2025/37

15.1.2025

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2025/37 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 19ης Δεκεμβρίου 2024

για την τροποποίηση του κανονισμού (ΕΕ) 2019/881 όσον αφορά τις διαχειριζόμενες υπηρεσίες ασφάλειας

(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],

Κατόπιν διαβούλευσης με την Επιτροπή των Περιφερειών,

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία [2],

Εκτιμώντας τα ακόλουθα:

(1) Ο κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [3] θεσπίζει ένα πλαίσιο για τη θέσπιση ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας με σκοπό τη διασφάλιση επαρκούς επιπέδου κυβερνοασφάλειας για τα προϊόντα τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ), τις υπηρεσίες ΤΠΕ και τις διαδικασίες ΤΠΕ στην Ένωση, καθώς και με σκοπό την αποφυγή του κατακερματισμού της εσωτερικής αγοράς όσον αφορά τα σχήματα πιστοποίησης της κυβερνοασφάλειας στην Ένωση.

(2) Προκειμένου να διασφαλιστεί η ανθεκτικότητα της Ένωσης σε κυβερνοεπιθέσεις και να προληφθούν τυχόν τρωτά σημεία στην εσωτερική αγορά, ο παρών κανονισμός αποσκοπεί στη συμπλήρωση του οριζόντιου κανονιστικού πλαισίου που θεσπίζει ολοκληρωμένες απαιτήσεις κυβερνοασφάλειας για όλα τα προϊόντα με ψηφιακά στοιχεία σύμφωνα με τον κανονισμό (ΕΕ) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [4], θεσπίζοντας στόχους ασφαλείας για τις διαχειριζόμενες υπηρεσίες ασφάλειας, την εφαρμογή τους και την αξιοπιστία των εν λόγω υπηρεσιών.

(3) Οι διαχειριζόμενες υπηρεσίες ασφάλειας είναι υπηρεσίες που παρέχονται από παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας όπως ορίζονται στο άρθρο 6 σημείο 40) της οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [5]. Συνεπώς, ο ορισμός των διαχειριζόμενων υπηρεσιών ασφάλειας στον παρόντα κανονισμό θα πρέπει να συνάδει με τον ορισμό των παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας στην οδηγία (ΕΕ) 2022/2555. Οι υπηρεσίες αυτές συνίστανται στην εκτέλεση ή την παροχή βοήθειας για δραστηριότητες που σχετίζονται με τη διαχείριση κινδύνων κυβερνοασφάλειας από τους πελάτες τους και αποκτούν ολοένα και μεγαλύτερη σημασία για την πρόληψη και τον μετριασμό των περιστατικών. Ως εκ τούτου, οι πάροχοι των εν λόγω υπηρεσιών θεωρούνται βασικές ή σημαντικές οντότητες που ανήκουν σε τομέα υψηλής κρισιμότητας σύμφωνα με την οδηγία (ΕΕ) 2022/2555. Όπως σημειώνεται στην αιτιολογική σκέψη 86 της εν λόγω οδηγίας, οι πάροχοι διαχειριζομένων υπηρεσιών ασφάλειας σε τομείς όπως η αντιμετώπιση περιστατικών, οι δοκιμές διείσδυσης, οι έλεγχοι ασφάλειας και η παροχή συμβουλών διαδραματίζουν ιδιαίτερα σημαντικό ρόλο στην παροχή συνδρομής σε οντότητες που καταβάλλουν προσπάθειες για την πρόληψη, τον εντοπισμό και την αντιμετώπιση περιστατικών ή την ανάκαμψη από αυτά. Ωστόσο, οι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας αποτέλεσαν και οι ίδιοι στόχο κυβερνοεπιθέσεων και ενέχουν ιδιαίτερο κίνδυνο λόγω της στενής ενσωμάτωσής τους στις δραστηριότητες των πελατών τους. Συνεπώς, είναι σημαντικό οι βασικές και σημαντικές οντότητες κατά την έννοια της οδηγίας (ΕΕ) 2022/2555 να επιδεικνύουν αυξημένη επιμέλεια κατά την επιλογή παρόχων διαχειριζομένων υπηρεσιών ασφάλειας.

---

[1] ΕΕ C 349 της 29.9.2023, σ. 167.

[2] Θέση του Ευρωπαϊκού Κοινοβουλίου της 24ης Απριλίου 2024 (δεν έχει ακόμη δημοσιευτεί στην Επίσημη Εφημερίδα) και θέση του Συμβουλίου της 2ας Δεκεμβρίου 2024.

[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] Κανονισμός (ΕΕ) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2024, 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, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[5] 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) Ο ορισμός των διαχειριζόμενων υπηρεσιών ασφάλειας στο πλαίσιο του παρόντος κανονισμού περιλαμβάνει μη εξαντλητικό κατάλογο διαχειριζόμενων υπηρεσιών ασφάλειας που θα μπορούσαν να πληρούν τις προϋποθέσεις για ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας, όπως ο χειρισμός περιστατικών, οι δοκιμές διείσδυσης, οι έλεγχοι ασφάλειας, καθώς και η παροχή συμβουλών σχετικά με την τεχνική υποστήριξη. Οι διαχειριζόμενες υπηρεσίες ασφάλειας θα μπορούσαν να περιλαμβάνουν υπηρεσίες κυβερνοασφάλειας που στηρίζουν την ετοιμότητα, την πρόληψη, τον εντοπισμό, την ανάλυση και τον μετριασμό, την αντιμετώπιση και την ανάκαμψη από περιστατικά. Η παροχή πληροφοριών για τις κυβερνοαπειλές και η εκτίμηση κινδύνου που σχετίζονται με την τεχνική υποστήριξη θα μπορούσαν επίσης να χαρακτηριστούν ως διαχειριζόμενες υπηρεσίες ασφάλειας. Ενδέχεται να υπάρχουν χωριστά ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας για διαφορετικές διαχειριζόμενες υπηρεσίες ασφάλειας. Τα ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας που εκδίδονται σύμφωνα με τα εν λόγω σχήματα θα πρέπει να αναφέρονται σε συγκεκριμένες διαχειριζόμενες υπηρεσίες ασφάλειας συγκεκριμένου παρόχου των εν λόγω υπηρεσιών.

