιούνται μεταγενέστερα, με φυσικά ή ψηφιακά μέσα, κατά τρόπο που δεν προβλέπεται από τον κατασκευαστή στην αρχική εκτίμηση κινδύνου και που μπορεί να συνεπάγεται ότι δεν πληρούν πλέον τις σχετικές ουσιώδεις απαιτήσεις κυβερνοασφάλειας, η τροποποίηση θα πρέπει να θεωρείται ουσιαστική. Για παράδειγμα οι επισκευές θα μπορούσαν να εξομοιωθούν με τις εργασίες συντήρησης, υπό τον όρο ότι δεν τροποποιούν προϊόν με ψηφιακά στοιχεία που έχει ήδη τεθεί σε κυκλοφορία στην αγορά κατά τρόπο που να επηρεάζει τη συμμόρφωση του τελευταίου με τις ισχύουσες απαιτήσεις, ή που να μπορεί να αλλάξει τον προβλεπόμενο σκοπό για τον οποίο έχει αξιολογηθεί το προϊόν.

(39) Όπως και στην περίπτωση υλικών επισκευών ή τροποποιήσεων, προϊόν με ψηφιακά στοιχεία θα πρέπει να θεωρείται ότι έχει τροποποιηθεί ουσιαστικά με αλλαγή στο λογισμικό, όταν η ενημέρωση λογισμικού τροποποιεί τον προβλεπόμενο σκοπό του προϊόντος και οι σχετικές αλλαγές δεν είχαν προβλεφθεί από τον κατασκευαστή στην αρχική εκτίμηση κινδύνου, ή όταν η φύση του κινδύνου έχει αλλάξει ή όταν έχει αυξηθεί το επίπεδο κινδύνου λόγω της ενημέρωσης λογισμικού, και η ενημερωμένη έκδοση του προϊόντος διατίθεται στην αγορά. Όταν ενημέρωση ασφαλείας που αποσκοπεί στη μείωση του επιπέδου κινδύνου κυβερνοασφάλειας ενός προϊόντος με ψηφιακά στοιχεία δεν τροποποιεί τον επιδιωκόμενο σκοπό ενός προϊόντος με ψηφιακά στοιχεία, δεν θεωρείται ουσιαστική τροποποίηση. Αυτό συνήθως περιλαμβάνει καταστάσεις στις οποίες η ενημέρωση ασφαλείας συνεπάγεται μικρές μόνο προσαρμογές του πηγαίου κώδικα. Για παράδειγμα, αυτό θα μπορούσε να συμβαίνει όταν μια ενημέρωση ασφάλειας αντιμετωπίζει γνωστή ευπάθεια, μεταξύ άλλων τροποποιώντας λειτουργίες ή τις επιδόσεις ενός προϊόντος με ψηφιακά στοιχεία με αποκλειστικό σκοπό τη μείωση του επιπέδου κινδύνου κυβερνοασφάλειας. Ομοίως, ήσσονος σημασίας ενημέρωση λειτουργικότητας, όπως οπτική βελτίωση ή προσθήκη νέων εικονογραμμάτων ή γλωσσών στη διασύνδεση χρήστη, δεν θα πρέπει γενικά να θεωρείται ουσιώδης τροποποίηση. Αντιθέτως, όταν μια ενημέρωση χαρακτηριστικών τροποποιεί τις αρχικές προβλεπόμενες λειτουργίες ή τον τύπο ή τις επιδόσεις ενός προϊόντος με ψηφιακά στοιχεία και πληροί τα ανωτέρω κριτήρια, θα πρέπει να θεωρείται ουσιαστική τροποποίηση, καθώς η προσθήκη νέων χαρακτηριστικών οδηγεί συνήθως σε ευρύτερη επιφάνεια επίθεσης, αυξάνοντας έτσι τον κίνδυνο κυβερνοασφάλειας. Για παράδειγμα, αυτό θα μπορούσε να συμβαίνει όταν προστίθεται νέο στοιχείο εισόδου σε μια εφαρμογή, όπου ο κατασκευαστής υποχρεώνεται να διασφαλίσει επαρκή επικύρωση εισόδου. Κατά την αξιολόγηση του κατά πόσον μια ενημέρωση χαρακτηριστικού θεωρείται ουσιαστική τροποποίηση, δεν έχει σημασία αν παρέχεται ως χωριστή ενημέρωση ή σε συνδυασμό με ενημέρωση ασφαλείας. Η Επιτροπή θα πρέπει να εκδώσει καθοδήγηση σχετικά με τον τρόπο προσδιορισμού του τι συνιστά ουσιαστική τροποποίηση.

(40) Λαμβανομένου υπόψη του επαναλαμβανόμενου χαρακτήρα της ανάπτυξης λογισμικού, οι κατασκευαστές που έχουν θέσει μεταγενέστερες εκδόσεις προϊόντος λογισμικού σε κυκλοφορία στην αγορά ως αποτέλεσμα μεταγενέστερης ουσιαστικής τροποποίησης του εν λόγω προϊόντος θα πρέπει να είναι σε θέση να παρέχουν ενημερώσεις ασφαλείας για την περίοδο υποστήριξης μόνο για την έκδοση του προϊόντος λογισμικού που έχουν θέσει για τελευταία φορά σε κυκλοφορία στην αγορά. Θα πρέπει να μπορούν να το πράξουν μόνο εάν οι χρήστες των σχετικών προηγούμενων εκδόσεων προϊόντων έχουν πρόσβαση στην τελευταία έκδοση προϊόντος που τέθηκε σε κυκλοφορία στην αγορά δωρεάν και δεν επιβαρύνονται με πρόσθετο κόστος για την προσαρμογή του περιβάλλοντος υλισμικού ή λογισμικού στο οποίο χρησιμοποιούν το προϊόν. Αυτό θα μπορούσε, για παράδειγμα, να συμβαίνει όταν η αναβάθμιση του λειτουργικού συστήματος επιτραπέζιου υπολογιστή δεν απαιτεί νέο υλισμικό, όπως ταχύτερη κεντρική μονάδα επεξεργασίας ή μεγαλύτερη μνήμη. Ωστόσο, ο κατασκευαστής θα πρέπει να συνεχίσει να συμμορφώνεται, για την περίοδο υποστήριξης, με άλλες απαιτήσεις χειρισμού ευπαθειών, όπως η ύπαρξη πολιτικής για συντονισμένη γνωστοποίηση ευπαθειών ή μέτρων για τη διευκόλυνση της ανταλλαγής πληροφοριών σχετικά με πιθανές ευπάθειες για όλες τις επακόλουθες σημαντικά τροποποιημένες εκδόσεις του προϊόντος λογισμικού που τέθηκε σε κυκλοφορία στην αγορά. Οι κατασκευαστές θα πρέπει να είναι σε θέση να παρέχουν ήσσονος σημασίας ενημερώσεις ασφάλειας ή λειτουργικότητας που δεν συνιστούν ουσιαστική τροποποίηση μόνο για την τελευταία έκδοση ή υποέκδοση προϊόντος λογισμικού που δεν έχει τροποποιηθεί ουσιαστικά. Ταυτόχρονα, όταν ένα προϊόν υλισμικού, όπως ένα έξυπνο τηλέφωνο, δεν είναι συμβατό με την τελευταία έκδοση του λειτουργικού συστήματος με το οποίο παραδόθηκε αρχικά, ο κατασκευαστής θα πρέπει να συνεχίσει να παρέχει ενημερώσεις ασφαλείας τουλάχιστον για την τελευταία συμβατή έκδοση του λειτουργικού συστήματος για την περίοδο υποστήριξης.

(41) 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 ψηφιακά στοιχεία προς 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, η αλλαγή που ενδέχεται να οδηγήσει σε ουσιαστική τροποποίηση θα πρέπει να κοινοποιείται στο τρίτο μέρος.

(42) Όταν προϊόν με ψηφιακά στοιχεία υπόκειται σε «ανακατασκευή», «συντήρηση» και «επισκευή» προϊόντος με ψηφιακά στοιχεία, όπως ορίζεται στο άρθρο 2 σημεία 18), 19) και 20) του κανονισμού (ΕΕ) 2024./1781 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[18], τούτο δεν συνεπάγεται κατ' ανάγκη ουσιαστική τροποποίηση του προϊόντος, για παράδειγμα εάν ο προβλεπόμενος σκοπός και οι λειτουργίες δεν αλλάξουν και το επίπεδο κινδύνου παραμένει αμετάβλητο. Ωστόσο, η αναβάθμιση ενός προϊόντος με ψηφιακά στοιχεία από τον κατασκευαστή ενδέχεται να οδηγήσει σε αλλαγές στον σχεδιασμό και την ανάπτυξη του εν λόγω προϊόντος και, ως εκ τούτου, ενδέχεται να επηρεάσει τον προβλεπόμενο σκοπό και τη συμμόρφωση προς τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό.

---

18 Κανονισμός (ΕΕ) 2024/1781 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουνίου 2024, για τη θέσπιση πλαισίου για τον καθορισμό απαιτήσεων οικολογικού σχεδιασμού όσον αφορά τα βιώσιμα προϊόντα, για την τροποποίηση της οδηγίας (ΕΕ) 2020/1828 και του κανονισμού (ΕΕ) 2023/1542 και για την κατάργηση της οδηγίας 2009/125/ΕΚ (ΕΕ L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

(43) Τα προϊόντα με ψηφιακά στοιχεία θα πρέπει να θεωρούνται σημαντικά εάν ο αρνητικός αντίκτυπος της εκμετάλλευσης δυνητικών ευπαθειών του προϊόντος μπορεί να είναι σοβαρός λόγω, μεταξύ άλλων, λειτουργικότητας συνδεόμενης με την κυβερνοασφάλεια ή λειτουργίας που ενέχει σημαντικό κίνδυνο δυσμενών επιπτώσεων όσον αφορά την ένταση και την ικανότητά της να διαταράξει, να ελέγξει ή να προκαλέσει ζημία σε μεγάλο αριθμό άλλων προϊόντων με ψηφιακά στοιχεία ή στην υγεία, την ασφάλεια ή την προστασία των χρηστών του μέσω άμεσης χειραγώγησης, όπως κεντρικής λειτουργίας συστήματος, συμπεριλαμβανομένων της διαχείρισης δικτύου, του ελέγχου διαμόρφωσης, της εικονικοποίησης ή της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Ειδικότερα, ευπάθειες σε προϊόντα με ψηφιακά στοιχεία που έχουν λειτουργία η οποία σχετίζεται με την κυβερνοασφάλεια, όπως τα συστήματα διαχείρισης εκκίνησης, μπορούν να οδηγήσουν στη διάδοση προβλημάτων ασφάλειας σε ολόκληρη την εφοδιαστική αλυσίδα. Η σοβαρότητα των επιπτώσεων ενός περιστατικού μπορεί επίσης να αυξηθεί όταν το προϊόν επιτελεί πρωτίστως κεντρική λειτουργία συστήματος, συμπεριλαμβανομένων της διαχείρισης δικτύου, του ελέγχου διαμόρφωσης, της εικονικοποίησης ή της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

(44) Ορισμένες κατηγορίες προϊόντων 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 σημαντικά προϊόντα με ψηφιακά στοιχεία θα πρέπει να χωρίζονται σε δύο κλάσεις, οι οποίες να αντικατοπτρίζουν το επίπεδο κινδύνου που συνδέεται με τις συγκεκριμένες τις κατηγορίες προϊόντων όσον αφορά την κυβερνοασφάλεια. Περιστατικό που αφορά σημαντικά προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στην κλάση ΙΙ ενδέχεται να έχει μεγαλύτερες αρνητικές επιπτώσεις από περιστατικό που αφορά σημαντικά προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στην κλάση Ι, για παράδειγμα λόγω της φύσης της λειτουργίας τους που σχετίζεται με την κυβερνοασφάλεια ή της εκτέλεσης άλλης λειτουργίας που ενέχει σημαντικό κίνδυνο δυσμενών επιπτώσεων. Ως ένδειξη των εν λόγω μεγαλύτερων αρνητικών επιπτώσεων, τα προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στην κλάση ΙΙ θα μπορούσαν είτε να εκτελούν λειτουργία σχετιζόμενη με την κυβερνοασφάλεια είτε άλλη λειτουργία που ενέχει σημαντικό κίνδυνο δυσμενών επιπτώσεων, ο οποίος είναι υψηλότερος από ό,τι για εκείνα που περιλαμβάνονται στην κλάση Ι, ή πληρούν αμφότερα τα προαναφερθέντα κριτήρια. Συνεπώς, τα σημαντικά προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στην κλάση ΙΙ θα πρέπει να υπόκεινται σε αυστηρότερη διαδικασία αξιολόγησης της συμμόρφωσης.

(45) Ως σημαντικά προϊόντα με ψηφιακά στοιχεία που αναφέρονται στον παρόντα κανονισμό θα πρέπει να νοούνται τα προϊόντα που έχουν τη βασική λειτουργικότητα μιας κατηγορίας σημαντικών προϊόντων με ψηφιακά στοιχεία που καθορίζεται στον παρόντα κανονισμό. Για παράδειγμα, ο παρών κανονισμός καθορίζει κατηγορίες σημαντικών προϊόντων με ψηφιακά στοιχεία τα οποία ορίζονται από τη βασική λειτουργικότητά τους ως τείχη προστασίας ή συστήματα ανίχνευσης ή πρόληψης εισβολής στην κλάση ΙΙ. Συνεπώς, τα τείχη προστασίας και τα συστήματα ανίχνευσης ή πρόληψης εισβολής υπόκεινται σε υποχρεωτική αξιολόγηση της συμμόρφωσης από τρίτους. Αυτό δεν ισχύει για άλλα προϊόντα με ψηφιακά στοιχεία που δεν κατατάσσονται στα σημαντικά προϊόντα με ψηφιακά στοιχεία τα οποία ενδέχεται να περιλαμβάνουν τείχη προστασίας ή συστήματα ανίχνευσης ή πρόληψης εισβολής. Η Επιτροπή θα πρέπει να εκδώσει εκτελεστική πράξη για τον καθορισμό της τεχνικής περιγραφής των κατηγοριών σημαντικών προϊόντων με ψηφιακά στοιχεία που εμπίπτουν στις κλάσεις Ι και ΙΙ του παρόντος κανονισμού.

(46) Οι κατηγορίες κρίσιμων προϊόντων με ψηφιακά στοιχεία που ορίζονται στον παρόντα κανονισμό έχουν λειτουργικότητα σχετική με την κυβερνοασφάλεια και επιτελούν λειτουργία η οποία ενέχει σημαντικό κίνδυνο δυσμενών επιπτώσεων όσον αφορά την ένταση και την ικανότητά της να διαταράξει, να ελέγξει ή να προκαλέσει ζημία σε μεγάλο αριθμό άλλων προϊόντων με ψηφιακά στοιχεία μέσω άμεσης χειραγώγησης. Επιπλέον, οι εν λόγω κατηγορίες προϊόντων με ψηφιακά στοιχεία θεωρούνται κρίσιμες εξαρτήσεις για τις βασικές οντότητες που αναφέρονται στο άρθρο 3 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555. Οι κατηγορίες κρίσιμων προϊόντων με ψηφιακά στοιχεία που καθορίζονται σε παράρτημα του παρόντος κανονισμού, λόγω της κρισιμότητάς τους, χρησιμοποιούν ήδη ευρέως διάφορες μορφές πιστοποίησης και καλύπτονται επίσης από το ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων (EUCC) που ορίζεται στον εκτελεστικό κανονισμό (ΕΕ) 2024/482 της Επιτροπής[19]. Επομένως, προκειμένου να διασφαλιστεί μια κοινή επαρκής προστασία της κυβερνοασφάλειας κρίσιμων προϊόντων με ψηφιακά στοιχεία στην Ένωση, θα μπορούσε να είναι επαρκής και αναλογική η υπαγωγή των εν λόγω κατηγοριών προϊόντων, μέσω κατ' εξουσιοδότηση πράξης, σε υποχρεωτική ευρωπαϊκή πιστοποίηση της κυβερνοασφάλειας, όταν υπάρχει ήδη σχετικό ευρωπαϊκό καθεστώς πιστοποίησης της κυβερνοασφάλειας που καλύπτει τα εν λόγω προϊόντα και έχει διενεργηθεί από την Επιτροπή εκτίμηση του δυνητικού αντικτύπου στην αγορά της προβλεπόμενης υποχρεωτικής πιστοποίησης. Η αξιολόγηση αυτή θα πρέπει να λαμβάνει υπόψη τόσο την προσφορά όσο και τη ζήτηση, συμπεριλαμβανομένου του κατά πόσον υπάρχει επαρκής ζήτηση για τα οικεία προϊόντα με ψηφιακά στοιχεία τόσο από τα κράτη μέλη όσο και από τους χρήστες ώστε να απαιτείται ευρωπαϊκή πιστοποίηση κυβερνοασφάλειας, καθώς και τους σκοπούς για τους οποίους προορίζονται να χρησιμοποιηθούν τα προϊόντα με ψηφιακά στοιχεία, συμπεριλαμβανομένης της κρίσιμης εξάρτησης από αυτά βασικών οντοτήτων όπως αναφέρονται στο άρθρο 3 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555. Η αξιολόγηση θα πρέπει επίσης να αναλύει τις πιθανές επιπτώσεις της υποχρεωτικής πιστοποίησης στη διαθεσιμότητα των εν λόγω προϊόντων στην εσωτερική αγορά, όπως επίσης τις ικανότητες και την ετοιμότητα των κρατών μελών για την εφαρμογή των σχετικών ευρωπαϊκών καθεστώτων πιστοποίησης της κυβερνοασφάλειας.

---

19 Εκτελεστικός κανονισμός (ΕΕ) 2024/482 της Επιτροπής, της 31ης Ιανουαρίου 2024, για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την έγκριση του ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων (EUCC) (ΕΕ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(47) Οι κατ' εξουσιοδότηση πράξεις που απαιτούν υποχρεωτική ευρωπαϊκή πιστοποίηση της κυβερνοασφάλειας θα πρέπει να προσδιορίζουν τα προϊόντα με ψηφιακά στοιχεία που έχουν τη βασική λειτουργικότητα μιας κατηγορίας κρίσιμων προϊόντων με ψηφιακά στοιχεία κατά τον παρόντα κανονισμό τα οποία πρέπει να υπόκεινται σε υποχρεωτική πιστοποίηση, καθώς και το απαιτούμενο επίπεδο διασφάλισης, το οποίο θα πρέπει να είναι τουλάχιστον «ουσιαστικό». Το απαιτούμενο επίπεδο διασφάλισης θα πρέπει να είναι ανάλογο προς το επίπεδο κινδύνου κυβερνοασφάλειας που συνδέεται με το προϊόν με ψηφιακά στοιχεία. Για παράδειγμα, όταν το προϊόν με ψηφιακά στοιχεία έχει τη βασική λειτουργικότητα μιας κατηγορίας κρίσιμων προϊόντων με ψηφιακά στοιχεία που ορίζεται στον παρόντα κανονισμό και προορίζεται για χρήση σε ευαίσθητο ή κρίσιμο περιβάλλον, όπως προϊόντα που προορίζονται για τη χρήση βασικών οντοτήτων που αναφέρονται στο άρθρο 3 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555, μπορεί να απαιτεί το υψηλότερο επίπεδο διασφάλισης.

(48) Προκειμένου να διασφαλιστεί κοινή επαρκής προστασία της κυβερνοασφάλειας στην Ένωση για προϊόντα με ψηφιακά στοιχεία που έχουν τη βασική λειτουργικότητα μιας κατηγορίας κρίσιμων προϊόντων με ψηφιακά στοιχεία κατά τον παρόντα κανονισμό, η Επιτροπή θα πρέπει επίσης να εξουσιοδοτηθεί να εκδίδει κατ' εξουσιοδότηση πράξεις για την τροποποίηση του παρόντος κανονισμού προσθέτοντας ή αποσύροντας κατηγορίες κρίσιμων προϊόντων με ψηφιακά στοιχεία για τα οποία οι κατασκευαστές θα μπορούσαν να υποχρεωθούν να λάβουν ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας στο πλαίσιο ευρωπαϊκού καθεστώτος πιστοποίησης της κυβερνοασφάλειας σύμφωνα με τον κανονισμό (ΕΕ) 2019/881, για να αποδείξουν τη συμμόρφωσή τους με τον παρόντα κανονισμό. Μια νέα κατηγορία κρίσιμων προϊόντων με ψηφιακά στοιχεία μπορεί να προστεθεί στις εν λόγω κατηγορίες, εάν υπάρχει κρίσιμη εξάρτηση από αυτά βασικών οντοτήτων όπως αναφέρονται στο άρθρο 3 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555 ή εάν, όταν επηρεάζονται από περιστατικά ή όταν περιέχουν ευπάθειες που αποτελούν αντικείμενο εκμετάλλευσης, αυτό θα μπορούσε να οδηγήσει σε διαταραχές κρίσιμων εφοδιαστικών αλυσίδων. Κατά την αξιολόγηση της ανάγκης για προσθήκη ή ανάκληση κατηγοριών κρίσιμων προϊόντων με ψηφιακά στοιχεία μέσω κατ' εξουσιοδότηση πράξης, η Επιτροπή θα πρέπει να είναι σε θέση να λαμβάνει υπόψη κατά πόσον τα κράτη μέλη έχουν προσδιορίσει σε εθνικό επίπεδο προϊόντα με ψηφιακά στοιχεία που διαδραματίζουν κρίσιμο ρόλο για την ανθεκτικότητα των βασικών οντοτήτων όπως αναφέρονται στο άρθρο 3 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555 και οι οποίες αντιμετωπίζουν διαρκώς περισσότερο κυβερνοεπιθέσεις στην εφοδιαστική αλυσίδα, με δυνητικές σοβαρές διαταραχές. Επιπλέον, η Επιτροπή θα πρέπει να είναι σε θέση να λαμβάνει υπόψη το αποτέλεσμα της συντονισμένης σε επίπεδο Ένωσης εκτίμησης κινδύνου για την ασφάλεια κρίσιμων εφοδιαστικών αλυσίδων που διενεργείται σύμφωνα με το άρθρο 22 της οδηγίας (ΕΕ) 2022/2555.

(49) Η Επιτροπή θα πρέπει να διασφαλίζει τη δομημένη και τακτική διαβούλευση με ευρύ φάσμα σχετικών ενδιαφερόμενων μερών κατά την προετοιμασία μέτρων για την εφαρμογή του παρόντος κανονισμού. Αυτό θα πρέπει να ισχύει ιδίως όταν η Επιτροπή αξιολογεί την ανάγκη για πιθανές ενημερώσεις των καταλόγων των κατηγοριών σημαντικών ή κρίσιμων προϊόντων με ψηφιακά στοιχεία, κατά περίπτωση θα πρέπει να ζητείται η γνώμη των κατασκευαστών και να λαμβάνονται υπόψη οι απόψεις τους προκειμένου να αναλύονται οι κίνδυνοι κυβερνοασφάλειας, καθώς και η ισορροπία κόστους και οφέλους του χαρακτηρισμού των εν λόγω κατηγοριών προϊόντων ως σημαντικών ή κρίσιμων.

(50) 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 πάντα με την κυβερνοασφάλεια αλλά μπορεί να είναι συνέπεια παραβίασης της ασφάλειας. Οι κίνδυνοι αυτοί θα πρέπει να εξακολουθήσουν να ρυθμίζονται από σχετική ενωσιακή νομοθεσία εναρμόνισης πέραν του παρόντος κανονισμού. Εάν δεν εφαρμόζεται άλλη ενωσιακή νομοθεσία εναρμόνισης πέραν του παρόντος κανονισμού, θα πρέπει να υπόκεινται στον κανονισμό (ΕΕ) 2023/988 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[20]. Επομένως, λόγω του στοχευμένου χαρακτήρα του παρόντος κανονισμού, κατά παρέκκλιση από το άρθρο 2 παράγραφος 1 τρίτο εδάφιο στοιχείο β) του κανονισμού (ΕΕ) 2023/988, το κεφάλαιο ΙΙΙ τμήμα 1, τα κεφάλαια V και VII και τα κεφάλαια IX έως XI του κανονισμού (ΕΕ) 2023/988 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 επιβαλλόμενες από άλλη ενωσιακή νομοθεσία εναρμόνισης πέραν του παρόντος κανονισμού κατά την έννοια του άρθρου 3 σημείο 27 του κανονισμού (ΕΕ) 2023/988.

---

[20] Κανονισμός (ΕΕ) 2023/988 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαΐου 2023, για τη γενική ασφάλεια των προϊόντων, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της οδηγίας (ΕΕ) 2020/1828 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, και την κατάργηση της οδηγίας 2001/95/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της οδηγίας 87/357/ΕΟΚ του Συμβουλίου (ΕΕ L 135 της 23.5.2023, σ. 1).

(51) Τα προϊόντα με ψηφιακά στοιχεία που ταξινομούνται ως συστήματα ΤΝ υψηλού κινδύνου σύμφωνα με το άρθρο 6 του κανονισμού (ΕΕ) 2024/1689 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[21] και τα οποία εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού θα πρέπει να συμμορφώνονται με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό. Όταν τα εν λόγω συστήματα ΤΝ υψηλού κινδύνου πληρούν τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό, θα πρέπει να θεωρείται ότι συμμορφώνονται με τις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο άρθρο 15 του κανονισμού (ΕΕ) 2024/1689, στον βαθμό που οι εν λόγω απαιτήσεις καλύπτονται από τη δήλωση συμμόρφωσης ΕΕ ή μέρη αυτής, όπως εκδίδεται δυνάμει του παρόντος κανονισμού. Για τον σκοπό αυτό, στην εκτίμηση των κινδύνων κυβερνοασφάλειας που συνδέονται με προϊόν με ψηφιακά στοιχεία χαρακτηριζόμενο ως σύστημα ΤΝ υψηλού κινδύνου δυνάμει του κανονισμού (ΕΕ) 2024/1689, το οποίο πρέπει να λαμβάνεται υπόψη κατά τις φάσεις σχεδιασμού, σχεδίασης, ανάπτυξης, παραγωγής, παράδοσης και συντήρησης του συγκεκριμένου προϊόντος, όπως απαιτείται από τον παρόντα κανονισμό, θα πρέπει να λαμβάνονται υπόψη οι κίνδυνοι για την κυβερνοανθεκτικότητα ενός συστήματος ΤΝ σε σχέση με απόπειρες από μη εξουσιοδοτημένα τρίτα μέρη για αλλαγή της χρήσης, της συμπεριφοράς ή της επιτέλεσης της λειτουργίας, συμπεριλαμβανομένων ευπαθειών σχετιζόμενων ειδικά με την ΤΝ, όπως η δηλητηρίαση δεδομένων ή οι αντιπαραθετικές επιθέσεις, καθώς επίσης, κατά περίπτωση, οι κίνδυνοι για τα θεμελιώδη δικαιώματα, σύμφωνα με τον κανονισμό (ΕΕ) 2024/1689. Όσον αφορά τις διαδικασίες αξιολόγησης της συμμόρφωσης που αφορούν τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας για ένα προϊόν με ψηφιακά στοιχεία που εμπίπτει στο πεδίο εφαρμογής του παρόντος κανονισμού και ταξινομείται ως σύστημα ΤΝ υψηλού κινδύνου, κατά κανόνα θα πρέπει να εφαρμόζονται οι σχετικές διατάξεις του άρθρου 43 του κανονισμού (ΕΕ) 2024/1689 αντί των σχετικών διατάξεων του παρόντος κανονισμού.

---

[21] Κανονισμός (ΕΕ) 2024/1689 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουνίου 2024, για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 300/2008, (ΕΕ) αριθ. 167/2013, (ΕΕ) αριθ. 168/2013, (ΕΕ) 2018/858, (ΕΕ) 2018/1139 και (ΕΕ) 2019/2144 και των οδηγιών 2014/90/ΕΕ, (ΕΕ) 2016/797 και (ΕΕ) 2020/1828 (κανονισμός για την τεχνητή νοημοσύνη) (ΕΕ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

Ωστόσο, ο κανόνας αυτός δεν θα πρέπει να έχει ως αποτέλεσμα τη μείωση του αναγκαίου επιπέδου διασφάλισης για τα σημαντικά ή κρίσιμα προϊόντα με ψηφιακά στοιχεία κατά τον παρόντα κανονισμό. Συνεπώς, κατά παρέκκλιση από τον εν λόγω κανόνα, τα συστήματα ΤΝ υψηλού κινδύνου που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού (ΕΕ) 2024/1689 και χαρακτηρίζονται επίσης ως σημαντικά ή κρίσιμα προϊόντα με ψηφιακά στοιχεία κατά τον παρόντα κανονισμό και στα οποία εφαρμόζεται η διαδικασία αξιολόγησης της συμμόρφωσης με βάση τον εσωτερικό έλεγχο που αναφέρεται στο παράρτημα VI του κανονισμού (ΕΕ) 2024/1689, θα πρέπει να υπόκεινται στις διατάξεις του παρόντος κανονισμού σχετικά με τις διαδικασίες αξιολόγησης της συμμόρφωσης, όσον αφορά τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό. Στην περίπτωση αυτή, για όλες τις άλλες πτυχές που καλύπτονται από τον κανονισμό (ΕΕ) 2024/1689 θα πρέπει να εφαρμόζονται οι σχετικές διατάξεις για την αξιολόγηση της συμμόρφωσης με βάση τον εσωτερικό έλεγχο, όπως ορίζεται στο παράρτημα VI του εν λόγω κανονισμού.

(52) Προκειμένου να βελτιωθεί η ασφάλεια των προϊόντων με ψηφιακά στοιχεία που διατίθενται στην εσωτερική αγορά, είναι αναγκαίο να καθοριστούν ουσιώδεις απαιτήσεις κυβερνοασφάλειας για τα συγκεκριμένα προϊόντα. Οι εν λόγω ουσιώδεις απαιτήσεις κυβερνοασφάλειας δεν θα πρέπει να θίγουν τις συντονισμένες σε επίπεδο Ένωσης εκτιμήσεις κινδύνου ασφάλειας των εφοδιαστικών αλυσίδων κρίσιμης σημασίας που προβλέπονται στο άρθρο 22 της οδηγίας (ΕΕ) 2022/2555, 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 θίγουν 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 της Επιτροπής[22], στη συντονισμένη σε επίπεδο Ένωσης εκτίμηση κινδύνων κυβερνοασφάλειας των δικτύων 5G και στην εργαλειοθήκη της ΕΕ για την κυβερνοασφάλεια των δικτύων 5G που συμφωνήθηκε από την ομάδα συνεργασίας που συστάθηκε δυνάμει του άρθρου 14 της οδηγίας (ΕΕ) 2022/2555.

[22] Σύσταση (ΕΕ) 2019/534 της Επιτροπής, της 26ης Μαρτίου 2019, Κυβερνοασφάλεια δικτύων 5G (ΕΕ L 88 της 29.3.2019, σ. 42).

(53) Οι κατασκευαστές προϊόντων που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού (ΕΕ) 2023/1230 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[23], τα οποία είναι επίσης προϊόντα με ψηφιακά στοιχεία κατά την έννοια του παρόντος κανονισμού, θα πρέπει να συμμορφώνονται τόσο με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στον παρόντα κανονισμό όσο και με τις ουσιώδεις απαιτήσεις υγιεινής και ασφάλειας που καθορίζονται στον κανονισμό (ΕΕ) 2023/1230. Οι ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στον παρόντα κανονισμό και ορισμένες ουσιώδεις απαιτήσεις του κανονισμού (ΕΕ) 2023/1230 ενδέχεται να αντιμετωπίζουν παρόμοιους κινδύνους κυβερνοασφάλειας. Κατά συνέπεια, η συμμόρφωση προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό θα μπορούσε να διευκολύνει τη συμμόρφωση προς τις ουσιώδεις απαιτήσεις που καλύπτουν επίσης ορισμένους κινδύνους κυβερνοασφάλειας, όπως καθορίζονται στον κανονισμό (ΕΕ) 2023/1230, και ιδίως εκείνους που αφορούν την προστασία από τη διαφθορά, και την ασφάλεια και αξιοπιστία των συστημάτων ελέγχου που καθορίζονται στα τμήματα 1.1.9 και 1.2.1 του παραρτήματος ΙΙΙ του εν λόγω κανονισμού. Οι συνέργειες αυτές πρέπει να αποδεικνύονται από τον κατασκευαστή, για παράδειγμα με την εφαρμογή, κατά περίπτωση, εναρμονισμένων προτύπων ή άλλων τεχνικών προδιαγραφών που καλύπτουν τις σχετικές ουσιώδεις απαιτήσεις κυβερνοασφάλειας κατόπιν εκτίμησης κινδύνου που καλύπτει τους εν λόγω κινδύνους κυβερνοασφάλειας. Ο κατασκευαστής θα πρέπει επίσης να ακολουθεί τις εφαρμοστέες διαδικασίες αξιολόγησης της συμμόρφωσης που ορίζονται στον παρόντα κανονισμό και στον κανονισμό (ΕΕ) 2023/1230. Η Επιτροπή και οι ευρωπαϊκοί οργανισμοί τυποποίησης, κατά τις προπαρασκευαστικές εργασίες για την υποστήριξη της εφαρμογής του παρόντος κανονισμού και του κανονισμού (ΕΕ) 2023/1230 και των σχετικών διαδικασιών τυποποίησης θα πρέπει να προάγουν τη συνέπεια στον τρόπο αξιολόγησης των κινδύνων κυβερνοασφάλειας και στον τρόπο με τον οποίο οι κίνδυνοι αυτοί πρέπει να καλύπτονται από εναρμονισμένα πρότυπα όσον αφορά τις σχετικές ουσιώδεις απαιτήσεις.

---

[23] Κανονισμός (ΕΕ) 2023/1230 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Ιουνίου 2023, σχετικά με τα μηχανήματα και την κατάργηση της οδηγίας 2006/42/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της οδηγίας 73/361/ΕΟΚ του Συμβουλίου (ΕΕ L 165 της 29.6.2023, σ. 1).

Ειδικότερα, η Επιτροπή και οι ευρωπαϊκοί οργανισμοί τυποποίησης θα πρέπει να λαμβάνουν υπόψη τον παρόντα κανονισμό κατά την κατάρτιση και την ανάπτυξη εναρμονισμένων προτύπων για τη διευκόλυνση της εφαρμογής του κανονισμού (ΕΕ) 2023/1230 όσον αφορά ιδίως τις πτυχές κυβερνοασφάλειας που σχετίζονται με την προστασία από τη διαφθορά, και την ασφάλεια και αξιοπιστία των συστημάτων ελέγχου που καθορίζονται στα τμήματα 1.1.9 και 1.2.1 του παραρτήματος ΙΙΙ του εν λόγω κανονισμού. Η Επιτροπή θα πρέπει να παρέχει καθοδήγηση για τη στήριξη των κατασκευαστών που υπόκεινται στον παρόντα κανονισμό και υπόκεινται επίσης στον κανονισμό (ΕΕ) 2023/1230, ιδίως για να διευκολύνει την απόδειξη της συμμόρφωσης με τις σχετικές ουσιώδεις απαιτήσεις που καθορίζονται στον παρόντα κανονισμό και στον κανονισμό (ΕΕ) 2023/1230.

(54) Προκειμένου να διασφαλιστεί ότι τα προϊόντα με ψηφιακά στοιχεία είναι ασφαλή τόσο κατά τη θέση τους σε κυκλοφορία στην αγορά όσο και κατά το διάστημα κατά το οποίο αναμένεται ότι θα χρησιμοποιείται το προϊόν με ψηφιακά στοιχεία, είναι αναγκαίο να καθοριστούν ουσιώδεις απαιτήσεις κυβερνοασφάλειας για τον χειρισμό ευπαθειών, 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 κυβερνοασφάλειας που σχετίζονται με τον χειρισμό ευπαθειών σε ολόκληρη την προβλεπόμενη περίοδο υποστήριξης του προϊόντος, θα πρέπει να προσδιορίζουν ποιες άλλες ουσιώδεις απαιτήσεις κυβερνοασφάλειας που σχετίζονται με τις ιδιότητες του προϊόντος είναι συναφείς για τον συγκεκριμένο τύπο προϊόντος με ψηφιακά στοιχεία. 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 κυβερνοασφάλειας για να καθιστούν διαθέσιμα τα προϊόντα τους χωρίς γνωστές εκμεταλλεύσιμες ευπάθειες που μπορεί να έχουν αντίκτυπο στην ασφάλεια των προϊόντων αυτών, και να εφαρμόζουν κατάλληλα εναρμονισμένα πρότυπα, κοινές προδιαγραφές ή ευρωπαϊκά ή διεθνή πρότυπα.

(55) Όταν ορισμένες ουσιώδεις απαιτήσεις κυβερνοασφάλειας δεν εφαρμόζονται στο προϊόν με ψηφιακά στοιχεία που διατίθεται στην αγορά, ο κατασκευαστής περιλαμβάνει σαφή αιτιολόγηση στην εκτίμηση κινδύνων κυβερνοασφάλειας που περιλαμβάνεται στον τεχνικό φάκελο. Αυτό θα μπορούσε να συμβαίνει όταν μια ουσιώδης απαίτηση κυβερνοασφάλειας δεν είναι συμβατή με τη φύση ενός προϊόντος με ψηφιακά στοιχεία. Για παράδειγμα, ο επιδιωκόμενος σκοπός ενός προϊόντος με ψηφιακά στοιχεία μπορεί να απαιτεί από τον κατασκευαστή να ακολουθεί ευρέως αναγνωρισμένα πρότυπα διαλειτουργικότητας, ακόμη και αν τα χαρακτηριστικά ασφαλείας του δεν θεωρούνται πια τα πλέον προηγμένα. Ομοίως, άλλη νομοθεσία της Ένωσης απαιτεί από τους κατασκευαστές να εφαρμόζουν ειδικές απαιτήσεις διαλειτουργικότητας. Όταν μια ουσιώδης απαίτηση κυβερνοασφάλειας δεν εφαρμόζεται σε προϊόν με ψηφιακά στοιχεία, αλλά ο κατασκευαστής έχει εντοπίσει κινδύνους κυβερνοασφάλειας σε σχέση με την εν λόγω ουσιώδη απαίτηση κυβερνοασφάλειας, θα πρέπει να λαμβάνει μέτρα για την αντιμετώπιση των εν λόγω κινδύνων με άλλα μέσα, για παράδειγμα περιορίζοντας τον επιδιωκόμενο σκοπό του προϊόντος σε αξιόπιστα περιβάλλοντα ή ενημερώνοντας τους χρήστες σχετικά με τους εν λόγω κινδύνους.

(56) Ένα από τα σημαντικότερα μέτρα που πρέπει να λαμβάνουν οι χρήστες προκειμένου να προστατεύουν τα προϊόντα τους με ψηφιακά στοιχεία από κυβερνοεπιθέσεις είναι η εγκατάσταση των τελευταίων διαθέσιμων ενημερώσεων ασφαλείας το συντομότερο δυνατόν. Για τούτο, οι κατασκευαστές θα πρέπει να σχεδιάζουν τα προϊόντα τους και να εφαρμόζουν διαδικασίες που διασφαλίζουν ότι τα προϊόντα με ψηφιακά στοιχεία περιλαμβάνουν λειτουργίες οι οποίες καθιστούν δυνατή την αυτόματη κοινοποίηση, διανομή, καταφόρτωση και εγκατάσταση ενημερώσεων ασφαλείας, ιδίως στην περίπτωση καταναλωτικών προϊόντων. Θα πρέπει επίσης να παρέχουν τη δυνατότητα έγκρισης της καταφόρτωσης και της εγκατάστασης των ενημερώσεων ασφαλείας ως τελικό στάδιο. Οι χρήστες θα πρέπει να διατηρούν τη δυνατότητα απενεργοποίησης των αυτόματων ενημερώσεων, με σαφή και εύχρηστο μηχανισμό, υποστηριζόμενοι από σαφείς οδηγίες σχετικά με τον τρόπο με τον οποίο οι χρήστες μπορούν να αυτοεξαιρεθούν. Οι απαιτήσεις σχετικά με τις αυτόματες ενημερώσεις όπως καθορίζονται σε παράρτημα του παρόντος κανονισμού δεν εφαρμόζονται σε προϊόντα με ψηφιακά στοιχεία που προορίζονται κυρίως να ενσωματωθούν ως συστατικά στοιχεία σε άλλα προϊόντα. Δεν εφαρμόζονται επίσης σε προϊόντα με ψηφιακά στοιχεία για τα οποία οι χρήστες δεν θα ανέμεναν εύλογα αυτόματες ενημερώσεις, συμπεριλαμβανομένων προϊόντων με ψηφιακά στοιχεία προοριζόμενων να χρησιμοποιηθούν σε επαγγελματικά δίκτυα ΤΠΕ, και ιδίως σε κρίσιμα και βιομηχανικά περιβάλλοντα όπου η αυτόματη ενημέρωση θα μπορούσε να προκαλέσει παρεμβολές στις λειτουργίες. Ανεξάρτητα από το αν ένα προϊόν με ψηφιακά στοιχεία έχει σχεδιαστεί για να λαμβάνει αυτόματες ενημερώσεις ή όχι, ο κατασκευαστής του θα πρέπει να ενημερώνει τους χρήστες σχετικά με τις ευπάθειες και να καθιστά διαθέσιμες τις ενημερώσεις ασφαλείας χωρίς καθυστέρηση. Όταν ένα προϊόν με ψηφιακά στοιχεία διαθέτει διασύνδεση χρήστη ή παρόμοια τεχνικά μέσα που επιτρέπουν την άμεση αλληλεπίδραση με τους χρήστες του, ο κατασκευαστής θα πρέπει να χρησιμοποιεί τα χαρακτηριστικά αυτά για να ενημερώνει τους χρήστες ότι το προϊόν του με ψηφιακά στοιχεία έχει φτάσει στο τέλος της περιόδου υποστήριξης. Οι κοινοποιήσεις θα πρέπει να περιορίζονται σε ό,τι είναι αναγκαίο για τη διασφάλιση της αποτελεσματικής λήψης των εν λόγω πληροφοριών και να μην έχουν αρνητικό αντίκτυπο στην εμπειρία του χρήστη από το προϊόν με ψηφιακά στοιχεία.

(57) Για να βελτιωθεί η διαφάνεια των διαδικασιών χειρισμού ευπαθειών και να διασφαλιστεί ότι οι χρήστες δεν υποχρεούνται να εγκαθιστούν νέες ενημερώσεις λειτουργικότητας με αποκλειστικό σκοπό τη λήψη των τελευταίων ενημερώσεων ασφαλείας, οι κατασκευαστές θα πρέπει να διασφαλίζουν, όπου είναι τεχνικά εφικτό, ότι οι νέες ενημερώσεις ασφαλείας παρέχονται χωριστά από τις ενημερώσεις λειτουργικότητας.

(58) Στην κοινή ανακοίνωση της Επιτροπής και του Ύπατου Εκπροσώπου της Ένωσης για Θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας, της 20ής Ιουνίου 2023, με τίτλο «Ευρωπαϊκή στρατηγική οικονομικής ασφάλειας» αναφέρεται ότι η Ένωση πρέπει να μεγιστοποιήσει τα οφέλη του οικονομικού της ανοίγματος, ελαχιστοποιώντας παράλληλα τους κινδύνους από οικονομικές εξαρτήσεις από πωλητές υψηλού κινδύνου, μέσω ενός κοινού στρατηγικού πλαισίου για την οικονομική ασφάλεια της Ένωσης. Οι εξαρτήσεις από υψηλού κινδύνου προμηθευτές κρίσιμων προϊόντων με ψηφιακά στοιχεία μπορεί να ενέχουν στρατηγικό κίνδυνο που θα πρέπει να αντιμετωπίζεται σε επίπεδο Ένωσης, ιδίως όταν τα προϊόντα με ψηφιακά στοιχεία προορίζονται για χρήση από βασικές οντότητες όπως αναφέρονται στο άρθρο 3 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555. Οι κίνδυνοι αυτοί μπορεί να συνδέονται μεταξύ άλλων με τη δικαιοδοσία που ισχύει για τον κατασκευαστή, τα χαρακτηριστικά της εταιρικής ιδιοκτησίας του και τους δεσμούς ελέγχου με κυβέρνηση τρίτης χώρας όπου είναι εγκατεστημένος, ιδίως όταν μια τρίτη χώρα επιδίδεται σε οικονομική κατασκοπεία ή ανεύθυνη κρατική συμπεριφορά στον κυβερνοχώρο και η νομοθεσία της επιτρέπει αυθαίρετη πρόσβαση σε οποιοδήποτε είδος εταιρικών δραστηριοτήτων ή δεδομένων, συμπεριλαμβανομένων εμπορικά ευαίσθητων δεδομένων, και μπορεί να επιβάλλει υποχρεώσεις για σκοπούς συλλογής πληροφοριών χωρίς δημοκρατικούς ελέγχους και εξισορροπήσεις, μηχανισμό εποπτείας, δέουσα διαδικασία ή δικαίωμα προσφυγής σε ανεξάρτητη δικαστική αρχή. Κατά τον προσδιορισμό της σημασίας ενός κινδύνου κυβερνοασφάλειας κατά την έννοια του παρόντος κανονισμού, η Επιτροπή και οι αρχές εποπτείας της αγοράς, σύμφωνα με τις αρμοδιότητές τους που ορίζονται στον παρόντα κανονισμό, θα πρέπει επίσης να λαμβάνουν υπόψη μη τεχνικούς παράγοντες κινδύνου, ιδίως εκείνους που καθορίζονται ως αποτέλεσμα συντονισμένων σε επίπεδο Ένωσης εκτιμήσεων κινδύνου για την ασφάλεια κρίσιμων εφοδιαστικών αλυσίδων, που διενεργούνται σύμφωνα με το άρθρο 22 της οδηγίας (ΕΕ) 2022/2555.

(59) Για τους σκοπούς της προστασίας της ασφάλειας των προϊόντων με ψηφιακά στοιχεία μετά τη θέση τους σε κυκλοφορία στην αγορά, οι κατασκευαστές θα πρέπει να καθορίζουν περιόδους υποστήριξης οι οποίες θα πρέπει να αντικατοπτρίζουν την αναμενόμενη διάρκεια χρήσης του προϊόντος με ψηφιακά στοιχεία. Κατά τον καθορισμό μιας περιόδου υποστήριξης, ο κατασκευαστής θα πρέπει να λαμβάνει υπόψη ιδίως τις εύλογες προσδοκίες των χρηστών, τη φύση του προϊόντος, καθώς και τη σχετική ενωσιακή νομοθεσία που καθορίζει τη διάρκεια ζωής των προϊόντων με ψηφιακά στοιχεία. Οι κατασκευαστές θα πρέπει επίσης να είναι σε θέση να λαμβάνουν υπόψη άλλους σχετικούς παράγοντες. Τα κριτήρια θα πρέπει να εφαρμόζονται κατά τρόπο που να διασφαλίζει την αναλογικότητα κατά τον καθορισμό της περιόδου υποστήριξης. Κατόπιν αιτήματος, ο κατασκευαστής θα πρέπει να παρέχει στις αρχές εποπτείας της αγοράς τις πληροφορίες που ελήφθησαν υπόψη για τον καθορισμό της περιόδου υποστήριξης ενός προϊόντος με ψηφιακά στοιχεία.

(60) Η περίοδος υποστήριξης για την οποία ο κατασκευαστής διασφαλίζει τον αποτελεσματικό χειρισμό ευπαθειών δεν θα πρέπει να είναι μικρότερη των πέντε ετών, εκτός εάν η διάρκεια ζωής του προϊόντος με ψηφιακά στοιχεία είναι μικρότερη από πέντε έτη, οπότε ο κατασκευαστής θα πρέπει να διασφαλίζει τον χειρισμό ευπαθειών για τη συγκεκριμένη διάρκεια ζωής. Όταν ο χρόνος χρήσης του προϊόντος με ψηφιακά στοιχεία είναι ευλόγως μεγαλύτερος από πέντε έτη, όπως συμβαίνει συχνά για τα δομοστοιχεία υλισμικού, όπως μητρικές κάρτες ή μικροεπεξεργαστές, συσκευές δικτύου όπως δρομολογητές, μόντεμ ή μεταγωγείς, καθώς και το λογισμικό, όπως λειτουργικά συστήματα ή εργαλεία επεξεργασίας βίντεο, οι κατασκευαστές θα πρέπει συνεπώς να εξασφαλίζουν μεγαλύτερες περιόδους υποστήριξης. Ειδικότερα, προϊόντα με ψηφιακά στοιχεία που προορίζονται για χρήση σε βιομηχανικά περιβάλλοντα, όπως βιομηχανικά συστήματα ελέγχου, χρησιμοποιούνται συχνά για σημαντικά μεγαλύτερα χρονικά διαστήματα. Ο κατασκευαστής θα πρέπει να είναι σε θέση να καθορίζει περίοδο υποστήριξης μικρότερη των πέντε ετών μόνο όταν αυτό δικαιολογείται από τη φύση του οικείου προϊόντος με ψηφιακά στοιχεία και όταν το εν λόγω προϊόν αναμένεται να χρησιμοποιηθεί για λιγότερο από πέντε έτη, οπότε η περίοδος υποστήριξης θα πρέπει να αντιστοιχεί στην αναμενόμενη διάρκεια χρήσης. Για παράδειγμα, η διάρκεια ζωής μιας εφαρμογής ιχνηλάτησης επαφών που προορίζεται για χρήση κατά τη διάρκεια πανδημίας θα μπορούσε να περιοριστεί στη διάρκεια της πανδημίας. Επιπλέον, ορισμένες εφαρμογές λογισμικού μπορούν από τη φύση τους να καθίστανται διαθέσιμες μόνο βάσει μοντέλου συνδρομής, ιδίως όταν η εφαρμογή καθίσταται μη διαθέσιμη στον χρήστη και, κατά συνέπεια, δεν χρησιμοποιείται πλέον μετά τη λήξη της συνδρομής.

(61) Όταν τα προϊόντα με ψηφιακά στοιχεία φθάσουν στο τέλος των περιόδων υποστήριξής τους, προκειμένου να διασφαλιστεί η δυνατότητα άρσης ευπαθειών μετά το τέλος της περιόδου υποστήριξης, οι κατασκευαστές θα πρέπει να εξετάσουν το ενδεχόμενο να ελευθερώσουν τον πηγαίο κώδικα των εν λόγω προϊόντων με ψηφιακά στοιχεία, είτε σε άλλες επιχειρήσεις που δεσμεύονται να επεκτείνουν την παροχή υπηρεσιών άρσης ευπαθειών είτε στο κοινό. Όταν οι κατασκευαστές ελευθερώνουν τον πηγαίο κώδικα για άλλες επιχειρήσεις, θα πρέπει να είναι σε θέση να προστατεύουν την κυριότητα του προϊόντος με ψηφιακά στοιχεία και να αποτρέπουν τη διάδοση του πηγαίου κώδικα στο κοινό, για παράδειγμα μέσω συμβατικών διευθετήσεων.

(62) Προκειμένου να διασφαλιστεί ότι οι κατασκευαστές σε ολόκληρη την Ένωση καθορίζουν παρόμοιες περιόδους υποστήριξης για συγκρίσιμα προϊόντα με ψηφιακά στοιχεία, η ΕΟΔΚ θα πρέπει να δημοσιεύει στατιστικές σχετικά με τις μέσες περιόδους υποστήριξης που καθορίζονται από τους κατασκευαστές για κατηγορίες προϊόντων με ψηφιακά στοιχεία και να εκδίδει καθοδήγηση στις οποίες θα αναφέρονται οι κατάλληλες περίοδοι υποστήριξης για τις εν λόγω κατηγορίες. Επιπλέον, προκειμένου να διασφαλιστεί εναρμονισμένη προσέγγιση σε ολόκληρη την εσωτερική αγορά, η Επιτροπή θα πρέπει να είναι σε θέση να εκδίδει κατ' εξουσιοδότηση πράξεις για τον καθορισμό ελάχιστων περιόδων υποστήριξης για συγκεκριμένες κατηγορίες προϊόντων όταν τα δεδομένα που παρέχονται από τις αρχές εποπτείας της αγοράς δείχνουν ότι οι περίοδοι υποστήριξης που καθορίζονται από τους κατασκευαστές είτε δεν συνάδουν συστηματικά με τα κριτήρια για τον καθορισμό των περιόδων υποστήριξης που ορίζονται στον παρόντα κανονισμό είτε ότι οι κατασκευαστές σε διαφορετικά κράτη μέλη καθορίζουν αδικαιολόγητα διαφορετικές περιόδους υποστήριξης.

(63) Οι κατασκευαστές θα πρέπει να δημιουργήσουν ενιαίο σημείο επαφής που θα επιτρέπει στους χρήστες να επικοινωνούν εύκολα μαζί τους, μεταξύ άλλων με σκοπό την αναφορά και τη λήψη πληροφοριών σχετικά με ευπάθειες του προϊόντος με ψηφιακό στοιχείο. Θα πρέπει να καθιστούν το ενιαίο σημείο επαφής εύκολα προσβάσιμο για τους χρήστες και να αναφέρουν σαφώς τη διαθεσιμότητά του, επικαιροποιώντας τις πληροφορίες αυτές. Όταν οι κατασκευαστές επιλέγουν να προσφέρουν αυτοματοποιημένα εργαλεία, π.χ. πεδίο συζήτησης, θα πρέπει επίσης να προσφέρουν έναν αριθμό τηλεφώνου ή άλλα ψηφιακά μέσα επικοινωνίας, όπως διεύθυνση ηλεκτρονικού ταχυδρομείου ή έντυπο επικοινωνίας. Το ενιαίο σημείο επαφής δεν θα πρέπει να βασίζεται αποκλειστικά σε αυτοματοποιημένα εργαλεία.

(64) Οι κατασκευαστές θα πρέπει να διαθέτουν τα προϊόντα τους με ψηφιακά στοιχεία στην αγορά με ασφαλή εξ ορισμού διαμόρφωση και να παρέχουν δωρεάν ενημερώσεις ασφαλείας στους χρήστες. Οι κατασκευαστές θα πρέπει να είναι σε θέση να παρεκκλίνουν από τις εν λόγω ουσιώδεις απαιτήσεις κυβερνοασφάλειας μόνο σε σχέση με εξατομικευμένα προϊόντα ειδικά διαμορφωμένα για συγκεκριμένο σκοπό, για συγκεκριμένο εμπορικό χρήστη, και όταν τόσο ο κατασκευαστής όσο και ο χρήστης έχουν συμφωνήσει ρητά σε διαφορετικό σύνολο συμβατικών όρων.

(65) Οι κατασκευαστές θα πρέπει να κοινοποιούν ταυτόχρονα μέσω της ενιαίας πλατφόρμας αναφοράς τόσο στην ομάδα αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (ΟΑΠΑΥ) που έχει οριστεί ως συντονιστής όσο και στον ENISA τις ευπάθειες σημεία που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και περιέχονται σε προϊόντα με ψηφιακά στοιχεία, καθώς και σοβαρά περιστατικά που έχουν αντίκτυπο στην ασφάλεια των εν λόγω προϊόντων. Οι κοινοποιήσεις θα πρέπει να υποβάλλονται μέσω του τελικού σημείου ηλεκτρονικής κοινοποίησης μιας ΟΑΠΑΥ που έχει οριστεί ως συντονιστής, και να είναι ταυτόχρονα προσβάσιμες από τον ENISA.

(66) Οι κατασκευαστές θα πρέπει να κοινοποιούν τις ευπάθειες που αποτελούν αντικείμενο ενεργού εκμετάλλευσης, ώστε να διασφαλίζεται ότι οι ΟΑΠΑΥ που ορίζονται ως συντονιστές, και ο ENISA, διαθέτουν επαρκή επισκόπηση των εν λόγω ευπαθειών και λαμβάνουν τις πληροφορίες που είναι αναγκαίες για την εκπλήρωση των καθηκόντων τους, όπως καθορίζονται στην οδηγία (ΕΕ) 2022/2555, και ότι αυξάνουν το συνολικό επίπεδο κυβερνοασφάλειας των βασικών και σημαντικών οντοτήτων όπως αναφέρονται στο άρθρο 3 της εν λόγω οδηγίας, καθώς και για τη διασφάλιση της αποτελεσματικής λειτουργίας των αρχών εποπτείας της αγοράς. Δεδομένου ότι τα περισσότερα προϊόντα με ψηφιακά στοιχεία διατίθενται σε ολόκληρη την εσωτερική αγορά, οποιαδήποτε εκμετάλλευση ευπάθειας σε προϊόν με ψηφιακά στοιχεία θα πρέπει να θεωρείται απειλή για τη λειτουργία της εσωτερικής αγοράς. Ο ENISA θα πρέπει, σε συμφωνία με τον κατασκευαστή, να γνωστοποιεί τις αρθείσες ευπάθειες στην ευρωπαϊκή βάση δεδομένων ευπαθειών που δημιουργήθηκε σύμφωνα με το άρθρο 12 παράγραφος 2 της οδηγίας (ΕΕ) 2022/2555. Η ευρωπαϊκή βάση δεδομένων ευπαθειών θα βοηθά τους κατασκευαστές στην ανίχνευση γνωστών εκμεταλλεύσιμων ευπαθειών στα προϊόντα τους, προκειμένου να διασφαλίζεται ότι στην αγορά διατίθενται ασφαλή προϊόντα.

(67) Οι κατασκευαστές θα πρέπει επίσης να κοινοποιούν κάθε σοβαρό περιστατικό που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία στην ΟΑΠΑΥ, ως ορισθέντα φορέα συντονισμού, και στον ENISA. Προκειμένου να διασφαλιστεί ότι οι χρήστες μπορούν να αντιδρούν γρήγορα σε σοβαρά περιστατικά που έχουν αντίκτυπο στην ασφάλεια των προϊόντων τους με ψηφιακά στοιχεία, οι κατασκευαστές θα πρέπει επίσης να ενημερώνουν τους χρήστες τους για κάθε σχετικό περιστατικό και, κατά περίπτωση, για τυχόν διορθωτικά μέτρα που μπορούν να εφαρμόσουν οι χρήστες για τον μετριασμό των επιπτώσεων του περιστατικού, για παράδειγμα δημοσιεύοντας σχετικές πληροφορίες στους ιστοτόπους τους ή, όταν ο κατασκευαστής είναι σε θέση να επικοινωνήσει με τους χρήστες και, όταν δικαιολογείται από τους κινδύνους κυβερνοασφάλειας, επικοινωνώντας απευθείας με τους χρήστες.

(68) Οι ευπάθειες που αποτελούν αντικείμενο ενεργού εκμετάλλευσης αφορούν περιπτώσεις στις οποίες ένας κατασκευαστής αποδεικνύει ότι μια παραβίαση της ασφάλειας που επηρεάζει τους χρήστες του ή οποιοδήποτε άλλο φυσικό ή νομικό πρόσωπο οφείλεται σε κακόβουλο παράγοντα ο οποίος εκμεταλλεύεται ελάττωμα σε ένα από τα προϊόντα με ψηφιακά στοιχεία που διατίθενται στην αγορά από τον κατασκευαστή. Παραδείγματα τέτοιων ευπαθειών θα μπορούσαν να είναι αδυναμίες στις λειτουργίες ταυτοποίησης και επαλήθευσης ταυτότητας ενός προϊόντος. Οι ευπάθειες που εντοπίζονται χωρίς κακόβουλη πρόθεση για σκοπούς καλόπιστης δοκιμής, διερεύνησης, διόρθωσης ή γνωστοποίησης για την προώθηση της ασφάλειας ή της προστασίας του ιδιοκτήτη του συστήματος και των χρηστών του δεν θα πρέπει να υπόκεινται σε υποχρεωτική κοινοποίηση. Από την άλλη πλευρά, τα σοβαρά περιστατικά που έχουν αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία αναφέρονται σε καταστάσεις στις οποίες ένα περιστατικό κυβερνοασφάλειας επηρεάζει τις διαδικασίες ανάπτυξης, παραγωγής ή συντήρησης του κατασκευαστή κατά τρόπο που θα μπορούσε να οδηγήσει σε αυξημένο κίνδυνο κυβερνοασφάλειας για τους χρήστες ή άλλα πρόσωπα. Τέτοιο σοβαρό περιστατικό θα μπορούσε να περιλαμβάνει κατάσταση κατά την οποία ο επιτιθέμενος έχει εισαγάγει επιτυχώς κακόβουλο κώδικα στον δίαυλο μέσω του οποίου ο κατασκευαστής διοχετεύει ενημερώσεις ασφαλείας στους χρήστες.

(69) Για να διασφαλιστεί ότι οι κοινοποιήσεις μπορούν να διαδίδονται γρήγορα σε όλες τις σχετικές ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού, και για να μπορούν οι κατασκευαστές να υποβάλλουν ενιαία κοινοποίηση σε κάθε στάδιο της διαδικασίας κοινοποίησης, θα πρέπει να δημιουργηθεί από τον ENISA ενιαία πλατφόρμα αναφοράς με εθνικά τελικά σημεία ηλεκτρονικής κοινοποίησης. Ο ENISA θα πρέπει να διαχειρίζεται και να συντηρεί τις καθημερινές λειτουργίες της ενιαίας πλατφόρμας αναφοράς.
Οι ΟΑΠΑΥ που ορίζονται ως φορείς συντονισμού θα πρέπει να ενημερώνουν τις αντίστοιχες αρχές εποπτείας της αγοράς τους σχετικά με κοινοποιημένες ευπάθειες ή συμβάντα. Η ενιαία πλατφόρμα αναφοράς θα πρέπει να σχεδιαστεί κατά τρόπο ώστε να διασφαλίζει την εμπιστευτικότητα των κοινοποιήσεων, ιδίως όσον αφορά ευπάθειες για τις οποίες δεν υπάρχει ακόμη ενημέρωση ασφαλείας. Επιπλέον, ο ENISA θα πρέπει να θεσπίσει διαδικασίες για τον χειρισμό των πληροφοριών με ασφαλή και εμπιστευτικό τρόπο. 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 συστάθηκε σύμφωνα με το άρθρο 14 της οδηγίας (ΕΕ) 2022/2555.

(70) Σε εξαιρετικές περιστάσεις και ιδίως κατόπιν αιτήματος του κατασκευαστή, η ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού και λαμβάνει αρχικά κοινοποίηση θα πρέπει να είναι σε θέση να αποφασίσει να καθυστερήσει τη διάδοσή της στις άλλες σχετικές ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού μέσω της ενιαίας πλατφόρμας αναφοράς, όταν αυτό μπορεί να δικαιολογηθεί για λόγους που σχετίζονται με την κυβερνοασφάλεια και για χρονικό διάστημα που είναι απολύτως αναγκαίο. Η ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού θα πρέπει να ενημερώνει αμέσως τον ENISA σχετικά με την απόφαση να καθυστερήσει και για ποιους λόγους, καθώς και σχετικά με το πότε προτίθεται να προβεί σε περαιτέρω διάδοση. Η Επιτροπή θα πρέπει να αναπτύξει, μέσω κατ' εξουσιοδότηση πράξης, προδιαγραφές σχετικά με τους όρους και τις προϋποθέσεις για τις περιπτώσεις στις οποίες θα μπορούσαν να εφαρμοστούν λόγοι που σχετίζονται με την κυβερνοασφάλεια, και να συνεργαστεί με το δίκτυο ΟΑΠΑΥ που συστάθηκε σύμφωνα με το άρθρο 15 της οδηγίας (ΕΕ) 2022/2555 και τον ENISA κατά την κατάρτιση του σχεδίου κατ' εξουσιοδότηση πράξης. Παραδείγματα λόγων που σχετίζονται με την κυβερνοασφάλεια είναι μια εν εξελίξει συντονισμένη διαδικασία γνωστοποίησης ευπαθειών ή καταστάσεις στις οποίες ένας κατασκευαστής αναμένεται να παράσχει σύντομα μέτρο μετριασμού και οι κίνδυνοι κυβερνοασφάλειας της άμεσης διάδοσης μέσω της ενιαίας πλατφόρμας αναφοράς υπερτερούν των οφελών της. Εάν ζητηθεί από την ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού, ο ENISA θα πρέπει να είναι σε θέση να υποστηρίζει την εν λόγω ΟΑΠΑΥ σε σχέση με την εφαρμογή λόγων που άπτονται της κυβερνοασφάλειας όσον αφορά την καθυστέρηση της διάδοσης της κοινοποίησης βάσει των πληροφοριών που έχει λάβει ο ENISA από την εν λόγω ΟΑΠΑΥ σχετικά με την απόφαση να μην προβεί σε κοινοποίηση για τους συγκεκριμένους λόγους που άπτονται της κυβερνοασφάλειας. Επιπλέον, σε ιδιαίτερα εξαιρετικές περιστάσεις, ο ENISA δεν θα πρέπει να λαμβάνει όλες τις λεπτομέρειες κοινοποίησης ευπάθειας που αποτελεί αντικείμενο ενεργού εκμετάλλευσης με ταυτόχρονο τρόπο.

Αυτό ισχύει όταν ο κατασκευαστής επισημαίνει στην κοινοποίησή του ότι η κοινοποιηθείσα ευπάθεια έχει αποτελέσει αντικείμενο ενεργού εκμετάλλευσης από κακόβουλο παράγοντα και ότι, σύμφωνα με τις διαθέσιμες πληροφορίες, δεν έχει αποτελέσει αντικείμενο εκμετάλλευσης σε κανένα άλλο κράτος μέλος εκτός από εκείνο της ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού, στην οποία ο κατασκευαστής έχει κοινοποιήσει την ευπάθεια, όταν οποιαδήποτε άμεση περαιτέρω διάδοση της πληροφορίας για την κοινοποιηθείσα ευπάθεια ενδέχεται να οδηγήσει στην παροχή πληροφοριών των οποίων η αποκάλυψη θα ήταν αντίθετη προς τα ουσιώδη συμφέροντα του εν λόγω κράτους μέλους, ή όταν η κοινοποιηθείσα ευπάθεια ενέχει άμεσο υψηλό κίνδυνο κυβερνοασφάλειας που απορρέει από την περαιτέρω διάδοση. Στις περιπτώσεις αυτές, ο ENISA θα λαμβάνει ταυτόχρονη πρόσβαση μόνο στις πληροφορίες ότι πραγματοποιήθηκε κοινοποίηση από τον κατασκευαστή, στις γενικές πληροφορίες σχετικά με το οικείο προϊόν με ψηφιακά στοιχεία, στις πληροφορίες σχετικά με τη γενική φύση της εκμετάλλευσης και στις πληροφορίες σχετικά με το γεγονός ότι οι εν λόγω λόγοι ασφάλειας προβλήθηκαν από τον κατασκευαστή και ότι, επομένως, τηρείται μυστικό το πλήρες περιεχόμενο της κοινοποίησης. Η πλήρης κοινοποίηση θα πρέπει στη συνέχεια να τίθεται στη διάθεση του ENISA και άλλων σχετικών ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού, όταν η ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού και λαμβάνει αρχικά την κοινοποίηση διαπιστώσει ότι οι εν λόγω λόγοι ασφάλειας, οι οποίοι αντικατοπτρίζουν ιδιαίτερα εξαιρετικές περιστάσεις όπως ορίζονται στον παρόντα κανονισμό, παύουν να υφίστανται. Όταν, βάσει των διαθέσιμων πληροφοριών, ο ENISA θεωρεί ότι υπάρχει συστημικός κίνδυνος που επηρεάζει την ασφάλεια της εσωτερικής αγοράς, ο ENISA θα πρέπει να συνιστά στην αποδέκτρια ΟΑΠΑΥ να διαδίδει την πλήρη κοινοποίηση στις άλλες ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού, καθώς και στον ίδιο τον ENISA.

(71) Όταν οι κατασκευαστές κοινοποιούν ευπάθεια ή σοβαρό περιστατικό που αποτελεί αντικείμενο ενεργού εκμετάλλευσης και έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία, θα πρέπει να αναφέρουν πόσο ευαίσθητες θεωρούν τις κοινοποιούμενες πληροφορίες. Η ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού, η οποία λαμβάνει αρχικά την κοινοποίηση, θα πρέπει να λαμβάνει υπόψη τις πληροφορίες αυτές κατά την αξιολόγηση του κατά πόσον η κοινοποίηση δημιουργεί εξαιρετικές περιστάσεις που δικαιολογούν καθυστέρηση στη διάδοση της κοινοποίησης στις άλλες σχετικές ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού, για τεκμηριωμένους λόγους σχετικούς με την κυβερνοασφάλεια. Θα πρέπει επίσης να λαμβάνει υπόψη τις εν λόγω πληροφορίες κατά την αξιολόγηση του κατά πόσον η κοινοποίηση μιας ευπάθειας, η οποία αποτελεί αντικείμενο ενεργού εκμετάλλευσης, δημιουργεί ιδιαίτερα εξαιρετικές περιστάσεις που δικαιολογούν το γεγονός ότι η πλήρης κοινοποίηση δεν διατίθεται ταυτόχρονα στον ENISA. Τέλος, οι ΟΑΠΑΥ που ορίζονται ως φορείς συντονισμού θα πρέπει να είναι σε θέση να λαμβάνουν υπόψη τις πληροφορίες αυτές κατά τον καθορισμό κατάλληλων μέτρων για τον μετριασμό των κινδύνων που απορρέουν από τις εν λόγω ευπάθειες και συμβάντα.

(72) Προκειμένου να απλουστευθεί η υποβολή των πληροφοριών που απαιτούνται βάσει του παρόντος κανονισμού, λαμβανομένων υπόψη άλλων συμπληρωματικών απαιτήσεων υποβολής εκθέσεων που προβλέπονται στο δίκαιο της Ένωσης, όπως ο κανονισμός (ΕΕ) 2016/679, ο κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[24], η οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[25] και η οδηγία (ΕΕ) 2022/2555, καθώς και για να μειωθεί ο διοικητικός φόρτος για τις οντότητες, τα κράτη μέλη ενθαρρύνονται να εξετάσουν το ενδεχόμενο να παρέχουν σε εθνικό επίπεδο ενιαία σημεία εισόδου για τις εν λόγω απαιτήσεις υποβολής εκθέσεων. Η χρήση αυτών των ενιαίων σημείων εισόδου για την αναφορά περιστατικών ασφάλειας δυνάμει του κανονισμού (ΕΕ) 2016/679 και της οδηγίας 2002/58/ΕΚ δεν θα πρέπει να επηρεάζει την εφαρμογή των διατάξεων του κανονισμού (ΕΕ) 2016/679 και της οδηγίας 2002/58/ΕΚ, ιδίως εκείνων που αφορούν την ανεξαρτησία των αρχών που αναφέρονται εκεί. Κατά τη δημιουργία της ενιαίας πλατφόρμας αναφοράς που αναφέρεται στον παρόντα κανονισμό, ο ENISA θα πρέπει να λαμβάνει υπόψη τη δυνατότητα ενσωμάτωσης των εθνικών τελικών σημείων ηλεκτρονικής κοινοποίησης που αναφέρονται στον παρόντα κανονισμό σε εθνικά ενιαία σημεία εισόδου που μπορούν επίσης να ενσωματώνουν άλλες κοινοποιήσεις οι οποίες απαιτούνται βάσει του ενωσιακού δικαίου.

---

24 Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).

25 Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (ΕΕ L 201 της 31.7.2002, σ. 37).

(73) Κατά τη δημιουργία της ενιαίας πλατφόρμας αναφοράς που αναφέρεται στον παρόντα κανονισμό, και προκειμένου να επωφεληθεί από την εμπειρία του παρελθόντος, ο ENISA θα πρέπει να συμβουλεύεται άλλα θεσμικά όργανα ή οργανισμούς της Ένωσης που διαχειρίζονται πλατφόρμες ή βάσεις δεδομένων που υπόκεινται σε αυστηρές απαιτήσεις ασφάλειας, όπως ο Οργανισμός της Ευρωπαϊκής Ένωσης για τη Λειτουργική Διαχείριση Συστημάτων ΤΠ Μεγάλης Κλίμακας στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης (eu-LISA). Ο ENISA θα πρέπει επίσης να αναλύει τις δυνητικές συμπληρωματικότητες με την ευρωπαϊκή βάση δεδομένων ευπαθειών που δημιουργήθηκε σύμφωνα με το άρθρο 12 παράγραφος 2 της οδηγίας (ΕΕ) 2022/2555.

(74) Οι κατασκευαστές και άλλα φυσικά και νομικά πρόσωπα θα πρέπει να είναι σε θέση να κοινοποιούν σε ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού ή στον ENISA, σε εθελοντική βάση, κάθε ευπάθεια που περιέχεται σε προϊόν με ψηφιακά στοιχεία, κυβερνοαπειλές που θα μπορούσαν να επηρεάσουν το προφίλ κινδύνου ενός προϊόντος με ψηφιακά στοιχεία, κάθε περιστατικό που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία, καθώς και παρ' ολίγον συμβάντα κινδύνου που θα μπορούσαν να έχουν οδηγήσει σε τέτοιο περιστατικό.

(75) Τα κράτη μέλη θα πρέπει να στοχεύουν στην αντιμετώπιση, στο μέτρο του δυνατού, των προκλήσεων που αντιμετωπίζουν τα πρόσωπα τα οποία ερευνούν ευπάθειες, συμπεριλαμβανομένης της ενδεχόμενης έκθεσής τους σε ποινική ευθύνη, σύμφωνα με την εθνική νομοθεσία τους. Δεδομένου ότι τα φυσικά και τα νομικά πρόσωπα που ερευνούν ευπάθειες θα μπορούσαν σε ορισμένα κράτη μέλη να εκτεθούν σε ποινική και αστική ευθύνη, τα κράτη μέλη ενθαρρύνονται να εγκρίνουν κατευθυντήριες γραμμές όσον αφορά τη μη δίωξη των ερευνητών στον τομέα της ασφάλειας των πληροφοριών και την απαλλαγή από την αστική ευθύνη για τις δραστηριότητές τους.

(76) Οι κατασκευαστές προϊόντων με ψηφιακά στοιχεία θα πρέπει να εφαρμόζουν συντονισμένες πολιτικές γνωστοποίησης ευπαθειών για τη διευκόλυνση της αναφοράς ευπαθειών από φυσικά πρόσωπα ή οντότητες είτε άμεσα στον κατασκευαστή είτε έμμεσα, και, όταν ζητείται ανώνυμα, μέσω ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού για τους σκοπούς της συντονισμένης γνωστοποίησης ευπαθειών σύμφωνα με το άρθρο 12 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555. Η συντονισμένη πολιτική των κατασκευαστών για τη γνωστοποίηση ευπαθειών θα πρέπει να προσδιορίζει μια δομημένη διαδικασία μέσω της οποίας οι ευπάθειες αναφέρονται σε κατασκευαστή κατά τρόπο που να επιτρέπει στον κατασκευαστή να διαγνώσει και να διορθώσει τις εν λόγω ευπάθειες πριν να αποκαλυφθούν σε τρίτα μέρη ή στο ευρύ κοινό λεπτομερείς πληροφορίες σχετικά με τις ευπάθειες. Επιπλέον, οι κατασκευαστές θα πρέπει επίσης να εξετάσουν το ενδεχόμενο δημοσίευσης των πολιτικών τους για την ασφάλεια σε μηχαναγνώσιμο μορφότυπο. Δεδομένου ότι οι πληροφορίες σχετικά με εκμεταλλεύσιμες ευπάθειες 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 ευπαθειών, με τα οποία θα παρέχουν κίνητρα για την αναφορά των ευπαθειών, διασφαλίζοντας ότι τα άτομα ή οι οντότητες λαμβάνουν αναγνώριση και αποζημίωση για τις προσπάθειές τους. Πρόκειται για προγράμματα γνωστά ως «bug bounty».

(77) Προκειμένου να διευκολυνθεί η ανάλυση ευπαθειών, οι κατασκευαστές θα πρέπει να εντοπίζουν και να τεκμηριώνουν τις συνιστώσες που περιέχονται στα προϊόντα με ψηφιακά στοιχεία, μεταξύ άλλων με την κατάρτιση ΚΥΛ. Ο ΚΥΛ μπορεί να παρέχει σε όσους κατασκευάζουν, αγοράζουν και χειρίζονται λογισμικό πληροφορίες που βελτιώνουν την κατανόηση της εφοδιαστικής αλυσίδας, γεγονός που έχει πολλαπλά οφέλη, ιδίως δε βοηθά τους κατασκευαστές και τους χρήστες να εντοπίζουν γνωστές νεοεμφανιζόμενες ευπάθειες και κινδύνους. Είναι ιδιαίτερα σημαντικό, οι κατασκευαστές να διασφαλίζουν ότι τα προϊόντα τους με ψηφιακά στοιχεία δεν περιέχουν ευπαθείς συνιστώσες που έχουν αναπτυχθεί από τρίτους. Οι κατασκευαστές δεν θα πρέπει να υποχρεούνται να δημοσιοποιούν το ΚΥΛ.

(78) Στο πλαίσιο των νέων σύνθετων επιχειρηματικών μοντέλων που συνδέονται με τις διαδικτυακές πωλήσεις, μια επιχείρηση που λειτουργεί επιγραμμικά μπορεί να παρέχει διάφορες υπηρεσίες. Ανάλογα με τη φύση των υπηρεσιών που παρέχονται σε σχέση με ένα δεδομένο προϊόν με ψηφιακά στοιχεία, η ίδια οντότητα μπορεί να εμπίπτει σε διαφορετικές κατηγορίες επιχειρηματικών μοντέλων ή οικονομικών φορέων. Όταν μια οντότητα παρέχει μόνο επιγραμμικές υπηρεσίες διαμεσολάβησης για ένα δεδομένο προϊόν με ψηφιακά στοιχεία και είναι απλώς πάροχος επιγραμμικής αγοράς, όπως ορίζεται στο άρθρο 3 παράγραφος 14 του κανονισμού (ΕΕ) 2023/988, δεν θεωρείται ότι εμπίπτει σε έναν από τους τύπους οικονομικών φορέων κατά την έννοια του παρόντος κανονισμού. Όταν η ίδια οντότητα είναι πάροχος επιγραμμικής αγοράς και ενεργεί επίσης ως οικονομικός φορέας, όπως ορίζεται στον παρόντα κανονισμό, για την πώληση συγκεκριμένων προϊόντων με ψηφιακά στοιχεία, θα πρέπει να υπόκειται στις υποχρεώσεις που καθορίζονται στον παρόντα κανονισμό για αυτόν τον τύπο οικονομικού φορέα. Για παράδειγμα, εάν πάροχος διαδικτυακής αγοράς διανέμει επίσης ένα προϊόν με ψηφιακά στοιχεία, θα θεωρείται όσον αφορά την πώληση του προϊόντος αυτού, ως διανομέας. Ομοίως, εάν η εν λόγω οντότητα πωλεί προϊόντα με δικό της σήμα, θα κατατασσόταν στους κατασκευαστές και θα έπρεπε, συνεπώς, να συμμορφώνεται με τις απαιτήσεις που ισχύουν για τους κατασκευαστές. Επίσης, ορισμένες οντότητες μπορούν να χαρακτηριστούν πάροχοι υπηρεσιών διεκπεραίωσης παραγγελιών, όπως ορίζονται στο άρθρο 3 σημείο 11) του κανονισμού (ΕΕ) 2019/1020 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[26], εάν προσφέρουν τέτοιες υπηρεσίες. Συνεπώς, οι περιπτώσεις αυτές θα πρέπει να αξιολογούνται κατά περίπτωση. Δεδομένου του εξέχοντος ρόλου που διαδραματίζουν οι επιγραμμικές αγορές στη διευκόλυνση του ηλεκτρονικού εμπορίου, θα πρέπει να προσπαθούν να συνεργάζονται με τις αρχές εποπτείας της αγοράς των κρατών μελών, προκειμένου να βοηθούν να διασφαλίζεται ότι τα προϊόντα με ψηφιακά στοιχεία που αγοράζονται μέσω επιγραμμικών αγορών συμμορφώνονται με τις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό.

---

26 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).

(79) 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 κυβερνοασφάλειας 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[27]. Ο εν λόγω κανονισμός προβλέπει διαδικασία διατύπωσης αντιρρήσεων σε εναρμονισμένα πρότυπα όταν τα εν λόγω πρότυπα δεν ικανοποιούν πλήρως τις απαιτήσεις του παρόντος κανονισμού. Η διαδικασία τυποποίησης θα πρέπει να διασφαλίζει ισόρροπη εκπροσώπηση των συμφερόντων και αποτελεσματική συμμετοχή των φορέων της κοινωνίας των πολιτών, συμπεριλαμβανομένων οργανισμών εκπροσώπησης των καταναλωτών. Θα πρέπει επίσης να λαμβάνονται υπόψη τα διεθνή πρότυπα που συνάδουν με το επίπεδο προστασίας της κυβερνοασφάλειας το οποίο επιδιώκεται από τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό, προκειμένου να διευκολυνθούν η ανάπτυξη εναρμονισμένων προτύπων και η εφαρμογή του παρόντος κανονισμού, καθώς και να διευκολυνθεί η συμμόρφωση των εταιρειών, ιδίως των πολύ μικρών και των μικρών και μεσαίων επιχειρήσεων, καθώς και εκείνων που δραστηριοποιούνται παγκοσμίως.

---

[27] 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).

(80) Η έγκαιρη ανάπτυξη εναρμονισμένων προτύπων κατά τη διάρκεια της μεταβατικής περιόδου για την εφαρμογή του παρόντος κανονισμού και η διαθεσιμότητά τους πριν από την ημερομηνία εφαρμογής του παρόντος κανονισμού θα είναι ιδιαίτερα σημαντική για την αποτελεσματική εφαρμογή του. Αυτό ισχύει ιδιαίτερα για σημαντικά προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στην κλάση I. Η διαθεσιμότητα εναρμονισμένων προτύπων θα επιτρέψει στους κατασκευαστές αυτών των προϊόντων να διενεργούν τις αξιολογήσεις της συμμόρφωσης μέσω της διαδικασίας εσωτερικού ελέγχου και, επομένως, να μπορούν να αποφεύγουν τα σημεία συμφόρησης και τις καθυστερήσεις στις δραστηριότητες των οργανισμών αξιολόγησης της συμμόρφωσης.

(81) Ο κανονισμός (ΕΕ) 2019/881 θεσπίζει εθελοντικό ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας για προϊόντα ΤΠΕ, διαδικασίες ΤΠΕ, και υπηρεσίες ΤΠΕ. Τα ευρωπαϊκά καθεστώτα πιστοποίησης κυβερνοασφάλειας παρέχουν ένα κοινό πλαίσιο εμπιστοσύνης για τους χρήστες όσον αφορά τη χρήση προϊόντων με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού. Ο παρών κανονισμός θα πρέπει επομένως 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 ευρωπαϊκού 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 κυβερνοασφάλειας που καθορίζονται στον παρόντα κανονισμό, εφόσον το ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας ή η δήλωση συμμόρφωσης ή μέρη τους καλύπτουν τις εν λόγω απαιτήσεις. Η ανάγκη για νέα ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία θα πρέπει να αξιολογηθεί υπό το πρίσμα του παρόντος κανονισμού, μεταξύ άλλων και κατά την προετοιμασία του κυλιόμενου προγράμματος εργασίας της Ένωσης σύμφωνα με τον κανονισμό (ΕΕ) 2019/881. Όταν υπάρχει ανάγκη για νέο σύστημα που να καλύπτει προϊόντα με ψηφιακά στοιχεία, μεταξύ άλλων για να διευκολυνθεί η συμμόρφωση με τον παρόντα κανονισμό, η Επιτροπή μπορεί να ζητά από τον ENISA να προετοιμάσει υποψήφια συστήματα σύμφωνα με το άρθρο 48 του κανονισμού (ΕΕ) 2019/881. Τα εν λόγω μελλοντικά ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας που καλύπτουν προϊόντα με ψηφιακά στοιχεία θα πρέπει να λαμβάνουν υπόψη τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας και τις διαδικασίες αξιολόγησης της συμμόρφωσης που ορίζονται στον παρόντα κανονισμό και να διευκολύνουν τη συμμόρφωση με τον παρόντα κανονισμό. Για τα ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας που τίθενται σε ισχύ πριν από την έναρξη ισχύος του παρόντος κανονισμού, ενδέχεται να χρειαστούν περαιτέρω προδιαγραφές σχετικά με λεπτομερείς πτυχές του τρόπου με τον οποίο μπορεί να εφαρμοστεί το τεκμήριο συμμόρφωσης.

Θα πρέπει να ανατεθεί μέσω κατ' εξουσιοδότηση πράξεων στην Επιτροπή η εξουσία να καθορίζει υπό ποιες προϋποθέσεις τα ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας μπορούν να χρησιμοποιηθούν για την απόδειξη της συμμόρφωσης με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό. Επιπλέον, προκειμένου να αποφευχθεί ο περιττός διοικητικός φόρτος για τους κατασκευαστές, δεν θα πρέπει να υπάρχει υποχρέωση των κατασκευαστών να διενεργούν αξιολόγηση της συμμόρφωσης από τρίτους, όπως προβλέπεται στον παρόντα κανονισμό για τις αντίστοιχες απαιτήσεις όταν ένα ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας έχει εκδοθεί στο πλαίσιο των εν λόγω ευρωπαϊκών καθεστώτων πιστοποίησης κυβερνοασφάλειας τουλάχιστον σε «σημαντικό» επίπεδο.

(82) Κατά την έναρξη ισχύος του εκτελεστικού κανονισμού (ΕΕ) 2024/482, ο οποίος αφορά προϊόντα που καλύπτονται από τον παρόντα κανονισμό, όπως μονάδες ασφάλειας υλισμικού και μικροεπεξεργαστές, η Επιτροπή θα πρέπει να είναι σε θέση να προσδιορίζει, μέσω κατ' εξουσιοδότηση πράξης, τον τρόπο με τον οποίο το EUCC παρέχει τεκμήριο συμμόρφωσης με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στο παράρτημα I του παρόντος κανονισμού ή με μέρη τους. Επιπλέον, η εν λόγω κατ' εξουσιοδότηση 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 απαιτείται σύμφωνα με τον παρόντα κανονισμό για τις αντίστοιχες απαιτήσεις.

(83) Το ισχύον ευρωπαϊκό πλαίσιο τυποποίησης, το οποίο βασίζεται στις αρχές της νέας προσέγγισης που καθορίζονται στο ψήφισμα του Συμβουλίου, της 7ης Μαΐου 1985, για νέα προσέγγιση στο θέμα της τεχνικής εναρμόνισης και τυποποίησης και στον κανονισμό (ΕΕ) αριθ. 1025/2012, αποτελεί το πλαίσιο για την εκπόνηση προτύπων που παρέχουν τεκμήριο συμμόρφωσης με τις σχετικές ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στον παρόντα κανονισμό. Τα ευρωπαϊκά πρότυπα θα πρέπει να διαμορφώνονται με γνώμονα την αγορά, να λαμβάνουν υπόψη το δημόσιο συμφέρον, καθώς και τους στόχους πολιτικής που διατυπώνονται ρητά στο αίτημα της Επιτροπής προς έναν ή περισσότερους ευρωπαϊκούς οργανισμούς τυποποίησης όσον αφορά την κατάρτιση εναρμονισμένων προτύπων τα οποία να αποτελούν προϊόν συναίνεσης, εντός καθορισμένης προθεσμίας. Ωστόσο, ελλείψει σχετικών παραπομπών σε εναρμονισμένα πρότυπα, η Επιτροπή θα πρέπει να είναι σε θέση να εκδίδει εκτελεστικές πράξεις σχετικά με τον καθορισμό κοινών προδιαγραφών για τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στον παρόντα κανονισμό, υπό την προϋπόθεση ότι σέβεται δεόντως τον ρόλο και τα καθήκοντα των οργανισμών τυποποίησης, ως έκτακτη εναλλακτική λύση προς διευκόλυνση του κατασκευαστή κατά την εκπλήρωση της υποχρέωσής του να συμμορφώνεται με τις εν λόγω ουσιώδεις απαιτήσεις κυβερνοασφάλειας, όταν παρεμποδίζεται η διαδικασία τυποποίησης ή όταν υπάρχουν καθυστερήσεις στη θέσπιση κατάλληλων εναρμονισμένων προτύπων. Εάν η καθυστέρηση αυτή οφείλεται στην τεχνική πολυπλοκότητα του εν λόγω προτύπου, η Επιτροπή θα πρέπει να λαμβάνει υπόψη το γεγονός αυτό πριν εξετάσει τη θέσπιση κοινών προδιαγραφών.

(84) Προκειμένου να καθοριστούν, με τον πλέον αποτελεσματικό τρόπο, κοινές προδιαγραφές που να καλύπτουν τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στον παρόντα κανονισμό, η Επιτροπή θα πρέπει να εξασφαλίσει τη συμμετοχή σχετικών ενδιαφερόμενων μερών στη διαδικασία.

(85) Ως «εύλογο χρονικό διάστημα» νοείται, σε σχέση με τη δημοσίευση αναφοράς σε εναρμονισμένα πρότυπα στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 1025/2012, περίοδος κατά την οποία αναμένεται η δημοσίευση στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* της αναφοράς στο πρότυπο, στο διορθωτικό του ή στην τροποποίησή του, και η οποία δεν θα πρέπει να υπερβαίνει το ένα έτος μετά τη λήξη της προθεσμίας για την κατάρτιση ευρωπαϊκού προτύπου που καθορίζεται σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 1025/2012.

(86) Προκειμένου να διευκολυνθεί η αξιολόγηση της συμμόρφωσης με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας 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.