(5) Οι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας μπορούν επίσης να διαδραματίσουν σημαντικό ρόλο σε σχέση με τις δράσεις της Ένωσης για τη στήριξη της αντίδρασης και της αρχικής ανάκαμψης σε περιπτώσεις σημαντικών περιστατικών κυβερνοασφάλειας και περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας, βασιζόμενοι σε υπηρεσίες αξιόπιστων ιδιωτικών παρόχων και σε δοκιμές κρίσιμων οντοτήτων για πιθανά τρωτά σημεία βάσει συντονισμένων σε ενωσιακό επίπεδο εκτιμήσεων κινδύνου. Η πιστοποίηση των διαχειριζόμενων υπηρεσιών ασφάλειας μπορεί να διαδραματίσει ρόλο στην επιλογή αξιόπιστων παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας όπως ορίζονται στον κανονισμό (ΕΕ) 2025/38 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]).

(6) Η πιστοποίηση των διαχειριζόμενων υπηρεσιών ασφάλειας δεν είναι μόνο σημαντική για τη διαδικασία επιλογής για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας που θεσπίζεται με τον κανονισμό (ΕΕ) 2025/38, αλλά αποτελεί επίσης βασικό δείκτη ποιότητας για τους ιδιωτικούς και δημόσιους φορείς που προτίθενται να αγοράσουν τέτοιες υπηρεσίες. Δεδομένης της κρισιμότητας των διαχειριζόμενων υπηρεσιών ασφάλειας και της ευαισθησίας των δεδομένων που υποβάλλονται σε επεξεργασία, η πιστοποίηση μπορεί να παράσχει στους δυνητικούς πελάτες σημαντική καθοδήγηση και διασφάλιση σχετικά με την αξιοπιστία των εν λόγω υπηρεσιών. Τα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας για τις διαχειριζόμενες υπηρεσίες ασφάλειας έχουν ως σκοπό να συμβάλουν στην αποφυγή του κατακερματισμού της εσωτερικής αγοράς. Ως εκ τούτου, ο παρών κανονισμός αποσκοπεί στην ενίσχυση της λειτουργίας της εσωτερικής αγοράς.

(7) Τα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας για διαχειριζόμενες υπηρεσίες ασφάλειας αναμένεται να οδηγήσουν στην υιοθέτηση των εν λόγω υπηρεσιών και στην αύξηση του ανταγωνισμού μεταξύ παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας. Με την επιφύλαξη του στόχου της διασφάλισης επαρκών και κατάλληλων επιπέδων σχετικών τεχνικών γνώσεων και επαγγελματικής ακεραιότητας των εν λόγω παρόχων, τα σχήματα πιστοποίησης θα πρέπει, ως εκ τούτου, να διευκολύνουν την είσοδο στην αγορά και την προσφορά διαχειριζόμενων υπηρεσιών ασφάλειας, απλουστεύοντας, στο μέτρο του δυνατού, τον πιθανό κανονιστικό, διοικητικό και οικονομικό φόρτο που ενδέχεται να αντιμετωπίσουν οι πάροχοι, ιδίως οι μικρές και μεσαίες επιχειρήσεις (ΜΜΕ), μεταξύ άλλων και οι πολύ μικρές επιχειρήσεις, όταν προσφέρουν διαχειριζόμενες υπηρεσίες ασφάλειας. Επιπλέον, προκειμένου να ενθαρρυνθεί η υιοθέτηση των διαχειριζόμενων υπηρεσιών ασφάλειας και να τονωθεί η ζήτηση για αυτές, τα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας θα πρέπει να συμβάλλουν στην προσβασιμότητά τους, ιδίως για τους μικρότερους φορείς, όπως οι ΜΜΕ, μεταξύ άλλων και οι πολύ μικρές επιχειρήσεις, καθώς και για τις τοπικές και περιφερειακές αρχές, οι οποίες διαθέτουν περιορισμένες ικανότητες και πόρους, αλλά είναι πιο ευάλωτες σε παραβιάσεις της κυβερνοασφάλειας που συνεπάγονται οικονομικές, νομικές και λειτουργικές επιπτώσεις, καθώς και επιπτώσεις στη φήμη τους.

(8) Είναι σημαντικό να παρασχεθεί στήριξη στις ΜΜΕ, μεταξύ άλλων και στις πολύ μικρές επιχειρήσεις, για την εφαρμογή του παρόντος κανονισμού και την απόκτηση των εξειδικευμένων δεξιοτήτων και της εμπειρογνωμοσύνης κυβερνοασφάλειας που απαιτούνται για την παροχή διαχειριζόμενων υπηρεσιών ασφάλειας σύμφωνα με τις απαιτήσεις του παρόντος κανονισμού. Το πρόγραμμα «Ψηφιακή Ευρώπη» που θεσπίστηκε με τον κανονισμό (ΕΕ) 2021/694 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]) και άλλα σχετικά προγράμματα της Ένωσης προβλέπουν ότι η Επιτροπή θεσπίζει χρηματοδοτική και τεχνική στήριξη που επιτρέπει στις εν λόγω επιχειρήσεις να συμβάλουν στην ανάπτυξη της οικονομίας της Ένωσης και στην ενίσχυση του κοινού επιπέδου κυβερνοασφάλειας στην Ένωση, μεταξύ άλλων με τον εξορθολογισμό της χρηματοδοτικής στήριξης από το πρόγραμμα «Ψηφιακή Ευρώπη» και άλλα σχετικά προγράμματα της Ένωσης και με τη στήριξη των πολύ μικρών επιχειρήσεων και των ΜΜΕ.

(9) Τα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας για διαχειριζόμενες υπηρεσίες ασφάλειας θα πρέπει να συμβάλουν στη διαθεσιμότητα ασφαλών και υψηλής ποιότητας υπηρεσιών που εγγυώνται ασφαλή ψηφιακή μετάβαση, και στην επίτευξη των στόχων που καθορίζονται στο πρόγραμμα πολιτικής 2030 «Ψηφιακή δεκαετία» που θεσπίστηκε με την απόφαση (ΕΕ) 2022/2481 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([8]), ιδίως όσον αφορά τον στόχο το 75 %

([6]) Κανονισμός (ΕΕ) 2025/38 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Δεκεμβρίου 2024, σχετικά με τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση κυβερνοαπειλών και περιστατικών κυβερνοασφάλειας και για την τροποποίηση του κανονισμού (ΕΕ) 2021/694 (κανονισμός για την αλληλεγγύη στον κυβερνοχώρο) (ΕΕ L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) Κανονισμός (ΕΕ) 2021/694 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 29ης Απριλίου 2021, για τη θέσπιση του προγράμματος Ψηφιακή Ευρώπη και την κατάργηση της απόφασης (ΕΕ) 2015/2240 (ΕΕ L 166 της 11.5.2021, σ. 1).