(87) Η εφαρμογή εναρμονισμένων προτύπων, κοινών προδιαγραφών ή ευρωπαϊκών καθεστώτων πιστοποίησης της κυβερνοασφάλειας που εγκρίνονται σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 και παρέχουν τεκμήριο συμμόρφωσης σε σχέση με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ισχύουν για τα προϊόντα με ψηφιακά στοιχεία θα διευκολύνει την αξιολόγηση της συμμόρφωσης από τους κατασκευαστές. Εάν ο κατασκευαστής επιλέξει να μην εφαρμόσει τα εν λόγω μέσα για ορισμένες απαιτήσεις, πρέπει να αναφέρει στην τεχνική του τεκμηρίωση τον τρόπο με τον οποίο επιτυγχάνεται διαφορετικά η συμμόρφωση. Επιπλέον, η εφαρμογή εναρμονισμένων προτύπων, κοινών προδιαγραφών ή ευρωπαϊκών καθεστώτων πιστοποίησης της κυβερνοασφάλειας που εγκρίνονται σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 και παρέχουν τεκμήριο συμμόρφωσης των κατασκευαστών θα διευκολύνει τον έλεγχο της συμμόρφωσης των προϊόντων με ψηφιακά στοιχεία από τις αρχές εποπτείας της αγοράς. Συνεπώς, οι κατασκευαστές προϊόντων με ψηφιακά στοιχεία ενθαρρύνονται να εφαρμόζουν τα εν λόγω εναρμονισμένα πρότυπα, κοινές προδιαγραφές ή ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας.

(88) 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 κυβερνοασφάλειας που καθορίζονται στον παρόντα κανονισμό και, κατά περίπτωση, άλλης συναφούς ενωσιακής νομοθεσίας εναρμόνισης, από την οποία καλύπτεται το προϊόν με ψηφιακά στοιχεία. Ενδέχεται να απαιτείται από τους κατασκευαστές να συντάσσουν δήλωση συμμόρφωσης ΕΕ και από άλλες νομικές πράξεις 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 νομικές 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.

(89) 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[28]. 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 που καθορίζονται στον παρόντα κανονισμό.

---

28 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).

(90) Για να δοθεί η δυνατότητα στους οικονομικούς φορείς να αποδείξουν τη συμμόρφωση προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στον παρόντα κανονισμό, και για να μπορέσουν οι αρμόδιες αρχές να εξασφαλίσουν ότι τα προϊόντα με ψηφιακά στοιχεία που διατίθενται στην αγορά συμμορφώνονται προς αυτές τις απαιτήσεις, είναι αναγκαίο να προβλεφθούν διαδικασίες αξιολόγησης της συμμόρφωσης. Η απόφαση αριθ. 768/2008/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[29] 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 κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό θα πρέπει να βασίζονται 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 καλύπτουν ολόκληρο τον κύκλο ζωής των προϊόντων με ψηφιακά στοιχεία, συμπεριλαμβανομένων του προγραμματισμού, του σχεδιασμού, της ανάπτυξης ή της παραγωγής, της δοκιμής και της συντήρησης του προϊόντος με ψηφιακά στοιχεία.

---

[29] 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).

(91) Η αξιολόγηση της συμμόρφωσης προϊόντων με ψηφιακά στοιχεία που δεν αναφέρονται ως σημαντικά ή κρίσιμα προϊόντα με ψηφιακά στοιχεία στον παρόντα κανονισμό μπορεί να διενεργείται από τον κατασκευαστή με δική του ευθύνη σύμφωνα με τη διαδικασία εσωτερικού ελέγχου που βασίζεται στην ενότητα Α της απόφασης 768/2008/ΕΚ σύμφωνα με τον παρόντα κανονισμό. Το ίδιο ισχύει και για τις περιπτώσεις στις οποίες ένας κατασκευαστής επιλέγει να μην εφαρμόσει εν όλω ή εν μέρει εφαρμοστέο εναρμονισμένο πρότυπο, κοινή προδιαγραφή ή ευρωπαϊκό καθεστώς πιστοποίησης της κυβερνοασφάλειας. Ο κατασκευαστής διατηρεί την ευελιξία να επιλέγει αυστηρότερη διαδικασία αξιολόγησης της συμμόρφωσης με τη συμμετοχή τρίτου. Στο πλαίσιο της διαδικασίας αξιολόγησης της συμμόρφωσης εσωτερικού ελέγχου, ο κατασκευαστής διασφαλίζει και δηλώνει με αποκλειστική του ευθύνη ότι το προϊόν με ψηφιακά στοιχεία και οι διαδικασίες του κατασκευαστή πληρούν τις εφαρμοστέες ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στον παρόντα κανονισμό. Εάν ένα σημαντικό προϊόν με ψηφιακά στοιχεία κατατάσσεται στην κλάση Ι, απαιτείται πρόσθετη διασφάλιση για να αποδειχθεί η συμμόρφωση με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στον παρόντα κανονισμό. Ο κατασκευαστής θα πρέπει να εφαρμόζει εναρμονισμένα πρότυπα, κοινές προδιαγραφές ή ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας που θεσπίζονται σύμφωνα με τον κανονισμό (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 ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας, θα πρέπει να υποβάλλεται σε αξιολόγηση της συμμόρφωσης με τη συμμετοχή τρίτου (με βάση τις ενότητες Β και Γ ή την ενότητα Η). 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 στις ενότητες Β και Γ ή Η της απόφασης αριθ. 768/2008/ΕΚ έχουν επιλεγεί ως οι πλέον κατάλληλες για την αξιολόγηση της συμμόρφωσης σημαντικών 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 σημαντικών προϊόντων με ψηφιακά στοιχεία που εμπίπτουν στην κλάση ΙΙ, στην αξιολόγηση της συμμόρφωσης θα πρέπει πάντα να συμμετέχει τρίτο μέρος, ακόμη και όταν το προϊόν συμμορφώνεται πλήρως ή εν μέρει με εναρμονισμένα πρότυπα, κοινές προδιαγραφές ή ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας. Οι κατασκευαστές σημαντικών προϊόντων με ψηφιακά στοιχεία που κατατάσσονται στο ελεύθερο λογισμικό ανοικτού κώδικα θα πρέπει να μπορούν να ακολουθούν τη διαδικασία εσωτερικού ελέγχου με βάση την ενότητα Α, υπό την προϋπόθεση ότι θέτουν την τεχνική τεκμηρίωση στη διάθεση του κοινού.

(92) 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 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 καταφόρτωση ή να αντιγραφούν σε υλικά μέσα προτού τεθούν σε κυκλοφορία 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 κυβερνοασφάλειας που καθορίζονται στον παρόντα κανονισμό σε όλα τα στάδια σχεδιασμού, ανάπτυξης και παραγωγής.

(93) Όσον αφορά τις πολύ μικρές και τις μικρές επιχειρήσεις, προκειμένου να διασφαλιστεί η αναλογικότητα, είναι σκόπιμο να μειωθεί το διοικητικό κόστος, χωρίς να επηρεάζονται το επίπεδο προστασίας της κυβερνοασφάλειας των προϊόντων με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού ούτε οι ίσοι όροι ανταγωνισμού μεταξύ των κατασκευαστών. Είναι επομένως σκόπιμο, η Επιτροπή να θεσπίσει ένα απλουστευμένο έντυπο τεχνικού φακέλου με στόχο τις ανάγκες των πολύ μικρών και των μικρών επιχειρήσεων. Το απλουστευμένο έντυπο τεχνικού φακέλου που εγκρίνεται από την Επιτροπή θα πρέπει να καλύπτει όλα τα εφαρμοστέα στοιχεία που σχετίζονται με τον τεχνικό φάκελο που καθορίζεται στον παρόντα κανονισμό, και να προσδιορίζει τον τρόπο με τον οποίο μια πολύ μικρή ή μικρή επιχείρηση μπορεί να παράσχει τα ζητούμενα στοιχεία με συνοπτικό τρόπο, όπως η περιγραφή του σχεδιασμού, της ανάπτυξης και της παραγωγής του προϊόντος με ψηφιακά στοιχεία. Με τον τρόπο αυτό, το έντυπο θα συμβάλει στην ελάφρυνση του διοικητικού φόρτου συμμόρφωσης, παρέχοντας στις ενδιαφερόμενες επιχειρήσεις ασφάλεια δικαίου σχετικά με την έκταση και τις λεπτομέρειες των πληροφοριών που πρέπει να παρέχονται. Οι πολύ μικρές και οι μικρές επιχειρήσεις θα πρέπει να έχουν τη δυνατότητα να επιλέγουν να παρέχουν τα εφαρμοστέα στοιχεία που σχετίζονται με την τεχνική τεκμηρίωση σε εκτενή μορφή και να μην επωφελούνται από τη δυνατότητά τους να παρέχουν απλουστευμένη τεχνική μορφή.

(94) Για την προώθηση και την προστασία της καινοτομίας, είναι σημαντικό να λαμβάνονται ιδιαιτέρως υπόψη τα συμφέροντα των κατασκευαστών που είναι πολύ μικρές επιχειρήσεις ή μικρές ή μεσαίες επιχειρήσεις, ιδίως πολύ μικρές και μικρές επιχειρήσεις, συμπεριλαμβανομένων των νεοφυών επιχειρήσεων. Για τον σκοπό αυτό, τα κράτη μέλη θα μπορούσαν να αναπτύξουν πρωτοβουλίες απευθυνόμενες σε κατασκευαστές που είναι πολύ μικρές ή μικρές επιχειρήσεις, μεταξύ άλλων όσον αφορά την κατάρτιση, την ευαισθητοποίηση, την ενημέρωση, τις δοκιμές και τις δραστηριότητες αξιολόγησης της συμμόρφωσης από τρίτους, καθώς και τη δημιουργία δοκιμαστηρίων. Οι δαπάνες μετάφρασης που σχετίζονται με την υποχρεωτική τεκμηρίωση, όπως ο τεχνικός φάκελος και οι πληροφορίες και οι οδηγίες προς τον χρήστη που απαιτούνται σύμφωνα με τον παρόντα κανονισμό, καθώς και η επικοινωνία με τις αρχές, μπορεί να συνιστούν σημαντικό κόστος για τους κατασκευαστές, ιδίως για κατασκευαστές μικρότερου μεγέθους. Τα κράτη μέλη θα πρέπει να έχουν τη δυνατότητα να επιλέγουν, μία από τις γλώσσες που καθορίζουν και αποδέχονται για τη σχετική τεκμηρίωση κατασκευαστή και για την επικοινωνία με τους κατασκευαστές να είναι γλώσσα ευρέως κατανοητή από τον μεγαλύτερο δυνατό αριθμό χρηστών.

(95) Για τη διασφάλιση της απρόσκοπτης εφαρμογής του παρόντος κανονισμού, τα κράτη μέλη θα πρέπει να διασφαλίσουν, πριν από την ημερομηνία εφαρμογής του παρόντος κανονισμού, ότι υπάρχει επαρκής αριθμός διαθέσιμων κοινοποιημένων οργανισμών για τη διενέργεια αξιολογήσεων της συμμόρφωσης από τρίτους. Η Επιτροπή θα πρέπει να επιδιώκει να βοηθά τα κράτη μέλη και άλλα ενδιαφερόμενα μέρη στην προσπάθεια αυτή, προκειμένου να αποφεύγονται τα σημεία συμφόρησης και τα εμπόδια εισόδου στην αγορά για τους κατασκευαστές. Οι στοχευμένες δραστηριότητες κατάρτισης υπό την καθοδήγηση των κρατών μελών, μεταξύ άλλων, κατά περίπτωση, με την υποστήριξη της Επιτροπής, μπορούν να συμβάλουν στη διαθεσιμότητα ειδικευμένων επαγγελματιών, μεταξύ άλλων για την υποστήριξη των δραστηριοτήτων των κοινοποιημένων οργανισμών δυνάμει του παρόντος κανονισμού. Επιπλέον, εν όψει του κόστους που μπορεί να συνεπάγεται η αξιολόγηση της συμμόρφωσης από τρίτους, θα πρέπει να εξεταστούν πρωτοβουλίες χρηματοδότησης σε ενωσιακό και εθνικό επίπεδο που να αποσκοπούν στην ελάφρυνση του εν λόγω κόστους για τις πολύ μικρές και τις μικρές επιχειρήσεις.

(96) Προκειμένου να διασφαλιστεί η αναλογικότητα, οι οργανισμοί αξιολόγησης της συμμόρφωσης, κατά τον καθορισμό των τελών για τις διαδικασίες αξιολόγησης της συμμόρφωσης, θα πρέπει να λαμβάνουν υπόψη τα ειδικά συμφέροντα και τις ανάγκες των πολύ μικρών και των μικρών και μεσαίων επιχειρήσεων, συμπεριλαμβανομένων των νεοφυών επιχειρήσεων. Ειδικότερα, οι οργανισμοί αξιολόγησης της συμμόρφωσης θα πρέπει να εφαρμόζουν τη σχετική διαδικασία εξέτασης και τις δοκιμές που προβλέπονται στον παρόντα κανονισμό μόνο κατά περίπτωση και ακολουθώντας προσέγγιση βάσει κινδύνου.

(97) Οι στόχοι των ρυθμιστικών δοκιμαστηρίων θα πρέπει να συνίστανται στην προώθηση της καινοτομίας και της ανταγωνιστικότητας των επιχειρήσεων με τη δημιουργία ελεγχόμενων περιβαλλόντων δοκιμών πριν από τη θέση σε κυκλοφορία στην αγορά προϊόντων με ψηφιακά στοιχεία. Τα ρυθμιστικά δοκιμαστήρια θα πρέπει να συμβάλλουν στη βελτίωση της ασφάλειας δικαίου για όλους τους παράγοντες που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού και να διευκολύνουν και να επιταχύνουν την πρόσβαση στην αγορά της Ένωσης προϊόντων με ψηφιακά στοιχεία, ιδίως όταν παρέχονται από πολύ μικρές και μικρές επιχειρήσεις, συμπεριλαμβανομένων των νεοφυών επιχειρήσεων.

(98) Για τη διενέργεια αξιολόγησης της συμμόρφωσης από τρίτους, 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.

(99) 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.

(100) Οι οργανισμοί αξιολόγησης της συμμόρφωσης που έχουν διαπιστευτεί και κοινοποιηθεί βάσει του ενωσιακού δικαίου για τον καθορισμό απαιτήσεων παρόμοιων με εκείνες που ορίζονται στον παρόντα κανονισμό, όπως οι οργανισμοί αξιολόγησης της συμμόρφωσης που έχουν κοινοποιηθεί για ευρωπαϊκό καθεστώς πιστοποίησης κυβερνοασφάλειας και είναι εγκεκριμένοι σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 ή έχουν κοινοποιηθεί δυνάμει του κατ' εξουσιοδότηση κανονισμού (ΕΕ) 2022/30, θα πρέπει να αξιολογηθούν και να κοινοποιηθούν εκ νέου δυνάμει του παρόντος κανονισμού. Ωστόσο, οι αρμόδιες αρχές μπορούν να καθορίσουν συνέργειες όσον αφορά τυχόν αλληλεπικαλυπτόμενες απαιτήσεις, προκειμένου να αποφευχθεί ο περιττός οικονομικός και διοικητικός φόρτος και να διασφαλιστεί η ομαλή και έγκαιρη διαδικασία κοινοποίησης.

(101) 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.

(102) 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 τίθενται σε κυκλοφορία 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.

(103) 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.

(104) 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.

(105) 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.

(106) Η εποπτεία της αγοράς αποτελεί βασικό εργαλείο για τη διασφάλιση της ορθής και ομοιόμορφης εφαρμογής του δικαίου της Ένωσης. Είναι επομένως 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 στην ενωσιακή αγορά, όπως προβλέπονται στον κανονισμό (ΕΕ) 2019/1020, εφαρμόζονται στα προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού.

(107) Σύμφωνα με τον κανονισμό (ΕΕ) 2019/1020, μια αρχή εποπτείας της αγοράς διενεργεί εποπτεία της αγοράς στην επικράτεια του κράτους μέλους που την ορίζει. Ο παρών κανονισμός δεν θα πρέπει να εμποδίζει τα κράτη μέλη να επιλέγουν τις αρμόδιες αρχές που θα ασκούν τα καθήκοντα εποπτείας της αγοράς. Κάθε κράτος μέλος θα πρέπει να ορίζει μία ή περισσότερες αρχές εποπτείας της αγοράς στο έδαφός του.Τα κράτη μέλη θα πρέπει να έχουν τη δυνατότητα να επιλέξουν να ορίσουν οποιαδήποτε υφιστάμενη ή νέα αρχή που θα ενεργεί ως αρχή εποπτείας της αγοράς, συμπεριλαμβανομένων των αρμόδιων αρχών που ορίζονται ή συστήνονται δυνάμει του άρθρου 8 της οδηγίας (ΕΕ) 2022/2555, εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας που ορίζονται δυνάμει του άρθρου 58 του κανονισμού (ΕΕ) 2019/881 ή των αρχών εποπτείας της αγοράς που ορίζονται για τους σκοπούς της οδηγίας 2014/53/ΕΕ. 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 της αγοράς 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 της αγοράς και για τη συνδρομή στη συνεργασία μεταξύ των αρχών εποπτείας της αγοράς στα διάφορα κράτη μέλη.

(108) Θα πρέπει να συσταθεί ειδική ομάδα διοικητικής συνεργασίας (ΕΟΔΚ) για την κυβερνοανθεκτικότητα προϊόντων με ψηφιακά στοιχεία για την ομοιόμορφη εφαρμογή του παρόντος κανονισμού, σύμφωνα με το άρθρο 30 παράγραφος 2 του κανονισμού (ΕΕ) 2019/1020. Η ΕΟΔΚ 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 υποστηρίζει και να ενθαρρύνει τη συνεργασία μεταξύ των αρχών εποπτείας της αγοράς μέσω του Ενωσιακού Δικτύου Συμμόρφωσης των Προϊόντων, το οποίο έχει συσταθεί σύμφωνα με το άρθρο 29 του κανονισμού (ΕΕ) 2019/1020 και απαρτίζεται από εκπροσώπους από κάθε κράτος μέλος, συμπεριλαμβανομένου ενός εκπροσώπου κάθε ενιαίου γραφείου σύνδεσης όπως αναφέρεται στο άρθρο 10 του εν λόγω κανονισμού και ενός προαιρετικού εθνικού εμπειρογνώμονα, των προέδρων των ΕΟΔΚ και εκπροσώπων της Επιτροπής. Η Επιτροπή θα πρέπει να συμμετέχει στις συνεδριάσεις του Ενωσιακού Δικτύου Συμμόρφωσης Προϊόντων, των υποομάδων του και της αντίστοιχης ΕΟΔΚ. Θα πρέπει επίσης να συνδράμει την ΕΟΔΚ μέσω μιας εκτελεστικής γραμματείας για την παροχή τεχνικής και υλικοτεχνικής υποστήριξης. Η ΕΟΔΚ μπορεί επίσης να καλεί ανεξάρτητους ειδικούς να συμμετάσχουν και να έρθουν σε επαφή με άλλες ΕΟΔΚ, όπως αυτή που θεσπίστηκε δυνάμει της οδηγίας 2014/53/ΕΕ.

(109) Οι αρχές εποπτείας της αγοράς, μέσω της ΕΟΔΚ που θεσπίζεται δυνάμει του παρόντος κανονισμού, θα πρέπει να συνεργάζονται στενά και να είναι σε θέση να καταρτίζουν έγγραφα καθοδήγησης για τη διευκόλυνση των δραστηριοτήτων εποπτείας της αγοράς σε εθνικό επίπεδο, όπως με την ανάπτυξη βέλτιστων πρακτικών και δεικτών για τον αποτελεσματικό έλεγχο της συμμόρφωσης των προϊόντων με ψηφιακά στοιχεία με τον παρόντα κανονισμό.

(110) 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 προβλέπεται 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 νωρίτερο 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.

(111) 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, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των υπηρεσιών που προσφέρονται με τη χρήση ηλεκτρονικού συστήματος πληροφοριών από βασικές οντότητες όπως αναφέρονται στο άρθρο 3 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555, ή για άλλες πτυχές προστασίας του δημόσιου συμφέροντος. Για τούτο, είναι αναγκαίο να θεσπιστούν κανόνες που να διασφαλίζουν τον μετριασμό των εν λόγω κινδύνων. Συνεπώς, 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 ψηφιακά στοιχεία 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 με ψηφιακά στοιχεία 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 σχετικό οικονομικό φορέα ή στους σχετικούς οικονομικούς φορείς. Εάν το μέτρο θεωρηθεί δικαιολογημένο, η Επιτροπή θα πρέπει επίσης να εξετάσει το ενδεχόμενο έκδοσης προτάσεων για την αναθεώρηση του σχετικού ενωσιακού δικαίου.

(112) 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, τη συμμόρφωση προς τις υποχρεώσεις δυνάμει του ενωσιακού ή του εθνικού δικαίου για την προστασία των θεμελιωδών δικαιωμάτων ή για τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των υπηρεσιών από βασικές οντότητες όπως αναφέρονται στο άρθρο 3 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555, η Επιτροπή θα πρέπει να έχει τη δυνατότητα να ζητήσει από τον ENISA να διενεργήσει αξιολόγηση. Με βάση την εν λόγω αξιολόγηση, η Επιτροπή θα πρέπει να έχει τη δυνατότητα να θεσπίσει, μέσω εκτελεστικών πράξεων, διορθωτικά ή περιοριστικά μέτρα σε επίπεδο Ένωσης, συμπεριλαμβανομένης απαίτησης για απόσυρση των εν λόγω προϊόντων με ψηφιακά στοιχεία από την αγορά ή της ανάκλησής τους, εντός εύλογου χρονικού διαστήματος, ανάλογου προς τη φύση του κινδύνου. Η Επιτροπή θα πρέπει να έχει τη δυνατότητα να κάνει χρήση της παρέμβασης αυτής μόνο σε εξαιρετικές περιστάσεις που αιτιολογούν άμεση παρέμβαση για τη διατήρηση της ορθής λειτουργίας της εσωτερικής αγοράς, και μόνον εφόσον δεν έχουν ληφθεί αποτελεσματικά μέτρα από τις αρχές εποπτείας της αγοράς για την αντιμετώπιση της κατάστασης. Τέτοιες εξαιρετικές περιστάσεις μπορεί να είναι καταστάσεις έκτακτης ανάγκης, όταν, για παράδειγμα, ένα μη συμμορφούμενο προϊόν με ψηφιακά στοιχεία διατίθεται ευρέως από τον κατασκευαστή σε διάφορα κράτη μέλη, χρησιμοποιείται επίσης σε βασικούς τομείς από οντότητες που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας (ΕΕ) 2022/2555, ενώ περιέχει γνωστές ευπάθειες, τις οποίες εκμεταλλεύονται κακόβουλοι παράγοντες και για τις οποίες ο κατασκευαστής δεν παρέχει διαθέσιμο διορθωτικό λογισμικό. Η Επιτροπή θα πρέπει να έχει τη δυνατότητα 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.

(113) Όταν 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.

(114) 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, σαρώσεις θα πρέπει να διεξάγονται σε περιπτώσεις κατά τις οποίες τάσεις της αγοράς, καταγγελίες καταναλωτών ή άλλες ενδείξεις υποδεικνύουν ότι ορισμένες κατηγορίες προϊόντων με ψηφιακά στοιχεία διαπιστώνεται συχνά ότι παρουσιάζουν σοβαρούς κινδύνους για την κυβερνοασφάλεια. Επιπλέον, κατά τον καθορισμό των κατηγοριών προϊόντων που πρόκειται να υποβληθούν σε σαρώσεις, οι αρχές εποπτείας της αγοράς θα πρέπει επίσης να λαμβάνουν υπόψη παράγοντες που σχετίζονται με μη τεχνικούς παράγοντες κινδύνου. Για τον σκοπό αυτό, οι αρχές εποπτείας της αγοράς θα πρέπει να έχουν τη δυνατότητα να λαμβάνουν υπόψη το αποτέλεσμα της συντονισμένης σε επίπεδο Ένωσης εκτίμησης κινδύνου για την ασφάλεια κρίσιμων εφοδιαστικών αλυσίδων που διενεργείται σύμφωνα με το άρθρο 22 της οδηγίας (ΕΕ) 2022/2555, συμπεριλαμβανομένων των μη τεχνικών παραγόντων κινδύνου. Ο ENISA θα πρέπει να υποβάλλει στις αρχές εποπτείας της αγοράς προτάσεις για κατηγορίες προϊόντων με ψηφιακά στοιχεία για τις οποίες θα πρέπει σαν να οργανωθούν σαρώσεις, με βάση, μεταξύ άλλων, τις κοινοποιήσεις σχετικά με ευπάθειες των προϊόντων και περιστατικά τις οποίες λαμβάνει.

(115) Εν όψει της πραγματογνωσίας και της εντολής του, ο ENISA θα πρέπει να είναι σε θέση να υποστηρίζει τη διαδικασία εφαρμογής του παρόντος κανονισμού. Ειδικότερα, ο ENISA 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 σαρώσεις. 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 ορθής λειτουργίας της εσωτερικής αγοράς.

(116) Ο παρών κανονισμός αναθέτει στον ENISA ορισμένα καθήκοντα, τα οποία απαιτούν κατάλληλους πόρους, τόσο από την άποψη της πραγματογνωσίας όσο και από την άποψη των ανθρώπινων πόρων, ώστε ο ENISA να είναι σε θέση να εκτελεί αποτελεσματικά τα εν λόγω καθήκοντα. Η Επιτροπή θα προτείνει τους αναγκαίους δημοσιονομικούς πόρους για τον πίνακα προσωπικού του ENISA, σύμφωνα με τη διαδικασία που ορίζεται στο άρθρο 29 του κανονισμού (ΕΕ) 2019/881, κατά την κατάρτιση του σχεδίου γενικού προϋπολογισμού της Ένωσης. Κατά τη διάρκεια της εν λόγω διαδικασίας, η Επιτροπή θα εξετάσει τους συνολικούς πόρους του ENISA ώστε να μπορέσει να εκπληρώσει τα καθήκοντά του, συμπεριλαμβανομένων εκείνων που ανατίθενται στον ENISA δυνάμει του παρόντος κανονισμού.

(117) Προκειμένου να διασφαλιστεί η δυνατότητα για τις απαιτούμενες προσαρμογές του ρυθμιστικού πλαισίου, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων σύμφωνα με το άρθρο 290 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) όσον αφορά την επικαιροποίηση παραρτήματος στο οποίο απαριθμούνται τα σημαντικά προϊόντα με ψηφιακά στοιχεία. 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, δυνάμει ευρωπαϊκού καθεστώτος πιστοποίησης της κυβερνοασφάλειας, των κρίσιμων προϊόντων με ψηφιακά στοιχεία που καθορίζονται σε παράρτημα του παρόντος κανονισμού, καθώς και για την επικαιροποίηση του καταλόγου κρίσιμων προϊόντων με ψηφιακά στοιχεία βάσει κριτηρίων κρισιμότητας που καθορίζονται στον παρόντα κανονισμό, και για τον προσδιορισμό των ευρωπαϊκών καθεστώτων πιστοποίησης της κυβερνοασφάλειας που εγκρίνονται σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 και τα οποία μπορούν να χρησιμοποιηθούν για την απόδειξη της συμμόρφωσης με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας ή μέρη τους, όπως ορίζεται σε παράρτημα του παρόντος κανονισμού. Θα πρέπει επίσης να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων για τον καθορισμό της ελάχιστης περιόδου υποστήριξης για συγκεκριμένες κατηγορίες προϊόντων για τις οποίες τα δεδομένα εποπτείας της αγοράς υποδεικνύουν ανεπαρκείς περιόδους υποστήριξης, καθώς και για τον καθορισμό των όρων και των προϋποθέσεων για την επίκληση λόγων κυβερνοασφάλειας σε σχέση με την καθυστέρηση της διάδοσης των κοινοποιήσεων ευπαθειών που αποτελούν αντικείμενο ενεργού εκμετάλλευσης.

Επιπλέον, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων για τη θέσπιση εθελοντικών προγραμμάτων πιστοποίησης ασφάλειας για την αξιολόγηση της συμμόρφωσης προϊόντων με ψηφιακά στοιχεία που κατατάσσονται στο ελεύθερο λογισμικό ανοικτού κώδικα με όλες ή ορισμένες από τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας ή άλλες υποχρεώσεις που ορίζονται στον παρόντα κανονισμό, καθώς και για τον καθορισμό 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, οι οποίες να πραγματοποιούνται σύμφωνα με τις αρχές που ορίζονται στη διοργανική συμφωνία της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου[30]. Πιο συγκεκριμένα, προκειμένου να διασφαλιστεί 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. Η εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων σύμφωνα με τον παρόντα κανονισμό θα πρέπει να ανατίθεται στην Επιτροπή για χρονικό διάστημα πέντε ετών από ... [ημερομηνία έναρξης ισχύος του παρόντος κανονισμού]. Η Επιτροπή θα πρέπει να υποβάλει έκθεση σχετικά με τις εξουσίες που της έχουν ανατεθεί το αργότερο εννέα μήνες πριν από τη λήξη της περιόδου των πέντε ετών. Η εξουσιοδότηση θα πρέπει να ανανεώνεται σιωπηρά για περιόδους ίδιας διάρκειας, εκτός αν το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο προβάλει αντιρρήσεις το αργότερο τρεις μήνες πριν από τη λήξη της κάθε περιόδου.

[30] ΕΕ L 123 της 12.5.2016, σ. 1.

(118) Προκειμένου να διασφαλιστούν ενιαίες προϋποθέσεις για την εφαρμογή του παρόντος κανονισμού, θα πρέπει να ανατεθούν στην Επιτροπή εκτελεστικές αρμοδιότητες για τον καθορισμό της τεχνικής περιγραφής των κατηγοριών σημαντικών προϊόντων με ψηφιακά στοιχεία που ορίζονται σε παράρτημα του παρόντος κανονισμού, για τον καθορισμό του μορφότυπου και των στοιχείων του ΚΥΛ, για τον περαιτέρω προσδιορισμό του μορφότυπου και της διαδικασίας των κοινοποιήσεων ευπαθειών και σοβαρών περιστατικών που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και σοβαρών περιστατικών που έχουν αντίκτυπο στην ασφάλεια των προϊόντων με ψηφιακά στοιχεία, υποβαλλόμενων από τους κατασκευαστές, καθώς και για τη θέσπιση κοινών προδιαγραφών που καλύπτουν τεχνικές απαιτήσεις οι οποίες παρέχουν μέσο συμμόρφωσης με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται σε παράρτημα του παρόντος κανονισμού, καθορίζουν τεχνικές προδιαγραφές για τις ετικέτες, τα εικονογράμματα ή οποιαδήποτε άλλα σήματα που σχετίζονται με την ασφάλεια των προϊόντων με ψηφιακά στοιχεία, την περίοδο υποστήριξής τους και μηχανισμούς για την προώθηση της χρήσης τους και την αύξηση της ευαισθητοποίησης του κοινού σχετικά με την ασφάλεια των προϊόντων με ψηφιακά στοιχεία, προσδιορίζουν το απλουστευμένο έντυπο τεκμηρίωσης που στοχεύει στις ανάγκες των πολύ μικρών και των μικρών επιχειρήσεων και αποφασίζουν σχετικά με διορθωτικά ή περιοριστικά μέτρα σε επίπεδο Ένωσης σε εξαιρετικές περιστάσεις που δικαιολογούν άμεση παρέμβαση για τη διατήρηση της ορθής 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[31].

(119) 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.

---

[31] 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, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(120) 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 ο κατασκευαστής είναι πολύ μικρή, μικρή ή μεσαία επιχείρηση, συμπεριλαμβανομένων των νεοφυών επιχειρήσεων και του κατά πόσον έχουν ήδη επιβληθεί διοικητικά πρόστιμα από τις ίδιες ή άλλες αρχές εποπτείας της αγοράς στον ίδιο οικονομικό φορέα για παρόμοιες παραβάσεις. Οι περιστάσεις αυτές θα μπορούσαν να είναι επιβαρυντικές, σε περιπτώσεις κατά τις οποίες η παράβαση από τον ίδιο οικονομικό φορέα συνεχίζεται στο έδαφος άλλων κρατών μελών άλλων από εκείνο 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. Δεδομένου ότι τα διοικητικά πρόστιμα δεν επιβάλλονται σε πολύ μικρές ή μικρές επιχειρήσεις για μη τήρηση της προθεσμίας των 24 ωρών για την κοινοποίηση έγκαιρης προειδοποίησης σχετικά με ευπάθειες ή σοβαρά περιστατικά που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και έχουν αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία, ούτε σε υποστηρικτές λογισμικού ανοικτού κώδικα για οποιαδήποτε παράβαση του παρόντος κανονισμού, και με την επιφύλαξη της αρχής ότι οι ποινές θα πρέπει να είναι αποτελεσματικές, αναλογικές και αποτρεπτικές, τα κράτη μέλη δεν θα πρέπει να επιβάλλουν άλλα είδη χρηματικών ποινών στις εν λόγω οντότητες.

(121) Όταν επιβάλλονται διοικητικά πρόστιμα 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.

(122) Τα κράτη μέλη θα πρέπει να εξετάσουν, λαμβάνοντας υπόψη τις εθνικές συνθήκες, τη δυνατότητα, τα έσοδα από τις κυρώσεις που προβλέπονται στον παρόντα κανονισμό ή το οικονομικό ισοδύναμό τους να χρησιμοποιηθούν για τη στήριξη πολιτικών κυβερνοασφάλειας και την αύξηση του επιπέδου κυβερνοασφάλειας στην Ένωση, μεταξύ άλλων με την αύξηση του αριθμού των ειδικευμένων επαγγελματιών στον τομέα της κυβερνοασφάλειας, την ενίσχυση της ανάπτυξης ικανοτήτων για τις πολύ μικρές και τις μικρές και μεσαίες επιχειρήσεις και τη βελτίωση της ευαισθητοποίησης του κοινού σχετικά με τις κυβερνοαπειλές.

(123) Η Ένωση, 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 με αρκετές τρίτες χώρες. Οι εν λόγω ΣΑΑ συμφωνίες αφορούν συγκεκριμένους τομείς που ενδέχεται να διαφέρουν από τρίτη χώρα σε τρίτη 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 ΣΛΕΕ. Η συνεργασία με τις τρίτες 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 Ένωσης.

(124) Οι καταναλωτές θα πρέπει να έχουν το δικαίωμα να επιβάλλουν τα δικαιώματά τους σε σχέση με τις υποχρεώσεις που επιβάλλονται στους οικονομικούς φορείς δυνάμει του παρόντος κανονισμού μέσω της άσκησης αντιπροσωπευτικών αγωγών σύμφωνα με την οδηγία (ΕΕ) 2020/1828 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[32]. Για τον σκοπό αυτό, ο παρών κανονισμός θα πρέπει να προβλέπει ότι η οδηγία (ΕΕ) 2020/1828 εφαρμόζεται στις αντιπροσωπευτικές αγωγές που αφορούν παραβάσεις του παρόντος κανονισμού οι οποίες θίγουν ή μπορούν να θίξουν τα συλλογικά συμφέροντα των καταναλωτών. Συνεπώς, το παράρτημα Ι της εν λόγω οδηγίας θα πρέπει να τροποποιηθεί αναλόγως. Εναπόκειται στα κράτη μέλη να διασφαλίσουν ότι οι τροποποιήσεις αυτές θα αποτυπώνονται στα μέτρα μεταφοράς στο εθνικό δίκαιο που θεσπίζουν σύμφωνα με την εν λόγω οδηγία, παρά το γεγονός ότι η θέσπιση σχετικών μέτρων μεταφοράς στο εθνικό δίκαιο δεν αποτελεί προϋπόθεση για τη δυνατότητα εφαρμογής της εν λόγω οδηγίας όσον αφορά τις αντιπροσωπευτικές αγωγές. Η εφαρμογή της εν λόγω οδηγίας στις αντιπροσωπευτικές αγωγές που ασκούνται σε σχέση με παραβάσεις των διατάξεων του παρόντος κανονισμού από οικονομικούς φορείς που βλάπτουν ή θα μπορούσαν να βλάψουν τα συλλογικά συμφέροντα των καταναλωτών θα πρέπει να αρχίσει από ... [36 μήνες από την έναρξη ισχύος του παρόντος κανονισμού].

(125) Η Επιτροπή θα πρέπει να αξιολογεί και να επανεξετάζει περιοδικά τον παρόντα κανονισμό, σε διαβούλευση με τους σχετικούς συμφεροντούχους, ιδίως προκειμένου να εξακριβώνεται αν απαιτείται τροποποίησή του υπό το πρίσμα της μεταβολής συνθηκών στην κοινωνία, την πολιτική, την τεχνολογία ή τις αγορές. Ο παρών κανονισμός θα διευκολύνει τη συμμόρφωση με τις υποχρεώσεις ασφάλειας της εφοδιαστικής αλυσίδας των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού (ΕΕ) 2022/2554 και της οδηγίας (ΕΕ) 2022/2555 και χρησιμοποιούν προϊόντα με ψηφιακά στοιχεία. Η Επιτροπή θα πρέπει να αξιολογήσει, στο πλαίσιο της εν λόγω περιοδικής επανεξέτασης, τα συνδυασμένα αποτελέσματα του ενωσιακού πλαισίου κυβερνοασφάλειας.

---

32 Οδηγία (ΕΕ) 2020/1828 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2020, σχετικά με τις αντιπροσωπευτικές αγωγές για την προστασία των συλλογικών συμφερόντων των καταναλωτών και για την κατάργηση της οδηγίας 2009/22/ΕΚ (ΕΕ L 409 της 4.12.2020, σ. 1).

(126) Θα πρέπει να δοθεί επαρκής χρόνος στους οικονομικούς φορείς ώστε να προσαρμοστούν στις απαιτήσεις του παρόντος κανονισμού. Ο παρών κανονισμός θα πρέπει να ισχύσει από ... [36 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], με εξαίρεση τις υποχρεώσεις αναφοράς σχετικά με ευπάθειες που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και τα σοβαρά περιστατικά που έχουν αντίκτυπο στην ασφάλεια προϊόντων με ψηφιακά στοιχεία, οι οποίες θα πρέπει να ισχύσουν από... [21 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού] και των διατάξεων σχετικά με την κοινοποίηση των φορέων αξιολόγησης της συμμόρφωσης, οι οποίες θα πρέπει να ισχύσουν από ... [18 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού].

(127) Είναι σημαντικό να παρασχεθεί στήριξη στις πολύ μικρές και τις μικρές και μεσαίες επιχειρήσεις, συμπεριλαμβανομένων των νεοφυών επιχειρήσεων, κατά την εφαρμογή του παρόντος κανονισμού και να ελαχιστοποιηθούν οι κίνδυνοι για την εφαρμογή που απορρέουν από την έλλειψη γνώσεων και πραγματογνωσίας στην αγορά, καθώς και προκειμένου να διευκολυνθεί η συμμόρφωση των κατασκευαστών με τις υποχρεώσεις τους που ορίζονται στον παρόντα κανονισμό. Το πρόγραμμα «Ψηφιακή Ευρώπη» και άλλα συναφή προγράμματα της Ένωσης παρέχουν χρηματοδοτική και τεχνική υποστήριξη που επιτρέπει στις επιχειρήσεις αυτές να συμβάλλουν στην ανάπτυξη της οικονομίας της Ένωσης και στην ενίσχυση του κοινού επιπέδου κυβερνοασφάλειας στην Ένωση. Το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Θέματα Κυβερνοασφάλειας και τα εθνικά κέντρα συντονισμού, όπως επίσης οι ευρωπαϊκοί κόμβοι ψηφιακής καινοτομίας που δημιουργούνται από την Επιτροπή και τα κράτη μέλη σε ενωσιακό ή εθνικό επίπεδο θα μπορούσαν επίσης να υποστηρίξουν εταιρείες και οργανισμούς του δημόσιου τομέα και θα μπορούσαν να συμβάλουν στην εφαρμογή του παρόντος κανονισμού. Στο πλαίσιο των αντίστοιχων αποστολών και πεδίων αρμοδιότητάς τους, θα μπορούσαν να παρέχουν τεχνική και επιστημονική υποστήριξη σε πολύ μικρές και μικρομεσαίες επιχειρήσεις, όπως για δραστηριότητες δοκιμών και αξιολογήσεις της συμμόρφωσης από τρίτους. Θα μπορούσαν επίσης να προωθήσουν την ανάπτυξη εργαλείων για τη διευκόλυνση της εφαρμογής του παρόντος κανονισμού.

(128) Επιπλέον, τα κράτη μέλη θα πρέπει να εξετάσουν τη δυνατότητα ανάληψης συμπληρωματικής δράσης για την παροχή καθοδήγησης και στήριξης στις πολύ μικρές, τις μικρές και τις μεσαίες επιχειρήσεις, όπως μέσω της δημιουργίας ρυθμιστικών δοκιμαστηρίων και ειδικών διαύλων επικοινωνίας. Προκειμένου να ενισχυθεί το επίπεδο κυβερνοασφάλειας στην Ένωση, τα κράτη μέλη μπορούν επίσης να εξετάσουν το ενδεχόμενο παροχής στήριξης για την ανάπτυξη ικανοτήτων και δεξιοτήτων που σχετίζονται με την κυβερνοασφάλεια προϊόντων με ψηφιακά στοιχεία, τη βελτίωση της κυβερνοανθεκτικότητας των οικονομικών φορέων, ιδίως των πολύ μικρών και των μικρών και μεσαίων επιχειρήσεων, και την προώθηση της ευαισθητοποίησης του κοινού σχετικά με την κυβερνοασφάλεια προϊόντων με ψηφιακά στοιχεία.

(129) Δεδομένου ότι ο στόχος του παρόντος κανονισμού δεν μπορεί να επιτευχθεί επαρκώς από τα κράτη μέλη, μπορεί όμως, λόγω των επιπτώσεων της δράσης, 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 διατυπώνεται στο ίδιο άρθρο, ο παρών κανονισμός δεν υπερβαίνει τα αναγκαία όρια για την επίτευξη των στόχων αυτών.

(130) Ζητήθηκε, σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[33], η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων και του Συμβουλίου, ο οποίος γνωμοδότησε στις 9 Νοεμβρίου 2022[34],

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

---

[33] 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).

[34] ΕΕ C 452 της 29.11.2022, σ. 23.

ΚΕΦΑΛΑΙΟ I
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 κυβερνοασφάλειας 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 κυβερνοασφάλειας για τις διαδικασίες χειρισμού ευπαθειών που εφαρμόζουν οι κατασκευαστές με σκοπό τη διασφάλιση της κυβερνοασφάλειας προϊόντων με ψηφιακά στοιχεία κατά το διάστημα κατά το οποίο αναμένεται ότι θα χρησιμοποιούνται, καθώς και υποχρεώσεις για τους οικονομικούς φορείς σε σχέση με τις εν λόγω διαδικασίες·

δ) κανόνες για την εποπτεία της αγοράς, συμπεριλαμβανομένης της παρακολούθησης, και για την επιβολή των κανόνων και των απαιτήσεων που αναφέρονται στο παρόν άρθρο.

Άρθρο 2

Πεδίο εφαρμογής

1. Ο παρών κανονισμός εφαρμόζεται σε προϊόντα με ψηφιακά στοιχεία που διατίθενται στην αγορά των οποίων ο προβλεπόμενος σκοπός ή η 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 νομικές 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. Ο παρών κανονισμός δεν εφαρμόζεται σε εξοπλισμό που εμπίπτει στο πεδίο εφαρμογής της οδηγίας 2014/90/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[35].

[35] Οδηγία 2014/90/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με τον εξοπλισμό πλοίων και για την κατάργηση της οδηγίας 96/98/ΕΚ του Συμβουλίου (ΕΕ L 257 της 28.8.2014, σ. 146).

5. 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 κυβερνοασφάλειας που ορίζονται στο παράρτημα I 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 ή υψηλότερο επίπεδο προστασίας από εκείνο που προβλέπεται στον παρόντα κανονισμό.

Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 61, προκειμένου να συμπληρώσει τον παρόντα κανονισμό προσδιορίζοντας αν ο εν λόγω περιορισμός ή αποκλεισμός είναι αναγκαίος, τα σχετικά προϊόντα και τους σχετικούς κανόνες, καθώς και το πεδίο εφαρμογής του περιορισμού, κατά περίπτωση.

6. Ο παρών κανονισμός δεν εφαρμόζεται στα ανταλλακτικά που διατίθενται στην αγορά για την αντικατάσταση πανομοιότυπων δομοστοιχείων σε προϊόντα με ψηφιακά στοιχεία και τα οποία κατασκευάζονται σύμφωνα με τις ίδιες προδιαγραφές με τα δομοστοιχεία τα οποία πρόκειται να αντικαταστήσουν.

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

8. Οι υποχρεώσεις που προβλέπονται στον παρόντα κανονισμό δεν συνεπάγονται την παροχή πληροφοριών, η γνωστοποίηση των οποίων θα ήταν αντίθετη προς τα ουσιώδη συμφέροντα εθνικής ασφάλειας, δημόσιας ασφάλειας ή άμυνας των κρατών μελών.

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 δομοστοιχείων λογισμικού ή υλισμικού που τίθενται σε κυκλοφορία στην αγορά χωριστά·

2) «εξ αποστάσεως επεξεργασία δεδομένων»: 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) «κυβερνοασφάλεια»: η κυβερνοασφάλεια όπως ορίζεται στο άρθρο 2 σημείο 1 του κανονισμού (ΕΕ) 2019/881·

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

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

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

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

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

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

10) «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·

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

12) «οικονομικός φορέας»: ο κατασκευαστής, ο εξουσιοδοτημένος αντιπρόσωπος, ο εισαγωγέας, ο διανομέας, ή άλλο φυσικό ή νομικό πρόσωπο που υπέχει υποχρεώσεις σχετικά με την κατασκευή προϊόντων με ψηφιακά στοιχεία ή σε σχέση με τη διάθεση στην αγορά προϊόντων με ψηφιακά στοιχεία σύμφωνα με τον παρόντα κανονισμό·

13) «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 πληρωμής ή οικονομικού οφέλους είτε δωρεάν·

14) «υποστηρικτής λογισμικού ανοικτού κώδικα»: νομικό πρόσωπο, άλλο από τον κατασκευαστή, το οποίο έχει σκοπό ή στόχο να παρέχει συστηματικά υποστήριξη σε διαρκή βάση για την ανάπτυξη συγκεκριμένων προϊόντων με ψηφιακά στοιχεία, που κατατάσσονται στο ελεύθερο λογισμικό ανοικτού κώδικα και προορίζονται για εμπορικές δραστηριότητες, και το οποίο διασφαλίζει τη βιωσιμότητα των εν λόγω προϊόντων·

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

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

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

18) «καταναλωτής»: φυσικό πρόσωπο το οποίο ενεργεί για σκοπούς που δεν εμπίπτουν στο πλαίσιο της εμπορικής, επιχειρηματικής, βιοτεχνικής ή επαγγελματικής δραστηριότητας του εν λόγω προσώπου·

19) «πολύ μικρές επιχειρήσεις», «μικρές επιχειρήσεις» και «μεσαίες επιχειρήσεις»: πολύ μικρές, μικρές και μεσαίες επιχειρήσεις, αντίστοιχα, όπως ορίζονται στο παράρτημα της σύστασης 2003/361/ΕΚ της Επιτροπής·

20) «περίοδος υποστήριξης»: η περίοδος κατά την οποία ο κατασκευαστής υποχρεούται να διασφαλίζει ότι οι ευπάθειες προϊόντος με ψηφιακά στοιχεία αντιμετωπίζονται αποτελεσματικά και σύμφωνα με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I τμήμα II·

21) «θέση σε κυκλοφορία στην αγορά»: η πρώτη φορά κατά την οποία ένα προϊόν με ψηφιακά στοιχεία διατίθεται στην αγορά της Ένωσης·

22) «διάθεση στην αγορά»: η προσφορά προϊόντος με ψηφιακά στοιχεία για διανομή ή χρήση στην ενωσιακή αγορά στο πλαίσιο εμπορικής δραστηριότητας, είτε έναντι πληρωμής είτε δωρεάν·

23) «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·

24) «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·

25) «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·

26) «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·

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

28) «φορέας αξιολόγησης της συμμόρφωσης»: φορέας αξιολόγησης της συμμόρφωσης όπως ορίζεται στο άρθρο 2 σημείο 13 του κανονισμού (ΕΚ) αριθ. 765/2008·

29) «κοινοποιημένος οργανισμός»: οργανισμός αξιολόγησης της συμμόρφωσης που ορίζεται σύμφωνα με το άρθρο 43 και άλλη σχετική ενωσιακή νομοθεσία εναρμόνισης·

30) «ουσιαστική τροποποίηση»: αλλαγή στο προϊόν με ψηφιακά στοιχεία μετά τη θέση του σε κυκλοφορία στην αγορά, η οποία επηρεάζει τη συμμόρφωση του προϊόντος με ψηφιακά στοιχεία προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος I ή έχει ως αποτέλεσμα τροποποίηση του προβλεπόμενου σκοπού για τον οποίο έχει αξιολογηθεί το προϊόν με ψηφιακά στοιχεία·

31) «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 κυβερνοασφάλειας που ορίζονται στο παράρτημα I και σε άλλη εφαρμοστέα ενωσιακή νομοθεσία εναρμόνισης που προβλέπει την τοποθέτηση της σήμανσης αυτής·

32) «ενωσιακή νομοθεσία εναρμόνισης»: η ενωσιακή νομοθεσία που παρατίθεται στο παράρτημα I του κανονισμού (ΕΕ) 2019/1020, καθώς και κάθε άλλη ενωσιακή νομοθεσία που εναρμονίζει τους όρους εμπορίας των προϊόντων στα οποία εφαρμόζεται ο εν λόγω κανονισμός·

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

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

35) «ευρωπαϊκό πρότυπο»: ευρωπαϊκό πρότυπο όπως ορίζεται στο άρθρο 2 σημείο 1 στοιχείο β) του κανονισμού (ΕΕ) αριθ. 1025/2012·

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

37) «κίνδυνος κυβερνοασφάλειας»: η πιθανότητα απώλειας ή διατάραξης που προκαλείται από περιστατικό και εκφράζεται ως συνδυασμός του μεγέθους της εν λόγω απώλειας ή διατάραξης και της πιθανότητας επέλευσης του περιστατικού·

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

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

40) «ευπάθεια»: αδυναμία, ευαισθησία ή ελάττωμα προϊόντος με ψηφιακά στοιχεία που μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης από κυβερνοαπειλή·

41) «εκμεταλλεύσιμη ευπάθεια»: ευπάθεια που θα μπορούσε να χρησιμοποιηθεί αποτελεσματικά από αντίπαλο υπό πρακτικές συνθήκες λειτουργίας·

42) «ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης»: ευπάθεια για την οποία υπάρχουν αξιόπιστα στοιχεία που αποδεικνύουν ότι κακόβουλος παράγοντας την έχει εκμεταλλευτεί σε ένα σύστημα χωρίς την άδεια του ιδιοκτήτη του συστήματος·

43) «περιστατικό»: περιστατικό όπως ορίζεται στο άρθρο 6 σημείο 6 της οδηγίας (ΕΕ) 2022/2555·

44) «περιστατικό που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία»: περιστατικό που επηρεάζει αρνητικά ή είναι ικανό να επηρεάσει αρνητικά την ικανότητα ενός προϊόντος με ψηφιακά στοιχεία να προστατεύει τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων ή των λειτουργιών·

45) «παρ' ολίγον περιστατικό»: παρ' ολίγον περιστατικό όπως ορίζεται στο άρθρο 6 σημείο 5 της οδηγίας (ΕΕ) 2022/2555·

46) «κυβερνοαπειλή»: κυβερνοαπειλή όπως ορίζεται στο άρθρο 2 σημείο 8 του κανονισμού (ΕΕ) 2019/881·

47) «δεδομένα προσωπικού χαρακτήρα»: τα δεδομένα προσωπικού χαρακτήρα όπως ορίζονται στο άρθρο 4 σημείο 1 του κανονισμού (ΕΕ) 2016/679·

48) «ελεύθερο λογισμικό ανοικτού κώδικα»: λογισμικό του οποίου ο πηγαίος κώδικας διανέμεται ανοικτά και το οποίο διατίθεται με άδεια ελεύθερης και ανοικτής πηγής η οποία περιλαμβάνει όλα τα δικαιώματα που καθιστούν το λογισμικό ελεύθερα προσβάσιμο, χρησιμοποιήσιμο, τροποποιήσιμο και αναδιανεμητέο·

49) «ανάκληση»: ανάκληση όπως ορίζεται στο άρθρο 3 σημείο 22 του κανονισμού (ΕΕ) 2019/1020·

50) «απόσυρση»: απόσυρση όπως ορίζεται στο άρθρο 3 σημείο 23 του κανονισμού (ΕΕ) 2019/1020·

51) «ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού»: ΟΑΠΑΥ με συντονιστικό ρόλο σύμφωνα με το άρθρο 12 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555.

Άρθρο 4

Ελεύθερη κυκλοφορία

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

2. Σε εμπορικές εκθέσεις, επιδείξεις ή παρόμοιες εκδηλώσεις, τα κράτη μέλη δεν εμποδίζουν την παρουσίαση ή τη χρήση προϊόντος με ψηφιακά στοιχεία που δεν συμμορφώνεται με τον παρόντα κανονισμό, συμπεριλαμβανομένων των πρωτοτύπων του, υπό την προϋπόθεση ότι το προϊόν παρουσιάζεται με ευδιάκριτο σήμα που υποδεικνύει σαφώς ότι δεν συμμορφώνεται με τον παρόντα κανονισμό και δεν πρόκειται να διατεθεί στην αγορά έως ότου συμμορφωθεί με τον παρόντα κανονισμό.

3. Τα κράτη μέλη δεν εμποδίζουν τη δωρεάν διάθεση στην αγορά 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 με ευδιάκριτο σήμα που υποδεικνύει σαφώς ότι το λογισμικό δεν συμμορφώνεται με τον παρόντα κανονισμό και δεν θα είναι διαθέσιμο στην αγορά για άλλους σκοπούς πέραν της δοκιμής.

4. Η παράγραφος 3 δεν εφαρμόζεται σε κατασκευαστικά στοιχεία ασφαλείας που αναφέρονται σε ενωσιακή νομοθεσία εναρμόνισης πέραν του παρόντος κανονισμού.

Άρθρο 5

Προμήθεια ή χρήση προϊόντων με ψηφιακά στοιχεία

1. Ο παρών κανονισμός δεν εμποδίζει τα κράτη μέλη να υποβάλλουν προϊόντα με ψηφιακά στοιχεία σε πρόσθετες απαιτήσεις κυβερνοασφάλειας για την προμήθεια ή τη χρήση των εν λόγω προϊόντων για συγκεκριμένους σκοπούς, μεταξύ άλλων όταν τα εν λόγω προϊόντα αγοράζονται ή χρησιμοποιούνται για σκοπούς εθνικής ασφάλειας ή άμυνας, υπό την προϋπόθεση ότι οι εν λόγω απαιτήσεις συνάδουν με τις υποχρεώσεις των κρατών μελών που ορίζονται στο δίκαιο της Ένωσης και είναι αναγκαίες και αναλογικές για την επίτευξη των εν λόγω σκοπών.

2. Με την επιφύλαξη των οδηγιών 2014/24/ΕΕ και 2014/25/ΕΕ, κατά την προμήθεια προϊόντων με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού, τα κράτη μέλη διασφαλίζουν ότι κατά τη διαδικασία προμήθειας λαμβάνεται υπόψη η συμμόρφωση με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι του παρόντος κανονισμού, συμπεριλαμβανομένης της ικανότητας των κατασκευαστών να χειρίζονται αποτελεσματικά τις ευπάθειες.

Άρθρο 6

Απαιτήσεις για προϊόντα με ψηφιακά στοιχεία

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

α) πληρούν τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος I, υπό την προϋπόθεση ότι έχουν εγκατασταθεί, συντηρούνται και χρησιμοποιούνται ορθά για τον επιδιωκόμενο σκοπό ή υπό εύλογα προβλέψιμες συνθήκες και, κατά περίπτωση, διαθέτουν εγκατεστημένες τις απαραίτητες ενημερώσεις ασφαλείας· και

β) οι διαδικασίες που εφαρμόζει ο κατασκευαστής συμμορφώνονται με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος II.

Άρθρο 7

Σημαντικά προϊόντα με ψηφιακά στοιχεία

1. Τα προϊόντα με ψηφιακά στοιχεία που έχουν τη βασική λειτουργικότητα μιας κατηγορίας προϊόντων που ορίζεται στο παράρτημα III θεωρούνται σημαντικά προϊόντα με ψηφιακά στοιχεία και υπόκεινται στις διαδικασίες αξιολόγησης της συμμόρφωσης που αναφέρονται στο άρθρο 32 παράγραφοι 2 και 3. Η ενσωμάτωση ενός προϊόντος με ψηφιακά στοιχεία που έχει τη βασική λειτουργικότητα μιας κατηγορίας προϊόντων που ορίζεται στο παράρτημα III δεν συνεπάγεται από μόνη της ότι το συνολικό προϊόν στο οποίο αυτό ενσωματώνεται, υπόκειται στις διαδικασίες αξιολόγησης της συμμόρφωσης που αναφέρονται στο άρθρο 32 παράγραφοι 2 και 3.

2. Οι κατηγορίες προϊόντων με ψηφιακά στοιχεία που αναφέρονται στην παράγραφο 1 του παρόντος άρθρου και υποδιαιρούνται σε κλάσεις I και II όπως ορίζονται στο παράρτημα III, πληρούν τουλάχιστον ένα από τα ακόλουθα κριτήρια:

α) το προϊόν με ψηφιακά στοιχεία εκτελεί πρωτίστως λειτουργίες κρίσιμης σημασίας για την κυβερνοασφάλεια άλλων προϊόντων, δικτύων ή υπηρεσιών, συμπεριλαμβανομένης της διασφάλισης της επαλήθευσης ταυτότητας και της πρόσβασης, της πρόληψης και ανίχνευσης εισβολών, της ασφάλειας τελικού σημείου ή της προστασίας δικτύων·

β) το προϊόν με ψηφιακά στοιχεία εκτελεί λειτουργία που ενέχει σημαντικό κίνδυνο δυσμενών επιπτώσεων όσον αφορά την ένταση και την ικανότητά της να διαταράξει, να ελέγξει ή να προκαλέσει ζημία σε μεγάλο αριθμό άλλων προϊόντων ή στην υγεία, την ασφάλεια ή την προστασία των χρηστών του μέσω άμεσης χειραγώγησης, όπως η κεντρική λειτουργία συστήματος, συμπεριλαμβανομένων της διαχείρισης δικτύου, του ελέγχου διαμόρφωσης, της εικονικοποίησης ή της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

3. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 61 προκειμένου να τροποποιεί το παράρτημα ΙΙΙ συμπεριλαμβάνοντας στον κατάλογο νέα κατηγορία εντός κάθε κλάσης των κατηγοριών προϊόντων με ψηφιακά στοιχεία και προσδιορίζοντας τον ορισμό της, καθώς και μεταφέροντας μια κατηγορία προϊόντων από τη μία κλάση στην άλλη ή αφαιρώντας υπάρχουσα κατηγορία από τον εν λόγω κατάλογο. Κατά την αξιολόγηση της ανάγκης τροποποίησης του καταλόγου που παρατίθεται στο παράρτημα ΙΙΙ, η Επιτροπή λαμβάνει υπόψη τις λειτουργικότητες που σχετίζονται με την κυβερνοασφάλεια ή τη λειτουργία και το επίπεδο κινδύνου για την κυβερνοασφάλεια που ενέχουν τα προϊόντα με ψηφιακά στοιχεία, όπως ορίζεται βάσει των κριτηρίων που αναφέρονται στην παράγραφο 2 του παρόντος άρθρου. Οι κατ' εξουσιοδότηση πράξεις που αναφέρονται στο πρώτο εδάφιο της παρούσας παραγράφου προβλέπουν, κατά περίπτωση, ελάχιστη μεταβατική περίοδο 12 μηνών, ιδίως όταν μια νέα κατηγορία σημαντικών προϊόντων με ψηφιακά στοιχεία προστίθεται στην κλάση Ι ή ΙΙ ή μεταφέρεται από την κλάση Ι στην κλάση ΙΙ, όπως ορίζεται στο παράρτημα ΙΙΙ, προτού αρχίσουν να εφαρμόζονται οι σχετικές διαδικασίες αξιολόγησης της συμμόρφωσης όπως αναφέρονται στο άρθρο 32 παράγραφοι 2 και 3, εκτός εάν δικαιολογείται συντομότερη μεταβατική περίοδος για επιτακτικούς λόγους επείγουσας ανάγκης.

4. Έως τις … [12 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], η Επιτροπή εκδίδει εκτελεστική πράξη για τον καθορισμό της τεχνικής περιγραφής των κατηγοριών προϊόντων με ψηφιακά στοιχεία στις κλάσεις Ι και ΙΙ όπως ορίζονται στο παράρτημα ΙΙΙ, και της τεχνικής περιγραφής των κατηγοριών προϊόντων με ψηφιακά στοιχεία όπως ορίζονται στο παράρτημα IV. Η εν λόγω εκτελεστική πράξη εκδίδεται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 62 παράγραφος 2.

Άρθρο 8

Κρίσιμα προϊόντα με ψηφιακά στοιχεία

1. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 61, προκειμένου να συμπληρώνει τον παρόντα κανονισμό, προσδιορίζοντας τα προϊόντα με ψηφιακά στοιχεία που έχουν τη βασική λειτουργικότητα μιας κατηγορίας προϊόντων που ορίζεται στο παράρτημα IV του παρόντος κανονισμού τα οποία απαιτείται να λαμβάνουν ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας σε επίπεδο διασφάλισης τουλάχιστον «σημαντικό» στο πλαίσιο ευρωπαϊκού καθεστώτος πιστοποίησης της κυβερνοασφάλειας που εγκρίνεται σύμφωνα με τον κανονισμό (ΕΕ) 2019/881, ώστε να αποδεικνύεται η συμμόρφωση με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I του παρόντος κανονισμού ή σε μέρη αυτού, υπό την προϋπόθεση ότι ένα ευρωπαϊκό καθεστώς πιστοποίησης της κυβερνοασφάλειας που καλύπτει τις εν λόγω κατηγορίες προϊόντων με ψηφιακά στοιχεία έχει εγκριθεί σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 και είναι διαθέσιμο στους κατασκευαστές. Οι εν λόγω κατ' εξουσιοδότηση πράξεις προσδιορίζουν το απαιτούμενο επίπεδο διασφάλισης που είναι αναλογικό προς το επίπεδο κινδύνου κυβερνοασφάλειας που συνδέεται με τα προϊόντα με ψηφιακά στοιχεία, και λαμβάνουν υπόψη τον προβλεπόμενο σκοπό τους, συμπεριλαμβανομένης της κρίσιμης εξάρτησής από αυτά βασικών οντοτήτων όπως αναφέρονται στο άρθρο 3 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555. Πριν από την έκδοση των εν λόγω κατ' εξουσιοδότηση πράξεων, η Επιτροπή διενεργεί εκτίμηση του δυνητικού αντικτύπου των προβλεπόμενων μέτρων στην αγορά και διεξάγει διαβουλεύσεις με τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένης της ευρωπαϊκής ομάδας πιστοποίησης της κυβερνοασφάλειας που θεσπίζεται βάσει του κανονισμού (ΕΕ) 2019/881. Η αξιολόγηση λαμβάνει υπόψη το επίπεδο ετοιμότητας και ικανότητας των κρατών μελών για την εφαρμογή του σχετικού ευρωπαϊκού καθεστώτος πιστοποίησης της κυβερνοασφάλειας. Όταν δεν έχουν εκδοθεί οι κατ' εξουσιοδότηση πράξεις που αναφέρονται στο πρώτο εδάφιο της παρούσας παραγράφου, τα προϊόντα με ψηφιακά στοιχεία που έχουν τη βασική λειτουργικότητα κατηγορίας προϊόντων όπως ορίζεται στο παράρτημα IV υπόκεινται στις διαδικασίες αξιολόγησης της συμμόρφωσης που αναφέρονται στο άρθρο 32 παράγραφος 3.

Οι κατ' εξουσιοδότηση πράξεις που αναφέρονται στο πρώτο εδάφιο προβλέπουν ελάχιστη μεταβατική περίοδο έξι μηνών, εκτός εάν δικαιολογείται βραχύτερη μεταβατική περίοδος για επιτακτικούς λόγους επείγουσας ανάγκης.

2. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 61 για την τροποποίηση του παραρτήματος IV με την προσθήκη ή την αφαίρεση κατηγοριών κρίσιμων προϊόντων με ψηφιακά στοιχεία. Κατά τον καθορισμό των εν λόγω κατηγοριών κρίσιμων προϊόντων με ψηφιακά στοιχεία και του απαιτούμενου επιπέδου διασφάλισης, σύμφωνα με την παράγραφο 1 του παρόντος άρθρου, η Επιτροπή λαμβάνει υπόψη τα κριτήρια που αναφέρονται στο άρθρο 7 παράγραφος 2 και διασφαλίζει ότι οι κατηγορίες προϊόντων με ψηφιακά στοιχεία πληρούν τουλάχιστον ένα από τα ακόλουθα κριτήρια:

α) υπάρχει κρίσιμη εξάρτηση των βασικών οντοτήτων όπως αναφέρονται στο άρθρο 3 της οδηγίας (ΕΕ) 2022/2555 από την κατηγορία προϊόντων με ψηφιακά στοιχεία·

β) τα περιστατικά και οι ευπάθειες που αποτελούν αντικείμενο εκμετάλλευσης όσον αφορά την κατηγορία των προϊόντων με ψηφιακά στοιχεία θα μπορούσαν να οδηγήσουν σε σοβαρές διαταραχές κρίσιμων αλυσίδων εφοδιασμού σε ολόκληρη την εσωτερική αγορά.

Πριν από την έκδοση των εν λόγω κατ' εξουσιοδότηση πράξεων, η Επιτροπή διενεργεί αξιολόγηση του τύπου που αναφέρεται στην παράγραφο 1.

Οι κατ' εξουσιοδότηση πράξεις που αναφέρονται στο πρώτο εδάφιο προβλέπουν ελάχιστη μεταβατική περίοδο έξι μηνών, εκτός εάν δικαιολογείται βραχύτερη μεταβατική περίοδος για επιτακτικούς λόγους επείγουσας ανάγκης.

Άρθρο 9

Διαβουλεύσεις με τα ενδιαφερόμενα μέρη

1. Κατά την κατάρτιση μέτρων για την εφαρμογή του παρόντος κανονισμού, η Επιτροπή διαβουλεύεται με τα σχετικά ενδιαφερόμενα μέρη και λαμβάνει υπόψη τις απόψεις τους, όπως οι αρμόδιες αρχές των κρατών μελών, οι επιχειρήσεις του ιδιωτικού τομέα, συμπεριλαμβανομένων των πολύ μικρών και των μικρών και μεσαίων επιχειρήσεων, η κοινότητα λογισμικού ανοικτού κώδικα, οι ενώσεις καταναλωτών, η ακαδημαϊκή κοινότητα και οι σχετικοί οργανισμοί και φορείς της Ένωσης, καθώς και οι ομάδες εμπειρογνωμόνων που έχουν συσταθεί σε επίπεδο Ένωσης. Ειδικότερα, η Επιτροπή διαβουλεύεται, κατά περίπτωση, με δομημένο τρόπο με τα εν λόγω ενδιαφερόμενα μέρη και ζητεί τις απόψεις τους κατά:

α) την κατάρτιση της καθοδήγησης που αναφέρεται στο άρθρο 26·

β) την κατάρτιση των τεχνικών περιγραφών των κατηγοριών προϊόντων που ορίζονται στο παράρτημα III σύμφωνα με το άρθρο 7 παράγραφος 4, την αξιολόγηση της ανάγκης για πιθανές επικαιροποιήσεις του καταλόγου των κατηγοριών προϊόντων σύμφωνα με το άρθρο 7 παράγραφος 3 και το άρθρο 8 παράγραφος 2, ή τη διενέργεια της εκτίμησης του δυνητικού αντικτύπου στην αγορά που αναφέρεται στο άρθρο 8 παράγραφος 1, με την επιφύλαξη του άρθρου 61·

γ) την ανάληψη προπαρασκευαστικών εργασιών για την αξιολόγηση και την επανεξέταση του παρόντος κανονισμού.

2. Η Επιτροπή διοργανώνει τακτικές διαβουλεύσεις και ενημερωτικές συναντήσεις, τουλάχιστον μία φορά ετησίως, για να συγκεντρώσει τις απόψεις των ενδιαφερόμενων μερών που αναφέρονται στην παράγραφο 1 σχετικά με την εφαρμογή του παρόντος κανονισμού.

Άρθρο 10

Ενίσχυση των δεξιοτήτων σε ένα ψηφιακό περιβάλλον κυβερνοανθεκτικότητας

Για τους σκοπούς του παρόντος κανονισμού και προκειμένου να ανταποκριθούν στις ανάγκες των επαγγελματιών προς υποστήριξη της εφαρμογής του παρόντος κανονισμού, τα κράτη μέλη, με την υποστήριξη, κατά περίπτωση, της Επιτροπής, του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Θέματα Κυβερνοασφάλειας και του ENISA, με πλήρη σεβασμό προς την αρμοδιότητα των κρατών μελών στον τομέα της εκπαίδευσης, προωθούν μέτρα και στρατηγικές που αποσκοπούν:

α) στην ανάπτυξη δεξιοτήτων κυβερνοασφάλειας και στη δημιουργία οργανωτικών και τεχνολογικών εργαλείων για τη διασφάλιση επαρκούς διαθεσιμότητας ειδικευμένων επαγγελματιών, προκειμένου να υποστηριχθούν οι δραστηριότητες των αρχών εποπτείας της αγοράς και των οργανισμών αξιολόγησης της συμμόρφωσης·

β) στην αύξηση της συνεργασίας μεταξύ του ιδιωτικού τομέα, των οικονομικών φορέων, μεταξύ άλλων μέσω της επανεκπαίδευσης ή της αναβάθμισης των δεξιοτήτων των εργαζομένων σε κατασκευαστές, των καταναλωτών, των παρόχων κατάρτισης, καθώς και των δημόσιων διοικήσεων, ώστε με τον τρόπο αυτόν να επεκταθούν οι δυνατότητες πρόσβασης των νέων σε θέσεις εργασίας στον τομέα της κυβερνοασφάλειας.

Άρθρο 11

Γενική ασφάλεια των προϊόντων

Κατά παρέκκλιση από το άρθρο 2 παράγραφος 1 τρίτο εδάφιο στοιχείο β) του κανονισμού (ΕΕ) 2023/988, το κεφάλαιο III τμήμα 1, τα κεφάλαια V και VII και τα κεφάλαια IX έως XI του εν λόγω κανονισμού εφαρμόζονται σε προϊόντα με ψηφιακά στοιχεία όσον αφορά τις πτυχές και τους κινδύνους ή τις κατηγορίες κινδύνων που δεν καλύπτονται από τον παρόντα κανονισμό, όταν τα εν λόγω προϊόντα δεν υπόκεινται σε ειδικές απαιτήσεις ασφαλείας που προβλέπονται σε άλλη «ενωσιακή νομοθεσία εναρμόνισης» όπως ορίζεται στο άρθρο 3 σημείο 27) του κανονισμού (ΕΕ) 2023/988.

Άρθρο 12

Συστήματα ΤΝ υψηλού κινδύνου

1. Με την επιφύλαξη των απαιτήσεων σε σχέση με την ακρίβεια και τη στιβαρότητα που ορίζονται στο άρθρο 15 του κανονισμού (ΕΕ) 2024/1689, τα προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού και τα οποία ταξινομούνται ως συστήματα ΤΝ υψηλού κινδύνου σύμφωνα με το άρθρο 6 του εν λόγω κανονισμού, θεωρείται ότι συμμορφώνονται με τις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο άρθρο 15 του εν λόγω κανονισμού όταν:

   α) τα εν λόγω προϊόντα πληρούν τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος I·

β) οι διαδικασίες που εφαρμόζει ο κατασκευαστής συμμορφώνονται με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος II· και

γ) η επίτευξη του επιπέδου προστασίας που απαιτείται δυνάμει του άρθρου 15 του κανονισμού (ΕΕ) 2024/1689 αποδεικνύεται στη δήλωση συμμόρφωσης ΕΕ που εκδίδεται δυνάμει του παρόντος κανονισμού.

2. Για τα προϊόντα με ψηφιακά στοιχεία και τις απαιτήσεις κυβερνοασφάλειας που αναφέρονται στην παράγραφο 1 του παρόντος άρθρου, εφαρμόζεται η σχετική διαδικασία αξιολόγησης της συμμόρφωσης που προβλέπεται στο άρθρο 43 του κανονισμού (ΕΕ) 2024/1689. Για τους σκοπούς της εν λόγω αξιολόγησης, οι κοινοποιημένοι οργανισμοί που είναι αρμόδιοι να ελέγχουν τη συμμόρφωση των συστημάτων ΤΝ υψηλού κινδύνου δυνάμει του κανονισμού (ΕΕ) 2024/1689 είναι επίσης αρμόδιοι να ελέγχουν τη συμμόρφωση 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 39 του παρόντος κανονισμού έχει αξιολογηθεί στο πλαίσιο της διαδικασίας κοινοποίησης δυνάμει του κανονισμού (ΕΕ) 2024/1689.

3. Κατά παρέκκλιση από την παράγραφο 2 του παρόντος άρθρου, σημαντικά προϊόντα με ψηφιακά στοιχεία που απαριθμούνται στο παράρτημα III του παρόντος κανονισμού, τα οποία υπόκεινται στις διαδικασίες αξιολόγησης της συμμόρφωσης που αναφέρονται στο άρθρο 32 παράγραφος 2 στοιχεία α) και β) και στο άρθρο 32 παράγραφος 3 του παρόντος κανονισμού και κρίσιμα προϊόντα με ψηφιακά στοιχεία που απαριθμούνται στο παράρτημα IV του παρόντος κανονισμού, τα οποία απαιτείται να λάβουν ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας σύμφωνα με το άρθρο 8 παράγραφος 1 του παρόντος κανονισμού ή, ελλείψει αυτού, τα οποία υπόκεινται στις διαδικασίες αξιολόγησης της συμμόρφωσης που αναφέρονται στο άρθρο 32 παράγραφος 3 του παρόντος κανονισμού, και τα οποία ταξινομούνται ως συστήματα ΤΝ υψηλού κινδύνου σύμφωνα με το άρθρο 6 του κανονισμού (ΕΕ) 2024/1689, και στα οποία εφαρμόζεται η διαδικασία αξιολόγησης της συμμόρφωσης βάσει εσωτερικού ελέγχου όπως αναφέρεται στο παράρτημα VI του κανονισμού (ΕΕ) 2024/1689, υπόκεινται στις διαδικασίες αξιολόγησης της συμμόρφωσης που ορίζονται στον παρόντα κανονισμό, στον βαθμό που αφορούν τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας του παρόντος κανονισμού.

4. Οι κατασκευαστές προϊόντων με ψηφιακά στοιχεία που αναφέρονται στην παράγραφο 1 του παρόντος άρθρου μπορούν να συμμετέχουν στα ρυθμιστικά δοκιμαστήρια ΤΝ που αναφέρονται στο άρθρο 57 του κανονισμού (ΕΕ) 2024/1689.

ΚΕΦΑΛΑΙΟ ΙΙ
ΥΠΟΧΡΕΩΣΕΙΣ ΤΩΝ ΟΙΚΟΝΟΜΙΚΩΝ ΦΟΡΕΩΝ ΚΑΙ ΔΙΑΤΑΞΕΙΣ ΣΕ ΣΧΕΣΗ ΜΕ ΤΟ ΕΛΕΥΘΕΡΟ ΛΟΓΙΣΜΙΚΟ ΑΝΟΙΚΤΟΥ ΚΩΔΙΚΑ

Άρθρο 13

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 κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι μέρος Ι.

2. Για τον σκοπό της συμμόρφωσης με την 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 περιστατικών και την ελαχιστοποίηση των επιπτώσεών τους, μεταξύ άλλων στην υγεία και την ασφάλεια των χρηστών.

3. Η εκτίμηση κινδύνων κυβερνοασφάλειας τεκμηριώνεται και επικαιροποιείται, κατά περίπτωση, κατά τη διάρκεια περιόδου υποστήριξης που καθορίζεται σύμφωνα με την παράγραφο 8 του παρόντος άρθρου. Η εν λόγω εκτίμηση κινδύνων κυβερνοασφάλειας περιλαμβάνει τουλάχιστον ανάλυση των κινδύνων κυβερνοασφάλειας με βάση τον προβλεπόμενο σκοπό και την ευλόγως προβλέψιμη χρήση, καθώς και τους όρους χρήσης, του προϊόντος με ψηφιακά στοιχεία, όπως το επιχειρησιακό περιβάλλον ή τα περιουσιακά στοιχεία που πρέπει να προστατευθούν, λαμβανομένου υπόψη του χρόνου που αναμένεται να χρησιμοποιηθεί το προϊόν. Στην εκτίμηση κινδύνων κυβερνοασφάλειας αναφέρεται κατά πόσον και, εάν ναι, με ποιον τρόπο, οι απαιτήσεις ασφάλειας που ορίζονται στο παράρτημα Ι μέρος Ι σημείο 2, εφαρμόζονται στο σχετικό προϊόν με ψηφιακά στοιχεία και πώς εφαρμόζονται οι εν λόγω απαιτήσεις, όπως τεκμηριώνεται από την εκτίμηση κινδύνων κυβερνοασφάλειας. Αναφέρεται επίσης ο τρόπος με τον οποίο ο κατασκευαστής εφαρμόζει το παράρτημα Ι μέρος Ι σημείο 1 και τις απαιτήσεις χειρισμού ευπαθειών που ορίζονται στο παράρτημα Ι μέρος ΙΙ.

4. Όταν ο κατασκευαστής θέτει προϊόν με ψηφιακά στοιχεία σε κυκλοφορία στην αγορά, περιλαμβάνει την εκτίμηση κινδύνων κυβερνοασφάλειας που αναφέρεται στην παράγραφο 3 του παρόντος άρθρου στον τεχνικό φάκελο που απαιτείται σύμφωνα με το άρθρο 31 και το παράρτημα VII. Για τα προϊόντα με ψηφιακά στοιχεία όπως αναφέρονται στο άρθρο 12, τα οποία υπόκεινται και σε άλλες νομικές πράξεις της Ένωσης, η εκτίμηση κινδύνων κυβερνοασφάλειας μπορεί να αποτελεί μέρος της εκτίμησης κινδύνου που απαιτείται από τις εν λόγω νομικές πράξεις της Ένωσης. Όταν ορισμένες ουσιώδεις απαιτήσεις κυβερνοασφάλειας δεν εφαρμόζονται στο προϊόν με ψηφιακά στοιχεία, ο κατασκευαστής περιλαμβάνει σαφή σχετική αιτιολόγηση στον εν λόγω τεχνικό φάκελο.

5. Για τους σκοπούς της συμμόρφωσης με την παράγραφο 1, οι κατασκευαστές επιδεικνύουν τη δέουσα επιμέλεια κατά την ενσωμάτωση δομοστοιχείων που προέρχονται από τρίτους, ώστε τα εν λόγω δομοστοιχεία να μη θέτουν σε κίνδυνο την κυβερνοασφάλεια του προϊόντος με ψηφιακά στοιχεία, μεταξύ άλλων όταν ενσωματώνουν δομοστοιχεία ελεύθερου λογισμικού ανοικτού κώδικα που δεν έχουν καταστεί διαθέσιμα στην αγορά στο πλαίσιο εμπορικής δραστηριότητας.

6. Οι κατασκευαστές, μόλις εντοπίσουν μια ευπάθεια σε δομοστοιχείο, μεταξύ άλλων σε δομοστοιχείο ανοικτού κώδικα, το οποίο είναι ενσωματωμένο στο προϊόν με ψηφιακά στοιχεία, αναφέρουν την ευπάθεια στο πρόσωπο ή την οντότητα που κατασκευάζει ή συντηρεί το δομοστοιχείο, και αντιμετωπίζουν και αίρουν την ευπάθεια σύμφωνα με τις απαιτήσεις χειρισμού ευπαθειών που ορίζονται στο παράρτημα I μέρος II. Όταν οι κατασκευαστές έχουν αναπτύξει τροποποίηση λογισμικού ή υλισμικού για την αντιμετώπιση της ευπάθειας του εν λόγω δομοστοιχείου, κοινοποιούν τον σχετικό κώδικα ή την τεκμηρίωση στο πρόσωπο ή την οντότητα που κατασκευάζει ή συντηρεί το δομοστοιχείο, κατά περίπτωση σε μηχαναγνώσιμο μορφότυπο.

7. Οι κατασκευαστές τεκμηριώνουν συστηματικά, κατά τρόπο αναλογικό προς τη φύση και τους κινδύνους για την κυβερνοασφάλεια, τις σχετικές πτυχές κυβερνοασφάλειας που αφορούν τα προϊόντα με ψηφιακά στοιχεία, συμπεριλαμβανομένων των ευπαθειών που υποπίπτουν στην αντίληψή τους και τυχόν σχετικές πληροφορίες που παρέχονται από τρίτους, και, κατά περίπτωση, επικαιροποιούν την εκτίμηση κινδύνων κυβερνοασφάλειας των προϊόντων.

8. Οι κατασκευαστές εξασφαλίζουν, όταν θέτουν προϊόν με ψηφιακά στοιχεία σε κυκλοφορία στην αγορά, και για την περίοδο υποστήριξης, ότι οι ευπάθειες του εν λόγω προϊόντος, συμπεριλαμβανομένων των δομοστοιχείων του, αντιμετωπίζονται αποτελεσματικά και σύμφωνα με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος II.

Οι κατασκευαστές καθορίζουν την περίοδο υποστήριξης κατά τρόπο ώστε αυτή να αντικατοπτρίζει το χρονικό διάστημα κατά το οποίο αναμένεται να χρησιμοποιηθεί το προϊόν, λαμβάνοντας υπόψη, ιδίως, τις εύλογες προσδοκίες των χρηστών, τη φύση του προϊόντος, συμπεριλαμβανομένου του προβλεπόμενου σκοπού του, καθώς και τη σχετική ενωσιακή νομοθεσία που καθορίζει τη διάρκεια ζωής των προϊόντων με ψηφιακά στοιχεία. Κατά τον καθορισμό της περιόδου υποστήριξης, οι κατασκευαστές μπορούν επίσης να λαμβάνουν υπόψη τις περιόδους υποστήριξης προϊόντων με ψηφιακά στοιχεία που προσφέρουν παρόμοια λειτουργικότητα και έχουν τεθεί σε κυκλοφορία στην αγορά από άλλους κατασκευαστές, τη διαθεσιμότητα του περιβάλλοντος λειτουργίας, τις περιόδους υποστήριξης των ενσωματωμένων δομοστοιχείων που παρέχουν βασικές λειτουργίες και προέρχονται από τρίτους, καθώς και τη σχετική καθοδήγηση που παρέχεται από την ειδική ομάδα διοικητικής συνεργασίας (ΕΟΔΚ) που συγκροτείται σύμφωνα με το άρθρο 52 παράγραφος 15 και την Επιτροπή. Τα ζητήματα που πρέπει να λαμβάνονται υπόψη για τον καθορισμό της περιόδου υποστήριξης εξετάζονται κατά τρόπο που διασφαλίζει την αναλογικότητα.

Με την επιφύλαξη του δεύτερου εδαφίου, η περίοδος υποστήριξης είναι τουλάχιστον πέντε έτη. Όταν το προϊόν με ψηφιακά στοιχεία αναμένεται να χρησιμοποιηθεί για λιγότερο από πέντε έτη, η περίοδος υποστήριξης αντιστοιχεί στον αναμενόμενο χρόνο χρήσης.

Λαμβάνοντας υπόψη τις συστάσεις της ΕΟΔΚ, όπως αναφέρονται στο άρθρο 52 παράγραφος 16, η Επιτροπή μπορεί να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 61, προκειμένου να συμπληρώσει τον παρόντα κανονισμό προσδιορίζοντας την ελάχιστη περίοδο υποστήριξης για συγκεκριμένες κατηγορίες προϊόντων για τις οποίες τα δεδομένα εποπτείας της αγοράς δείχνουν ότι οι περίοδοι υποστήριξης είναι ανεπαρκείς.

Οι κατασκευαστές περιλαμβάνουν στον τεχνικό φάκελο, όπως ορίζεται στο παράρτημα VII, τις πληροφορίες που ελήφθησαν υπόψη για τον καθορισμό της περιόδου υποστήριξης ενός προϊόντος με ψηφιακά στοιχεία.

Οι κατασκευαστές διαθέτουν κατάλληλες πολιτικές και διαδικασίες, συμπεριλαμβανομένων συντονισμένων πολιτικών γνωστοποίησης ευπαθειών, όπως αναφέρονται στο παράρτημα I μέρος II σημείο 5, για την επεξεργασία και την αποκατάσταση πιθανών ευπαθειών του προϊόντος με ψηφιακά στοιχεία που αναφέρονται από εσωτερικές ή εξωτερικές πηγές.

9. Οι κατασκευαστές διασφαλίζουν ότι κάθε ενημέρωση ασφαλείας, όπως αναφέρεται στο παράρτημα I μέρος II σημείο 8, η οποία έχει καταστεί διαθέσιμη στους χρήστες κατά τη διάρκεια της περιόδου υποστήριξης, παραμένει διαθέσιμη μετά την έκδοσή της για τουλάχιστον 10 έτη ή για το υπόλοιπο της περιόδου υποστήριξης, ανάλογα με το ποιο διάστημα είναι μεγαλύτερο.

10. Όταν ένας κατασκευαστής έχει θέσει σε κυκλοφορία στην αγορά μεταγενέστερες ουσιωδώς τροποποιημένες εκδόσεις προϊόντος λογισμικού, ο εν λόγω κατασκευαστής μπορεί να διασφαλίσει τη συμμόρφωση με την ουσιώδη απαίτηση κυβερνοασφάλειας που ορίζεται στο παράρτημα I μέρος II σημείο 2, μόνο για την έκδοση που έθεσε τελευταία σε κυκλοφορία στην αγορά ο εν λόγω κατασκευαστής, υπό την προϋπόθεση ότι οι χρήστες των εκδόσεων που είχαν τεθεί προηγουμένως σε κυκλοφορία στην αγορά, έχουν πρόσβαση στην τελευταία έκδοση που τέθηκε σε κυκλοφορία στην αγορά δωρεάν και δεν επιβαρύνονται με πρόσθετες δαπάνες για την προσαρμογή του περιβάλλοντος υλισμικού και λογισμικού στο οποίο χρησιμοποιούν την αρχική έκδοση του εν λόγω προϊόντος.

11. Οι κατασκευαστές μπορούν να διατηρούν δημόσια αρχεία λογισμικού που ενισχύουν την πρόσβαση των χρηστών σε ιστορικές εκδόσεις. Στις περιπτώσεις αυτές, οι χρήστες ενημερώνονται σαφώς και με εύκολα προσβάσιμο τρόπο σχετικά με τους κινδύνους που συνδέονται με τη χρήση μη υποστηριζόμενου λογισμικού.

12. Πριν από τη διάθεση προϊόντος με ψηφιακά στοιχεία στην αγορά, οι κατασκευαστές καταρτίζουν τον τεχνικό φάκελο που αναφέρεται στο άρθρο 31.

Διενεργούν τις επιλεγμένες διαδικασίες αξιολόγησης της συμμόρφωσης όπως αναφέρονται στο άρθρο 32 ή αναθέτουν τη διενέργειά τους σε τρίτους.

Όταν η συμμόρφωση του προϊόντος με ψηφιακά στοιχεία με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στο παράρτημα I μέρος I, και των διαδικασιών που εφαρμόζει ο κατασκευαστής με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο τμήμα 2 του παραρτήματος I μέρος II, αποδεικνύεται με την εν λόγω διαδικασία αξιολόγησης της συμμόρφωσης, οι κατασκευαστές καταρτίζουν τη δήλωση συμμόρφωσης ΕΕ σύμφωνα με το άρθρο 28 και τοποθετούν τη σήμανση CE σύμφωνα με το άρθρο 30.

13. Οι κατασκευαστές διατηρούν τον τεχνικό φάκελο και τη δήλωση συμμόρφωσης ΕΕ στη διάθεση των αρχών εποπτείας της αγοράς τουλάχιστον επί δέκα έτη αφότου το προϊόν με ψηφιακά στοιχεία τεθεί σε κυκλοφορία στην αγορά ή για την περίοδο υποστήριξης, ανάλογα με το ποιο διάστημα είναι μεγαλύτερο.

14. Οι κατασκευαστές διασφαλίζουν ότι εφαρμόζονται διαδικασίες ώστε τα προϊόντα με ψηφιακά στοιχεία που αποτελούν μέρος σειράς παραγωγής να συμμορφώνονται διαρκώς με τον παρόντα κανονισμό. Οι κατασκευαστές λαμβάνουν 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 καθεστώτα πιστοποίησης της κυβερνοασφάλειας ή στις κοινές προδιαγραφές όπως αναφέρονται στο άρθρο 27 και με βάση τις οποίες δηλώνεται η συμμόρφωση του προϊόντος με ψηφιακά στοιχεία ή με την εφαρμογή των οποίων επαληθεύεται η συμμόρφωσή του.

15. Οι κατασκευαστές διασφαλίζουν ότι τα προϊόντα τους με ψηφιακά στοιχεία φέρουν αριθμό τύπου, παρτίδας ή σειράς ή άλλο στοιχείο που επιτρέπει την ταυτοποίησή τους ή, όταν αυτό δεν είναι δυνατό, ότι οι εν λόγω πληροφορίες αναγράφονται στη συσκευασία τους ή σε έγγραφο που συνοδεύει το προϊόν με ψηφιακά στοιχεία.

16. Οι κατασκευαστές αναγράφουν το όνομα, την καταχωρισμένη εμπορική επωνυμία ή το καταχωρισμένο εμπορικό σήμα του κατασκευαστή, και την ταχυδρομική διεύθυνση, τη διεύθυνση ηλεκτρονικού ταχυδρομείου ή άλλα ψηφιακά στοιχεία επικοινωνίας, καθώς και, κατά περίπτωση, τον ιστότοπο μέσω του οποίου μπορεί να υπάρξει επικοινωνία με τον κατασκευαστή, στο προϊόν με ψηφιακά στοιχεία, στη συσκευασία του ή σε έγγραφο που συνοδεύει το προϊόν με ψηφιακά στοιχεία. Οι πληροφορίες αυτές περιλαμβάνονται επίσης στις πληροφορίες και τις οδηγίες προς τον χρήστη που ορίζονται στο παράρτημα II. Τα στοιχεία επικοινωνίας παρέχονται σε γλώσσα εύκολα κατανοητή από τους χρήστες και τις αρχές εποπτείας της αγοράς.