([8]) Απόφαση (ΕΕ) 2022/2481 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, για τη θέσπιση του προγράμματος πολιτικής 2030 «Ψηφιακή Δεκαετία» (ΕΕ L 323 της 19.12.2022, σ. 4).

των επιχειρήσεων της ΕΕ να αρχίσουν να χρησιμοποιούν υπολογιστικό νέφος, μαζικά δεδομένα ή τεχνητή νοημοσύνη, τον στόχο πάνω από το 90 % των ΜΜΕ, μεταξύ άλλων και των πολύ μικρών επιχειρήσεων, να κατακτήσει τουλάχιστον ένα βασικό επίπεδο ψηφιακής έντασης και τον στόχο να είναι προσβάσιμες επιγραμμικά οι βασικές δημόσιες υπηρεσίες.

(10) Εκτός από την ανάπτυξη προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ, οι διαχειριζόμενες υπηρεσίες ασφάλειας περιλαμβάνουν συχνά πρόσθετα χαρακτηριστικά υπηρεσιών που βασίζονται στις ικανότητες, την εμπειρογνωσία και την πείρα του προσωπικού των παρόχων των εν λόγω υπηρεσιών. Προκειμένου να διασφαλίζεται πολύ υψηλή ποιότητα των παρεχόμενων διαχειριζόμενων υπηρεσιών ασφάλειας, μέρος των στόχων ασφάλειας θα πρέπει να είναι το πολύ υψηλό επίπεδο των εν λόγω ικανοτήτων, εμπειρογνωσίας και πείρας, καθώς και κατάλληλες εσωτερικές διαδικασίες. Συνεπώς, για να εξασφαλιστεί ότι όλες οι πτυχές των διαχειριζόμενων υπηρεσιών ασφάλειας μπορούν να καλυφθούν από ειδικά ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας, είναι αναγκαίο να τροποποιηθεί ο κανονισμός (ΕΕ) 2019/881. Θα πρέπει να ληφθούν υπόψη τα αποτελέσματα και οι συστάσεις της αξιολόγησης και επανεξέτασης που προβλέπονται στον κανονισμό (ΕΕ) 2019/881.

(11) Με σκοπό να διευκολυνθεί η ανάπτυξη μιας αξιόπιστης εσωτερικής αγοράς και παράλληλα να δημιουργηθούν εταιρικές σχέσεις με ομόφρονες τρίτες χώρες, η διαδικασία πιστοποίησης που θεσπίστηκε εντός του πλαισίου της ευρωπαϊκής πιστοποίησης της κυβερνοασφάλειας που προβλέπεται από τον κανονισμό (ΕΕ) 2019/881 θα πρέπει να υλοποιείται κατά τρόπο που διευκολύνει τη διεθνή αναγνώριση και την εναρμόνιση με διεθνή πρότυπα.

(12) Η Ένωση βρίσκεται αντιμέτωπη με μια έλλειψη ταλέντων, χαρακτηριστικό της οποίας είναι η έλλειψη ειδικευμένων επαγγελματιών, και με ένα ταχέως εξελισσόμενο τοπίο απειλών, όπως αναγνωρίζεται στην ανακοίνωση της Επιτροπής, της 18ης Απριλίου 2023, με τίτλο «Κάλυψη της έλλειψης ταλέντων στον τομέα της κυβερνοασφάλειας για την ενίσχυση της ανταγωνιστικότητας, της ανάπτυξης και της ανθεκτικότητας της ΕΕ (“Η Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας”)». Οι εκπαιδευτικοί πόροι και οι μορφές επίσημης κατάρτισης ποικίλλουν και οι γνώσεις μπορούν να αποκτηθούν με διάφορους τρόπους: τυπικούς, για παράδειγμα μέσω πανεπιστημίων ή μαθημάτων, ή μη τυπικούς, για παράδειγμα μέσω προγραμμάτων επαγγελματικής κατάρτισης ή μακροχρόνιας εργασιακής πείρας στον σχετικό τομέα. Συνεπώς, προκειμένου να διευκολυνθεί η εμφάνιση υψηλής ποιότητας διαχειριζόμενων υπηρεσιών ασφάλειας και να υπάρξει καλύτερη επισκόπηση της σύνθεσης του εργατικού δυναμικού της Ένωσης στον τομέα της κυβερνοασφάλειας, είναι σημαντικό να ενισχυθεί η συνεργασία μεταξύ των κρατών μελών, της Επιτροπής, του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια που θεσπίστηκε με τον κανονισμό (ΕΕ) 2019/881 (ENISA) και των ενδιαφερόμενων μερών, συμπεριλαμβανομένου του ιδιωτικού τομέα και της πανεπιστημιακής κοινότητας, μέσω της ανάπτυξης συμπράξεων δημόσιου και ιδιωτικού τομέα, της στήριξης πρωτοβουλιών έρευνας και καινοτομίας, της ανάπτυξης και αμοιβαίας αναγνώρισης κοινών προτύπων και πιστοποιήσεων δεξιοτήτων κυβερνοασφάλειας, μεταξύ άλλων μέσω του ευρωπαϊκού πλαισίου δεξιοτήτων κυβερνοασφάλειας. Η συνεργασία αυτή θα διευκολύνει την κινητικότητα των επαγγελματιών της κυβερνοασφάλειας εντός της Ένωσης, καθώς και την ενσωμάτωση των γνώσεων και της κατάρτισης στον τομέα της κυβερνοασφάλειας στα εκπαιδευτικά προγράμματα, διασφαλίζοντας παράλληλα την πρόσβαση των νέων, συμπεριλαμβανομένων των ατόμων που ζουν σε μειονεκτούσες περιοχές όπως νησιά, αραιοκατοικημένες, αγροτικές και απομακρυσμένες περιοχές, σε θέσεις μαθητείας και πρακτικής άσκησης. Είναι σημαντικό η εν λόγω συνεργασία να αποσκοπεί στην προσέλκυση περισσότερων γυναικών και κοριτσιών στον τομέα και να συμβάλει στην αντιμετώπιση του χάσματος μεταξύ των φύλων στους τομείς των θετικών επιστημών, της τεχνολογίας, της μηχανικής και των μαθηματικών, και ο ιδιωτικός τομέας να επιδιώκει την παροχή κατάρτισης στον χώρο εργασίας για την αντιμετώπιση των πιο περιζήτητων δεξιοτήτων, με τη συμμετοχή της δημόσιας διοίκησης και των νεοφυών επιχειρήσεων, καθώς και των ΜΜΕ, μεταξύ άλλων και των πολύ μικρών επιχειρήσεων. Είναι επίσης σημαντικό οι πάροχοι και τα κράτη μέλη να συνεργάζονται και να συμβάλλουν στη συλλογή δεδομένων σχετικά με την κατάσταση και την εξέλιξη της αγοράς εργασίας στον τομέα της κυβερνοασφάλειας.