17. Για τους σκοπούς του παρόντος κανονισμού, οι κατασκευαστές ορίζουν ενιαίο σημείο επαφής που επιτρέπει στους χρήστες να επικοινωνούν απευθείας και γρήγορα μαζί τους, μεταξύ άλλων προκειμένου να διευκολύνεται η αναφορά ευπαθειών του προϊόντος με ψηφιακά στοιχεία.

Οι κατασκευαστές εξασφαλίζουν ότι το ενιαίο σημείο επαφής μπορεί να αναγνωριστεί εύκολα από τους χρήστες. Περιλαμβάνουν επίσης το ενιαίο σημείο επαφής στις πληροφορίες και τις οδηγίες προς τον χρήστη που ορίζονται στο παράρτημα II.

Το ενιαίο σημείο επαφής επιτρέπει στους χρήστες να επιλέγουν τα μέσα επικοινωνίας που προτιμούν και δεν περιορίζει τα μέσα αυτά σε αυτοματοποιημένα εργαλεία.

18. Οι κατασκευαστές διασφαλίζουν ότι τα προϊόντα με ψηφιακά στοιχεία συνοδεύονται από τις πληροφορίες και τις οδηγίες προς τον χρήστη που ορίζονται στο παράρτημα II, σε έντυπη ή ηλεκτρονική μορφή. Οι εν λόγω πληροφορίες και οδηγίες παρέχονται σε γλώσσα εύκολα κατανοητή από τους χρήστες και τις αρχές εποπτείας της αγοράς. Είναι σαφείς, κατανοητές, εύληπτες και ευανάγνωστες. Επιτρέπουν την ασφαλή εγκατάσταση, λειτουργία και χρήση των προϊόντων με ψηφιακά στοιχεία. Οι κατασκευαστές διατηρούν τις πληροφορίες και τις οδηγίες προς τον χρήστη που ορίζονται στο παράρτημα II στη διάθεση των χρηστών και των αρχών εποπτείας της αγοράς τουλάχιστον επί δέκα έτη αφότου το προϊόν με ψηφιακά στοιχεία τεθεί σε κυκλοφορία στην αγορά ή για την περίοδο υποστήριξης, ανάλογα με το ποιο διάστημα είναι μεγαλύτερο. Όταν οι εν λόγω πληροφορίες και οδηγίες παρέχονται διαδικτυακά, οι κατασκευαστές εξασφαλίζουν ότι είναι προσβάσιμες, εύχρηστες και διαθέσιμες διαδικτυακά επί τουλάχιστον δέκα έτη αφότου το προϊόν με ψηφιακά στοιχεία τεθεί σε κυκλοφορία στην αγορά ή για την περίοδο υποστήριξης, ανάλογα με το ποιο διάστημα είναι μεγαλύτερο.

19. Οι κατασκευαστές διασφαλίζουν ότι η ημερομηνία λήξης της περιόδου υποστήριξης που αναφέρεται στην παράγραφο 8, συμπεριλαμβανομένου τουλάχιστον του μήνα και του έτους, προσδιορίζεται σαφώς και κατανοητά κατά τη στιγμή της αγοράς, με εύκολα προσβάσιμο τρόπο και, κατά περίπτωση, στο προϊόν με ψηφιακά στοιχεία, στη συσκευασία του ή με ψηφιακά μέσα.

Όπου είναι τεχνικά εφικτό λόγω της φύσης του προϊόντος με ψηφιακά στοιχεία, οι κατασκευαστές εμφανίζουν κοινοποίηση προς τους χρήστες με την οποία τους ενημερώνουν ότι το προϊόν τους με ψηφιακά στοιχεία έχει φτάσει στο τέλος της περιόδου υποστήριξής του.

20. Οι κατασκευαστές παρέχουν είτε αντίγραφο της δήλωσης συμμόρφωσης ΕΕ είτε απλουστευμένη δήλωση συμμόρφωσης ΕΕ με το προϊόν με ψηφιακά στοιχεία. Στην περίπτωση που παρέχεται απλουστευμένη δήλωση συμμόρφωσης ΕΕ, αυτή περιλαμβάνει την ακριβή διαδικτυακή διεύθυνση στην οποία διατίθεται πρόσβαση στο πλήρες κείμενο της δήλωσης συμμόρφωσης ΕΕ.

21. Από τη διάθεση στην αγορά και για την περίοδο υποστήριξης, 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 κυβερνοασφάλειας που ορίζονται στο παράρτημα I, 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.

22. Οι κατασκευαστές παρέχουν στην αρχή εποπτείας της αγοράς, κατόπιν αιτιολογημένου αιτήματος της εν λόγω αρχής, σε γλώσσα εύκολα κατανοητή από την εν λόγω αρχή, 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 κυβερνοασφάλειας που ορίζονται στο παράρτημα I. Οι κατασκευαστές 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.

23. Ο κατασκευαστής που παύει τις δραστηριότητές του και, ως εκ τούτου, δεν είναι σε θέση να συμμορφωθεί με τον παρόντα κανονισμό ενημερώνει, πριν από την έναρξη ισχύος της παύσης των δραστηριοτήτων του, τις αρμόδιες αρχές εποπτείας της αγοράς, καθώς και τους χρήστες των σχετικών προϊόντων με ψηφιακά στοιχεία που έχουν τεθεί σε κυκλοφορία στην αγορά, με κάθε διαθέσιμο μέσο και στο μέτρο του δυνατού, σχετικά με την επικείμενη παύση των δραστηριοτήτων του.

24. Η Επιτροπή μπορεί, με εκτελεστικές πράξεις και λαμβάνοντας υπόψη τα ευρωπαϊκά ή διεθνή πρότυπα και βέλτιστες πρακτικές, να καθορίζει τον μορφότυπο και τα στοιχεία του καταλόγου υλικών λογισμικού που αναφέρεται στο παράρτημα I μέρος II σημείο 1. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 62 παράγραφος 2.

25. Προκειμένου να αξιολογηθεί η εξάρτηση των κρατών μελών και της Ένωσης στο σύνολό της από δομοστοιχεία λογισμικού και ιδίως από δομοστοιχεία που χαρακτηρίζονται ως ελεύθερο λογισμικό ανοικτού κώδικα, η ΕΟΔΚ μπορεί να αποφασίσει να διενεργήσει αξιολόγηση της εξάρτησης σε επίπεδο Ένωσης για συγκεκριμένες κατηγορίες προϊόντων με ψηφιακά στοιχεία. Για τον σκοπό αυτό, οι αρχές εποπτείας της αγοράς μπορούν να ζητήσουν από τους κατασκευαστές των εν λόγω κατηγοριών προϊόντων με ψηφιακά στοιχεία να παράσχουν τους σχετικούς καταλόγους υλικών λογισμικού, όπως αναφέρεται στο παράρτημα I μέρος II σημείο 1. Βάσει των εν λόγω πληροφοριών, οι αρχές εποπτείας της αγοράς μπορούν να παράσχουν στην ΕΟΔΚ ανωνυμοποιημένες και συγκεντρωτικές πληροφορίες σχετικά με τις εξαρτήσεις λογισμικού. Η ΕΟΔΚ υποβάλλει έκθεση σχετικά με τα αποτελέσματα της αξιολόγησης εξάρτησης στην ομάδα συνεργασίας που συγκροτείται σύμφωνα με το άρθρο 14 της οδηγίας (ΕΕ) 2022/2555.

Άρθρο 14

Υποχρεώσεις αναφοράς για τους κατασκευαστές

1. Ο κατασκευαστής κοινοποιεί κάθε ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης και περιέχεται στο προϊόν με ψηφιακά στοιχεία, και η οποία υποπίπτει στην αντίληψή του, ταυτόχρονα στην ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού, σύμφωνα με την παράγραφο 7 του παρόντος άρθρου, και στον ENISA. Ο κατασκευαστής κοινοποιεί την εν λόγω ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης μέσω της ενιαίας πλατφόρμας αναφοράς που δημιουργείται σύμφωνα με το άρθρο 16.

2. Για τους σκοπούς της κοινοποίησης που αναφέρεται στην παράγραφο 1, ο κατασκευαστής υποβάλλει:

   α) κοινοποίηση έγκαιρης προειδοποίησης σχετικά με ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης, χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που η ευπάθεια υπέπεσε στην αντίληψη του κατασκευαστή, αναφέροντας, κατά περίπτωση, τα κράτη μέλη στην επικράτεια των οποίων έχει καταστεί διαθέσιμο το προϊόν με ψηφιακά στοιχεία εξ όσων γνωρίζει ο κατασκευαστής·

β) εκτός εάν έχουν ήδη παρασχεθεί οι σχετικές πληροφορίες, κοινοποίηση ευπάθειας, χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 72 ωρών από τη στιγμή που η ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης υπέπεσε στην αντίληψη του κατασκευαστή, η οποία παρέχει γενικές πληροφορίες, εφόσον είναι διαθέσιμες, σχετικά με το οικείο προϊόν με ψηφιακά στοιχεία, τον γενικό χαρακτήρα της εκμετάλλευσης και της σχετικής ευπάθειας, καθώς και τυχόν διορθωτικά μέτρα ή μέτρα μετριασμού που έχουν ληφθεί, και διορθωτικά μέτρα ή μέτρα μετριασμού που μπορούν να λάβουν οι χρήστες, και η οποία αναφέρει επίσης, κατά περίπτωση, πόσο ευαίσθητες θεωρεί ο κατασκευαστής τις κοινοποιηθείσες πληροφορίες·

γ) εκτός εάν έχουν ήδη παρασχεθεί οι σχετικές πληροφορίες, τελική έκθεση, το αργότερο 14 ημέρες μετά τη λήψη διορθωτικού μέτρου ή μέτρου μετριασμού, η οποία περιλαμβάνει τουλάχιστον τα ακόλουθα:

i) λεπτομερή περιγραφή της ευπάθειας, συμπεριλαμβανομένων της σοβαρότητας και των επιπτώσεών της·

ii) εφόσον είναι διαθέσιμες, πληροφορίες σχετικά με οποιονδήποτε κακόβουλο παράγοντα που έχει εκμεταλλευτεί ή εκμεταλλεύεται την ευπάθεια·

iii) λεπτομέρειες σχετικά με την ενημέρωση ασφαλείας ή άλλα διορθωτικά μέτρα που έχουν διατεθεί για την αντιμετώπιση της ευπάθειας.

3. Ο κατασκευαστής κοινοποιεί κάθε σοβαρό περιστατικό που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία και το οποίο υποπίπτει στην αντίληψή του, ταυτόχρονα στην ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού, σύμφωνα με την παράγραφο 7 του παρόντος άρθρου, και στον ENISA. Ο κατασκευαστής κοινοποιεί το εν λόγω περιστατικό μέσω της ενιαίας πλατφόρμας αναφοράς που δημιουργείται σύμφωνα με το άρθρο 16.

4. Για τους σκοπούς της κοινοποίησης που αναφέρεται στην παράγραφο 3, ο κατασκευαστής υποβάλλει:

α) κοινοποίηση έγκαιρης προειδοποίησης σχετικά με σοβαρό περιστατικό που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία, χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που το περιστατικό υπέπεσε στην αντίληψη του κατασκευαστή, δηλώνοντας τουλάχιστον εάν υπάρχει υπόνοια ότι το περιστατικό έχει προκληθεί από παράνομες ή κακόβουλες ενέργειες, και αναφέροντας επίσης, κατά περίπτωση, τα κράτη μέλη στην επικράτεια των οποίων έχει καταστεί διαθέσιμο το προϊόν με ψηφιακά στοιχεία εξ όσων γνωρίζει ο κατασκευαστής·

β) εκτός εάν έχουν ήδη παρασχεθεί οι σχετικές πληροφορίες, κοινοποίηση περιστατικού, χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 72 ωρών από τη στιγμή που το περιστατικό υπέπεσε στην αντίληψη του κατασκευαστή, η οποία παρέχει γενικές πληροφορίες, εφόσον είναι διαθέσιμες, σχετικά με τη φύση του περιστατικού, αρχική αξιολόγηση του περιστατικού, καθώς και τυχόν διορθωτικά μέτρα ή μέτρα μετριασμού που έχουν ληφθεί, και διορθωτικά μέτρα ή μέτρα μετριασμού που μπορούν να λάβουν οι χρήστες, και η οποία αναφέρει επίσης, κατά περίπτωση, πόσο ευαίσθητες θεωρεί ο κατασκευαστής τις κοινοποιηθείσες πληροφορίες·

γ) εκτός εάν έχουν ήδη παρασχεθεί οι σχετικές πληροφορίες, τελική έκθεση το αργότερο ένα μήνα μετά την υποβολή της κοινοποίησης περιστατικού σύμφωνα με το στοιχείο β), η οποία περιλαμβάνει τουλάχιστον τα ακόλουθα:

i) λεπτομερή περιγραφή του περιστατικού, μεταξύ άλλων της σοβαρότητάς του και των επιπτώσεών του·

ii) το είδος της απειλής ή τη βασική αιτία που ενδεχομένως προκάλεσε το περιστατικό·

iii) τα εφαρμοζόμενα και εν εξελίξει μέτρα μετριασμού.

5. Για τους σκοπούς της παραγράφου 3, περιστατικό που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία θεωρείται σοβαρό όταν:

α) επηρεάζει αρνητικά ή είναι ικανό να επηρεάσει αρνητικά την ικανότητα ενός προϊόντος με ψηφιακά στοιχεία να προστατεύει τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα ευαίσθητων ή σημαντικών δεδομένων ή λειτουργιών· ή

β) έχει οδηγήσει ή είναι ικανό να οδηγήσει στην εισαγωγή ή την εκτέλεση κακόβουλου κώδικα σε προϊόν με ψηφιακά στοιχεία ή στα συστήματα δικτύου και πληροφοριών ενός χρήστη του προϊόντος με ψηφιακά στοιχεία.

6. Όπου είναι αναγκαίο, η ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού και η οποία λαμβάνει πρώτη την κοινοποίηση μπορεί να ζητήσει από τους κατασκευαστές να υποβάλουν ενδιάμεση έκθεση σχετικά με τις οικείες επικαιροποιήσεις της κατάστασης όσον αφορά την ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης ή το σοβαρό περιστατικό που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία.

7. Οι κοινοποιήσεις που αναφέρονται στις παραγράφους 1 και 3 του παρόντος άρθρου υποβάλλονται μέσω της ενιαίας πλατφόρμας αναφοράς που αναφέρεται στο άρθρο 16 με τη χρήση ενός από τα τελικά σημεία ηλεκτρονικής κοινοποίησης που αναφέρονται στο άρθρο 16 παράγραφος 1. Η κοινοποίηση υποβάλλεται μέσω του τελικού σημείου ηλεκτρονικής κοινοποίησης της ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού, του κράτους μέλους στο οποίο οι κατασκευαστές έχουν την κύρια εγκατάστασή τους στην Ένωση, και είναι ταυτόχρονα προσβάσιμη στον ENISA.

Για τους σκοπούς του παρόντος κανονισμού, ένας κατασκευαστής θεωρείται ότι έχει την κύρια εγκατάστασή του στην Ένωση στο κράτος μέλος όπου λαμβάνονται κυρίως οι αποφάσεις σχετικά με την κυβερνοασφάλεια των προϊόντων του με ψηφιακά στοιχεία. Εάν το εν λόγω κράτος μέλος δεν μπορεί να προσδιοριστεί, η κύρια εγκατάσταση θεωρείται ότι βρίσκεται στο κράτος μέλος στο οποίο ο οικείος κατασκευαστής έχει την εγκατάσταση με τον μεγαλύτερο αριθμό εργαζομένων στην Ένωση.

Όταν ένας κατασκευαστής δεν έχει κύρια εγκατάσταση στην Ένωση, υποβάλλει τις κοινοποιήσεις που αναφέρονται στις παραγράφους 1 και 3 χρησιμοποιώντας το τελικό σημείο ηλεκτρονικής κοινοποίησης της ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού στο κράτος μέλος που καθορίζεται σύμφωνα με την ακόλουθη σειρά και με βάση τις πληροφορίες που έχει στη διάθεσή του ο κατασκευαστής:

α) το κράτος μέλος στο οποίο είναι εγκατεστημένος ο εξουσιοδοτημένος αντιπρόσωπος που ενεργεί για λογαριασμό του κατασκευαστή για τον μεγαλύτερο αριθμό προϊόντων με ψηφιακά στοιχεία του εν λόγω κατασκευαστή·

β) το κράτος μέλος στο οποίο είναι εγκατεστημένος ο εισαγωγέας που θέτει σε κυκλοφορία στην αγορά τον μεγαλύτερο αριθμό προϊόντων με ψηφιακά στοιχεία του εν λόγω κατασκευαστή·

γ) το κράτος μέλος στο οποίο είναι εγκατεστημένος ο διανομέας που διαθέτει στην αγορά τον μεγαλύτερο αριθμό προϊόντων με ψηφιακά στοιχεία του εν λόγω κατασκευαστή·

δ) το κράτος μέλος στο οποίο βρίσκεται ο μεγαλύτερος αριθμός χρηστών προϊόντων με ψηφιακά στοιχεία του εν λόγω κατασκευαστή.

Όσον αφορά το τρίτο εδάφιο στοιχείο δ), ο κατασκευαστής μπορεί να υποβάλλει κοινοποιήσεις σχετικά με οποιαδήποτε μεταγενέστερη ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης ή οποιοδήποτε μεταγενέστερο σοβαρό περιστατικό που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία στην ίδια ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού και στην οποία υπέβαλε αναφορά την πρώτη φορά.

8. Αφού αντιληφθεί μια ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης ή ένα σοβαρό περιστατικό που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία, ο κατασκευαστής ενημερώνει τους επηρεαζόμενους χρήστες του προϊόντος με ψηφιακά στοιχεία και, κατά περίπτωση, όλους τους χρήστες, σχετικά με την εν λόγω ευπάθεια ή το σοβαρό περιστατικό και, κατά περίπτωση, σχετικά με τυχόν μέτρα μετριασμού του κινδύνου και διορθωτικά μέτρα που μπορούν να λάβουν οι χρήστες για τον μετριασμό των επιπτώσεων της εν λόγω ευπάθειας ή συμβάντος, κατά περίπτωση σε δομημένο και μηχαναγνώσιμο μορφότυπο που μπορεί να υποβληθεί εύκολα σε αυτόματη επεξεργασία. Σε περίπτωση που ο κατασκευαστής δεν ενημερώσει εγκαίρως τους χρήστες του προϊόντος με ψηφιακά στοιχεία, οι κοινοποιημένες ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού μπορούν να παρέχουν τις εν λόγω πληροφορίες στους χρήστες όταν αυτό θεωρείται αναλογικό και αναγκαίο για την πρόληψη ή τον μετριασμό των επιπτώσεων της εν λόγω ευπάθειας ή συμβάντος.

9. Έως τις … [12 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], η Επιτροπή εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 61 του παρόντος κανονισμού, για τη συμπλήρωση του παρόντος κανονισμού με τον προσδιορισμό των όρων και προϋποθέσεων για την επίκληση λόγων κυβερνοασφάλειας σε σχέση με την καθυστέρηση της διάδοσης των κοινοποιήσεων, όπως αναφέρεται στο άρθρο 16 παράγραφος 2 του παρόντος κανονισμού. Η Επιτροπή συνεργάζεται με το δίκτυο ΟΑΠΑΥ που συγκροτείται σύμφωνα με το άρθρο 15 της οδηγίας (ΕΕ) 2022/2555, και με τον ENISA κατά την κατάρτιση των σχεδίων κατ' εξουσιοδότηση πράξεων.

10. Η Επιτροπή μπορεί, με εκτελεστικές πράξεις, να προσδιορίσει περαιτέρω τον μορφότυπο και τις διαδικασίες των κοινοποιήσεων που αναφέρονται στο παρόν άρθρο, καθώς και στα άρθρα 15 και 16. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 62 παράγραφος 2. Η Επιτροπή συνεργάζεται με το δίκτυο ΟΑΠΑΥ και τον ENISA κατά την κατάρτιση των εν λόγω σχεδίων εκτελεστικών πράξεων.

Άρθρο 15

Εθελοντική αναφορά

1. Οι κατασκευαστές, καθώς και άλλα φυσικά ή νομικά πρόσωπα, μπορούν να κοινοποιούν κάθε ευπάθεια που περιέχεται σε προϊόν με ψηφιακά στοιχεία, καθώς και κυβερνοαπειλές που θα μπορούσαν να επηρεάσουν το προφίλ κινδύνου ενός προϊόντος με ψηφιακά στοιχεία, σε εθελοντική βάση, σε ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού ή στον ENISA.

2. Οι κατασκευαστές, καθώς και άλλα φυσικά ή νομικά πρόσωπα, μπορούν να κοινοποιούν κάθε περιστατικό που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία, καθώς και παρ' ολίγον περιστατικά που θα μπορούσαν να έχουν οδηγήσει σε τέτοιο περιστατικό, σε εθελοντική βάση, σε ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού ή στον ENISA.

3. Η ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού ή ο ENISA επεξεργάζεται τις κοινοποιήσεις που αναφέρονται στις παραγράφους 1 και 2 του παρόντος άρθρου σύμφωνα με τη διαδικασία του άρθρου 16.

   Η ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού μπορεί να δίνει προτεραιότητα στην επεξεργασία των υποχρεωτικών κοινοποιήσεων έναντι των εθελοντικών κοινοποιήσεων.

4. Όταν ένα φυσικό ή νομικό πρόσωπο άλλο από τον κατασκευαστή κοινοποιεί ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης ή σοβαρό περιστατικό που έχει αντίκτυπο στην ασφάλεια προϊόντος με ψηφιακά στοιχεία σύμφωνα με την παράγραφο 1 ή 2, η ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού ενημερώνει χωρίς αδικαιολόγητη καθυστέρηση τον κατασκευαστή.

5. Οι ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού, καθώς και ο ENISA διασφαλίζουν την εμπιστευτικότητα και την κατάλληλη προστασία των πληροφοριών που παρέχει το κοινοποιούν φυσικό ή νομικό πρόσωπο. Με την επιφύλαξη της πρόληψης, της διερεύνησης, της διακρίβωσης και της δίωξης ποινικών αδικημάτων, η εθελοντική αναφορά δεν συνεπάγεται την επιβολή πρόσθετων υποχρεώσεων στο κοινοποιούν φυσικό ή νομικό πρόσωπο, τις οποίες δεν θα υπείχε αν δεν είχε υποβάλει την κοινοποίηση.

Άρθρο 16

Σύσταση ενιαίας πλατφόρμας αναφοράς

1. Για τους σκοπούς των κοινοποιήσεων που αναφέρονται στο άρθρο 14 παράγραφοι 1 και 3 και στο άρθρο 15 παράγραφοι 1 και 2 και προκειμένου να απλουστευθούν οι υποχρεώσεις αναφοράς των κατασκευαστών, ο ENISA δημιουργεί ενιαία πλατφόρμα αναφοράς.
Ο ENISA διαχειρίζεται και συντηρεί τις καθημερινές λειτουργίες της εν λόγω ενιαίας πλατφόρμας αναφοράς. Η αρχιτεκτονική της ενιαίας πλατφόρμας αναφοράς επιτρέπει στα κράτη μέλη και στον ENISA να δημιουργήσουν τα δικά τους τελικά σημεία ηλεκτρονικής κοινοποίησης.

2. Μετά τη λήψη κοινοποίησης, η ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού και η οποία λαμβάνει πρώτη την κοινοποίηση διαδίδει, χωρίς καθυστέρηση, την κοινοποίηση μέσω της ενιαίας πλατφόρμας αναφοράς στις ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού στην επικράτεια στην οποία ο κατασκευαστής έχει δηλώσει ότι έχει καταστεί διαθέσιμο το προϊόν με ψηφιακά στοιχεία.

Σε εξαιρετικές περιστάσεις και, ιδίως, κατόπιν αιτήματος του κατασκευαστή και υπό το πρίσμα του επιπέδου ευαισθησίας των κοινοποιημένων πληροφοριών, όπως αυτό δηλώνεται από τον κατασκευαστή σύμφωνα με το άρθρο 14 παράγραφος 2 στοιχείο α) του παρόντος κανονισμού, η διάδοση της κοινοποίησης μπορεί να καθυστερήσει για αιτιολογημένους λόγους που σχετίζονται με την κυβερνοασφάλεια για χρονικό διάστημα κατά το οποίο αυτό είναι απολύτως αναγκαίο, μεταξύ άλλων όταν μια ευπάθεια υπόκειται σε διαδικασία συντονισμένης γνωστοποίησης ευπαθειών, όπως αναφέρεται στο άρθρο 12 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555. Όταν μια ΟΑΠΑΥ αποφασίζει να μην προβεί σε κοινοποίηση, ενημερώνει αμέσως τον ENISA σχετικά με την απόφαση αυτή και παρέχει αιτιολόγηση για την άρνηση της κοινοποίησης, καθώς και ένδειξη σχετικά με το πότε θα διαδώσει την κοινοποίηση σύμφωνα με τη διαδικασία διάδοσης που ορίζεται στην παρούσα παράγραφο. Ο ENISA μπορεί να παρέχει στήριξη στην ΟΑΠΑΥ ως προς την επίκληση λόγων κυβερνοασφάλειας σε σχέση με την καθυστέρηση της διάδοσης της κοινοποίησης.

Σε ιδιαίτερα εξαιρετικές περιστάσεις, όταν ο κατασκευαστής αναφέρει στην κοινοποίηση που αναφέρεται στο άρθρο 14 παράγραφος 2 στοιχείο β):

α) ότι η κοινοποιηθείσα ευπάθεια έχει αποτελέσει αντικείμενο ενεργού εκμετάλλευσης από κακόβουλο παράγοντα και, σύμφωνα με τις διαθέσιμες πληροφορίες, δεν έχει αποτελέσει αντικείμενο εκμετάλλευσης σε κανένα άλλο κράτος μέλος εκτός από εκείνο της ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού και στην οποία ο κατασκευαστής έχει κοινοποιήσει την ευπάθεια·

β) ότι οποιαδήποτε άμεση περαιτέρω διάδοση της κοινοποιηθείσας ευπάθειας ενδέχεται να έχει ως αποτέλεσμα την παροχή πληροφοριών των οποίων η αποκάλυψη θα ήταν αντίθετη προς τα ουσιώδη συμφέροντα του εν λόγω κράτους μέλους· ή

γ) ότι η κοινοποιηθείσα ευπάθεια συνεπάγεται άμεσο υψηλό κίνδυνο κυβερνοασφάλειας που απορρέει από την περαιτέρω διάδοση·

μόνο οι πληροφορίες ότι πραγματοποιήθηκε κοινοποίηση από τον κατασκευαστή, οι γενικές πληροφορίες σχετικά με το προϊόν, οι πληροφορίες σχετικά με τον γενικό χαρακτήρα της εκμετάλλευσης και η πληροφορία ότι έχουν προβληθεί λόγοι ασφαλείας, πρέπει να τίθενται ταυτόχρονα στη διάθεση του ENISA μέχρι να διαδοθεί η πλήρης κοινοποίηση στις οικείες ΟΑΠΑΥ και στον ENISA. Όταν, βάσει των εν λόγω πληροφοριών, ο ENISA θεωρεί ότι υπάρχει συστημικός κίνδυνος που επηρεάζει την ασφάλεια της εσωτερικής αγοράς, συνιστά στην αποδέκτρια ΟΑΠΑΥ να διαδώσει την πλήρη κοινοποίηση στις άλλες ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού, καθώς και στον ίδιο τον ENISA.

3. Αφότου λάβουν κοινοποίηση ευπάθειας που αποτελεί αντικείμενο ενεργού εκμετάλλευσης σε προϊόν με ψηφιακά στοιχεία ή σοβαρού περιστατικού που έχει αντίκτυπο στην ασφάλεια προϊόντος με ψηφιακά στοιχεία, οι ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού παρέχουν στις αρχές εποπτείας της αγοράς των αντίστοιχων κρατών μελών τους τις κοινοποιηθείσες πληροφορίες που είναι απαραίτητες προκειμένου οι αρχές εποπτείας της αγοράς να εκπληρώσουν τις υποχρεώσεις τους δυνάμει του παρόντος κανονισμού.

4. Ο ENISA λαμβάνει κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων που απειλούν την ασφάλεια της ενιαίας πλατφόρμας αναφοράς και των πληροφοριών που υποβάλλονται ή διαδίδονται μέσω της ενιαίας πλατφόρμας αναφοράς. Κοινοποιεί χωρίς αδικαιολόγητη καθυστέρηση κάθε περιστατικό ασφαλείας που επηρεάζει την ενιαία πλατφόρμα αναφοράς στο δίκτυο ΟΑΠΑΥ, καθώς και στην Επιτροπή.

5. Ο ENISA, σε συνεργασία με το δίκτυο ΟΑΠΑΥ, παρέχει και εφαρμόζει προδιαγραφές σχετικά με τα τεχνικά, επιχειρησιακά και οργανωτικά μέτρα όσον αφορά τη δημιουργία, τη συντήρηση και την ασφαλή λειτουργία της ενιαίας πλατφόρμας αναφοράς που αναφέρεται στην παράγραφο 1, συμπεριλαμβανομένων τουλάχιστον των ρυθμίσεων ασφάλειας που σχετίζονται με τη δημιουργία, τη λειτουργία και τη συντήρηση της ενιαίας πλατφόρμας αναφοράς, καθώς και των τελικών σημείων ηλεκτρονικής κοινοποίησης που καθορίζονται από τις ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού σε εθνικό επίπεδο και τον ENISA σε επίπεδο Ένωσης, συμπεριλαμβανομένων διαδικαστικών πτυχών ώστε να διασφαλίζεται ότι, όταν δεν διατίθενται διορθωτικά μέτρα ή μέτρα μετριασμού για μια κοινοποιηθείσα ευπάθεια, οι πληροφορίες σχετικά με την εν λόγω ευπάθεια ανταλλάσσονται σύμφωνα με αυστηρά πρωτόκολλα ασφαλείας και με βάση την ανάγκη γνώσης.

6. Όταν μια ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού έχει ενημερωθεί για μια ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης στο πλαίσιο διαδικασίας συντονισμένης γνωστοποίησης ευπαθειών, όπως αναφέρεται στο άρθρο 12 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555, η ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού και η οποία λαμβάνει πρώτη την κοινοποίηση, μπορεί να καθυστερήσει τη διάδοση της σχετικής κοινοποίησης μέσω της ενιαίας πλατφόρμας αναφοράς για αιτιολογημένους λόγους που σχετίζονται με την κυβερνοασφάλεια για χρονικό διάστημα που δεν υπερβαίνει το απολύτως αναγκαίο και έως ότου δοθεί η συγκατάθεση για γνωστοποίηση από τα μέρη που εμπλέκονται στη συντονισμένη γνωστοποίηση ευπαθειών. Η απαίτηση αυτή δεν εμποδίζει τους κατασκευαστές να κοινοποιούν τις εν λόγω ευπάθειες σε εθελοντική βάση σύμφωνα με τη διαδικασία του παρόντος άρθρου.

Άρθρο 17

Άλλες διατάξεις σε σχέση με την αναφορά

1. Ο ENISA υποβάλλει στο ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για τις κυβερνοκρίσεις (EU-CyCLONe) που συγκροτείται δυνάμει του άρθρου 16 της οδηγίας (ΕΕ) 2022/2555 πληροφορίες που κοινοποιούνται σύμφωνα με το άρθρο 14 παράγραφοι 1 και 3 και το άρθρο 15 παράγραφοι 1 και 2 του παρόντος κανονισμού, εάν οι πληροφορίες αυτές είναι σημαντικές για τη συντονισμένη διαχείριση μεγάλης κλίμακας περιστατικών και κρίσεων κυβερνοασφάλειας σε επιχειρησιακό επίπεδο. Για να προσδιοριστεί κατά πόσον είναι σημαντικές οι πληροφορίες αυτές, ο ENISA μπορεί να εξετάζει τεχνικές αναλύσεις που διενεργούνται από το δίκτυο ΟΑΠΑΥ, εφόσον είναι διαθέσιμες.

2. Όταν η ευαισθητοποίηση του κοινού είναι αναγκαία για την πρόληψη ή τον μετριασμό σοβαρού περιστατικού που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία ή για τον χειρισμό εν εξελίξει περιστατικού, ή όταν η γνωστοποίηση του περιστατικού εξυπηρετεί με άλλον τρόπο το δημόσιο συμφέρον, η ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού στο οικείο κράτος μέλος μπορεί, κατόπιν διαβούλευσης με τον οικείο κατασκευαστή και, κατά περίπτωση, σε συνεργασία με τον ENISA, να ενημερώσει το κοινό σχετικά με το περιστατικό ή να απαιτήσει από τον κατασκευαστή να το πράξει.

3. Ο ENISA, με βάση τις κοινοποιήσεις που λαμβάνει σύμφωνα με το άρθρο 14 παράγραφοι 1 και 3 και το άρθρο 15 παράγραφοι 1 και 2 του παρόντος κανονισμού, καταρτίζει, κάθε 24 μήνες, 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 συγκροτείται δυνάμει του άρθρου 14 της οδηγίας (ΕΕ) 2022/2555. Η πρώτη τέτοια έκθεση υποβάλλεται εντός 24 μηνών από την ημερομηνία εφαρμογής των υποχρεώσεων που ορίζονται στο άρθρο 14 παράγραφοι 1 και 3 του παρόντος κανονισμού. Ο ENISA περιλαμβάνει σχετικές πληροφορίες από τις τεχνικές εκθέσεις του στην έκθεσή του σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση σύμφωνα με το άρθρο 18 της οδηγίας (ΕΕ) 2022/2555.

4. Η κοινοποίηση σύμφωνα με το άρθρο 14 παράγραφοι 1 και 3 ή το άρθρο 15 παράγραφοι 1 και 2 δεν συνεπάγεται από μόνη της αυξημένη ευθύνη του κοινοποιούντος φυσικού ή νομικού προσώπου.

5. Μόλις διατεθεί ενημέρωση ασφαλείας ή άλλης μορφής διορθωτικό μέτρο ή μέτρο μετριασμού, ο ENISA, σε συμφωνία με τον κατασκευαστή του οικείου προϊόντος με ψηφιακά στοιχεία, προσθέτει τη δημοσίως γνωστή ευπάθεια που κοινοποιείται σύμφωνα με το άρθρο 14 παράγραφος 1 ή το άρθρο 15 παράγραφος 1 του παρόντος κανονισμού στην ευρωπαϊκή βάση δεδομένων ευπαθειών που δημιουργείται σύμφωνα με το άρθρο 12 παράγραφος 2 της οδηγίας (ΕΕ) 2022/2555.

6. Οι ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού παρέχουν τεχνική υποστήριξη σε σχέση με τις υποχρεώσεις αναφοράς σύμφωνα με το άρθρο 14 στους κατασκευαστές και ιδίως στους κατασκευαστές που χαρακτηρίζονται ως πολύ μικρές ή μικρές ή μεσαίες επιχειρήσεις.

Άρθρο 18

Εξουσιοδοτημένοι αντιπρόσωποι

1. Ο κατασκευαστής μπορεί να διορίζει, με γραπτή εντολή, εξουσιοδοτημένο αντιπρόσωπο.

2. Οι υποχρεώσεις που ορίζονται στο άρθρο 13 παράγραφοι 1 έως 11, στο άρθρο 13 παράγραφος 12 πρώτο εδάφιο και στο άρθρο 13 παράγραφος 14 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. Ο εξουσιοδοτημένος αντιπρόσωπος παρέχει αντίγραφο της εντολής στις αρχές εποπτείας της αγοράς κατόπιν αιτήματος. Η εντολή επιτρέπει στον εξουσιοδοτημένο αντιπρόσωπο τουλάχιστον τα ακόλουθα:

α) να τηρεί τη δήλωση συμμόρφωσης ΕΕ που αναφέρεται στο άρθρο 28 και τον τεχνικό φάκελο που αναφέρεται στο άρθρο 31 στη διάθεση των αρχών εποπτείας της αγοράς τουλάχιστον επί δέκα έτη αφότου τεθεί το προϊόν με ψηφιακά στοιχεία σε κυκλοφορία στην αγορά ή για την περίοδο υποστήριξης, ανάλογα με το ποιο διάστημα είναι μεγαλύτερο·

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 19

Υποχρεώσεις των εισαγωγέων

1. Οι εισαγωγείς θέτουν σε κυκλοφορία στην αγορά μόνο προϊόντα με ψηφιακά στοιχεία που συμμορφώνονται προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος I, και εφόσον οι διαδικασίες που εφαρμόζει ο κατασκευαστής συμμορφώνονται προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος II.

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

   α) ο κατασκευαστής έχει διενεργήσει τις κατάλληλες διαδικασίες αξιολόγησης της συμμόρφωσης όπως αναφέρονται στο άρθρο 32·

   β) ο κατασκευαστής έχει καταρτίσει τεχνικό φάκελο·

   γ) το προϊόν με ψηφιακά στοιχεία φέρει τη σήμανση CE που αναφέρεται στο άρθρο 30 και συνοδεύεται από τη δήλωση συμμόρφωσης ΕΕ, που αναφέρεται στο άρθρο 13 παράγραφος 20, και τις πληροφορίες και οδηγίες προς τον χρήστη, όπως ορίζονται στο παράρτημα II, σε γλώσσα εύκολα κατανοητή από τους χρήστες και τις αρχές εποπτείας της αγοράς·

   δ) ο κατασκευαστής έχει συμμορφωθεί με τις απαιτήσεις που καθορίζονται στο άρθρο 13 παράγραφοι 15, 16 και 19.

   Για τους σκοπούς της παρούσας παραγράφου, οι εισαγωγείς πρέπει να είναι σε θέση να προσκομίσουν τα αναγκαία έγγραφα που αποδεικνύουν την εκπλήρωση των απαιτήσεων που ορίζονται στο παρόν άρθρο.

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 τον παρόντα κανονισμό, ο εισαγωγέας δεν θέτει το προϊόν σε κυκλοφορία στην αγορά έως ότου το εν λόγω προϊόν ή οι διαδικασίες που εφαρμόζει ο κατασκευαστής συμμορφωθούν με τον παρόντα κανονισμό. 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.

Όταν ένας εισαγωγέας θεωρεί ή έχει λόγους να πιστεύει ότι ένα προϊόν με ψηφιακά στοιχεία μπορεί να παρουσιάζει σημαντικό κίνδυνο κυβερνοασφάλειας λόγω μη τεχνικών παραγόντων κινδύνου, ο εισαγωγέας ενημερώνει σχετικά τις αρχές εποπτείας της αγοράς. Μόλις λάβουν τις εν λόγω πληροφορίες, οι αρχές εποπτείας της αγοράς ακολουθούν τις διαδικασίες που αναφέρονται στο άρθρο 54 παράγραφος 2.

4. Οι εισαγωγείς αναγράφουν το όνομα, την καταχωρισμένη εμπορική επωνυμία ή το καταχωρισμένο εμπορικό σήμα, την ταχυδρομική διεύθυνση, τη διεύθυνση ηλεκτρονικού ταχυδρομείου ή άλλα ψηφιακά στοιχεία επικοινωνίας τους, καθώς και, κατά περίπτωση, τον ιστότοπο μέσω του οποίου μπορεί κανείς να επικοινωνήσει μαζί τους, στο προϊόν με ψηφιακά στοιχεία ή στη συσκευασία του ή σε έγγραφο που συνοδεύει το προϊόν με ψηφιακά στοιχεία. Τα στοιχεία επικοινωνίας παρέχονται σε γλώσσα εύκολα κατανοητή από τους χρήστες και τις αρχές εποπτείας της αγοράς.

5. Οι εισαγωγείς που γνωρίζουν ή έχουν λόγο να πιστεύουν ότι προϊόν με ψηφιακά στοιχεία που έχουν θέσει σε κυκλοφορία στην αγορά δεν συμμορφούται προς τον παρόντα κανονισμό λαμβάνουν αμέσως τα αναγκαία διορθωτικά μέτρα για να εξασφαλίσουν τη συμμόρφωση του προϊόντος με τον παρόντα κανονισμό, ή για να αποσύρουν ή να ανακαλέσουν το προϊόν, κατά περίπτωση.

Αμέσως μόλις αντιληφθούν την ύπαρξη ευπάθειας στο προϊόν με ψηφιακά στοιχεία, οι εισαγωγείς ενημερώνουν τον κατασκευαστή χωρίς αδικαιολόγητη καθυστέρηση σχετικά με την εν λόγω ευπάθεια. 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.

6. Οι εισαγωγείς τηρούν τουλάχιστον επί δέκα έτη αφότου το προϊόν με ψηφιακά στοιχεία τεθεί σε κυκλοφορία στην αγορά ή για την περίοδο υποστήριξης, ανάλογα με το ποιο διάστημα είναι μεγαλύτερο, 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.

7. 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 κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος I, καθώς και των διαδικασιών που εφαρμόζει ο κατασκευαστής προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος II, 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 κυβερνοασφάλειας τους οποίους ενέχουν τα προϊόντα με ψηφιακά στοιχεία που έχουν θέσει σε κυκλοφορία στην αγορά.

8. 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 έχουν τεθεί σε κυκλοφορία στην αγορά, με κάθε διαθέσιμο μέσο και στο μέτρο του δυνατού.

Άρθρο 20

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 που ορίζονται στον παρόντα κανονισμό.

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 στο άρθρο 13 παράγραφοι 15, 16, 18, 19 και 20 και στο άρθρο 19 παράγραφος 4, και έχουν διαβιβάσει όλα τα απαραίτητα έγγραφα στον διανομέα.

3. Όταν ο διανομέας θεωρεί ή έχει λόγους να πιστεύει, με βάση πληροφορίες που διαθέτει, ότι ένα προϊόν με ψηφιακά στοιχεία ή οι διαδικασίες που εφαρμόζει ο κατασκευαστής δεν συμμορφώνονται με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας 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 με τον παρόντα κανονισμό. 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, χωρίς αδικαιολόγητη καθυστέρηση.

4. Οι διανομείς που γνωρίζουν ή έχουν λόγο να πιστεύουν, με βάση τις πληροφορίες που διαθέτουν, ότι ένα προϊόν με ψηφιακά στοιχεία το οποίο έχουν διαθέσει στην αγορά ή οι διαδικασίες που εφαρμόζει ο κατασκευαστής του δεν συμμορφώνονται με τον παρόντα κανονισμό, 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 αντιληφθούν την ύπαρξη ευπάθειας στο προϊόν με ψηφιακά στοιχεία, οι διανομείς ενημερώνουν τον κατασκευαστή χωρίς αδικαιολόγητη καθυστέρηση σχετικά με την εν λόγω ευπάθεια. 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 με τον παρόντα κανονισμό, 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 κυβερνοασφάλειας τους οποίους ενέχουν τα προϊόντα με ψηφιακά στοιχεία που έχουν καταστεί διαθέσιμα στην αγορά.

6. Όταν ο διανομέας προϊόντος με ψηφιακά στοιχεία αντιληφθεί, με βάση τις πληροφορίες που διαθέτει, 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, χωρίς αδικαιολόγητη καθυστέρηση, τις αρμόδιες αρχές εποπτείας της αγοράς σχετικά με την κατάσταση αυτή, καθώς και τους χρήστες των προϊόντων με ψηφιακά στοιχεία που έχουν τεθεί σε κυκλοφορία στην αγορά, με κάθε διαθέσιμο μέσο και στο μέτρο του δυνατού.

Άρθρο 21

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

Ένας εισαγωγέας ή διανομέας θεωρείται κατασκευαστής για τους σκοπούς του παρόντος κανονισμού και υπόκειται στα άρθρα 13 και 14 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 προϊόν με ψηφιακά στοιχεία που έχει ήδη τεθεί σε κυκλοφορία στην αγορά.

Άρθρο 22

Άλλες περιπτώσεις στις οποίες εφαρμόζονται οι υποχρεώσεις των κατασκευαστών

1. Φυσικό ή νομικό πρόσωπο, πέραν του κατασκευαστή, του εισαγωγέα ή του διανομέα, που πραγματοποιεί ουσιαστική τροποποίηση προϊόντος με ψηφιακά στοιχεία και διαθέτει το εν λόγω προϊόν στην αγορά, θεωρείται κατασκευαστής για τους σκοπούς του παρόντος κανονισμού.