(13) Ο ENISA διαδραματίζει σημαντικό ρόλο στην προετοιμασία των υποψήφιων ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας. Η Επιτροπή θα πρέπει να αξιολογήσει 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.

(14) Ο παρών κανονισμός προβλέπει στοχευμένες τροποποιήσεις του κανονισμού (ΕΕ) 2019/881, ώστε να καταστεί δυνατή η θέσπιση ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας για τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας. Στο πλαίσιο αυτό, επίσης αποσαφηνίζει και διευκρινίζει ορισμένες διατάξεις του εν λόγω κανονισμού σχετικά με την προετοιμασία και τη λειτουργία όλων των ευρωπαϊκών σχημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο, με σκοπό τη διασφάλιση της διαφάνειας και του ανοικτού χαρακτήρα τους. Οι τελευταίες τροποποιήσεις, οι οποίες περιορίζονται στην αποσαφήνιση ή τη διευκρίνιση του κανονισμού (ΕΕ) 2019/881, ιδίως οι τροποποιήσεις σχετικά με τις πληροφορίες που πρέπει να παρέχει ο ENISA όταν κατά την διαβίβαση του υποψήφιου σχήματος, τις ad hoc ομάδες εργασίας που συστήνονται για κάθε υποψήφιο σχήμα, και τις πληροφορίες και διαβουλεύσεις όσον αφορά τα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας, δεν θα πρέπει να προδικάζουν με κανέναν τρόπο την ευρύτερη αξιολόγηση και επανεξέταση του εν λόγω κανονισμού που απαιτείται βάσει του άρθρου 67 του εν λόγω κανονισμού, ιδίως της αξιολόγησης του αντικτύπου, της αποτελεσματικότητας και της απόδοσης του τίτλου του εν λόγω κανονισμού που αφορά το πλαίσιο πιστοποίησης της κυβερνοασφάλειας. Η αξιολόγηση και επανεξέταση όσον αφορά τον εν λόγω τίτλο θα πρέπει να βασίζεται σε ευρεία διαβούλευση με τα ενδιαφερόμενα μέρη και σε πλήρη και διεξοδική ανάλυση των σχετικών διαδικασιών.

(15) Δεδομένου ότι ο στόχος του παρόντος κανονισμού, δηλαδή να καταστεί δυνατή η θέσπιση ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας για τις διαχειριζόμενες υπηρεσίες ασφάλειας, δεν μπορεί να επιτευχθεί επαρκώς από τα κράτη μέλη, μπορεί όμως, λόγω της κλίμακας και των επιπτώσεών του, να επιτευχθεί καλύτερα στο επίπεδο της Ένωσης, η Ένωση μπορεί 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 του στόχου αυτού.

(16) Ζητήθηκε, σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([9]), η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος γνωμοδότησε στις 10 Ιανουαρίου 2024,

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

Τροποποιήσεις του κανονισμού (ΕΕ) 2019/881

Ο κανονισμός (ΕΕ) 2019/881 τροποποιείται ως εξής:

1) Στο άρθρο 1 παράγραφος 1 πρώτο εδάφιο, το στοιχείο β) αντικαθίσταται από το ακόλουθο κείμενο:

«β) το πλαίσιο για τη θέσπιση ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας με σκοπό τη διασφάλιση επαρκούς επιπέδου κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας στην Ένωση, καθώς και για τον σκοπό της αποφυγής του κατακερματισμού της εσωτερικής αγοράς όσον αφορά τα σχήματα πιστοποίησης της κυβερνοασφάλειας στην Ένωση.».

2) Το άρθρο 2 τροποποιείται ως εξής:

α) τα σημεία 9), 10) και 11) αντικαθίστανται από το ακόλουθο κείμενο:

«9) “ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας”: πλήρες σύνολο κανόνων, τεχνικών απαιτήσεων, προτύπων και διαδικασιών που θεσπίζονται σε επίπεδο Ένωσης και που εφαρμόζονται στην πιστοποίηση ή την αξιολόγηση της συμμόρφωσης συγκεκριμένων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας,

10) “εθνικό σχήμα πιστοποίησης της κυβερνοασφάλειας”: πλήρες σύνολο κανόνων, τεχνικών απαιτήσεων, προτύπων και διαδικασιών που έχουν αναπτυχθεί και εγκριθεί από εθνική δημόσια αρχή και που εφαρμόζονται για την πιστοποίηση ή την αξιολόγηση της συμμόρφωσης των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας που εμπίπτουν στο πεδίο εφαρμογής του συγκεκριμένου σχήματος,

11) “ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας”: έγγραφο το οποίο εκδίδεται από τον αρμόδιο οργανισμό και βεβαιώνει ότι ένα συγκεκριμένο προϊόν ΤΠΕ, μια συγκεκριμένη υπηρεσία ΤΠΕ, διαδικασία ΤΠΕ ή διαχειριζόμενη υπηρεσία ασφάλειας έχει αξιολογηθεί ως προς τη συμμόρφωση με συγκεκριμένες απαιτήσεις ασφαλείας που προβλέπει ένα ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας,»·

β) προστίθεται το ακόλουθο σημείο:

«14α) “διαχειριζόμενη υπηρεσία ασφάλειας”: υπηρεσία που παρέχεται σε τρίτο μέρος και που συνίσταται στην εκτέλεση ή την παροχή βοήθειας ή συμβουλών για δραστηριότητες που σχετίζονται με τη διαχείριση κινδύνων κυβερνοασφάλειας, συμπεριλαμβανομένων του χειρισμού συμβάντων, των δοκιμών διείσδυσης, των ελέγχων ασφάλειας και της παροχής συμβουλών, μεταξύ άλλων από εμπειρογνώμονες, σχετικά με την τεχνική υποστήριξη,»·

γ) τα σημεία 20), 21) και 22) αντικαθίστανται από το ακόλουθο κείμενο:

«20) “τεχνική προδιαγραφή”: έγγραφο με το οποίο ορίζονται οι τεχνικές απαιτήσεις που πρέπει να πληρούνται από προϊόν ΤΠΕ, υπηρεσία ΤΠΕ, διαδικασία ΤΠΕ ή διαχειριζόμενη υπηρεσία ασφάλειας ή οι σχετικές με αυτά διαδικασίες αξιολόγησης της συμμόρφωσης,

([9]) 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).

21) "επίπεδο διασφάλισης": η βάση για την εμπιστοσύνη ότι ένα προϊόν ΤΠΕ, μια υπηρεσία ΤΠΕ, μια διαδικασία ΤΠΕ ή μια διαχειριζόμενη υπηρεσία ασφάλειας πληροί τις απαιτήσεις ασφαλείας συγκεκριμένου ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας, το οποίο δείχνει το επίπεδο στο οποίο έχει αξιολογηθεί ένα προϊόν ΤΠΕ, μια υπηρεσία ΤΠΕ, μια διαδικασία ΤΠΕ ή μια διαχειριζόμενη υπηρεσία ασφάλειας αλλά δεν μετρά από μόνο του την ασφάλεια του σχετικού προϊόντος ΤΠΕ, υπηρεσίας ΤΠΕ, διαδικασίας ΤΠΕ ή διαχειριζόμενης υπηρεσίας ασφάλειας,

22) "αυτοαξιολόγηση της συμμόρφωσης": ενέργεια που πραγματοποιείται από κατασκευαστή ή πάροχο προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας, η οποία αξιολογεί αν τα εν λόγω προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ ή διαχειριζόμενες υπηρεσίες ασφάλειας πληρούν τις απαιτήσεις συγκεκριμένου ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας.».

3) Στο άρθρο 4, η παράγραφος 6 αντικαθίσταται από το ακόλουθο κείμενο:

«6. Ο ENISA προάγει τη χρήση της ευρωπαϊκής πιστοποίησης της κυβερνοασφάλειας προκειμένου να αποφευχθεί ο κατακερματισμός της εσωτερικής αγοράς. Ο ENISA συμβάλλει στη θέσπιση και τη διατήρηση ενός ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας σύμφωνα με τον τίτλο ΙΙΙ του παρόντος κανονισμού, προκειμένου να αυξηθεί η διαφάνεια της κυβερνοασφάλειας των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας και, επομένως, να ενισχυθεί η εμπιστοσύνη στην ψηφιακή εσωτερική αγορά και η ανταγωνιστικότητά της.».

4) Το άρθρο 8 τροποποιείται ως εξής:

α) η παράγραφος 1 τροποποιείται ως εξής:

i) το εισαγωγικό μέρος αντικαθίσταται από το ακόλουθο κείμενο:

«1. Ο ENISA υποστηρίζει και προάγει τη χάραξη και την εφαρμογή της πολιτικής της Ένωσης για την πιστοποίηση της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας, όπως καθορίζονται στον τίτλο ΙΙΙ του παρόντος κανονισμού:»·

ii) το στοιχείο β) αντικαθίσταται από το ακόλουθο κείμενο:

«β) επεξεργαζόμενος υποψήφια ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας ("υποψήφια σχήματα") για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας σύμφωνα με το άρθρο 49·»·

β) η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. Ο ENISA συντάσσει και δημοσιεύει κατευθυντήριες γραμμές και αναπτύσσει ορθές πρακτικές, όσον αφορά τις απαιτήσεις κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας, σε συνεργασία με τις εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας και με τον κλάδο, με τρόπο επίσημο και δομημένο και με διαφάνεια.»·

γ) η παράγραφος 5 αντικαθίσταται από το ακόλουθο κείμενο:

«5. Ο ENISA διευκολύνει την καθιέρωση και χρήση ευρωπαϊκών και διεθνών προτύπων για τη διαχείριση κινδύνου και την ασφάλεια των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας.».

5) Το άρθρο 46 αντικαθίσταται από το ακόλουθο κείμενο:

«Άρθρο 46

Ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας

1. Το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας θεσπίζεται με στόχο να βελτιωθούν οι συνθήκες για τη λειτουργία της εσωτερικής αγοράς μέσω αναβάθμισης του επιπέδου κυβερνοασφάλειας εντός της Ένωσης και επιτρέποντας εναρμονισμένη προσέγγιση, σε επίπεδο Ένωσης, των ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας, με απώτερο στόχο τη δημιουργία ψηφιακής ενιαίας αγοράς για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας.

2. Το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας προβλέπει μηχανισμό μέσω του οποίου θεσπίζονται ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας και βεβαιώνεται ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ που έχουν αξιολογηθεί σύμφωνα με τα εν λόγω σχήματα συμμορφώνονται με συγκεκριμένες απαιτήσεις ασφάλειας με σκοπό να διαφυλάσσεται η διαθεσιμότητα, η γνησιότητα, η ακεραιότητα και η εμπιστευτικότητα αποθηκευμένων ή διαβιβαζόμενων ή επεξεργασμένων δεδομένων ή των σχετικών λειτουργιών ή υπηρεσιών που παρέχονται ή είναι προσβάσιμες

μέσω των εν λόγω προϊόντων, υπηρεσιών και διαδικασιών σε όλη τη διάρκεια του κύκλου ζωής τους. Επιπλέον, βεβαιώνει ότι οι διαχειριζόμενες υπηρεσίες ασφάλειας που έχουν αξιολογηθεί σύμφωνα με τα εν λόγω σχήματα συμμορφώνονται με συγκεκριμένες απαιτήσεις ασφάλειας με σκοπό την προστασία της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων τα οποία είναι προσβάσιμα, υποβάλλονται σε επεξεργασία, αποθηκεύονται ή διαβιβάζονται σε σχέση με την παροχή των εν λόγω υπηρεσιών, και ότι οι εν λόγω υπηρεσίες παρέχονται συνεχώς με την απαιτούμενη επάρκεια, εμπειρογνωσία και πείρα από προσωπικό με επαρκές και κατάλληλο επίπεδο σχετικών τεχνικών γνώσεων και επαγγελματικής ακεραιότητας.».