2. Το πρόσωπο που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου υπόκειται στις υποχρεώσεις που ορίζονται στα άρθρα 13 και 14, για το μέρος του προϊόντος με ψηφιακά στοιχεία 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 23

Ταυτοποίηση των οικονομικών φορέων

1. Οι οικονομικοί φορείς παρέχουν, κατόπιν αιτήματος, στις αρχές εποπτείας της αγοράς τις ακόλουθες πληροφορίες:

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

   β) εφόσον υπάρχουν, το όνομα και τη 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 10 έτη αφότου έχουν προμηθευτεί το προϊόν με ψηφιακά στοιχεία και επί 10 έτη αφότου έχουν προμηθεύσει το προϊόν με ψηφιακά στοιχεία.

Άρθρο 24

Υποχρεώσεις υποστηρικτών ελεύθερου λογισμικού ανοικτού κώδικα

1. Οι υποστηρικτές λογισμικού ανοικτού κώδικα θεσπίζουν και τεκμηριώνουν με επαληθεύσιμο τρόπο μια πολιτική κυβερνοασφάλειας προκειμένου να προωθήσουν την ανάπτυξη ενός ασφαλούς προϊόντος με ψηφιακά στοιχεία, καθώς και τον αποτελεσματικό χειρισμό των ευπαθειών από τους φορείς ανάπτυξης του εν λόγω προϊόντος. Η εν λόγω πολιτική προωθεί επίσης την εθελοντική αναφορά ευπαθειών, όπως ορίζεται στο άρθρο 15, από τους φορείς ανάπτυξης του εν λόγω προϊόντος και λαμβάνει υπόψη την ειδική φύση του υποστηρικτή λογισμικού ανοικτού κώδικα και τις νομικές και οργανωτικές ρυθμίσεις στις οποίες αυτός υπόκειται. Η εν λόγω πολιτική περιλαμβάνει, ειδικότερα, πτυχές που σχετίζονται με την τεκμηρίωση, την αντιμετώπιση και τη διόρθωση ευπαθειών και προωθεί την ανταλλαγή πληροφοριών εντός της κοινότητας ανοικτού κώδικα σχετικά με τις ευπάθειες που ανακαλύπτονται.

2. Οι υποστηρικτές λογισμικού ανοικτού κώδικα συνεργάζονται με τις αρχές εποπτείας της αγοράς, κατόπιν αιτήματός τους, με σκοπό τον μετριασμό των κινδύνων κυβερνοασφάλειας που ενέχει ένα προϊόν με ψηφιακά στοιχεία που χαρακτηρίζεται ως ελεύθερο λογισμικό ανοικτού κώδικα.

   Κατόπιν αιτιολογημένου αιτήματος αρχής εποπτείας της αγοράς, οι υποστηρικτές λογισμικού ανοικτού κώδικα παρέχουν στην εν λόγω αρχή, σε γλώσσα εύκολα κατανοητή από την εν λόγω αρχή, την τεκμηρίωση που αναφέρεται στην παράγραφο 1, σε έντυπη ή ηλεκτρονική μορφή.

3. Οι υποχρεώσεις που ορίζονται στο άρθρο 14 παράγραφος 1 ισχύουν για τους υποστηρικτές λογισμικού ανοικτού κώδικα στον βαθμό που συμμετέχουν στην ανάπτυξη των προϊόντων με ψηφιακά στοιχεία. Οι υποχρεώσεις που ορίζονται στο άρθρο 14 παράγραφοι 3 και 8 ισχύουν για τους υποστηρικτές λογισμικού ανοικτού κώδικα στον βαθμό που σοβαρά περιστατικά που έχουν αντίκτυπο στην ασφάλεια προϊόντων με ψηφιακά στοιχεία επηρεάζουν τα συστήματα δικτύου και πληροφοριών που παρέχονται από τους υποστηρικτές λογισμικού ανοικτού κώδικα για την ανάπτυξη των εν λόγω προϊόντων.

Άρθρο 25

Πιστοποίηση ασφάλειας για ελεύθερο λογισμικό ανοικτού κώδικα

Προκειμένου να διευκολυνθεί η εκπλήρωση της υποχρέωσης δέουσας επιμέλειας που ορίζεται στο άρθρο 13 παράγραφος 5, ιδίως όσον αφορά τους κατασκευαστές που ενσωματώνουν δομοστοιχεία ελεύθερου λογισμικού ανοικτού κώδικα στα προϊόντα τους με ψηφιακά στοιχεία, ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 61 για τη συμπλήρωση του παρόντος κανονισμού με τη θέσπιση εθελοντικών προγραμμάτων πιστοποίησης ασφάλειας που επιτρέπουν στους φορείς ανάπτυξης ή τους χρήστες προϊόντων με ψηφιακά στοιχεία που χαρακτηρίζονται ως ελεύθερο λογισμικό ανοικτού κώδικα, καθώς και σε άλλα τρίτα μέρη, να αξιολογούν τη συμμόρφωση των εν λόγω προϊόντων με όλες ή ορισμένες από τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας ή άλλες υποχρεώσεις που ορίζονται στον παρόντα κανονισμό.

Άρθρο 26

Καθοδήγηση

1. Προκειμένου να διευκολυνθεί η εφαρμογή και να διασφαλιστεί η συνέπεια της εν λόγω εφαρμογής, η Επιτροπή δημοσιεύει καθοδήγηση για να βοηθήσει τους οικονομικούς φορείς στην εφαρμογή του παρόντος κανονισμού, με ιδιαίτερη έμφαση στη διευκόλυνση της συμμόρφωσης των πολύ μικρών και των μικρών και μεσαίων επιχειρήσεων.

2. Όταν προτίθεται να παράσχει καθοδήγηση όπως αναφέρεται στην παράγραφο 1, η Επιτροπή εξετάζει τουλάχιστον τις ακόλουθες πτυχές:

   α) το πεδίο εφαρμογής του παρόντος κανονισμού, με ιδιαίτερη έμφαση σε λύσεις εξ αποστάσεως επεξεργασίας δεδομένων και σε ελεύθερο λογισμικό ανοικτού κώδικα·

   β) την εφαρμογή περιόδων υποστήριξης σε σχέση με συγκεκριμένες κατηγορίες προϊόντων με ψηφιακά στοιχεία·

   γ) καθοδήγηση που απευθύνεται στους κατασκευαστές που υπόκεινται στον παρόντα κανονισμό και παράλληλα σε ενωσιακή νομοθεσία εναρμόνισης πέραν του παρόντος κανονισμού ή σε άλλες συναφείς νομικές πράξεις της Ένωσης·

   δ) την έννοια της ουσιαστικής τροποποίησης.

   Η Επιτροπή τηρεί επίσης εύκολα προσβάσιμο κατάλογο των κατ' εξουσιοδότηση και εκτελεστικών πράξεων που εκδίδονται δυνάμει του παρόντος κανονισμού.

3. Κατά την κατάρτιση της καθοδήγησης σύμφωνα με το παρόν άρθρο, η Επιτροπή διαβουλεύεται με σχετικά ενδιαφερόμενα μέρη.

Κεφάλαιο III

Συμμόρφωση του προϊόντος με ψηφιακά στοιχεία

Άρθρο 27

Τεκμήριο συμμόρφωσης

1. Τα προϊόντα με ψηφιακά στοιχεία και οι διαδικασίες που εφαρμόζει ο κατασκευαστής που συμμορφώνονται με εναρμονισμένα πρότυπα ή μέρη τους, τα στοιχεία αναφοράς των οποίων έχουν δημοσιευθεί στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* τεκμαίρεται ότι συμμορφώνονται προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι και τις οποίες αφορούν τα εν λόγω πρότυπα ή τα μέρη αυτών.

Η Επιτροπή, σύμφωνα με το άρθρο 10 παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 1025/2012, ζητά από έναν ή περισσότερους ευρωπαϊκούς οργανισμούς τυποποίησης να καταρτίσουν εναρμονισμένα πρότυπα για τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι του παρόντος κανονισμού. Κατά την προετοιμασία των αιτημάτων τυποποίησης για τον παρόντα κανονισμό, η Επιτροπή προσπαθεί να λάβει υπόψη τα υφιστάμενα ευρωπαϊκά και διεθνή πρότυπα κυβερνοασφάλειας που ισχύουν ήδη ή βρίσκονται υπό ανάπτυξη, προκειμένου να απλουστευθεί η ανάπτυξη εναρμονισμένων προτύπων, σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 1025/2012.

2. Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις με σκοπό τη θέσπιση κοινών προδιαγραφών που καλύπτουν τεχνικές απαιτήσεις οι οποίες παρέχουν μέσο συμμόρφωσης με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι για προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού.

Οι εν λόγω εκτελεστικές πράξεις εκδίδονται μόνον όταν πληρούνται οι ακόλουθες προϋποθέσεις:

α) η Επιτροπή έχει ζητήσει, σύμφωνα με το άρθρο 10 παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 1025/2012, από έναν ή περισσότερους ευρωπαϊκούς οργανισμούς τυποποίησης να καταρτίσουν εναρμονισμένο πρότυπο για τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι και:

i) το αίτημα δεν έχει γίνει δεκτό·

ii) τα εναρμονισμένα πρότυπα που αφορούν το εν λόγω αίτημα δεν παραδίδονται εντός της προθεσμίας που ορίζεται σύμφωνα με το άρθρο 10 παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 1025/2012· ή

iii) τα εναρμονισμένα πρότυπα δεν συνάδουν με το αίτημα· και

β) δεν έχει δημοσιευθεί στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* αναφορά σε εναρμονισμένα πρότυπα που καλύπτουν τις σχετικές ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I του παρόντος κανονισμού σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 1025/2012 ούτε αναμένεται να δημοσιευθεί τέτοια αναφορά σε εύλογο χρονικό διάστημα.

Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 62 παράγραφος 2.

3. Πριν από την κατάρτιση του σχεδίου εκτελεστικής πράξης που αναφέρεται στην παράγραφο 2 του παρόντος άρθρου, η Επιτροπή ενημερώνει την επιτροπή του άρθρου 22 του κανονισμού (ΕΕ) αριθ. 1025/2012 ότι θεωρεί ότι έχουν εκπληρωθεί οι προϋποθέσεις της παραγράφου 2 του παρόντος άρθρου.

4. Κατά την κατάρτιση του σχεδίου εκτελεστικής πράξης που αναφέρεται στην παράγραφο 2, η Επιτροπή λαμβάνει υπόψη τις απόψεις των σχετικών οργανισμών και διαβουλεύεται δεόντως με όλα τα σχετικά ενδιαφερόμενα μέρη.

5. Τα προϊόντα με ψηφιακά στοιχεία και οι διαδικασίες που εφαρμόζει ο κατασκευαστής που συμμορφώνονται με τις κοινές προδιαγραφές που θεσπίζονται με τις εκτελεστικές πράξεις που αναφέρονται στην παράγραφο 2 του παρόντος άρθρου, ή με μέρη αυτών, τεκμαίρεται ότι συμμορφώνονται προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας του παραρτήματος I που καλύπτονται από τις εν λόγω κοινές προδιαγραφές ή από μέρη αυτών.

6. Όταν ένα εναρμονισμένο πρότυπο εκδίδεται από ευρωπαϊκό οργανισμό τυποποίησης και προτείνεται στην Επιτροπή με σκοπό τη δημοσίευση των στοιχείων αναφοράς του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, η Επιτροπή αξιολογεί το εναρμονισμένο πρότυπο σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 1025/2012. Όταν τα στοιχεία αναφοράς εναρμονισμένου προτύπου δημοσιεύονται στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, η Επιτροπή καταργεί τις εκτελεστικές πράξεις που αναφέρονται στην παράγραφο 2 ή μέρη αυτών που καλύπτουν τις ίδιες ουσιώδεις απαιτήσεις κυβερνοασφάλειας με εκείνες που καλύπτονται από το εν λόγω εναρμονισμένο πρότυπο.

7. Όταν ένα κράτος μέλος θεωρεί ότι μια κοινή προδιαγραφή δεν πληροί πλήρως τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I, ενημερώνει σχετικά την Επιτροπή υποβάλλοντας λεπτομερή εξήγηση. Η Επιτροπή αξιολογεί την εν λόγω λεπτομερή εξήγηση και μπορεί, κατά περίπτωση, να τροποποιήσει την εκτελεστική πράξη με την οποία θεσπίζεται η εν λόγω κοινή προδιαγραφή.

8. 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 καθεστώτος πιστοποίησης της κυβερνοασφάλειας που έχει εγκριθεί δυνάμει του κανονισμού (ΕΕ) 2019/881 τεκμαίρεται ότι συμμορφώνονται με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I, εφόσον η δήλωση συμμόρφωσης ΕΕ ή το ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας, ή μέρη αυτών, καλύπτουν τις εν λόγω απαιτήσεις.

9. Η Επιτροπή εξουσιοδοτείται να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 61 του παρόντος κανονισμού για τη συμπλήρωση του παρόντος κανονισμού με τον προσδιορισμό των ευρωπαϊκών καθεστώτων πιστοποίησης της κυβερνοασφάλειας που θεσπίζονται σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 και τα οποία μπορούν να χρησιμοποιηθούν για την απόδειξη της συμμόρφωσης των προϊόντων με ψηφιακά στοιχεία προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας ή μέρη αυτών, όπως ορίζεται στο παράρτημα Ι του παρόντος κανονισμού. Επιπλέον, με την έκδοση ευρωπαϊκού πιστοποιητικού κυβερνοασφάλειας που εκδίδεται στο πλαίσιο των εν λόγω καθεστώτων, τουλάχιστον σε «σημαντικό» επίπεδο διασφάλισης, αίρεται η υποχρέωση του κατασκευαστή να διενεργεί αξιολόγηση της συμμόρφωσης από τρίτους για τις αντίστοιχες απαιτήσεις, όπως ορίζεται στο άρθρο 32 παράγραφος 2 στοιχεία α) και β), και στο άρθρο 32 παράγραφος 3 στοιχεία α) και β) του παρόντος κανονισμού.

Άρθρο 28

Δήλωση συμμόρφωσης ΕΕ

1. Η δήλωση συμμόρφωσης ΕΕ καταρτίζεται από τους κατασκευαστές σύμφωνα με το άρθρο 13 παράγραφος 12 και αναφέρει ότι πληρούνται αποδεδειγμένα οι ισχύουσες ουσιώδεις απαιτήσεις κυβερνοασφάλειας του παραρτήματος Ι.

2. Η δήλωση συμμόρφωσης ΕΕ έχει τη δομή που ορίζει το παράρτημα V και περιλαμβάνει τα στοιχεία που καθορίζονται στις σχετικές διαδικασίες αξιολόγησης της συμμόρφωσης οι οποίες προβλέπονται στο παράρτημα VIII. Η δήλωση αυτή επικαιροποιείται κατά περίπτωση. Καθίσταται διαθέσιμη στις γλώσσες που απαιτεί το κράτος μέλος στην αγορά του οποίου τίθεται σε κυκλοφορία ή διατίθεται το προϊόν με ψηφιακά στοιχεία.

Η απλουστευμένη δήλωση συμμόρφωσης ΕΕ που αναφέρεται στο άρθρο 13 παράγραφος 20 έχει τη δομή που ορίζει το παράρτημα VI. Καθίσταται διαθέσιμη στις γλώσσες που απαιτεί το κράτος μέλος στην αγορά του οποίου τίθεται σε κυκλοφορία ή διατίθεται το προϊόν με ψηφιακά στοιχεία.

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

5. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 61 για τη συμπλήρωση του παρόντος κανονισμού, με την προσθήκη στοιχείων στο ελάχιστο περιεχόμενο της δήλωσης συμμόρφωσης ΕΕ που παρατίθεται στο παράρτημα V, ώστε να λαμβάνονται υπόψη οι τεχνολογικές εξελίξεις.

Άρθρο 29

Γενικές αρχές της σήμανσης CE

Η σήμανση CE υπόκειται στις γενικές αρχές του άρθρου 30 του κανονισμού (ΕΚ) αριθ. 765/2008.

Άρθρο 30

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 του προϊόντος με ψηφιακά στοιχεία, τοποθετείται στη συσκευασία και στη δήλωση συμμόρφωσης ΕΕ που αναφέρεται στο άρθρο 28 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 28 είτε στον ιστότοπο που συνοδεύει το προϊόν λογισμικού. Στην τελευταία περίπτωση, το σχετικό τμήμα στον ιστότοπο είναι εύκολα και άμεσα προσβάσιμο στους καταναλωτές.

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 για την κυβερνοασφάλεια 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 32.

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 ενωσιακή νομοθεσία εναρμόνισης πέραν του παρόντος κανονισμού η οποία επίσης προβλέπει την τοποθέτηση της σήμανσης CE, η σήμανση CE δηλώνει ότι το προϊόν πληροί επίσης τις απαιτήσεις αυτής της άλλης ενωσιακής νομοθεσίας εναρμόνισης.

6. Η Επιτροπή μπορεί, με εκτελεστικές πράξεις, να καθορίζει τεχνικές προδιαγραφές για ετικέτες, εικονογράμματα ή άλλα σήματα που σχετίζονται με την ασφάλεια των προϊόντων με ψηφιακά στοιχεία, τις περιόδους υποστήριξής τους και μηχανισμούς για την προώθηση της χρήσης τους, καθώς και για την ενίσχυση της ευαισθητοποίησης του κοινού σχετικά με την ασφάλεια των προϊόντων με ψηφιακά στοιχεία. Κατά την κατάρτιση των σχεδίων εκτελεστικών πράξεων, η Επιτροπή διαβουλεύεται με τα σχετικά ενδιαφερόμενα μέρη και, εάν έχει ήδη θεσπιστεί σύμφωνα με το άρθρο 52 παράγραφος 15, με την ΕΟΔΚ. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 62 παράγραφος 2.

Άρθρο 31

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 κυβερνοασφάλειας που καθορίζονται στο παράρτημα Ι. Περιέχει τουλάχιστον τα στοιχεία που καθορίζονται στο παράρτημα VII.

2. Ο τεχνικός φάκελος καταρτίζεται προτού το προϊόν με ψηφιακά στοιχεία τεθεί σε κυκλοφορία στην αγορά και επικαιροποιείται συνεχώς, κατά περίπτωση, τουλάχιστον κατά τη διάρκεια της περιόδου υποστήριξης.

3. Για τα προϊόντα με ψηφιακά στοιχεία όπως αναφέρονται στο άρθρο 12, τα οποία διέπονται και από άλλες νομικές πράξεις της Ένωσης που προβλέπουν την κατάρτιση τεχνικού φακέλου, καταρτίζεται ενιαίος τεχνικός φάκελος που περιέχει τις πληροφορίες που αναφέρονται στο παράρτημα VII και τις πληροφορίες που απαιτούνται από τις εν λόγω νομικές 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 61 για τη συμπλήρωση του παρόντος κανονισμού με την προσθήκη στοιχείων που πρέπει να περιλαμβάνονται στον τεχνικό φάκελο του παραρτήματος VII, ώστε να λαμβάνονται υπόψη οι τεχνολογικές εξελίξεις, καθώς και οι εξελίξεις που προκύπτουν κατά τη διαδικασία εφαρμογής του παρόντος κανονισμού. Για τον σκοπό αυτό, η Επιτροπή επιδιώκει να διασφαλίσει ότι ο διοικητικός φόρτος για τις πολύ μικρές και τις μικρές και μεσαίες επιχειρήσεις είναι αναλογικός.

Άρθρο 32

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 κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι. Ο κατασκευαστής αποδεικνύει τη συμμόρφωση προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας εφαρμόζοντας οποιαδήποτε από τις ακόλουθες διαδικασίες:

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

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

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

δ) εφόσον είναι διαθέσιμο και εφαρμοστέο, ευρωπαϊκό καθεστώς πιστοποίησης της κυβερνοασφάλειας, σύμφωνα με το άρθρο 27 παράγραφος 9.

2. Όταν, κατά την αξιολόγηση της συμμόρφωσης σημαντικού προϊόντος με ψηφιακά στοιχεία που εμπίπτει στην κλάση I που ορίζεται στο παράρτημα III και των διαδικασιών που εφαρμόζει ο κατασκευαστής του προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I, ο κατασκευαστής δεν έχει εφαρμόσει ή έχει εφαρμόσει μόνο εν μέρει εναρμονισμένα πρότυπα, κοινές προδιαγραφές ή ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας σε επίπεδο διασφάλισης τουλάχιστον «σημαντικό», όπως αναφέρονται στο άρθρο 27, ή όταν δεν υπάρχουν τα εν λόγω εναρμονισμένα πρότυπα, κοινές προδιαγραφές ή ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας, το σχετικό προϊόν με ψηφιακά στοιχεία και οι διαδικασίες που εφαρμόζει ο κατασκευαστής υποβάλλονται, όσον αφορά τις εν λόγω ουσιώδεις απαιτήσεις κυβερνοασφάλειας, σε οποιαδήποτε από τις ακόλουθες διαδικασίες:

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

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

3. Όταν το προϊόν είναι σημαντικό προϊόν με ψηφιακά στοιχεία που εμπίπτει στην κλάση ΙΙ, όπως ορίζεται στο παράρτημα ΙΙΙ, ο κατασκευαστής αποδεικνύει τη συμμόρφωση προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι εφαρμόζοντας οποιαδήποτε από τις ακόλουθες διαδικασίες:

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

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

γ) εφόσον είναι διαθέσιμο και εφαρμοστέο, ευρωπαϊκό καθεστώς πιστοποίησης της κυβερνοασφάλειας σύμφωνα με το άρθρο 27 παράγραφος 9 του παρόντος κανονισμού σε επίπεδο διασφάλισης τουλάχιστον «σημαντικό» σύμφωνα με τον κανονισμό (ΕΕ) 2019/881.

4. Για τα κρίσιμα προϊόντα με ψηφιακά στοιχεία που απαριθμούνται στο παράρτημα IV, η συμμόρφωση προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στο παράρτημα Ι αποδεικνύεται με την εφαρμογή μίας από τις ακόλουθες διαδικασίες:

α) ευρωπαϊκού καθεστώτος πιστοποίησης της κυβερνοασφάλειας σύμφωνα με το άρθρο 8 παράγραφος 1· ή

β) όταν δεν πληρούνται οι προϋποθέσεις του άρθρου 8 παράγραφος 1, οποιασδήποτε από τις διαδικασίες που αναφέρονται στην παράγραφο 3 του παρόντος άρθρου.

5. Οι κατασκευαστές προϊόντων με ψηφιακά στοιχεία που χαρακτηρίζονται ως ελεύθερο λογισμικό ανοικτού κώδικα και τα οποία εμπίπτουν στις κατηγορίες που ορίζονται στο παράρτημα ΙΙΙ, είναι σε θέση να αποδείξουν τη συμμόρφωση με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι χρησιμοποιώντας μία από τις διαδικασίες που αναφέρονται στην παράγραφο 1 του παρόντος άρθρου, υπό την προϋπόθεση ότι ο τεχνικός φάκελος που αναφέρεται στο άρθρο 31 διατίθεται στο κοινό τη στιγμή που τα εν λόγω προϊόντα τίθενται σε κυκλοφορία στην αγορά.

6. Τα ειδικά συμφέροντα και οι ανάγκες των πολύ μικρών και των μικρών και μεσαίων επιχειρήσεων, συμπεριλαμβανομένων των νεοφυών επιχειρήσεων, λαμβάνονται υπόψη κατά τον καθορισμό των τελών για τις διαδικασίες αξιολόγησης της συμμόρφωσης και τα εν λόγω τέλη μειώνονται κατ' αναλογία προς τα ειδικά συμφέροντα και τις ανάγκες τους.

Άρθρο 33

Μέτρα στήριξης για τις πολύ μικρές και τις μικρές και μεσαίες επιχειρήσεις, συμπεριλαμβανομένων των νεοφυών επιχειρήσεων

1. Τα κράτη μέλη λαμβάνουν, κατά περίπτωση, τα ακόλουθα μέτρα, προσαρμοσμένα στις ανάγκες των πολύ μικρών και των μικρών επιχειρήσεων:

α) οργανώνουν ειδικές δραστηριότητες ευαισθητοποίησης και κατάρτισης σχετικά με την εφαρμογή του παρόντος κανονισμού·

β) δημιουργούν ειδικό δίαυλο επικοινωνίας με τις πολύ μικρές και τις μικρές επιχειρήσεις και, κατά περίπτωση, με τις τοπικές δημόσιες αρχές για την παροχή συμβουλών και απαντήσεων σε ερωτήματα σχετικά με την εφαρμογή του παρόντος κανονισμού·

γ) υποστηρίζουν δραστηριότητες δοκιμών και αξιολόγησης της συμμόρφωσης, μεταξύ άλλων, κατά περίπτωση, με την υποστήριξη του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Θέματα Κυβερνοασφάλειας.

2. Τα κράτη μέλη μπορούν, κατά περίπτωση, να δημιουργούν ρυθμιστικά δοκιμαστήρια κυβερνοανθεκτικότητας. Τα εν λόγω ρυθμιστικά δοκιμαστήρια παρέχουν ελεγχόμενα περιβάλλοντα δοκιμών για καινοτόμα προϊόντα με ψηφιακά στοιχεία, προκειμένου να διευκολύνεται η ανάπτυξη, ο σχεδιασμός, η επικύρωση και η δοκιμή τους με σκοπό τη συμμόρφωση με τον παρόντα κανονισμό για περιορισμένο χρονικό διάστημα πριν από τη θέση σε κυκλοφορία στην αγορά. Η Επιτροπή και, κατά περίπτωση, ο ENISA μπορούν να παρέχουν τεχνική υποστήριξη, συμβουλές και εργαλεία για τη δημιουργία και τη λειτουργία ρυθμιστικών δοκιμαστηρίων. Τα ρυθμιστικά δοκιμαστήρια δημιουργούνται υπό την άμεση εποπτεία, καθοδήγηση και υποστήριξη των αρχών εποπτείας της αγοράς. Τα κράτη μέλη ενημερώνουν την Επιτροπή και τις άλλες αρχές εποπτείας της αγοράς σχετικά με τη δημιουργία ρυθμιστικού δοκιμαστηρίου μέσω της ΕΟΔΚ. Τα ρυθμιστικά δοκιμαστήρια δεν θίγουν τις εποπτικές και διορθωτικές εξουσίες των αρμόδιων αρχών. Τα κράτη μέλη διασφαλίζουν την ανοικτή, δίκαιη και διαφανή πρόσβαση σε ρυθμιστικά δοκιμαστήρια, και ιδίως διευκολύνουν την πρόσβαση των πολύ μικρών και των μικρών επιχειρήσεων, συμπεριλαμβανομένων των νεοφυών επιχειρήσεων.

3. Σύμφωνα με το άρθρο 26, η Επιτροπή παρέχει καθοδήγηση στις πολύ μικρές και τις μικρές και μεσαίες επιχειρήσεις σε σχέση με την εφαρμογή του παρόντος κανονισμού.

4. Η Επιτροπή παρέχει ενημέρωση σχετικά με τη διαθέσιμη χρηματοδοτική στήριξη στο κανονιστικό πλαίσιο των υφιστάμενων προγραμμάτων της Ένωσης, ιδίως προκειμένου να μειωθεί ο οικονομικός φόρτος για τις πολύ μικρές και τις μικρές επιχειρήσεις.

5. Οι πολύ μικρές και οι μικρές επιχειρήσεις μπορούν να παρέχουν όλα τα στοιχεία του τεχνικού φακέλου που καθορίζεται στο παράρτημα VII χρησιμοποιώντας απλουστευμένο μορφότυπο. Για τον σκοπό αυτό, η Επιτροπή προσδιορίζει, μέσω εκτελεστικών πράξεων, το απλουστευμένο έντυπο τεχνικού φακέλου που απευθύνεται στις ανάγκες των πολύ μικρών και των μικρών επιχειρήσεων, συμπεριλαμβανομένου του τρόπου με τον οποίο πρέπει να παρέχονται τα στοιχεία που ορίζονται στο παράρτημα VII. Όταν μια πολύ μικρή ή μικρή επιχείρηση επιλέγει να παράσχει τις πληροφορίες που ορίζονται στο παράρτημα VII με απλουστευμένο τρόπο, χρησιμοποιεί το έντυπο που αναφέρεται στην παρούσα παράγραφο. Οι κοινοποιημένοι οργανισμοί αποδέχονται το έντυπο αυτό για τους σκοπούς της αξιολόγησης της συμμόρφωσης.

   Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 62 παράγραφος 2.

Άρθρο 34

Συμφωνίες αμοιβαίας αναγνώρισης

Λαμβάνοντας υπόψη το επίπεδο τεχνικής ανάπτυξης και την προσέγγιση που ακολουθεί τρίτη χώρα για την αξιολόγηση της συμμόρφωσης, η Ένωση μπορεί να συνάπτει συμφωνίες αμοιβαίας αναγνώρισης με τρίτες χώρες, σύμφωνα με το άρθρο 218 ΣΛΕΕ, με σκοπό την προώθηση και τη διευκόλυνση του διεθνούς εμπορίου.

Κεφάλαιο IV

Κοινοποίηση των οργανισμών αξιολόγησης της συμμόρφωσης

Άρθρο 35

Κοινοποίηση

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

2. Τα κράτη μέλη επιδιώκουν να διασφαλίσουν, έως τις … [24 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], ότι υπάρχει επαρκής αριθμός κοινοποιημένων οργανισμών στην Ένωση για τη διενέργεια αξιολογήσεων της συμμόρφωσης, ώστε να αποφεύγονται τα σημεία συμφόρησης και τα εμπόδια στην είσοδο στην αγορά.

Άρθρο 36

Κοινοποιούσες αρχές

1. Κάθε κράτος μέλος ορίζει μία κοινοποιούσα αρχή η οποία είναι υπεύθυνη για τον καθορισμό και τη διεξαγωγή των αναγκαίων διαδικασιών αξιολόγησης, ορισμού και κοινοποίησης των οργανισμών αξιολόγησης της συμμόρφωσης και για την παρακολούθησή τους, συμπεριλαμβανομένης της συμμόρφωσης με τις διατάξεις του άρθρου 41.

2. Τα κράτη μέλη μπορούν να αποφασίζουν ότι η αξιολόγηση και η παρακολούθηση στις οποίες αναφέρεται η παράγραφος 1 διεξάγονται από εθνικό οργανισμό διαπίστευσης, κατά την έννοια του κανονισμού (ΕΚ) αριθ. 765/2008 και σύμφωνα με αυτόν.

3. Εφόσον η κοινοποιούσα αρχή εκχωρήσει ή αναθέσει με άλλον τρόπο την αξιολόγηση, κοινοποίηση ή παρακολούθηση που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου σε οργανισμό που δεν είναι κρατική οντότητα, ο οργανισμός αυτός είναι νομικό πρόσωπο και συμμορφώνεται, κατ' αναλογία, με το άρθρο 37. Επιπλέον, προβαίνει σε διευθετήσεις ώστε να καλύπτει τις ευθύνες που προκύπτουν από τις δραστηριότητές του.

4. Η κοινοποιούσα αρχή αναλαμβάνει πλήρως την ευθύνη για τα καθήκοντα τα οποία εκτελεί ο οργανισμός που αναφέρεται στην παράγραφο 3.

Άρθρο 37

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 38

Υποχρέωση ενημέρωσης που υπέχουν οι 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 τις πληροφορίες που αναφέρονται στην παράγραφο 1.

Άρθρο 39

Απαιτήσεις που αφορούν 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 με ψηφιακά στοιχεία 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 τέτοιος ανεξάρτητος 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 τον σχεδιαστή, προγραμματιστή, κατασκευαστή, προμηθευτή, εισαγωγέα, διανομέα, 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 εισαγωγή, τη διανομή, την εμπορία, την εγκατάσταση, τη χρήση ή τη συντήρηση των εν λόγω προϊόντων με ψηφιακά στοιχεία που αξιολογούν, 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 VIII 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) προσωπικό με τις τεχνικές γνώσεις και την επαρκή και κατάλληλη πείρα για την εκτέλεση των καθηκόντων αξιολόγησης της συμμόρφωσης·

β) περιγραφές των διαδικασιών σύμφωνα με τις οποίες πρέπει να διενεργείται η αξιολόγηση της συμμόρφωσης, ώστε να 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.

Ο οργανισμός αξιολόγησης της συμμόρφωσης διαθέτει τα αναγκαία μέσα για την εκτέλεση των τεχνικών και διοικητικών καθηκόντων που συνδέονται με τις δραστηριότητες αξιολόγησης της συμμόρφωσης και έχει πρόσβαση σε όλον 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 ουσιωδών απαιτήσεων κυβερνοασφάλειας που καθορίζονται στο παράρτημα I, των εφαρμοστέων εναρμονισμένων προτύπων και κοινών προδιαγραφών, και των σχετικών διατάξεων της ενωσιακής νομοθεσίας εναρμόνισης και των εκτελεστικών πράξεων·

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

8. Εξασφαλίζεται η αμεροληψία του οργανισμού αξιολόγησης της συμμόρφωσης, των διευθυντικών στελεχών του και του προσωπικού αξιολόγησης.

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. Οι οργανισμοί αξιολόγησης της συμμόρφωσης συνάπτουν ασφάλεια αστικής ευθύνης, εκτός εάν η ευθύνη αυτή καλύπτεται από το οικείο κράτος μέλος βάσει του εθνικού δικαίου, ή εκτός εάν η αξιολόγηση της συμμόρφωσης 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 VIII 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 51, 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, αναλογικών και εύλογων όρων και προϋποθέσεων, αποφεύγοντας τις περιττές επιβαρύνσεις για τους οικονομικούς φορείς και λαμβάνοντας ιδίως υπόψη τα συμφέροντα των πολύ μικρών, μικρών και μεσαίων επιχειρήσεων σε σχέση με τα τέλη.

Άρθρο 40

Τεκμήριο συμμόρφωσης των κοινοποιημένων οργανισμών

Αν ο οργανισμός αξιολόγησης της συμμόρφωσης αποδείξει ότι πληροί τα κριτήρια που ορίζονται στα σχετικά εναρμονισμένα πρότυπα ή σε μέρη αυτών, τα στοιχεία των οποίων έχουν δημοσιευτεί στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, τότε τεκμαίρεται ότι συμμορφούται προς τις απαιτήσεις του άρθρου 39 εφόσον τα εφαρμοστέα εναρμονισμένα πρότυπα τηρούν τις απαιτήσεις αυτές.

Άρθρο 41

Θυγατρικές και υπεργολάβοι κοινοποιημένων οργανισμών

1. Όταν ο κοινοποιημένος οργανισμός αναθέτει με υπεργολαβία 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 39 και ενημερώνει αναλόγως την κοινοποιούσα αρχή.

2. Οι κοινοποιημένοι οργανισμοί αναλαμβάνουν 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 42

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 με ψηφιακά στοιχεία για τα οποία ο οργανισμός δηλώνει ότι είναι αρμόδιος, καθώς και, κατά περίπτωση, από πιστοποιητικό διαπίστευσης το οποίο έχει εκδοθεί από εθνικό οργανισμό διαπίστευσης, δια του οποίου πιστοποιείται ότι ο οργανισμός αξιολόγησης της συμμόρφωσης πληροί τις απαιτήσεις του άρθρου 39.

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 39.

Άρθρο 43

Διαδικασία κοινοποίησης

1. Οι κοινοποιούσες αρχές κοινοποιούν μόνο τους οργανισμούς αξιολόγησης της συμμόρφωσης που πληρούν τις απαιτήσεις του άρθρου 39.

2. Η κοινοποιούσα αρχή ενημερώνει την Επιτροπή και τα άλλα κράτη μέλη που χρησιμοποιούν το σύστημα πληροφόρησης των κοινοποιημένων και διαπιστευμένων οργανισμών νέας προσέγγισης 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 οικείο προϊόν ή τα οικεία προϊόντα με ψηφιακά στοιχεία και τη σχετική βεβαίωση επάρκειας.

4. Όταν η κοινοποίηση δεν βασίζεται σε πιστοποιητικό διαπίστευσης του άρθρου 42 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 39.

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 σχετικές αλλαγές στην κοινοποίηση.

Άρθρο 44

Αριθμοί μητρώου και κατάλογοι κοινοποιημένων οργανισμών

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

   Χορηγεί έναν μοναδικό αριθμό, ακόμη και αν ο οργανισμός είναι κοινοποιημένος βάσει διαφόρων νομικών 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 45

Αλλαγές στις κοινοποιήσεις

1. Όταν κοινοποιούσα αρχή διαπιστώνει ή πληροφορείται ότι κοινοποιημένος οργανισμός δεν πληροί πλέον τις απαιτήσεις του άρθρου 39, 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 46

Αμφισβήτηση της επάρκειας 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 47

Λειτουργικές υποχρεώσεις των κοινοποιημένων οργανισμών

1. Οι κοινοποιημένοι οργανισμοί διενεργούν αξιολογήσεις συμμόρφωσης σύμφωνα με τις διαδικασίες αξιολόγησης της συμμόρφωσης που προβλέπονται στο άρθρο 32 και στο παράρτημα VIII.

2. Οι αξιολογήσεις της συμμόρφωσης διενεργούνται κατά τρόπο αναλογικό, 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, ιδίως όσον αφορά τις πολύ μικρές και τις μικρές και μεσαίες επιχειρήσεις, τον τομέα στον οποίο αυτές δραστηριοποιούνται, τη δομή τους, την πολυπλοκότητα και το επίπεδο κινδύνου κυβερνοασφάλειας των εν λόγω προϊόντων με ψηφιακά στοιχεία και της εν λόγω τεχνολογίας και τον μαζικό ή εν σειρά χαρακτήρα της διαδικασίας παραγωγής.

3. Οι κοινοποιημένοι οργανισμοί τηρούν ωστόσο τον βαθμό αυστηρότητας και το επίπεδο προστασίας που απαιτούνται για τη συμμόρφωση του προϊόντος με ψηφιακά στοιχεία 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 27 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 με ψηφιακά στοιχεία 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 48

Προσφυγή κατά αποφάσεων των κοινοποιημένων οργανισμών

Τα κράτη μέλη διασφαλίζουν ότι προβλέπεται διαδικασία προσφυγής κατά των αποφάσεων των κοινοποιημένων οργανισμών.

Άρθρο 49

Υποχρέωση ενημέρωσης που υπέχουν οι κοινοποιημένοι οργανισμοί

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 με ψηφιακά στοιχεία, τις σχετικές πληροφορίες για ζητήματα που αφορούν αρνητικά και, εάν τους ζητηθεί, θετικά αποτελέσματα αξιολόγησης της συμμόρφωσης.

Άρθρο 50

Ανταλλαγή εμπειριών

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

Άρθρο 51

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.

Κεφάλαιο V

Εποπτεία της αγοράς και επιβολή της νομοθεσίας

Άρθρο 52

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. Οι αρχές εποπτείας της αγοράς που ορίζονται σύμφωνα με την παράγραφο 2 του παρόντος άρθρου είναι επίσης υπεύθυνες για τη διεξαγωγή δραστηριοτήτων εποπτείας της αγοράς σε σχέση με τις υποχρεώσεις για τους υποστηρικτές λογισμικού ανοικτού κώδικα που ορίζονται στο άρθρο 24. Όταν μια αρχή εποπτείας της αγοράς διαπιστώνει ότι ένας υποστηρικτής λογισμικού ανοικτού κώδικα δεν συμμορφώνεται με τις υποχρεώσεις που ορίζονται στο εν λόγω άρθρο, απαιτεί από τον υποστηρικτή λογισμικού ανοικτού κώδικα να διασφαλίσει ότι λαμβάνονται όλα τα κατάλληλα διορθωτικά μέτρα. Οι υποστηρικτές λογισμικού ανοικτού κώδικα διασφαλίζουν ότι λαμβάνονται όλα τα κατάλληλα διορθωτικά μέτρα όσον αφορά τις υποχρεώσεις τους βάσει του παρόντος κανονισμού.

4. Κατά περίπτωση, οι αρχές εποπτείας της αγοράς συνεργάζονται με τις εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας σύμφωνα με το άρθρο 58 του κανονισμού (ΕΕ) 2019/881 και ανταλλάσσουν πληροφορίες σε τακτική βάση. Όσον αφορά την εποπτεία της εφαρμογής των υποχρεώσεων αναφοράς σύμφωνα με το άρθρο 14 του παρόντος κανονισμού, οι ορισθείσες αρχές εποπτείας της αγοράς συνεργάζονται και ανταλλάσσουν πληροφορίες σε τακτική βάση με τις ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού και με τον ENISA.

5. Οι αρχές εποπτείας της αγοράς μπορούν να ζητήσουν από μια ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού ή από τον ENISA τεχνικές συμβουλές σε θέματα που σχετίζονται με την εφαρμογή και επιβολή του παρόντος κανονισμού. Κατά τη διενέργεια έρευνας δυνάμει του άρθρου 54, οι αρχές εποπτείας της αγοράς μπορούν να ζητήσουν από τη ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού ή από τον ENISA την παροχή ανάλυσης προς στήριξη των αξιολογήσεων της συμμόρφωσης προϊόντων με ψηφιακά στοιχεία.

6. Κατά περίπτωση, οι αρχές εποπτείας της αγοράς συνεργάζονται με άλλες αρχές εποπτείας της αγοράς που ορίζονται βάσει άλλης ενωσιακής νομοθεσίας εναρμόνισης πέραν του παρόντος κανονισμού, και ανταλλάσσουν πληροφορίες σε τακτική βάση.

7. 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 καθοδήγησης και συμβουλών σύμφωνα με την παράγραφο 10, εάν η εν λόγω καθοδήγηση 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.

8. Τα κράτη μέλη μεριμνούν ώστε οι ορισθείσες αρχές εποπτείας της αγοράς να διαθέτουν επαρκείς οικονομικούς και τεχνικούς πόρους, συμπεριλαμβανομένων, κατά περίπτωση, εργαλείων αυτοματοποίησης της επεξεργασίας, καθώς και ανθρώπινους πόρους με τις αναγκαίες δεξιότητες κυβερνοασφάλειας για την εκπλήρωση των καθηκόντων τους δυνάμει του παρόντος κανονισμού.

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

10. 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 και, κατά περίπτωση, των ΟΑΠΑΥ και του ENISA.

11. Οι αρχές εποπτείας της αγοράς ενημερώνουν τους καταναλωτές σχετικά με το πού μπορούν να υποβάλουν καταγγελίες για πιθανή μη συμμόρφωση με τον παρόντα κανονισμό, σύμφωνα με το άρθρο 11 του κανονισμού (ΕΕ) 2019/1020, και παρέχουν πληροφορίες στους καταναλωτές σχετικά με το πού και το πώς μπορούν να αποκτήσουν πρόσβαση σε μηχανισμούς για τη διευκόλυνση της αναφοράς ευπαθειών, περιστατικών και κυβερνοαπειλών που ενδέχεται να επηρεάσουν προϊόντα με ψηφιακά στοιχεία.

12. Οι αρχές εποπτείας της αγοράς διευκολύνουν, κατά περίπτωση, τη συνεργασία με σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των επιστημονικών και ερευνητικών οργανώσεων και των οργανώσεων καταναλωτών.

13. 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.

14. 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 6 του κανονισμού (ΕΕ) 2024/1689, οι αρχές εποπτείας της αγοράς που ορίζονται για τους σκοπούς του κανονισμού (ΕΕ) 2024/1689 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 (ΕΕ) 2024/1689 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 αναφοράς σύμφωνα με το άρθρο 14 του παρόντος κανονισμού, με τις ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού και με τον ENISA. Οι αρχές εποπτείας της αγοράς που ορίζονται σύμφωνα με τον κανονισμό (ΕΕ) 2024/1689 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.

15. Συγκροτείται ειδική ομάδα διοικητικής συνεργασίας (ΕΟΔΚ) για την ομοιόμορφη εφαρμογή του παρόντος κανονισμού, σύμφωνα με το άρθρο 30 παράγραφος 2 του κανονισμού (ΕΕ) 2019/1020. Η ΕΟΔΚ αποτελείται από εκπροσώπους των καθορισμένων αρχών εποπτείας της αγοράς και, κατά περίπτωση, εκπροσώπους των ενιαίων γραφείων σύνδεσης. Η ΕΟΔΚ ασχολείται επίσης με ειδικά θέματα που σχετίζονται με τις δραστηριότητες εποπτείας της αγοράς σε σχέση με τις υποχρεώσεις που επιβάλλονται στους υποστηρικτές λογισμικού ανοικτού κώδικα.

16. Οι αρχές εποπτείας της αγοράς παρακολουθούν τον τρόπο με τον οποίο οι κατασκευαστές έχουν εφαρμόσει τα κριτήρια που αναφέρονται στο άρθρο 13 παράγραφος 8 κατά τον καθορισμό της περιόδου υποστήριξης των προϊόντων τους με ψηφιακά στοιχεία.

Η ΕΟΔΚ δημοσιεύει σε δημόσια προσβάσιμη και φιλική προς τον χρήστη μορφή σχετικές στατιστικές για τις κατηγορίες προϊόντων με ψηφιακά στοιχεία, συμπεριλαμβανομένων των μέσων περιόδων υποστήριξής τους, όπως καθορίζεται από τον κατασκευαστή σύμφωνα με το άρθρο 13 παράγραφος 8, και παρέχει καθοδήγηση που περιλαμβάνει ενδεικτικές περιόδους υποστήριξης για κατηγορίες προϊόντων με ψηφιακά στοιχεία.