6) Το άρθρο 47 τροποποιείται ως εξής:

α) η παράγραφος 2 αντικαθίσταται από το ακόλουθο κείμενο:

«2. Το κυλιόμενο πρόγραμμα εργασίας της Ένωσης περιλαμβάνει ειδικότερα κατάλογο των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας, ή των κατηγοριών τους, που μπορούν να έχουν όφελος από τη συμπερίληψή τους στο πεδίο εφαρμογής ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας.»·

β) η παράγραφος 3 τροποποιείται ως εξής:

i) το εισαγωγικό μέρος αντικαθίσταται από το ακόλουθο κείμενο:

«3. Η προσθήκη στο κυλιόμενο πρόγραμμα εργασίας της Ένωσης συγκεκριμένων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ, ή διαχειριζόμενων υπηρεσιών ασφάλειας, ή κατηγοριών τους, αιτιολογείται βάσει ενός ή περισσότερων από τους ακόλουθους λόγους:»·

ii) το στοιχείο α) αντικαθίσταται από το ακόλουθο κείμενο:

«α) της διαθεσιμότητας και της ανάπτυξης των εθνικών σχημάτων πιστοποίησης της κυβερνοασφάλειας που καλύπτουν συγκεκριμένη κατηγορία προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας και ιδίως όσον αφορά τον κίνδυνο κατακερματισμού,»·

iii) παρεμβάλλεται το ακόλουθο στοιχείο:

«γα) των τεχνολογικών εξελίξεων και της διαθεσιμότητας και ανάπτυξης διεθνών σχημάτων πιστοποίησης της κυβερνοασφάλειας και διεθνών προτύπων και προτύπων που χρησιμοποιούνται στον κλάδο·».

7) Το άρθρο 49 τροποποιείται ως εξής:

α) οι παράγραφοι 1 έως 4 αντικαθίστανται από το ακόλουθο κείμενο:

«1. Κατόπιν αιτήματος της Επιτροπής σύμφωνα με το άρθρο 48, ο ENISA επεξεργάζεται ένα υποψήφιο σχήμα που πληροί τις εφαρμοστέες απαιτήσεις που ορίζονται στα άρθρα 51, 51α, 52 και 54.

2. Κατόπιν αιτήματος της ΕΟΠΙΚ σύμφωνα με το άρθρο 48 παράγραφος 2, ο ENISA μπορεί να επεξεργάζεται ένα υποψήφιο σχήμα που πληροί τις εφαρμοστέες απαιτήσεις που ορίζονται στα άρθρα 51, 51α, 52 και 54. Σε περίπτωση που ο ENISA αρνηθεί το εν λόγω αίτημα, εκθέτει τους λόγους της άρνησής του. Κάθε απόφαση άρνησης τέτοιου αιτήματος λαμβάνεται από το διοικητικό συμβούλιο.

3. Κατά την επεξεργασία υποψήφιου σχήματος, ο ENISA διαβουλεύεται εγκαίρως με όλους τους σχετικούς συμφεροντούχους μέσω επίσημης, ανοικτής, διαφανούς και χωρίς αποκλεισμούς διαδικασίας διαβούλευσης. Κατά τη διαβίβαση του υποψήφιου σχήματος στην Επιτροπή, δυνάμει της παραγράφου 6, ο ENISA παρέχει πληροφορίες σχετικά με τον τρόπο με τον οποίο συμμορφώθηκε με την παρούσα παράγραφο.

4. Για κάθε υποψήφιο σχήμα, ο ENISA συγκροτεί ad hoc ομάδα εργασίας σύμφωνα με το άρθρο 20 παράγραφος 4 με σκοπό να παρέχει στον ENISA ειδικές συμβουλές και εμπειρογνωμοσύνη. Οι εν λόγω ad hoc ομάδες εργασίας, κατά περίπτωση και με την επιφύλαξη των διαδικασιών και της διακριτικής ευχέρειας που καθορίζονται στο άρθρο 20 παράγραφος 4, περιλαμβάνουν εμπειρογνώμονες από τις δημόσιες διοικήσεις των κρατών μελών, τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης και τον ιδιωτικό τομέα.»·

β) η παράγραφος 7 αντικαθίσταται από το ακόλουθο κείμενο:

«7. Η Επιτροπή μπορεί, με βάση το υποψήφιο σχήμα που προετοιμάζει ο ENISA, να εκδίδει εκτελεστικές πράξεις οι οποίες προβλέπουν σε σχέση με ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας που πληρούν τις σχετικές απαιτήσεις των άρθρων 51, 51α, 52 και 54. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 66 παράγραφος 2.».

8) Παρεμβάλλεται το ακόλουθο άρθρο:

«Άρθρο 49α

Ενημέρωση και διαβούλευση σχετικά με τα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας

1. Η Επιτροπή δημοσιοποιεί τις πληροφορίες σχετικά με το αίτημά της προς τον ENISA να καταρτίσει υποψήφιο σχήμα ή να επανεξετάσει υφιστάμενο ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας όπως αναφέρεται στο άρθρο 48.

2. Κατά την κατάρτιση υποψήφιου σχήματος από τον ENISA δυνάμει του άρθρου 49, το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, ή αμφότερα, μπορούν να ζητήσουν από την Επιτροπή, υπό την ιδιότητά της ως προέδρου της ΕΟΠΙΚ και του ENISA, να υποβάλουν σχετικές πληροφορίες για σχέδιο υποψήφιου σχήματος σε τριμηνιαία βάση. Κατόπιν αιτήματος του Ευρωπαϊκού Κοινοβουλίου ή του Συμβουλίου, ο ENISA, σε συμφωνία με την Επιτροπή και με την επιφύλαξη του άρθρου 27, μπορεί να θέτει στη διάθεση του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου τα σχετικά μέρη σχεδίου υποψήφιου σχήματος κατά τρόπο κατάλληλο για το απαιτούμενο επίπεδο εμπιστευτικότητας και, κατά περίπτωση, με περιορισμούς.

3. Προκειμένου να ενισχύσουν τον διάλογο μεταξύ των θεσμικών οργάνων της Ένωσης και να συμβάλουν σε μια επίσημη, ανοικτή, διαφανή και χωρίς αποκλεισμούς διαδικασία διαβούλευσης, το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, ή αμφότερα, μπορούν να καλέσουν την Επιτροπή και τον ENISA να συζητήσουν θέματα που αφορούν τη λειτουργία των ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ ή διαχειριζόμενες υπηρεσίες ασφάλειας.