Όταν από τα δεδομένα προκύπτει ότι οι περίοδοι υποστήριξης για συγκεκριμένες κατηγορίες προϊόντων με ψηφιακά στοιχεία είναι ανεπαρκείς, η ΕΟΔΚ μπορεί να εκδίδει συστάσεις προς τις αρχές εποπτείας της αγοράς ώστε να εστιάσουν τις δραστηριότητές τους στις εν λόγω κατηγορίες προϊόντων με ψηφιακά στοιχεία.

Άρθρο 53

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 κυβερνοασφάλειας που καθορίζονται στο παράρτημα Ι, οι αρχές εποπτείας της αγοράς, κατόπιν αιτιολογημένου αιτήματος, έχουν πρόσβαση στα δεδομένα, σε γλώσσα εύκολα κατανοητή από αυτές, που απαιτούνται για την αξιολόγηση του σχεδιασμού, της ανάπτυξης, της παραγωγής και του χειρισμού των ευπαθειών των εν λόγω προϊόντων, συμπεριλαμβανομένης της σχετικής εσωτερικής τεκμηρίωσης του σχετικού οικονομικού φορέα.

Άρθρο 54

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 ευπαθειών του, παρουσιάζει σημαντικό κίνδυνο για την κυβερνοασφάλεια, διενεργεί αμελλητί, και αν είναι σκόπιμο σε συνεργασία με τη σχετικό ΟΑΠΑΥ, 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 οικονομικό φορέα να λάβει όλα τα αναγκαία διορθωτικά μέτρα για να θέσει το προϊόν με ψηφιακά στοιχεία 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 για την κυβερνοασφάλεια, το οποίο μπορεί να ορίσει η αρχή εποπτείας της αγοράς.

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

2. Κατά τον προσδιορισμό της σημασίας ενός κινδύνου κυβερνοασφάλειας όπως αναφέρεται στην παράγραφο 1 του παρόντος άρθρου, οι αρχές εποπτείας της αγοράς λαμβάνουν επίσης υπόψη μη τεχνικούς παράγοντες κινδύνου, ιδίως εκείνους που καθορίζονται ως αποτέλεσμα συντονισμένων σε επίπεδο Ένωσης εκτιμήσεων κινδύνου για την ασφάλεια κρίσιμων εφοδιαστικών αλυσίδων, που διενεργούνται σύμφωνα με το άρθρο 22 της οδηγίας (ΕΕ) 2022/2555. Όταν η αρχή εποπτείας της αγοράς έχει επαρκείς λόγους να θεωρεί ότι ένα προϊόν με ψηφιακά στοιχεία παρουσιάζει σημαντικό κίνδυνο για την κυβερνοασφάλεια λόγω μη τεχνικών παραγόντων κινδύνου, ενημερώνει τις αρμόδιες αρχές που έχουν οριστεί ή συσταθεί δυνάμει του άρθρου 8 της οδηγίας (ΕΕ) 2022/2555 και συνεργάζεται με τις εν λόγω αρχές όπως απαιτείται.

3. 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 οικονομικός φορέας.

4. Ο οικονομικός φορέας 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.

5. Εάν ο οικονομικός φορέας 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 με ψηφιακά στοιχεία 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.

6. Οι αναφερόμενες στην παράγραφο 5 πληροφορίες περιλαμβάνουν όλες τις διαθέσιμες λεπτομέρειες, ιδίως τα στοιχεία που απαιτούνται για την ταυτοποίηση του μη συμμορφούμενου προϊόντος με ψηφιακά στοιχεία, την καταγωγή του εν λόγω 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 οικονομικός φορέας. Ειδικότερα, η αρχή εποπτείας της αγοράς αναφέρει αν η μη συμμόρφωση οφείλεται σε έναν ή περισσότερους από τους παρακάτω λόγους:

α) το προϊόν με ψηφιακά στοιχεία ή οι διαδικασίες που εφαρμόζει ο κατασκευαστής δεν πληρούν τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στο παράρτημα I·

β) ελλείψεις στα εναρμονισμένα πρότυπα, στα ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας ή στις κοινές προδιαγραφές, όπως αναφέρονται στο άρθρο 27.

7. 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 με ψηφιακά στοιχεία και, σε περίπτωση διαφωνίας με το κοινοποιηθέν εθνικό μέτρο, τις τυχόν αντιρρήσεις τους.

8. Εάν εντός τριών μηνών από την παραλαβή της κοινοποίησης που αναφέρεται στην παράγραφο 5 του παρόντος άρθρου, δεν διατυπωθεί αντίρρηση από κράτος μέλος ή από την Επιτροπή σε σχέση με προσωρινό μέτρο που έχει λάβει κράτος μέλος, τότε το μέτρο θεωρείται δικαιολογημένο. Αυτό ισχύει με την επιφύλαξη των διαδικαστικών δικαιωμάτων του ενδιαφερόμενου οικονομικού φορέα σύμφωνα με το άρθρο 18 του κανονισμού (ΕΕ) 2019/1020.

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

Άρθρο 55

Ενωσιακή διαδικασία διασφάλισης

1. Αν, εντός τριών μηνών από την παραλαβή της κοινοποίησης του άρθρου 54 παράγραφος 5, ένα κράτος μέλος διατυπώσει αντιρρήσεις για μέτρο που έλαβε άλλο κράτος μέλος ή αν η Επιτροπή κρίνει ότι το μέτρο αντιβαίνει στο δίκαιο 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 54 παράγραφος 5 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 δεν θεωρηθεί δικαιολογημένο, τότε το 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 11 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 καθεστώτος πιστοποίησης της κυβερνοασφάλειας, όπως αναφέρεται στο άρθρο 27, η Επιτροπή εξετάζει αν θα τροποποιήσει ή θα καταργήσει οποιαδήποτε κατ' εξουσιοδότηση πράξη που εκδίδεται δυνάμει του άρθρου 27 παράγραφος 9, η οποία προσδιορίζει το τεκμήριο συμμόρφωσης όσον αφορά το εν λόγω καθεστώς 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 27, η Επιτροπή εξετάζει αν θα τροποποιήσει ή θα καταργήσει οποιαδήποτε εκτελεστική πράξη έχει εκδοθεί δυνάμει του άρθρου 27 παράγραφος 2 για τον καθορισμό των εν λόγω κοινών προδιαγραφών.

Άρθρο 56

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, ενημερώνει τις αρμόδιες αρχές εποπτείας της αγοράς. Όταν οι αρχές εποπτείας της αγοράς διενεργούν αξιολόγηση του εν λόγω προϊόντος με ψηφιακά στοιχεία που ενδέχεται να παρουσιάζει σημαντικό κίνδυνο κυβερνοασφάλειας όσον αφορά τη συμμόρφωσή του με τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό, εφαρμόζονται οι διαδικασίες που αναφέρονται στα άρθρα 54 και 55.

2. Όταν η Επιτροπή έχει επαρκείς λόγους να θεωρεί ότι ένα προϊόν με ψηφιακά στοιχεία παρουσιάζει σημαντικό κίνδυνο για την κυβερνοασφάλεια λόγω μη τεχνικών παραγόντων κινδύνου, ενημερώνει τις αρμόδιες αρχές εποπτείας της αγοράς και, κατά περίπτωση, τις αρμόδιες αρχές που έχουν οριστεί ή συσταθεί δυνάμει του άρθρου 8 της οδηγίας (ΕΕ) 2022/2555 και συνεργάζεται με τις εν λόγω αρχές όπως απαιτείται. Η Επιτροπή εξετάζει επίσης τη συνάφεια των εντοπισθέντων κινδύνων για το εν λόγω προϊόν με ψηφιακά στοιχεία υπό το πρίσμα των καθηκόντων της όσον αφορά τις συντονισμένες σε επίπεδο Ένωσης εκτιμήσεις κινδύνου για την ασφάλεια κρίσιμων αλυσίδων εφοδιασμού που προβλέπονται στο άρθρο 22 της οδηγίας (ΕΕ) 2022/2555, και διαβουλεύεται, κατά περίπτωση, με την ομάδα συνεργασίας που έχει συσταθεί σύμφωνα με το άρθρο 14 της οδηγίας (ΕΕ) 2022/2555 και τον ENISA.

3. Σε περιστάσεις που δικαιολογούν άμεση παρέμβαση για τη διατήρηση της ορθής λειτουργίας της εσωτερικής αγοράς και όταν η Επιτροπή έχει επαρκείς λόγους να θεωρεί ότι το προϊόν με ψηφιακά στοιχεία 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 διενεργεί αξιολόγηση της συμμόρφωσης και μπορεί να ζητήσει από τον ENISA να παράσχει ανάλυση προς στήριξη της εν λόγω αξιολόγησης. Η Επιτροπή ενημερώνει σχετικά τις αρμόδιες αρχές εποπτείας της αγοράς. Οι σχετικοί οικονομικοί φορείς συνεργάζονται όπως απαιτείται με τον ENISA.

4. Με βάση την αξιολόγηση που αναφέρεται στην παράγραφο 3, 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 οικονομικό φορέα ή τους φορείς.

5. Με βάση τη διαβούλευση που αναφέρεται στην παράγραφο 4 του παρόντος άρθρου, η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις για να προβλέπει τη λήψη διορθωτικών ή περιοριστικών μέτρων σε επίπεδο Ένωσης, συμπεριλαμβανομένης της απαίτησης να αποσυρθούν από την αγορά ή να ανακληθούν τα εν λόγω προϊόντα με ψηφιακά στοιχεία, εντός εύλογου χρονικού διαστήματος, ανάλογου προς τη φύση του κινδύνου. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 62 παράγραφος 2.

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

7. Οι παράγραφοι 3 έως 6 εφαρμόζονται καθ' όλη τη διάρκεια της εξαιρετικής περίπτωσης που αιτιολογεί την παρέμβαση της Επιτροπής, εφόσον δεν εξασφαλίζεται η συμμόρφωση του οικείου προϊόντος με ψηφιακά στοιχεία με τον παρόντα κανονισμό.

Άρθρο 57

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

1. Η αρχή εποπτείας της αγοράς ενός κράτους μέλους απαιτεί από έναν οικονομικό φορέα να λάβει όλα τα κατάλληλα μέτρα όταν, αφού διενεργήσει αξιολόγηση σύμφωνα με το άρθρο 54, διαπιστώσει ότι ένα προϊόν με ψηφιακά στοιχεία και οι διαδικασίες που εφαρμόζει ο κατασκευαστής, μολονότι συμμορφώνονται με τον παρόντα κανονισμό, παρουσιάζουν σημαντικό κίνδυνο για την κυβερνοασφάλεια, καθώς και κίνδυνο για:

α) την υγεία ή την ασφάλεια των προσώπων·

β) τη συμμόρφωση με υποχρεώσεις βάσει του ενωσιακού ή του εθνικού δικαίου που αποσκοπούν στην προστασία των θεμελιωδών δικαιωμάτων·

γ) τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των υπηρεσιών που προσφέρονται μέσω ηλεκτρονικού συστήματος πληροφοριών από βασικές οντότητες όπως αναφέρονται στο άρθρο 3 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555· ή

δ) άλλες πτυχές προστασίας του δημόσιου συμφέροντος.

Τα μέτρα που αναφέρονται στο πρώτο εδάφιο μπορούν να περιλαμβάνουν μέτρα που διασφαλίζουν ότι το σχετικό προϊόν με ψηφιακά στοιχεία και οι διαδικασίες που εφαρμόζει ο κατασκευαστής δεν παρουσιάζουν πλέον τους σχετικούς κινδύνους όταν αυτό διατίθεται στην αγορά, την απόσυρση από την αγορά του εν λόγω προϊόντος με ψηφιακά στοιχεία ή την ανάκλησή του, και είναι ανάλογα προς τη φύση των εν λόγω κινδύνων.

2. Ο κατασκευαστής ή άλλοι σχετικοί οικονομικοί 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 στα κράτη μέλη την απόφαση που αναφέρεται στην παράγραφο 4.

6. Εάν η Επιτροπή έχει επαρκείς λόγους να πιστεύει, μεταξύ άλλων βασιζόμενη σε 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 του παρόντος άρθρου, ενημερώνει τη σχετική ή τις σχετικές αρχές εποπτείας της αγοράς και μπορεί να τους ζητήσει να διενεργήσουν αξιολόγηση και να ακολουθήσουν τις διαδικασίες που αναφέρονται στο άρθρο 54 και στις παραγράφους 1, 2 και 3 του παρόντος άρθρου.

7. Σε περιστάσεις που δικαιολογούν άμεση παρέμβαση για τη διατήρηση της ορθής λειτουργίας της εσωτερικής αγοράς και όταν η Επιτροπή έχει επαρκείς λόγους να θεωρεί ότι το προϊόν με ψηφιακά στοιχεία 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 διενεργεί αξιολόγηση των κινδύνων που παρουσιάζει το εν λόγω προϊόν με ψηφιακά στοιχεία και μπορεί να ζητήσει από τον ENISA να παράσχει ανάλυση προς στήριξη της εν λόγω αξιολόγησης, και ενημερώνει σχετικά τις αρμόδιες αρχές εποπτείας της αγοράς. Οι σχετικοί οικονομικοί φορείς συνεργάζονται όπως απαιτείται με τον ENISA.

8. Με βάση την αξιολόγηση 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 οικονομικό φορέα ή τους φορείς.

9. Με βάση τη διαβούλευση που αναφέρεται στην παράγραφο 8 του παρόντος άρθρου, η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις για να αποφασίζει σχετικά με τη λήψη διορθωτικών ή περιοριστικών μέτρων σε επίπεδο Ένωσης, συμπεριλαμβανομένης της απαίτησης να αποσυρθούν από την αγορά ή να ανακληθούν τα εν λόγω προϊόντα με ψηφιακά στοιχεία, εντός εύλογου χρονικού διαστήματος, ανάλογου προς τη φύση του κινδύνου. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 62 παράγραφος 2.

10. Η Επιτροπή ανακοινώνει αμέσως τις εκτελεστικές πράξεις που αναφέρονται στην παράγραφο 9 στον σχετικό οικονομικό φορέα ή τους φορείς. Τα κράτη μέλη εφαρμόζουν αμελλητί τις εν λόγω εκτελεστικές 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 οικείο προϊόν με ψηφιακά στοιχεία εξακολουθεί να παρουσιάζει τους κινδύνους που αναφέρονται στην παράγραφο 1.

Άρθρο 58

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 CE έχει τεθεί κατά παράβαση του άρθρου 29 ή του άρθρου 30·

β) δεν έχει τεθεί η σήμανση CE·

γ) δεν έχει καταρτισθεί δήλωση συμμόρφωσης ΕΕ·

δ) η δήλωση συμμόρφωσης ΕΕ δεν έχει καταρτισθεί σωστά·

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

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 59

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 τίθενται σε κυκλοφορία στην αγορά ή διατίθενται στην αγορά, ιδίως προϊόντα με ψηφιακά στοιχεία για τα οποία διαπιστώνεται συχνά ότι ενέχουν κινδύνους για την κυβερνοασφάλεια.

2. Η Επιτροπή ή ο ENISA 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 με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού σε διάφορα κράτη μέλη, προς τις απαιτήσεις που καθορίζονται στον παρόντα κανονισμό.

3. Οι αρχές εποπτείας της αγοράς και, κατά περίπτωση, η Επιτροπή 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 λαμβάνει ως αποτέλεσμα των κοινών δραστηριοτήτων που εκτελούνται στο πλαίσιο οποιασδήποτε έρευνας την οποία αυτή διεξάγει.

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

Άρθρο 60

Σαρώσεις

1. Οι αρχές εποπτείας της αγοράς διενεργούν ταυτόχρονες, συντονισμένες δράσεις 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. Οι σαρώσεις αυτές μπορούν να περιλαμβάνουν επιθεωρήσεις προϊόντων με ψηφιακά στοιχεία που αποκτήθηκαν με καλυμμένη ταυτότητα.

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

3. Όταν, κατά την εκτέλεση των καθηκόντων του, μεταξύ άλλων με βάση τις κοινοποιήσεις που λαμβάνει σύμφωνα με το άρθρο 14 παράγραφοι 1 και 3, ο ENISA εντοπίζει κατηγορίες προϊόντων με ψηφιακά στοιχεία για τις οποίες μπορούν να οργανωθούν σαρώσεις, υποβάλλει πρόταση για σάρωση στον συντονιστή που αναφέρεται στην παράγραφο 2 του παρόντος άρθρου, 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 52 έως 58, 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.

Κεφάλαιο VI

Κατ' εξουσιοδότηση αρμοδιότητες και διαδικασία επιτροπής

Άρθρο 61

Άσκηση της εξουσιοδότησης

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

2. Η εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων που προβλέπεται στο άρθρο 2 παράγραφος 5 δεύτερο εδάφιο, στο άρθρο 7 παράγραφος 3, στο άρθρο 8 παράγραφοι 1 και 2, στο άρθρο 13 παράγραφος 8 τέταρτο εδάφιο, στο άρθρο 14 παράγραφος 9, στο άρθρο 25, στο άρθρο 27 παράγραφος 9, στο άρθρο 28 παράγραφος 5 και στο άρθρο 31 παράγραφος 5 ανατίθεται στην Επιτροπή για πέντε έτη από … [ημερομηνία έναρξης ισχύος του παρόντος κανονισμού]. Η Επιτροπή υποβάλλει έκθεση σχετικά με τις εξουσίες που της έχουν ανατεθεί το αργότερο εννέα μήνες πριν από τη λήξη της περιόδου των πέντε ετών. Η εξουσιοδότηση ανανεώνεται σιωπηρά για περιόδους ίδιας διάρκειας, εκτός αν το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο προβάλλει αντιρρήσεις το αργότερο τρεις μήνες πριν από τη λήξη της κάθε περιόδου.

3. Η εξουσιοδότηση που προβλέπεται στο άρθρο 2 παράγραφος 5 δεύτερο εδάφιο, στο άρθρο 7 παράγραφος 3, στο άρθρο 8 παράγραφοι 1 και 2, στο άρθρο 13 παράγραφος 8 τέταρτο εδάφιο, στο άρθρο 14 παράγραφος 9, στο άρθρο 25, στο άρθρο 27 παράγραφος 9, στο άρθρο 28 παράγραφος 5 και στο άρθρο 31 παράγραφος 5 μπορεί να ανακληθεί ανά πάσα στιγμή από το Ευρωπαϊκό Κοινοβούλιο ή 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 αυτή. Δεν θίγει το κύρος των κατ' εξουσιοδότηση πράξεων που ισχύουν ήδη.

4. Πριν από την έκδοση μιας κατ' εξουσιοδότηση πράξης, η Επιτροπή διεξάγει διαβουλεύσεις με εμπειρογνώμονες που ορίζουν τα κράτη μέλη σύμφωνα με τις αρχές της διοργανικής συμφωνίας της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου.

5. Μόλις εκδώσει μια 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 5 δεύτερο εδάφιο, το άρθρο 7 παράγραφος 3, το άρθρο 8 παράγραφος 1 ή 2, το άρθρο 13 παράγραφος 8 τέταρτο εδάφιο, το άρθρο 14 παράγραφος 9, το άρθρο 25, το άρθρο 27 παράγραφος 9, το άρθρο 28 παράγραφος 5 ή το άρθρο 31 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 62

Διαδικασία επιτροπής

1. Η Επιτροπή επικουρείται από επιτροπή. Η εν λόγω επιτροπή αποτελεί επιτροπή κατά την έννοια του κανονισμού (ΕΕ) αριθ. 182/2011.

2. Όταν γίνεται παραπομπή 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.

Κεφάλαιο VII

Εμπιστευτικότητα και κυρώσεις

Άρθρο 63

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 (ΕΕ) 2016/943 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[36]·

   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.

---

[36] 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).

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 64

Κυρώσεις

1. Τα κράτη μέλη καθορίζουν τους κανόνες για τις κυρώσεις που επιβάλλονται σε περίπτωση παραβιάσεων των διατάξεων του παρόντος κανονισμού και λαμβάνουν τα αναγκαία μέτρα για να διασφαλίσουν την εφαρμογή τους. Οι προβλεπόμενες κυρώσεις είναι αποτελεσματικές, αναλογικές και αποτρεπτικές. Τα κράτη μέλη κοινοποιούν αμελλητί τους εν λόγω κανόνες και τα εν λόγω μέτρα στην Επιτροπή και την ενημερώνουν αμελλητί σχετικά με κάθε μεταγενέστερη τροποποίησή τους.

2. Η μη συμμόρφωση με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I και τις υποχρεώσεις που ορίζονται στα άρθρα 13 και 14 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.

3. Η μη συμμόρφωση με τις υποχρεώσεις που ορίζονται στα άρθρα 18 έως 23, στο άρθρο 28, στο άρθρο 30 παράγραφοι 1 έως 4, στο άρθρο 31 παράγραφοι 1 έως 4, στο άρθρο 32 παράγραφοι 1, 2 και 3, στο άρθρο 33 παράγραφος 5, και στα άρθρα 39, 41, 47, 49 και 53 επισύρει διοικητικά πρόστιμα ύψους έως 10 000 000 EUR ή, εάν ο παραβάτης είναι επιχείρηση, έως το 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της για το προηγούμενο οικονομικό έτος, ανάλογα με το ποιο ποσό είναι υψηλότερο.

4. 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.

5. 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 τις ίδιες ή από άλλες αρχές εποπτείας της αγοράς στον ίδιο οικονομικό φορέα για παρόμοια παράβαση·

γ) το μέγεθος, ιδίως όσον αφορά τις πολύ μικρές και τις μικρές και μεσαίες επιχειρήσεις, συμπεριλαμβανομένων των νεοφυών επιχειρήσεων, και το μερίδιο αγοράς του οικονομικού φορέα που διαπράττει την παράβαση.

6. Οι αρχές εποπτείας της αγοράς που επιβάλλουν διοικητικά πρόστιμα κοινοποιούν την εν λόγω επιβολή προστίμων στις αρχές εποπτείας της αγοράς άλλων κρατών μελών μέσω του συστήματος πληροφοριών και επικοινωνίας που αναφέρεται στο άρθρο 34 του κανονισμού (ΕΕ) 2019/1020.

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

8. 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.

9. 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.

10. Κατά παρέκκλιση από τις παραγράφους 3 έως 9, τα διοικητικά πρόστιμα που αναφέρονται στις εν λόγω παραγράφους δεν εφαρμόζονται στα ακόλουθα:

α) σε κατασκευαστές που χαρακτηρίζονται ως πολύ μικρές ή μικρές επιχειρήσεις σε σχέση με τη μη τήρηση της προθεσμίας που αναφέρεται στο άρθρο 14 παράγραφος 2 στοιχείο α) ή στο άρθρο 14 παράγραφος 4 στοιχείο α)·

β) σε οποιαδήποτε παραβίαση του παρόντος κανονισμού από υποστηρικτές λογισμικού ανοικτού κώδικα.

Άρθρο 65

Αντιπροσωπευτικές αγωγές

Η οδηγία (ΕΕ) 2020/1828 εφαρμόζεται στις αντιπροσωπευτικές αγωγές που ασκούνται κατά οικονομικών φορέων όσον αφορά παραβιάσεις διατάξεων του παρόντος κανονισμού που θίγουν ή δύνανται να θίξουν τα συλλογικά συμφέροντα των καταναλωτών.

Κεφάλαιο VIII

Μεταβατικές και τελικές διατάξεις

Άρθρο 66

Τροποποίηση του κανονισμού (ΕΕ) 2019/1020

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

«ΧΧ[+]. Κανονισμός (ΕΕ) 2024/… του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου*[++].

---

* Κανονισμός (ΕΕ) 2024/... του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της ..., σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 168/2013 και (ΕΕ) 2019/1020 και της οδηγίας (ΕΕ) 2020/1828 (κανονισμός για την κυβερνοανθεκτικότητα) (ΕΕ L ..., ELI: …).».

[+] ΕΕ: να προστεθεί στο κείμενο ο επόμενος αύξων αριθμός του καταλόγου του παραρτήματος Ι του κανονισμού (ΕΕ) 2019/1020.

[++] ΕΕ: να προστεθεί στο κείμενο ο αριθμός του κανονισμού που περιέχεται στο έγγραφο PE-CONS 100/23 (2022/0272(COD)) και να συμπληρωθούν ο αριθμός, η ημερομηνία και τα στοιχεία ΕΕ του εν λόγω κανονισμού στην υποσημείωση.

Άρθρο 67

Τροποποίηση της οδηγίας (ΕΕ) 2020/1828

Στο παράρτημα Ι της οδηγίας (ΕΕ) 2020/1828, προστίθεται το ακόλουθο σημείο:

«(ΧΧ[+]) Κανονισμός (ΕΕ) 2024/… του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου*[++]«.

---

* Κανονισμός (ΕΕ) 2024/... του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της ..., σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 168/2013 και (ΕΕ) 2019/1020 και της οδηγίας (ΕΕ) 2020/1828 (κανονισμός για την κυβερνοανθεκτικότητα) (ΕΕ L ..., ELI: …).».

[+] ΕΕ: να προστεθεί στο κείμενο ο επόμενος αύξων αριθμός του καταλόγου του παραρτήματος Ι της οδηγίας (ΕΕ) 2020/1828.

[++] ΕΕ: να προστεθεί στο κείμενο ο αριθμός του κανονισμού που περιέχεται στο έγγραφο PE-CONS 100/23 (2022/0272(COD)) και να συμπληρωθούν ο αριθμός, η ημερομηνία και τα στοιχεία ΕΕ του εν λόγω κανονισμού στην υποσημείωση.

Άρθρο 68

Τροποποίηση του κανονισμού (ΕΕ) αριθ. 168/2013

Το παράρτημα ΙΙ του κανονισμού (ΕΕ) αριθ. 168/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[37] τροποποιείται ως εξής:

Στο μέρος Γ1, προστίθεται στον πίνακα η ακόλουθη εγγραφή:

«

XX+	18	Προστασία των οχημάτων από επιθέσεις στον κυβερνοχώρο		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

».

[37] Κανονισμός (ΕΕ) αριθ. 168/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Ιανουαρίου 2013, για την έγκριση και την εποπτεία της αγοράς δίκυκλων ή τρίκυκλων οχημάτων και τετράκυκλων (ΕΕ L 60 της 2.3.2013, σ. 52).

+ ΕΕ: να προστεθεί ο επόμενος αύξων αριθμός κάτω από τον τίτλο Γ1 του παραρτήματος ΙΙ του κανονισμού (ΕΕ) αριθ. 168/2013.

Άρθρο 69

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 πέραν του παρόντος κανονισμού παραμένουν σε ισχύ έως … [42 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], εκτός εάν λήγουν πριν από την εν λόγω ημερομηνία, ή εκτός εάν ορίζεται διαφορετικά στην εν λόγω άλλη ενωσιακή νομοθεσία εναρμόνισης, οπότε εξακολουθούν να ισχύουν όπως αναφέρεται στην εν λόγω νομοθεσία.

2. Τα προϊόντα με ψηφιακά στοιχεία που έχουν τεθεί σε κυκλοφορία στην αγορά πριν από … [36 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], υπόκεινται στις απαιτήσεις του παρόντος κανονισμού μόνον εάν, από τη συγκεκριμένη ημερομηνία, τα εν λόγω προϊόντα υπόκεινται σε ουσιαστικές τροποποιήσεις.

3. Κατά παρέκκλιση από την παράγραφο 2 του παρόντος άρθρου, οι υποχρεώσεις που ορίζονται στο άρθρο 14 εφαρμόζονται σε όλα τα προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού και έχουν τεθεί σε κυκλοφορία στην αγορά πριν από … [36 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού].

Άρθρο 70

Αξιολόγηση και επανεξέταση

1. Έως τις ... [72 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού] και στη συνέχεια ανά τετραετία, η Επιτροπή υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο έκθεση σχετικά με την αξιολόγηση και την επανεξέταση του παρόντος κανονισμού. Οι εκθέσεις αυτές δημοσιοποιούνται.

2. Έως τις … [45 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], η Επιτροπή, κατόπιν διαβούλευσης με τον ENISA και το δίκτυο ΟΑΠΑΥ, υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, αξιολογώντας την αποτελεσματικότητα της ενιαίας πλατφόρμας αναφοράς που ορίζεται στο άρθρο 16, καθώς και τον αντίκτυπο της επίκλησης λόγων κυβερνοασφάλειας που αναφέρεται στο άρθρο 16 παράγραφος 2 από τις ΟΑΠΑΥ στις οποίες έχουν ανατεθεί καθήκοντα συντονισμού, στην αποτελεσματικότητα της ενιαίας πλατφόρμας αναφοράς όσον αφορά την έγκαιρη διάδοση των λαμβανόμενων κοινοποιήσεων σε άλλες σχετικές ΟΑΠΑΥ.

Άρθρο 71

Έναρξη ισχύος και εφαρμογή

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

2. Ο παρών κανονισμός εφαρμόζεται από την ... [36 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού].

   Ωστόσο, το άρθρο 14 εφαρμόζεται από την ... [21 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού] και το κεφάλαιο IV (άρθρα 35 έως 51) εφαρμόζεται από την … [18 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού].

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

…,

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Η Πρόεδρος	*Ο/Η Πρόεδρος*

ΠΑΡΑΡΤΗΜΑ I

ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Μέρος I Απαιτήσεις κυβερνοασφάλειας σχετικά με τις ιδιότητες των προϊόντων με ψηφιακά στοιχεία

1) Τα προϊόντα με ψηφιακά στοιχεία σχεδιάζονται, αναπτύσσονται και παράγονται κατά τρόπο ώστε να εγγυώνται κατάλληλο επίπεδο κυβερνοασφάλειας βάσει των κινδύνων·

2) Με βάση την εκτίμηση κινδύνων κυβερνοασφάλειας που αναφέρεται στο άρθρο 13 παράγραφος 2 και κατά περίπτωση, τα προϊόντα με ψηφιακά στοιχεία:

   α) διατίθενται στην αγορά χωρίς γνωστές εκμεταλλεύσιμες ευπάθειες·

   β) διατίθενται στην αγορά με ασφαλή εξ ορισμού διαμόρφωση, εκτός εάν υπάρχει διαφορετική συμφωνία μεταξύ κατασκευαστή και επιχειρηματικού χρήστη σε σχέση με εξατομικευμένο προϊόν με ψηφιακά στοιχεία, συμπεριλαμβανομένης της δυνατότητας επαναφοράς του προϊόντος στην αρχική του κατάσταση·

   γ) διασφαλίζουν ότι οι ευπάθειες μπορούν να αντιμετωπιστούν μέσω ενημερώσεων ασφαλείας, μεταξύ άλλων, κατά περίπτωση, μέσω αυτόματων ενημερώσεων ασφαλείας που εγκαθίστανται εντός κατάλληλου χρονικού πλαισίου και είναι ενεργοποιημένες ως προεπιλεγμένη ρύθμιση, με σαφή και εύχρηστο μηχανισμό εξαίρεσης, μέσω της κοινοποίησης των διαθέσιμων ενημερώσεων στους χρήστες, και της παροχής δυνατότητας προσωρινής αναβολής·

δ) διασφαλίζουν την προστασία από μη εξουσιοδοτημένη πρόσβαση με κατάλληλους μηχανισμούς ελέγχου, συμπεριλαμβανομένων, μεταξύ άλλων, συστημάτων επαλήθευσης ταυτότητας, διαχείρισης ταυτότητας ή πρόσβασης, και αναφέρουν κάθε πιθανή μη εξουσιοδοτημένη πρόσβαση·

ε) προστατεύουν την εμπιστευτικότητα των δεδομένων που αποθηκεύονται, διαβιβάζονται ή υποβάλλονται σε οποιουδήποτε άλλου είδους επεξεργασία, μέσω της κρυπτογράφησης των σχετικών δεδομένων που βρίσκονται σε αδράνεια ή σε κίνηση μέσω μηχανισμών προηγμένης τεχνολογίας και με τη χρήση άλλων τεχνικών μέσων·

στ) προστατεύουν την ακεραιότητα των δεδομένων που αποθηκεύονται, διαβιβάζονται ή υποβάλλονται σε οποιουδήποτε άλλου είδους επεξεργασία, είτε αυτά είναι προσωπικού χαρακτήρα είτε άλλου είδους, καθώς και εντολών, προγραμμάτων και διαμορφώσεων, από κάθε παραποίηση ή τροποποίηση που δεν έχει την άδεια του χρήστη, και αναφέρουν πιθανές αλλοιώσεις·

ζ) επεξεργάζονται μόνο δεδομένα, προσωπικού χαρακτήρα ή άλλου είδους, τα οποία είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τον προβλεπόμενο σκοπό του προϊόντος με ψηφιακά στοιχεία (ελαχιστοποίηση των δεδομένων)·

η) προστατεύουν τη διαθεσιμότητα ουσιωδών και βασικών λειτουργιών, ακόμη και μετά από περιστατικό, μεταξύ άλλων μέσω μέτρων ανθεκτικότητας και μετριασμού έναντι επιθέσεων άρνησης παροχής υπηρεσίας·

θ) ελαχιστοποιούν τις αρνητικές επιπτώσεις από τα ίδια τα προϊόντα ή από συνδεδεμένες συσκευές στη διαθεσιμότητα των υπηρεσιών που παρέχονται από άλλες συσκευές ή δίκτυα·

ι) σχεδιάζονται, αναπτύσσονται και παράγονται κατά τρόπο ώστε να περιορίζονται οι επιφάνειες επίθεσης, συμπεριλαμβανομένων των εξωτερικών διεπαφών·

ια) σχεδιάζονται, αναπτύσσονται και παράγονται με σκοπό τη μείωση των επιπτώσεων ενός συμβάντος με τη χρήση κατάλληλων μηχανισμών και τεχνικών μετριασμού της εκμετάλλευσης·

ιβ) παρέχουν πληροφορίες σχετικά με την ασφάλεια μέσω της καταγραφής και της παρακολούθησης σχετικών εσωτερικών δραστηριοτήτων, συμπεριλαμβανομένης της πρόσβασης σε δεδομένα, υπηρεσίες ή λειτουργίες ή της τροποποίησής τους, με μηχανισμό εξαίρεσης για τον χρήστη·

ιγ) παρέχουν στους χρήστες τη δυνατότητα να αφαιρούν με ασφάλεια και ευκολία, σε μόνιμη βάση, όλα τα δεδομένα και τις ρυθμίσεις και, όταν τα εν λόγω δεδομένα μπορούν να μεταφερθούν σε άλλα προϊόντα ή συστήματα, διασφαλίζουν ότι αυτό γίνεται με ασφαλή τρόπο.

Μέρος ΙΙ Απαιτήσεις χειρισμού ευπαθειών

Οι κατασκευαστές των προϊόντων με ψηφιακά στοιχεία:

1) εντοπίζουν και τεκμηριώνουν τις ευπάθειες και τα δομοστοιχεία που περιέχονται στα προϊόντα με ψηφιακά στοιχεία, μεταξύ άλλων με την κατάρτιση καταλόγου υλικών λογισμικού σε ευρέως χρησιμοποιούμενο και μηχαναγνώσιμο μορφότυπο που καλύπτει τουλάχιστον τις σημαντικότερες εξαρτήσεις των προϊόντων·

2) σε σχέση με τους κινδύνους που παρουσιάζονται για προϊόντα με ψηφιακά στοιχεία, αντιμετωπίζουν και διορθώνουν τις ευπάθειες χωρίς καθυστέρηση, μεταξύ άλλων με την παροχή ενημερώσεων ασφαλείας· όπου είναι τεχνικά εφικτό, παρέχονται νέες ενημερώσεις ασφαλείας χωριστά από τις ενημερώσεις λειτουργικότητας·

3) εφαρμόζουν αποτελεσματικές και τακτικές δοκιμές και αξιολογήσεις της ασφάλειας του προϊόντος με ψηφιακά στοιχεία·

4) μόλις καταστεί διαθέσιμη η ενημέρωση ασφαλείας, κοινοποιούν και δημοσιοποιούν πληροφορίες σχετικά με τις διορθωμένες ευπάθειες, οι οποίες περιλαμβάνουν περιγραφή των ευπαθειών, πληροφορίες που επιτρέπουν στους χρήστες να προσδιορίσουν το προϊόν με ψηφιακά στοιχεία που επηρεάζεται, τις επιπτώσεις των ευπαθειών, τη σοβαρότητά τους και σαφείς και προσβάσιμες πληροφορίες που βοηθούν τους χρήστες να άρουν τις ευπάθειες· σε δεόντως αιτιολογημένες περιπτώσεις, όταν οι κατασκευαστές θεωρούν ότι οι κίνδυνοι ασφαλείας που συνεπάγεται η δημοσίευση υπερτερούν των οφελών για την ασφάλεια, μπορούν να καθυστερήσουν τη δημοσιοποίηση πληροφοριών σχετικά με μια διορθωμένη ευπάθεια έως ότου δοθεί στους χρήστες η δυνατότητα να εφαρμόσουν τη σχετική επιδιόρθωση·

5) θέτουν σε εφαρμογή και επιβάλλουν πολιτική για τη συντονισμένη γνωστοποίηση ευπαθειών·

6) λαμβάνουν μέτρα για τη διευκόλυνση της ανταλλαγής πληροφοριών σχετικά με πιθανές ευπάθειες στο προϊόν τους με ψηφιακά στοιχεία, καθώς και σε δομοστοιχεία τρίτων που περιέχονται στο εν λόγω προϊόν, μεταξύ άλλων με την παροχή διεύθυνσης επικοινωνίας για την αναφορά των ευπαθειών που εντοπίζονται στο προϊόν με ψηφιακά στοιχεία·

7) προβλέπουν μηχανισμούς για την ασφαλή διανομή ενημερώσεων για προϊόντα με ψηφιακά στοιχεία, ώστε να διασφαλίζεται ότι οι ευπάθειες διορθώνονται ή μετριάζονται εγκαίρως και, κατά περίπτωση για τις ενημερώσεις ασφαλείας, με αυτόματο τρόπο·

8) διασφαλίζουν ότι, όταν υπάρχουν ενημερώσεις ασφαλείας για την αντιμετώπιση ζητημάτων ασφάλειας που εντοπίζονται, αυτές διανέμονται χωρίς καθυστέρηση και, εκτός εάν υπάρχει διαφορετική συμφωνία μεταξύ κατασκευαστή και επιχειρηματικού χρήστη σε σχέση με εξατομικευμένο προϊόν με ψηφιακά στοιχεία, δωρεάν, ενώ συνοδεύονται και από συμβουλές που παρέχουν στους χρήστες τις σχετικές πληροφορίες, μεταξύ άλλων σχετικά με τα πιθανά μέτρα που πρέπει να ληφθούν.

ΠΑΡΑΡΤΗΜΑ ΙΙ

ΠΛΗΡΟΦΟΡΙΕΣ ΚΑΙ ΟΔΗΓΙΕΣ ΠΡΟΣ ΤΟΝ ΧΡΗΣΤΗ

Κατ' ελάχιστο, το προϊόν με ψηφιακά στοιχεία συνοδεύεται από:

1. το όνομα, την καταχωρισμένη εμπορική επωνυμία ή το καταχωρισμένο εμπορικό σήμα του κατασκευαστή και την ταχυδρομική διεύθυνση, τη διεύθυνση ηλεκτρονικού ταχυδρομείου ή άλλα ψηφιακά στοιχεία επικοινωνίας, καθώς και, κατά περίπτωση, τον ιστότοπο μέσω του οποίου μπορεί κανείς να επικοινωνήσει με τον κατασκευαστή·

2. το ενιαίο σημείο επαφής στο οποίο μπορούν να αναφέρονται και να λαμβάνονται πληροφορίες σχετικά με ευπάθειες του προϊόντος με ψηφιακά στοιχεία, και πληροφορίες σχετικά με το πού μπορεί κανείς να βρει την πολιτική του κατασκευαστή σχετικά με τη συντονισμένη γνωστοποίηση ευπαθειών·

3. το όνομα και τον τύπο καθώς και οποιεσδήποτε πρόσθετες πληροφορίες που επιτρέπουν τη μοναδική ταυτοποίηση του προϊόντος με ψηφιακά στοιχεία·

4. τον προβλεπόμενο σκοπό του προϊόντος με ψηφιακά στοιχεία, συμπεριλαμβανομένου του περιβάλλοντος ασφάλειας που παρέχει ο κατασκευαστής, καθώς και τις βασικές λειτουργίες του προϊόντος και πληροφορίες σχετικά με τις ιδιότητες ασφάλειας·

5. κάθε γνωστή ή προβλέψιμη περίσταση που σχετίζεται με τη χρήση του προϊόντος με ψηφιακά στοιχεία σύμφωνα με τον προβλεπόμενο σκοπό του ή υπό συνθήκες ευλόγως προβλέψιμης κακής χρήσης, η οποία μπορεί να οδηγήσει σε σημαντικούς κινδύνους για την κυβερνοασφάλεια·

6. κατά περίπτωση, τη διεύθυνση στο διαδίκτυο όπου είναι διαθέσιμη η δήλωση συμμόρφωσης ΕΕ·

7. το είδος της τεχνικής υποστήριξης ασφάλειας που παρέχεται από τον κατασκευαστή και την ημερομηνία λήξης της περιόδου υποστήριξης κατά την οποία οι χρήστες μπορούν να αναμένουν ότι οι ευπάθειες θα αντιμετωπίζονται και θα λαμβάνουν ενημερώσεις ασφαλείας·

8. λεπτομερείς οδηγίες ή διεύθυνση στο διαδίκτυο όπου είναι διαθέσιμες αυτές οι λεπτομερείς οδηγίες και πληροφορίες σχετικά με:

α) τα αναγκαία μέτρα κατά την αρχική θέση σε λειτουργία και καθ' όλη τη διάρκεια ζωής του προϊόντος με ψηφιακά στοιχεία, ώστε να διασφαλίζεται η ασφαλής χρήση του·

β) τον τρόπο με τον οποίο οι αλλαγές στο προϊόν με ψηφιακά στοιχεία μπορούν να επηρεάσουν την ασφάλεια των δεδομένων·

γ) τον τρόπο με τον οποίο μπορούν να εγκατασταθούν ενημερώσεις σχετικές με την ασφάλεια·

δ) την ασφαλή θέση του προϊόντος με ψηφιακά στοιχεία εκτός λειτουργίας, συμπεριλαμβανομένων πληροφοριών σχετικά με τον τρόπο με τον οποίο τα δεδομένα χρήστη μπορούν να διαγραφούν με ασφάλεια·

ε) τον τρόπο με τον οποίο μπορεί να απενεργοποιηθεί η προεπιλεγμένη ρύθμιση που επιτρέπει την αυτόματη εγκατάσταση ενημερώσεων ασφαλείας, σύμφωνα με την απαίτηση του παραρτήματος Ι μέρος Ι σημείο 2 στοιχείο γ)·

στ) όταν το προϊόν με ψηφιακά στοιχεία προορίζεται για ενσωμάτωση σε άλλα προϊόντα με ψηφιακά στοιχεία, τις πληροφορίες που χρειάζεται ο συναρμολογητής προκειμένου να συμμορφώνεται με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι και τις απαιτήσεις τεκμηρίωσης που ορίζονται στο παράρτημα VII.

9. Εάν ο κατασκευαστής αποφασίσει να διαθέσει τον κατάλογο υλικών λογισμικού στον χρήστη, πληροφορίες σχετικά με το πού μπορεί κανείς να αποκτήσει πρόσβαση στον κατάλογο υλικών λογισμικού.

ΠΑΡΑΡΤΗΜΑ ΙΙΙ

ΣΗΜΑΝΤΙΚΑ ΠΡΟΪΟΝΤΑ ΜΕ ΨΗΦΙΑΚΑ ΣΤΟΙΧΕΙΑ

Κλάση Ι

1. Λογισμικό και υλισμικό συστημάτων διαχείρισης ταυτότητας και διαχείρισης προνομιακής πρόσβασης, συμπεριλαμβανομένων συσκευών ανάγνωσης επαλήθευσης ταυτότητας και ελέγχου πρόσβασης, μεταξύ των οποίων συσκευές ανάγνωσης βιομετρικών δεδομένων·

2. Αυτόνομα και ενσωματωμένα προγράμματα περιήγησης·

3. Διαχειριστές κωδικών πρόσβασης·

4. Λογισμικό που αναζητεί, αφαιρεί ή θέτει σε καραντίνα κακόβουλο λογισμικό·

5. Προϊόντα με ψηφιακά στοιχεία με τη λειτουργία εικονικού ιδιωτικού δικτύου (VPN)·

6. Συστήματα διαχείρισης δικτύου·

7. Συστήματα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM)·

8. Συστήματα διαχείρισης εκκίνησης·

9. Λογισμικό έκδοσης υποδομών δημόσιου κλειδιού και ψηφιακών πιστοποιητικών·

10. Φυσικές και εικονικές διεπαφές δικτύου·

11. Λειτουργικά συστήματα ·

12. Δρομολογητές, μόντεμ που προορίζονται για σύνδεση στο διαδίκτυο, και διακόπτες ·

13. Μικροεπεξεργαστές με λειτουργίες σχετικές με την ασφάλεια·

14. Μικροελεγκτές με λειτουργίες σχετικές με την ασφάλεια·

15. Ολοκληρωμένα κυκλώματα ειδικών εφαρμογών (ASIC) και συστοιχίες επιτόπια προγραμματιζόμενων πυλών (FPGA) με λειτουργίες σχετικές με την ασφάλεια·

16. Εικονικοί βοηθοί γενικής χρήσης για έξυπνες κατοικίες·

17. Προϊόντα έξυπνης κατοικίας με λειτουργίες ασφαλείας, μεταξύ των οποίων έξυπνες κλειδαριές θυρών, κάμερες ασφαλείας, συστήματα ενδοεπικοινωνίας για βρέφη και συστήματα συναγερμού·

18. Παιχνίδια συνδεδεμένα με το διαδίκτυο που καλύπτονται από την οδηγία 2009/48/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[1], τα οποία διαθέτουν κοινωνικά διαδραστικά χαρακτηριστικά (π.χ. ομιλία ή βιντεοσκόπηση) ή διαθέτουν χαρακτηριστικά εντοπισμού θέσης·

19. Ατομικά φορετά προϊόντα που φοριούνται ή τοποθετούνται στο ανθρώπινο σώμα με σκοπό την παρακολούθηση της υγείας (π.χ. με καταγραφή δεδομένων) και στα οποία δεν εφαρμόζεται ο κανονισμός (ΕΕ) 2017/745 ή ο κανονισμός (ΕΕ) 2017/746, ή ατομικά φορετά προϊόντα που προορίζονται για χρήση από και για παιδιά.