4. Η Επιτροπή λαμβάνει υπόψη, κατά περίπτωση, στοιχεία που προκύπτουν από τις απόψεις που εκφράζονται από το Ευρωπαϊκό Κοινοβούλιο και από το Συμβούλιο σχετικά με τα θέματα που αναφέρονται στην παράγραφο 3 του παρόντος άρθρου κατά την αξιολόγηση του παρόντος κανονισμού δυνάμει του άρθρου 67.».

9) Το άρθρο 51 τροποποιείται ως εξής:

α) ο τίτλος αντικαθίσταται από το ακόλουθο κείμενο:

«Στόχοι ασφάλειας των ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ»·

β) η εισαγωγική περίοδος αντικαθίσταται από το ακόλουθο κείμενο:

«Ένα ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ ή διαδικασίες ΤΠΕ σχεδιάζεται με τέτοιο τρόπο ώστε να επιτυγχάνει, κατά περίπτωση, τουλάχιστον τους ακόλουθους στόχους ασφάλειας:».

10) Προστίθεται το ακόλουθο άρθρο:

«Άρθρο 51α

Στόχοι ασφάλειας των ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας για τις διαχειριζόμενες υπηρεσίες ασφάλειας

Ένα ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας για διαχειριζόμενες υπηρεσίες ασφάλειας σχεδιάζεται κατά τέτοιο τρόπο ώστε να επιτυγχάνει, κατά περίπτωση, τουλάχιστον τους ακόλουθους στόχους ασφάλειας:

α) ότι οι διαχειριζόμενες υπηρεσίες ασφάλειας παρέχονται με την απαιτούμενη επάρκεια, εμπειρογνωσία και πείρα, μεταξύ άλλων ότι το προσωπικό που είναι επιφορτισμένο με την παροχή των υπηρεσιών αυτών διαθέτει επαρκές και κατάλληλο επίπεδο τεχνικών γνώσεων και ικανοτήτων στον συγκεκριμένο τομέα, επαρκή και κατάλληλη πείρα, καθώς και το υψηλότερο επίπεδο επαγγελματικής ακεραιότητας,

β) ότι ο πάροχος εφαρμόζει κατάλληλες εσωτερικές διαδικασίες που εξασφαλίζουν ότι το επίπεδο ποιότητας των παρεχόμενων διαχειριζόμενων υπηρεσιών ασφάλειας είναι πάντοτε επαρκές και κατάλληλο,

γ) ότι τα δεδομένα τα οποία είναι προσβάσιμα, αποθηκεύονται, διαβιβάζονται ή αποτελούν με άλλο τρόπο αντικείμενο επεξεργασίας σε σχέση με την παροχή διαχειριζόμενων υπηρεσιών ασφαλείας προστατεύονται από τυχαία ή μη εγκεκριμένη πρόσβαση, αποθήκευση, κοινοποίηση, καταστροφή, άλλη επεξεργασία, ή απώλεια ή αλλοίωση ή έλλειψη διαθεσιμότητας,

δ) την έγκαιρη αποκατάσταση της διαθεσιμότητας και της πρόσβασης σε δεδομένα, υπηρεσίες και λειτουργίες σε περίπτωση φυσικών ή τεχνικών συμβάντων,

ε) ότι εγκεκριμένα άτομα, προγράμματα ή μηχανήματα μπορούν να έχουν πρόσβαση μόνο σε δεδομένα, υπηρεσίες ή λειτουργίες που καλύπτονται από το δικαίωμα πρόσβασης που τους παρέχεται,

στ) ότι τηρείται αρχείο και είναι διαθέσιμο για την αξιολόγηση των δεδομένων, των υπηρεσιών ή των λειτουργιών στα οποία υπήρξε πρόσβαση, τα οποία χρησιμοποιήθηκαν ή αποτέλεσαν με άλλον τρόπο αντικείμενο επεξεργασίας καθώς και τις χρονικές στιγμές κατά τις οποίες έλαβαν χώρα τα παραπάνω και από ποιον,

ζ) ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ που αναπτύσσονται κατά την παροχή των διαχειριζόμενων υπηρεσιών ασφάλειας είναι εκ σχεδιασμού και εξ ορισμού ασφαλή και, κατά περίπτωση, περιλαμβάνουν τις τελευταίες επικαιροποιήσεις ασφάλειας και δεν περιέχουν δημοσίως γνωστά τρωτά σημεία.».

11) Το άρθρο 52 τροποποιείται ως εξής:

α) η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Ένα ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας μπορεί να προσδιορίζει ένα ή περισσότερα από τα ακόλουθα επίπεδα διασφάλισης για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας: “βασικό”, “σημαντικό” ή “υψηλό”. Το επίπεδο διασφάλισης είναι ανάλογο του επιπέδου του κινδύνου ο οποίος συνδέεται με την προβλεπόμενη χρήση του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ, της διαδικασίας ΤΠΕ ή της διαχειριζόμενης υπηρεσίας ασφάλειας από άποψη πιθανότητας και αντικτύπου ενός συμβάντος.»·

β) η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. Οι απαιτήσεις ασφάλειας που αντιστοιχούν σε κάθε επίπεδο διασφάλισης παρέχονται στο σχετικό ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας, συμπεριλαμβανομένων των αντίστοιχων λειτουργιών ασφάλειας και της αντίστοιχης αυστηρότητας και βάθους της αξιολόγησης στην οποία θα υποβληθεί το προϊόν ΤΠΕ, η υπηρεσία ΤΠΕ, η διαδικασία ΤΠΕ ή η διαχειριζόμενη υπηρεσία ασφάλειας.»·

γ) οι παράγραφοι 5, 6 και 7 αντικαθίστανται από το ακόλουθο κείμενο:

«5. Ένα ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας ή μία δήλωση συμμόρφωσης ΕΕ που αναφέρεται σε “βασικό” επίπεδο διασφάλισης παρέχει τη διασφάλιση ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ, οι διαδικασίες ΤΠΕ ή οι διαχειριζόμενες υπηρεσίες ασφάλειας για τα οποία εκδόθηκε το εν λόγω πιστοποιητικό ή η εν λόγω δήλωση συμμόρφωσης ΕΕ πληρούν τις αντίστοιχες απαιτήσεις ασφάλειας, συμπεριλαμβανομένων των λειτουργιών ασφάλειας, και ότι έχουν αξιολογηθεί σε επίπεδο με σκοπό την ελαχιστοποίηση των γνωστών βασικών κινδύνων των συμβάντων και των κυβερνοεπιθέσεων. Οι δραστηριότητες αξιολόγησης που πρόκειται να διεξαχθούν περιλαμβάνουν τουλάχιστον επανεξέταση της τεχνικής τεκμηρίωσης. Εφόσον δεν είναι κατάλληλη τέτοια επανεξέταση, διεξάγονται υποκατάστατες δραστηριότητες αξιολόγησης με ισοδύναμο αποτέλεσμα.