Κλάση II

1. Επόπτες (hypervisors) και συστήματα χρόνου λειτουργίας που υποστηρίζουν εικονική εκτέλεση λειτουργικών συστημάτων και παρόμοια περιβάλλοντα·

2. Τείχη προστασίας, συστήματα ανίχνευσης και πρόληψης εισβολών ·

3. Μικροεπεξεργαστές ανθεκτικοί στην παραποίηση·

4. Μικροελεγκτές ανθεκτικοί στην παραποίηση.

---

[1] Οδηγία 2009/48/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Ιουνίου 2009, σχετικά με την ασφάλεια των παιχνιδιών (ΕΕ L 170 της 30.6.2009, σ. 1).

ΠΑΡΑΡΤΗΜΑ IV

ΚΡΙΣΙΜΑ ΠΡΟΪΟΝΤΑ ΜΕ ΨΗΦΙΑΚΑ ΣΤΟΙΧΕΙΑ

1. Συσκευές υλισμικού με θυρίδες ασφαλείας·

2. Πύλες έξυπνων μετρητών στο πλαίσιο έξυπνων συστημάτων μέτρησης, όπως ορίζονται στο άρθρο 2 παράγραφος 23 της οδηγίας (ΕΕ) 2019/944 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[1] και άλλες συσκευές για προηγμένους σκοπούς ασφάλειας, συμπεριλαμβανομένης της ασφαλούς κρυπτοεπεξεργασίας·

3. Έξυπνες κάρτες ή παρόμοιες συσκευές, συμπεριλαμβανομένων των ασφαλών στοιχείων.

---

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

ΠΑΡΑΡΤΗΜΑ V

ΔΗΛΩΣΗ ΣΥΜΜΟΡΦΩΣΗΣ ΕΕ

Στη δήλωση συμμόρφωσης ΕΕ που αναφέρεται στο άρθρο 28, περιλαμβάνονται όλες οι ακόλουθες πληροφορίες:

1. Όνομα και τύπος και πρόσθετες πληροφορίες που επιτρέπουν τη μοναδική ταυτοποίηση του προϊόντος με ψηφιακά στοιχεία·

2. Όνομα/Επωνυμία και διεύθυνση του κατασκευαστή ή του εξουσιοδοτημένου αντιπροσώπου του·

3. Βεβαίωση ότι η δήλωση συμμόρφωσης ΕΕ εκδίδεται με αποκλειστική ευθύνη του παρόχου·

4. Αντικείμενο της δήλωσης (ταυτοποίηση του προϊόντος με ψηφιακά στοιχεία που επιτρέπει την ιχνηλασιμότητα, η οποία μπορεί να περιλαμβάνει φωτογραφία, κατά περίπτωση)·

5. Δήλωση ότι το αντικείμενο της δήλωσης που περιγράφεται παραπάνω είναι σύμφωνο με την οικεία ενωσιακή νομοθεσία εναρμόνισης·

6. Μνεία τυχόν σχετικών εναρμονισμένων προτύπων που χρησιμοποιούνται ή τυχόν άλλων κοινών προδιαγραφών ή πιστοποίησης κυβερνοασφάλειας σε σχέση με τις οποίες δηλώνεται η συμμόρφωση·

7. Κατά περίπτωση, επωνυμία και αριθμός του κοινοποιημένου οργανισμού, περιγραφή της διαδικασίας αξιολόγησης της συμμόρφωσης που διενεργήθηκε και ταυτοποίηση του εκδοθέντος πιστοποιητικού·

8. Συμπληρωματικές πληροφορίες:

Υπογραφή για λογαριασμό και εξ ονόματος:……

(τόπος και ημερομηνία έκδοσης):

(όνομα, θέση) (υπογραφή):

ΠΑΡΑΡΤΗΜΑ VI

ΑΠΛΟΥΣΤΕΥΜΕΝΗ ΔΗΛΩΣΗ ΣΥΜΜΟΡΦΩΣΗΣ ΕΕ

Η απλουστευμένη δήλωση συμμόρφωσης ΕΕ που αναφέρεται στο άρθρο 13 παράγραφος 20 έχει ως εξής:

Με το παρόν, ο/η [επωνυμία κατασκευαστή] δηλώνει ότι το προϊόν με ψηφιακά στοιχεία τύπου [ονομασία τύπου προϊόντος με ψηφιακά στοιχεία] συμμορφώνεται με τον κανονισμό (ΕΕ) .../... του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[1].

Το πλήρες κείμενο της δήλωσης συμμόρφωσης ΕΕ διατίθεται στην ακόλουθη ιστοσελίδα στο διαδίκτυο:

---

[1] ΕΕ: να προστεθεί στο κείμενο ο αριθμός του κανονισμού που περιέχεται στο έγγραφο PE-CONS …/… (2022/0272(COD)).

ΠΑΡΑΡΤΗΜΑ VII

ΠΕΡΙΕΧΟΜΕΝΑ ΤΟΥ ΤΕΧΝΙΚΟΥ ΦΑΚΕΛΟΥ

Ο τεχνικός φάκελος που αναφέρεται στο άρθρο 31 περιλαμβάνει τουλάχιστον τις ακόλουθες πληροφορίες, ανάλογα με το σχετικό προϊόν με ψηφιακά στοιχεία:

1. γενική περιγραφή του προϊόντος με ψηφιακά στοιχεία, η οποία περιλαμβάνει τα εξής:

   α) τον προβλεπόμενο σκοπό του·

   β) εκδόσεις λογισμικού που επηρεάζουν τη συμμόρφωση προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας·

   γ) όταν το προϊόν με ψηφιακά στοιχεία είναι προϊόν υλισμικού, φωτογραφίες ή εικόνες που παρουσιάζουν εξωτερικά χαρακτηριστικά, σήμανση και εσωτερική διάταξη·

   δ) πληροφορίες και οδηγίες για τους χρήστες, όπως ορίζονται στο παράρτημα II·

2. περιγραφή του σχεδιασμού, της ανάπτυξης και της παραγωγής του προϊόντος με ψηφιακά στοιχεία και των διαδικασιών χειρισμού ευπαθειών, η οποία περιλαμβάνει τα εξής:

   α) απαραίτητες πληροφορίες σχετικά με τον σχεδιασμό και την ανάπτυξη του προϊόντος με ψηφιακά στοιχεία, συμπεριλαμβανομένων, κατά περίπτωση, σχεδίων και διαγραμμάτων και περιγραφής της αρχιτεκτονικής του συστήματος που εξηγεί τον τρόπο με τον οποίο τα δομοστοιχεία του λογισμικού βασίζονται ή τροφοδοτούνται μεταξύ τους και ενσωματώνονται στη συνολική επεξεργασία·

β) απαραίτητες πληροφορίες και προδιαγραφές για τις διαδικασίες χειρισμού ευπαθειών που εφαρμόζει ο κατασκευαστής, συμπεριλαμβανομένου του καταλόγου υλικών λογισμικού, της συντονισμένης πολιτικής γνωστοποίησης ευπαθειών, στοιχείων που αποδεικνύουν την παροχή διεύθυνσης επικοινωνίας για την αναφορά των ευπαθειών και περιγραφή των τεχνικών λύσεων που επιλέγονται για την ασφαλή διανομή των ενημερώσεων·

γ) απαραίτητες πληροφορίες και προδιαγραφές για τις διαδικασίες παραγωγής και παρακολούθησης του προϊόντος με ψηφιακά στοιχεία και την επικύρωση των εν λόγω διαδικασιών·

3. αξιολόγηση των κινδύνων κυβερνοασφάλειας βάσει των οποίων έχει σχεδιαστεί, αναπτυχθεί, παραχθεί, παραδοθεί και συντηρηθεί το προϊόν με ψηφιακά στοιχεία, δυνάμει του άρθρου 13, συμπεριλαμβανομένου του τρόπου εφαρμογής των ουσιωδών απαιτήσεων κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος 1·

4. σχετικές πληροφορίες που ελήφθησαν υπόψη για τον καθορισμό της περιόδου στήριξης, δυνάμει του άρθρου 13 παράγραφος 8 του προϊόντος με ψηφιακά στοιχεία·

5. κατάλογο των εναρμονισμένων προτύπων που εφαρμόζονται πλήρως ή εν μέρει, των οποίων τα στοιχεία έχουν δημοσιευτεί στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, των κοινών προδιαγραφών που ορίζονται στο άρθρο 27 του παρόντος κανονισμού ή των ευρωπαϊκών καθεστώτων πιστοποίησης της κυβερνοασφάλειας που θεσπίζονται σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 σύμφωνα με το άρθρο 27 παράγραφος 8 του παρόντος κανονισμού και, όπου τα εναρμονισμένα αυτά πρότυπα, οι κοινές προδιαγραφές ή τα ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας δεν έχουν εφαρμοστεί, περιγραφές των λύσεων που εφαρμόζονται για την τήρηση των ουσιωδών απαιτήσεων κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρη I και II, συμπεριλαμβανομένου καταλόγου των άλλων σχετικών τεχνικών προδιαγραφών που έχουν εφαρμοστεί. Σε περίπτωση μερικώς εφαρμοζόμενων εναρμονισμένων προτύπων, κοινών προδιαγραφών ή ευρωπαϊκών καθεστώτων πιστοποίησης της κυβερνοασφάλειας, ο τεχνικός φάκελος προσδιορίζει τα μέρη που έχουν εφαρμοστεί·

6. εκθέσεις των δοκιμών που διενεργήθηκαν για την επαλήθευση της συμμόρφωσης του προϊόντος με ψηφιακά στοιχεία και των διαδικασιών χειρισμού ευπαθειών με τις εφαρμοστέες ουσιώδεις απαιτήσεις κυβερνοασφάλειας, όπως ορίζονται στο παράρτημα I μέρη I και II·

7. αντίγραφο της δήλωσης συμμόρφωσης ΕΕ·

8. κατά περίπτωση, τον κατάλογο υλικών του λογισμικού, κατόπιν αιτιολογημένου αιτήματος αρχής εποπτείας της αγοράς, υπό την προϋπόθεση ότι είναι αναγκαίος προκειμένου η εν λόγω αρχή να είναι σε θέση να ελέγξει τη συμμόρφωση με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I.

ΠΑΡΑΡΤΗΜΑ VIII

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ

Μέρος Ι Διαδικασία αξιολόγησης της συμμόρφωσης βάσει εσωτερικού ελέγχου (βάσει της ενότητας Α)

1. Ο εσωτερικός έλεγχος είναι η διαδικασία αξιολόγησης της συμμόρφωσης με την οποία ο κατασκευαστής εκπληρώνει τις υποχρεώσεις που καθορίζονται στα σημεία 2, 3 και 4 του παρόντος μέρους, και βεβαιώνει και δηλώνει, με αποκλειστική του ευθύνη, ότι τα προϊόντα με ψηφιακά στοιχεία πληρούν όλες τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στο παράρτημα Ι μέρος Ι, και ότι ο κατασκευαστής πληροί τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στο παράρτημα Ι μέρος ΙΙ.

2. Ο κατασκευαστής καταρτίζει τον τεχνικό φάκελο που περιγράφεται στο παράρτημα VII.

3. Σχεδιασμός, ανάπτυξη, παραγωγή και χειρισμός ευπαθειών προϊόντων με ψηφιακά στοιχεία

   Ο κατασκευαστής λαμβάνει όλα τα αναγκαία μέτρα ώστε οι διαδικασίες σχεδιασμού, ανάπτυξης, παραγωγής και χειρισμού των ευπαθειών και η παρακολούθησή τους να διασφαλίζουν τη συμμόρφωση των προϊόντων με ψηφιακά στοιχεία που έχουν κατασκευαστεί ή αναπτυχθεί και των διαδικασιών που εφαρμόζει ο κατασκευαστής με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι μέρη Ι και ΙΙ.

4. Σήμανση συμμόρφωσης και δήλωση συμμόρφωσης

4.1. Ο κατασκευαστής τοποθετεί τη σήμανση CE σε κάθε μεμονωμένο προϊόν με ψηφιακά στοιχεία που πληροί τις εφαρμοστέες απαιτήσεις του παρόντος κανονισμού.

4.2. Ο κατασκευαστής συντάσσει γραπτή δήλωση συμμόρφωσης ΕΕ για κάθε προϊόν με ψηφιακά στοιχεία σύμφωνα με το άρθρο 28 και τη θέτει, μαζί με τον τεχνικό φάκελο, στη διάθεση των εθνικών αρχών επί 10 έτη αφότου το προϊόν με ψηφιακά στοιχεία τεθεί σε κυκλοφορία στην αγορά ή για την περίοδο υποστήριξης, ανάλογα με το ποιο διάστημα είναι μεγαλύτερο. Η δήλωση συμμόρφωσης ΕΕ αναφέρει το προϊόν με ψηφιακά στοιχεία για το οποίο έχει συνταχθεί. Στις αρμόδιες αρχές διατίθεται αντίγραφο της δήλωσης συμμόρφωσης ΕΕ, κατόπιν σχετικού αιτήματος.

5. Εξουσιοδοτημένοι αντιπρόσωποι

Οι υποχρεώσεις του κατασκευαστή που καθορίζονται στο σημείο 4 είναι δυνατό να εκπληρώνονται από τον εξουσιοδοτημένο αντιπρόσωπό του, εξ ονόματός του και υπό την ευθύνη του, υπό την προϋπόθεση ότι οι σχετικές υποχρεώσεις προσδιορίζονται στην εντολή.

Μέρος ΙΙ Εξέταση τύπου ΕΕ (βάσει της ενότητας Β)

1. Η εξέταση τύπου ΕΕ είναι το μέρος της διαδικασίας αξιολόγησης της συμμόρφωσης με το οποίο ο κοινοποιημένος οργανισμός εξετάζει τον τεχνικό σχεδιασμό και την ανάπτυξη ενός προϊόντος με ψηφιακά στοιχεία και τις διαδικασίες χειρισμού ευπαθειών που εφαρμόζει ο κατασκευαστής, και βεβαιώνει ότι ένα προϊόν με ψηφιακά στοιχεία πληροί τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι μέρος Ι, και ότι ο κατασκευαστής πληροί τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι μέρος ΙΙ.

2. Η εξέταση τύπου ΕΕ διενεργείται με αξιολόγηση της επάρκειας του τεχνικού σχεδιασμού και της ανάπτυξης του προϊόντος με ψηφιακά στοιχεία μέσω της εξέτασης του τεχνικού φακέλου και των κατά το σημείο 3 δικαιολογητικών και της εξέτασης δειγμάτων από ένα ή περισσότερα κρίσιμα μέρη του προϊόντος (συνδυασμός τύπου παραγωγής και τύπου σχεδιασμού).

3. Η αίτηση για εξέταση τύπου ΕΕ υποβάλλεται από τον κατασκευαστή σε έναν και μόνο κοινοποιημένο οργανισμό της επιλογής του.

   Η αίτηση περιλαμβάνει:

   3.1 την επωνυμία και τη διεύθυνση του κατασκευαστή και, εάν η αίτηση υποβάλλεται από τον εξουσιοδοτημένο αντιπρόσωπο, την επωνυμία και τη διεύθυνση και του εξουσιοδοτημένου αντιπροσώπου·

3.2 γραπτή δήλωση ότι η ίδια αίτηση δεν έχει υποβληθεί σε άλλον κοινοποιημένο οργανισμό·

3.3 τον τεχνικό φάκελο, ο οποίος καθιστά δυνατή την αξιολόγηση της συμμόρφωσης του προϊόντος με ψηφιακά στοιχεία προς τις εφαρμοστέες ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στο παράρτημα I μέρος I και τις διαδικασίες που εφαρμόζει ο κατασκευαστής για τον χειρισμό ευπαθειών, όπως ορίζονται στο παράρτημα I μέρος II, και περιλαμβάνει επαρκή ανάλυση και εκτίμηση των κινδύνων. Ο τεχνικός φάκελος προσδιορίζει τις εφαρμοστέες απαιτήσεις και καλύπτει – στον βαθμό που αυτό απαιτείται για την αξιολόγηση – τον σχεδιασμό, την κατασκευή και τη λειτουργία του προϊόντος με ψηφιακά στοιχεία. Ο τεχνικός φάκελος περιέχει, κατά περίπτωση, τουλάχιστον τα στοιχεία που ορίζονται στο παράρτημα VII·

3.4 τα δικαιολογητικά που αποδεικνύουν την επάρκεια των λύσεων τεχνικού σχεδιασμού και ανάπτυξης και των διαδικασιών χειρισμού ευπαθειών. Τα εν λόγω δικαιολογητικά μνημονεύουν όλα τα σχετικά έγγραφα που έχουν χρησιμοποιηθεί, ιδίως στις περιπτώσεις που δεν έχουν εφαρμοστεί πλήρως τα σχετικά εναρμονισμένα πρότυπα ή οι τεχνικές προδιαγραφές. Τα δικαιολογητικά περιλαμβάνουν, εφόσον είναι αναγκαίο, τα αποτελέσματα των δοκιμών που διενεργήθηκαν από το κατάλληλο εργαστήριο του κατασκευαστή ή από άλλο εργαστήριο δοκιμών για λογαριασμό του και υπ’ ευθύνη του.

4. Ο κοινοποιημένος οργανισμός:

4.1. εξετάζει τον τεχνικό φάκελο και τα δικαιολογητικά για να εκτιμήσει την καταλληλότητα του τεχνικού σχεδιασμού και της ανάπτυξης του προϊόντος με ψηφιακά στοιχεία με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος I και των διαδικασιών χειρισμού ευπαθειών που εφαρμόζει ο κατασκευαστής με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος II·

4.2. επαληθεύει ότι τα δείγματα αναπτύχθηκαν ή κατασκευάστηκαν σε συμμόρφωση με τον τεχνικό φάκελο και προσδιορίζει τα στοιχεία που σχεδιάστηκαν και αναπτύχθηκαν σύμφωνα με τις εφαρμοστέες διατάξεις των σχετικών εναρμονισμένων προτύπων ή τεχνικών προδιαγραφών, καθώς και τα στοιχεία που σχεδιάστηκαν και αναπτύχθηκαν χωρίς την εφαρμογή των αντίστοιχων διατάξεων των εν λόγω προτύπων·

4.3. αναλαμβάνει ή αναθέτει τη διεξαγωγή των κατάλληλων ελέγχων και δοκιμών, για να εξακριβώσει ότι, εφόσον ο κατασκευαστής επέλεξε να εφαρμόσει τις λύσεις των σχετικών εναρμονισμένων προτύπων ή τεχνικών προδιαγραφών για τις απαιτήσεις που ορίζονται στο παράρτημα I, εφαρμόστηκαν ορθά·

4.4. αναλαμβάνει ή αναθέτει τη διεξαγωγή των κατάλληλων ελέγχων και δοκιμών, για να εξακριβώσει ότι, όπου δεν εφαρμόστηκαν οι λύσεις των σχετικών εναρμονισμένων προτύπων ή τεχνικών προδιαγραφών για τις απαιτήσεις που ορίζονται στο παράρτημα I, οι λύσεις που επέλεξε ο κατασκευαστής πληρούν τις αντίστοιχες ουσιώδεις απαιτήσεις κυβερνοασφάλειας·

4.5. συμφωνεί με τον κατασκευαστή τον τόπο στον οποίο θα διεξαχθούν οι εξετάσεις και οι δοκιμές.

5. Ο κοινοποιημένος οργανισμός συντάσσει έκθεση αξιολόγησης στην οποία καταγράφονται οι ενέργειες που πραγματοποιήθηκαν σύμφωνα με το σημείο 4, καθώς και η έκβασή τους. Ο κοινοποιημένος οργανισμός, με την επιφύλαξη των υποχρεώσεών του έναντι των κοινοποιουσών αρχών, δημοσιοποιεί το περιεχόμενο της έκθεσης αυτής, εν μέρει ή εξ ολοκλήρου, μόνο κατόπιν συμφωνίας του κατασκευαστή.

6. Στην περίπτωση που ο τύπος και οι διαδικασίες χειρισμού ευπαθειών πληρούν τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I, ο κοινοποιημένος οργανισμός χορηγεί στον κατασκευαστή πιστοποιητικό εξέτασης τύπου ΕΕ. Το πιστοποιητικό περιλαμβάνει την επωνυμία και τη διεύθυνση του κατασκευαστή, τα πορίσματα της εξέτασης, τους (τυχόν) όρους υπό τους οποίους ισχύει το πιστοποιητικό και τα απαραίτητα στοιχεία για την ταυτοποίηση του εγκεκριμένου τύπου και των διαδικασιών χειρισμού ευπαθειών. Στο πιστοποιητικό είναι δυνατό να επισυνάπτονται ένα ή περισσότερα παραρτήματα.

Το πιστοποιητικό και τα παραρτήματά του περιλαμβάνουν όλες τις απαραίτητες πληροφορίες για την αξιολόγηση της συμμόρφωσης των προϊόντων με ψηφιακά στοιχεία που κατασκευάστηκαν ή αναπτύχθηκαν προς τον εξετασθέντα τύπο και των διαδικασιών χειρισμού ευπαθειών για τον έλεγχο εν λειτουργία.

Στην περίπτωση που ο τύπος και οι διαδικασίες χειρισμού ευπαθειών δεν πληρούν τις εφαρμοστέες ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι, ο κοινοποιημένος οργανισμός αρνείται να χορηγήσει πιστοποιητικό εξέτασης τύπου ΕΕ και ενημερώνει τον αιτούντα σχετικά, αιτιολογεί δε λεπτομερώς την άρνηση χορήγησης του πιστοποιητικού.

7. Ο κοινοποιημένος οργανισμός παρακολουθεί όλες τις εξελίξεις της γενικώς αναγνωρισμένης τεχνολογίας, από τις οποίες προκύπτει ότι ο εγκεκριμένος τύπος και οι διαδικασίες χειρισμού ευπαθειών μπορεί να μην πληρούν πλέον τις εφαρμοστέες ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι του παρόντος κανονισμού και αποφασίζει εάν οι εξελίξεις αυτές απαιτούν περαιτέρω έρευνες. Στην περίπτωση αυτή, ο κοινοποιημένος οργανισμός ενημερώνει σχετικά τον κατασκευαστή.

Ο κατασκευαστής γνωστοποιεί στον κοινοποιημένο οργανισμό, ο οποίος έχει στην κατοχή του τον τεχνικό φάκελο για το πιστοποιητικό εξέτασης τύπου ΕΕ, κάθε τροποποίηση του εγκεκριμένου τύπου και των διαδικασιών χειρισμού ευπαθειών που ενδέχεται να επηρεάσει τη συμμόρφωση προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι, ή προς τους όρους υπό τους οποίους ισχύει το πιστοποιητικό. Για τις τροποποιήσεις αυτές απαιτείται συμπληρωματική έγκριση υπό μορφή προσθήκης στο αρχικό πιστοποιητικό εξέτασης τύπου ΕΕ.

8. Ο κοινοποιημένος οργανισμός διενεργεί περιοδικούς ελέγχους για να εξασφαλίζει ότι οι διαδικασίες χειρισμού ευπαθειών που ορίζονται στο παράρτημα I μέρος II εφαρμόζονται επαρκώς.

9. Κάθε κοινοποιημένος οργανισμός ενημερώνει τις οικείες κοινοποιούσες αρχές σχετικά με τα πιστοποιητικά εξέτασης τύπου ΕΕ ή κάθε προσθήκη τους που εξέδωσε ή απέσυρε και θέτει στη διάθεση των οικείων κοινοποιουσών αρχών, περιοδικά ή εφόσον του ζητηθεί, κατάλογο των πιστοποιητικών και τυχόν προσθηκών τους που έχει απορρίψει, αναστείλει ή περιορίσει με άλλο τρόπο.

Κάθε κοινοποιημένος οργανισμός πληροφορεί τους άλλους κοινοποιημένους οργανισμούς σχετικά με τα πιστοποιητικά εξέτασης τύπου ΕΕ και τυχόν προσθήκες σε πιστοποιητικά που έχει απορρίψει, αποσύρει ή αναστείλει ή στα οποία/στις οποίες έχει επιβάλει περιορισμούς με άλλον τρόπο και, κατόπιν αιτήματος, σχετικά με τα πιστοποιητικά και τις προσθήκες σε πιστοποιητικά που έχει χορηγήσει.

Η Επιτροπή, τα κράτη μέλη και οι άλλοι κοινοποιημένοι οργανισμοί μπορούν, εφόσον το ζητήσουν, να λάβουν αντίγραφο των πιστοποιητικών εξέτασης τύπου ΕΕ και τυχόν προσθηκών τους. Κατόπιν αιτήματος, η Επιτροπή και τα κράτη μέλη μπορούν να λάβουν αντίγραφο του τεχνικού φακέλου και των πορισμάτων των εξετάσεων που διενεργήθηκαν από τον κοινοποιημένο οργανισμό. Ο κοινοποιημένος οργανισμός διατηρεί αντίγραφο του πιστοποιητικού εξέτασης τύπου ΕΕ, των παραρτημάτων και των προσθηκών του, καθώς και τον τεχνικό φάκελο που περιλαμβάνει τα έγγραφα που υπέβαλε ο κατασκευαστής, έως τη λήξη ισχύος του πιστοποιητικού.

10. Ο κατασκευαστής διατηρεί στη διάθεση των εθνικών αρχών αντίγραφο του πιστοποιητικού εξέτασης τύπου ΕΕ, των παραρτημάτων και των προσθηκών του μαζί με τον τεχνικό φάκελο, επί 10 έτη αφότου το προϊόν με ψηφιακά στοιχεία τεθεί σε κυκλοφορία στην αγορά ή για την περίοδο υποστήριξης, ανάλογα με το ποιο διάστημα είναι μεγαλύτερο.

11. Ο εξουσιοδοτημένος αντιπρόσωπος του κατασκευαστή μπορεί να υποβάλει την αίτηση που προβλέπεται στο σημείο 3 και να εκπληρώσει τις υποχρεώσεις που προβλέπονται στα σημεία 7 και 10, υπό την προϋπόθεση ότι οι σχετικές υποχρεώσεις προσδιορίζονται λεπτομερώς στην εντολή.

Μέρος ΙΙΙ Συμμόρφωση προς τον τύπο βάσει εσωτερικού ελέγχου παραγωγής (βάσει της ενότητας Γ)

1. Η συμμόρφωση προς τον τύπο βάσει εσωτερικού ελέγχου παραγωγής είναι το μέρος της διαδικασίας αξιολόγησης της συμμόρφωσης με το οποίο ο κατασκευαστής εκπληρώνει τις υποχρεώσεις που καθορίζονται στα σημεία 2 και 3 του παρόντος μέρους, και βεβαιώνει και δηλώνει ότι τα σχετικά προϊόντα με ψηφιακά στοιχεία είναι σύμφωνα προς τον τύπο που περιγράφεται στο πιστοποιητικό εξέτασης τύπου ΕΕ και πληρούν τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι μέρος Ι, και ότι ο κατασκευαστής πληροί τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα Ι μέρος ΙΙ.

2. Παραγωγή

Ο κατασκευαστής λαμβάνει όλα τα αναγκαία μέτρα, ώστε η παραγωγή και η παρακολούθησή της να εξασφαλίζουν τη συμμόρφωση των προϊόντων με ψηφιακά στοιχεία που κατασκευάζονται προς τον εγκεκριμένο τύπο που περιγράφεται στο πιστοποιητικό εξέτασης τύπου ΕΕ και προς τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος I, και διασφαλίζει ότι ο κατασκευαστής πληροί τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος II.

3. Σήμανση συμμόρφωσης και δήλωση συμμόρφωσης

3.1. Ο κατασκευαστής τοποθετεί τη σήμανση CE σε κάθε προϊόν με ψηφιακά στοιχεία που είναι σύμφωνο προς τον τύπο που περιγράφεται στο πιστοποιητικό εξέτασης τύπου ΕΕ και πληροί τις ισχύουσες απαιτήσεις της νομοθετικής πράξης.

3.2. Ο κατασκευαστής συντάσσει γραπτή δήλωση συμμόρφωσης για κάθε μοντέλο προϊόντος και την θέτει στη διάθεση των εθνικών αρχών επί δέκα έτη αφότου το προϊόν με ψηφιακά στοιχεία τεθεί σε κυκλοφορία στην αγορά ή για την περίοδο υποστήριξης, ανάλογα με το ποιο διάστημα είναι μεγαλύτερο. Η δήλωση συμμόρφωσης αναφέρει το μοντέλο του προϊόντος για το οποίο έχει συνταχθεί. Στις αρμόδιες αρχές, εφόσον το ζητήσουν, διατίθεται αντίγραφο της δήλωσης συμμόρφωσης.

4. Εξουσιοδοτημένος αντιπρόσωπος

Οι υποχρεώσεις του κατασκευαστή που καθορίζονται στο σημείο 3 είναι δυνατό να εκπληρώνονται από τον εξουσιοδοτημένο αντιπρόσωπό του, εξ ονόματός του και υπό την ευθύνη του, υπό την προϋπόθεση ότι οι σχετικές υποχρεώσεις προσδιορίζονται στην εντολή.

Μέρος IV Συμμόρφωση βάσει πλήρους διασφάλισης ποιότητας (βάσει της ενότητας Η)

1. Η συμμόρφωση βάσει πλήρους διασφάλισης ποιότητας είναι η διαδικασία αξιολόγησης της συμμόρφωσης με την οποία ο κατασκευαστής εκπληρώνει τις υποχρεώσεις που καθορίζονται στα σημεία 2 και 5 του παρόντος μέρους, και βεβαιώνει και δηλώνει, με αποκλειστική του ευθύνη, ότι τα σχετικά προϊόντα με ψηφιακά στοιχεία ή οι σχετικές κατηγορίες προϊόντων πληρούν τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που καθορίζονται στο παράρτημα Ι μέρος Ι, και ότι οι διαδικασίες χειρισμού ευπαθειών που εφαρμόζει ο κατασκευαστής πληρούν τις απαιτήσεις που καθορίζονται στο παράρτημα Ι μέρος ΙΙ.

2. Σχεδιασμός, ανάπτυξη, παραγωγή και χειρισμός ευπαθειών προϊόντων με ψηφιακά στοιχεία

Ο κατασκευαστής εφαρμόζει εγκεκριμένο σύστημα ποιότητας, όπως ορίζεται στο σημείο 3, για τον σχεδιασμό, την ανάπτυξη και την επιθεώρηση και τη δοκιμή των σχετικών τελικών προϊόντων με ψηφιακά στοιχεία και για τον χειρισμό των ευπαθειών, διατηρεί την αποτελεσματικότητά του καθ' όλη τη διάρκεια της περιόδου υποστήριξης και υπόκειται σε επιτήρηση όπως ορίζεται στο σημείο 4.

3. Σύστημα ποιότητας

3.1. Ο κατασκευαστής υποβάλλει σε κοινοποιημένο οργανισμό της επιλογής του αίτηση για την αξιολόγηση του συστήματος ποιότητας που εφαρμόζει όσον αφορά τα σχετικά προϊόντα με ψηφιακά στοιχεία.

Η αίτηση περιλαμβάνει:

– την επωνυμία και τη διεύθυνση του κατασκευαστή και, εάν η αίτηση υποβάλλεται από τον εξουσιοδοτημένο αντιπρόσωπο, την επωνυμία και τη διεύθυνση και του εξουσιοδοτημένου αντιπροσώπου·

– τον τεχνικό φάκελο για ένα μοντέλο από κάθε κατηγορία προϊόντων με ψηφιακά στοιχεία που προβλέπεται να κατασκευαστεί ή να αναπτυχθεί. Ο τεχνικός φάκελος περιέχει, κατά περίπτωση, τα στοιχεία που ορίζονται στο παράρτημα VII·

– τον φάκελο τεκμηρίωσης του συστήματος ποιότητας· και

– γραπτή δήλωση ότι η ίδια αίτηση δεν έχει υποβληθεί σε άλλον κοινοποιημένο οργανισμό.

3.2. Το σύστημα ποιότητας διασφαλίζει τη συμμόρφωση των προϊόντων με ψηφιακά στοιχεία με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος I και τη συμμόρφωση των διαδικασιών χειρισμού ευπαθειών που εφαρμόζει ο κατασκευαστής με τις απαιτήσεις που ορίζονται στο παράρτημα I μέρος II.

Όλα τα στοιχεία, οι απαιτήσεις και οι διατάξεις που εφαρμόζει ο κατασκευαστής τεκμηριώνονται, συστηματικά και με τάξη, σε μορφή γραπτών πολιτικών, διαδικασιών και οδηγιών. Ο εν λόγω φάκελος τεκμηρίωσης του συστήματος ποιότητας καθιστά δυνατή την ενιαία ερμηνεία των προγραμμάτων, σχεδίων, εγχειριδίων και αρχείων ποιότητας.

Ειδικότερα, ο φάκελος περιλαμβάνει κατάλληλη περιγραφή:

– των στόχων ποιότητας, του οργανογράμματος, των ευθυνών και των αρμοδιοτήτων των διοικητικών στελεχών όσον αφορά τον σχεδιασμό, την ανάπτυξη, την ποιότητα των προϊόντων και τον χειρισμό των ευπαθειών·

– των προδιαγραφών τεχνικού σχεδιασμού και ανάπτυξης, συμπεριλαμβανομένων των προτύπων που εφαρμόζονται, και, όταν τα σχετικά εναρμονισμένα πρότυπα ή τεχνικές προδιαγραφές δεν εφαρμόζονται πλήρως, των μέσων που θα χρησιμοποιηθούν ώστε να διασφαλίζεται ότι τηρούνται οι ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος I και ισχύουν για τα προϊόντα με ψηφιακά στοιχεία·

– των διαδικαστικών προδιαγραφών, συμπεριλαμβανομένων των προτύπων που εφαρμόζονται, και, όταν τα σχετικά εναρμονισμένα πρότυπα ή οι τεχνικές προδιαγραφές δεν εφαρμόζονται πλήρως, των μέσων που θα χρησιμοποιηθούν ώστε να διασφαλίζεται ότι τηρούνται οι ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος II και που ισχύουν για τον κατασκευαστή·

– του ελέγχου σχεδιασμού και ανάπτυξης, καθώς και των τεχνικών επαλήθευσης του σχεδιασμού και της ανάπτυξης, των διαδικασιών και συστηματικών δραστηριοτήτων που θα χρησιμοποιούνται κατά τον σχεδιασμό και την ανάπτυξη των προϊόντων με ψηφιακά στοιχεία όσον αφορά την καλυπτόμενη κατηγορία προϊόντων·

– των αντίστοιχων τεχνικών παραγωγής, ποιοτικού ελέγχου και διασφάλισης της ποιότητας, των διαδικασιών και των συστηματικών δραστηριοτήτων που θα εφαρμόζονται·

– των εξετάσεων και των δοκιμών που θα διεξάγονται πριν από, κατά και μετά την παραγωγή, καθώς και της συχνότητας διεξαγωγής τους·

– των φακέλων ποιότητας, όπως των εκθέσεων επιθεώρησης και των στοιχείων δοκιμών, των στοιχείων βαθμονόμησης και των εκθέσεων προσόντων για το αρμόδιο προσωπικό·

– των μέσων παρακολούθησης που επιτρέπουν να ελέγχονται η ποιότητα σχεδιασμού και προϊόντων και η αποτελεσματική λειτουργία του συστήματος ποιότητας.

3.3. Ο κοινοποιημένος οργανισμός αξιολογεί το σύστημα ποιότητας για να διαπιστώσει αν πληροί τις απαιτήσεις που αναφέρονται στο σημείο 3.2.

Ο κοινοποιημένος οργανισμός θεωρεί ότι ανταποκρίνονται στις απαιτήσεις αυτές τα στοιχεία του συστήματος ποιότητας που πληρούν τις αντίστοιχες προδιαγραφές του εθνικού προτύπου το οποίο εφαρμόζει το σχετικό εναρμονισμένο πρότυπο ή τις τεχνικές προδιαγραφές.

Εκτός από τα μέλη με πείρα στα συστήματα διαχείρισης της ποιότητας, η ομάδα ελεγκτών περιλαμβάνει τουλάχιστον ένα μέλος το οποίο έχει πείρα αξιολόγησης στον τομέα του σχετικού προϊόντος και της τεχνολογίας του και γνωρίζει τις εφαρμοστέες απαιτήσεις του παρόντος κανονισμού. Ο έλεγχος περιλαμβάνει επίσκεψη αξιολόγησης στις εγκαταστάσεις του κατασκευαστή, εφόσον αυτές υπάρχουν. Η ομάδα ελεγκτών ελέγχει τον τεχνικό φάκελο στον οποίο αναφέρεται το σημείο 3.1 δεύτερη περίπτωση, για να επαληθεύσει την ικανότητα του κατασκευαστή να εντοπίζει τις σχετικές απαιτήσεις του παρόντος κανονισμού και να πραγματοποιεί τους αναγκαίους ελέγχους με σκοπό τη διασφάλιση της συμμόρφωσης του προϊόντος με ψηφιακά στοιχεία προς τις απαιτήσεις αυτές.

Η απόφαση κοινοποιείται στον κατασκευαστή ή στον εξουσιοδοτημένο αντιπρόσωπό του.

Η κοινοποίηση περιέχει τα συμπεράσματα του ελέγχου και την αιτιολογημένη απόφαση αξιολόγησης.

3.4. Ο κατασκευαστής αναλαμβάνει τη δέσμευση να εκπληρώνει τις υποχρεώσεις που απορρέουν από το σύστημα ποιότητας, όπως έχει εγκριθεί, και να μεριμνά ώστε το σύστημα ποιότητας να παραμένει επαρκές και αποτελεσματικό.

3.5. Ο κατασκευαστής ενημερώνει τον κοινοποιημένο οργανισμό που έχει εγκρίνει το σύστημα ποιότητας για κάθε σχεδιαζόμενη τροποποίηση του συστήματος ποιότητας.

Ο κοινοποιημένος οργανισμός αξιολογεί κάθε προτεινόμενη αλλαγή και αποφασίζει αν το τροποποιημένο σύστημα ποιότητας θα εξακολουθεί να ανταποκρίνεται στις απαιτήσεις που αναφέρονται στο σημείο 3.2 ή αν κρίνεται αναγκαία η επαναξιολόγησή του.

Η απόφασή του κοινοποιείται στον κατασκευαστή. Η κοινοποίηση περιέχει τα συμπεράσματα της εξέτασης και την αιτιολογημένη απόφαση αξιολόγησης.

4. Εποπτεία υπό την ευθύνη του κοινοποιημένου οργανισμού

4.1. Σκοπός της εποπτείας είναι να διασφαλίζει ότι ο κατασκευαστής εκπληρώνει δεόντως τις υποχρεώσεις που προκύπτουν από το εγκεκριμένο σύστημα ποιότητας.

4.2. Ο κατασκευαστής πρέπει να επιτρέπει στον κοινοποιημένο οργανισμό την πρόσβαση, για λόγους αξιολόγησης, στους χώρους σχεδιασμού, ανάπτυξης, παραγωγής, επιθεώρησης, δοκιμών και αποθήκευσης και του παρέχει όλες τις απαραίτητες πληροφορίες, και ιδίως:

– τον φάκελο τεκμηρίωσης του συστήματος ποιότητας·

– τα αρχεία ποιότητας που προβλέπονται στο σχεδιαστικό μέρος του συστήματος ποιότητας, όπως αποτελέσματα αναλύσεων, υπολογισμών και δοκιμών,

– τα αρχεία ποιότητας που προβλέπονται στο κατασκευαστικό μέρος του συστήματος ποιότητας, όπως εκθέσεις επιθεώρησης και στοιχεία δοκιμών, στοιχεία βαθμονόμησης και εκθέσεις προσόντων του αρμόδιου προσωπικού.

4.3. Ο κοινοποιημένος οργανισμός διενεργεί περιοδικούς ελέγχους για να βεβαιώνεται ότι ο κατασκευαστής συντηρεί και εφαρμόζει το σύστημα ποιότητας, και παραδίδει έκθεση ελέγχου στον κατασκευαστή.

5. Σήμανση συμμόρφωσης και δήλωση συμμόρφωσης

5.1. Ο κατασκευαστής τοποθετεί τη σήμανση CE και, με ευθύνη του κοινοποιημένου οργανισμού που αναφέρεται στο σημείο 3.1, τον αριθμό μητρώου του εν λόγω κοινοποιημένου οργανισμού σε κάθε μεμονωμένο προϊόν με ψηφιακά στοιχεία που πληροί τις απαιτήσεις που ορίζονται στο παράρτημα I μέρος I του παρόντος κανονισμού.

5.2. Ο κατασκευαστής συντάσσει γραπτή δήλωση συμμόρφωσης για κάθε μοντέλο προϊόντος και την θέτει στη διάθεση των εθνικών αρχών επί δέκα έτη αφότου το προϊόν με ψηφιακά στοιχεία τεθεί σε κυκλοφορία στην αγορά ή για την περίοδο υποστήριξης, ανάλογα με το ποιο διάστημα είναι μεγαλύτερο. Η δήλωση συμμόρφωσης αναφέρει το μοντέλο του προϊόντος για το οποίο έχει συνταχθεί.

Στις αρμόδιες αρχές, εφόσον το ζητήσουν, διατίθεται αντίγραφο της δήλωσης συμμόρφωσης.

6. Για περίοδο τουλάχιστον 10 ετών αφότου το προϊόν με ψηφιακά στοιχεία τεθεί σε κυκλοφορία στην αγορά ή για την περίοδο υποστήριξης, ανάλογα με το ποιο διάστημα είναι μεγαλύτερο, ο κατασκευαστής διατηρεί στη διάθεση των εθνικών αρχών:

6.1 τον τεχνικό φάκελο που αναφέρεται στο σημείο 3.1·

6.2 τον φάκελο τεκμηρίωσης του συστήματος ποιότητας που αναφέρεται στο σημείο 3.1·

6.3 την τροποποίηση που αναφέρεται στο σημείο 3.5, όπως εγκρίθηκε·

6.4 τις αποφάσεις και τις εκθέσεις του κοινοποιημένου οργανισμού, που αναφέρονται στα σημεία 3.5 και 4.3.

7. Κάθε κοινοποιημένος οργανισμός ενημερώνει τις οικείες κοινοποιούσες αρχές για τις εγκρίσεις του συστήματος ποιότητας που χορηγούνται ή ανακαλούνται, και θέτει στη διάθεση των οικείων κοινοποιουσών αρχών, περιοδικά ή εφόσον του ζητηθεί, τον κατάλογο των εγκρίσεων των συστημάτων ποιότητας που έχουν απορριφθεί, ανασταλεί ή στις οποίες έχουν επιβληθεί περιορισμοί με άλλο τρόπο.

Κάθε κοινοποιημένος οργανισμός ενημερώνει τους άλλους κοινοποιημένους οργανισμούς για τις εγκρίσεις των συστημάτων ποιότητας τις οποίες έχει απορρίψει, αναστείλει ή ανακαλέσει, και, εφόσον του ζητηθεί, για τις εγκρίσεις των συστημάτων ποιότητας τις οποίες χορήγησε.

8. Εξουσιοδοτημένος αντιπρόσωπος

Οι υποχρεώσεις του κατασκευαστή που καθορίζονται στα σημεία 3.1, 3.5, 5 και 6 είναι δυνατό να εκπληρώνονται από τον εξουσιοδοτημένο αντιπρόσωπό του, εξ ονόματός του και υπό την ευθύνη του, υπό την προϋπόθεση ότι οι σχετικές υποχρεώσεις ορίζονται λεπτομερώς στην εντολή.

Έχει γίνει δήλωση σχετικά με τον παρόντα κανονισμό, η οποία βρίσκεται στην [ΕΕ να σημειωθεί: ΕΕ C XXX της XX.XX.2024, σ. XX] και στον ακόλουθο σύνδεσμο: [ΕΕ: να εισαχθεί ο σύνδεσμος στη δήλωση].