6. Ένα ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας που αναφέρεται σε “σημαντικό” επίπεδο διασφάλισης παρέχει τη διασφάλιση ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ, οι διαδικασίες ΤΠΕ ή οι διαχειριζόμενες υπηρεσίες ασφάλειας για τα οποία εκδόθηκε το εν λόγω πιστοποιητικό πληρούν τις αντίστοιχες απαιτήσεις ασφάλειας, συμπεριλαμβανομένων των λειτουργιών ασφάλειας, και ότι έχουν αξιολογηθεί σε επίπεδο με σκοπό την ελαχιστοποίηση των γνωστών κινδύνων κυβερνοασφάλειας και του κινδύνου συμβάντων και κυβερνοεπιθέσεων που πραγματοποιούνται από δράστες με περιορισμένες δεξιότητες και πόρους. Οι δραστηριότητες αξιολόγησης που πρόκειται να διεξαχθούν περιλαμβάνουν τουλάχιστον τα ακόλουθα: επανεξέταση για να καταδειχθεί η απουσία δημοσίως γνωστών τρωτών σημείων και δοκιμές για να αποδειχθεί ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ, οι διαδικασίες ΤΠΕ ή οι διαχειριζόμενες υπηρεσίες ασφάλειας εφαρμόζουν ορθά τις απαραίτητες λειτουργίες ασφάλειας. Εφόσον οποιεσδήποτε τέτοιες δραστηριότητες αξιολόγησης δεν είναι κατάλληλες, διεξάγονται υποκατάστατες δραστηριότητες αξιολόγησης με ισοδύναμο αποτέλεσμα.

7. Ένα ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας που αναφέρεται σε “υψηλό” επίπεδο διασφάλισης παρέχει τη διασφάλιση ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ, οι διαδικασίες ΤΠΕ ή οι διαχειριζόμενες υπηρεσίες ασφάλειας για τα οποία εκδόθηκε το εν λόγω πιστοποιητικό πληρούν τις αντίστοιχες απαιτήσεις ασφάλειας, συμπεριλαμβανομένων των λειτουργιών ασφάλειας, και ότι έχουν αξιολογηθεί σε επίπεδο με σκοπό την ελαχιστοποίηση του κινδύνου κυβερνοεπιθέσεων προηγμένης τεχνολογίας που πραγματοποιούνται από δράστες με σημαντικές δεξιότητες και πόρους. Οι δραστηριότητες αξιολόγησης που πρόκειται να διεξαχθούν περιλαμβάνουν τουλάχιστον τα ακόλουθα: επανεξέταση για να καταδειχθεί η απουσία δημοσίως γνωστών τρωτών σημείων, δοκιμές για να αποδειχθεί ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ, οι διαδικασίες ΤΠΕ ή οι διαχειριζόμενες υπηρεσίες ασφάλειας εφαρμόζουν ορθά τις απαραίτητες λειτουργίες ασφάλειας με την πλέον προηγμένη τεχνολογία, και αξιολόγηση της αντοχής τους σε ειδικευμένους επιτιθέμενους, με τη χρήση δοκιμών διείσδυσης. Εφόσον οποιεσδήποτε τέτοιες δραστηριότητες αξιολόγησης δεν είναι κατάλληλες, διεξάγονται υποκατάστατες δραστηριότητες αξιολόγησης με ισοδύναμο αποτέλεσμα.».

12) Στο άρθρο 53, οι παράγραφοι 1, 2 και 3 αντικαθίστανται από το ακόλουθο κείμενο:

«1. Ένα ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας μπορεί να επιτρέπει την αυτοαξιολόγηση της συμμόρφωσης υπό την αποκλειστική ευθύνη του κατασκευαστή ή του παρόχου προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας. Η αυτοαξιολόγηση της συμμόρφωσης επιτρέπεται μόνο σχετικά με προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ ή διαχειριζόμενες υπηρεσίες ασφάλειας χαμηλού κινδύνου που αντιστοιχούν σε "βασικό" επίπεδο διασφάλισης.

2. Ο κατασκευαστής ή ο πάροχος προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας μπορεί να εκδώσει δήλωση συμμόρφωσης ΕΕ στην οποία να αναφέρεται ότι έχει καταδειχθεί η εκπλήρωση των απαιτήσεων που ορίζονται στο σχήμα. Με την έκδοση της εν λόγω δήλωσης, ο κατασκευαστής ή ο πάροχος προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας αναλαμβάνει την ευθύνη για τη συμμόρφωση του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ, της διαδικασίας ΤΠΕ ή της διαχειριζόμενης υπηρεσίας ασφάλειας με τις απαιτήσεις που ορίζονται στο εν λόγω σχήμα.

3. Ο κατασκευαστής ή ο πάροχος προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας καθιστά τη δήλωση συμμόρφωσης ΕΕ, την τεχνική τεκμηρίωση και όλες τις άλλες σχετικές πληροφορίες που αφορούν τη συμμόρφωση των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ ή των διαχειριζόμενων υπηρεσιών ασφάλειας με το σχήμα διαθέσιμα στην εθνική αρχή πιστοποίησης της κυβερνοασφάλειας που ορίζεται δυνάμει του άρθρου 58 για περίοδο που καθορίζεται στο αντίστοιχο ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας. Αντίγραφο της δήλωσης συμμόρφωσης ΕΕ υποβάλλεται στην εθνική αρχή πιστοποίησης της κυβερνοασφάλειας και στον ENISA.».

13) Στο άρθρο 54, η παράγραφος 1 τροποποιείται ως εξής:

α) το στοιχείο α) αντικαθίσταται από το ακόλουθο κείμενο:

«α) το αντικείμενο και το πεδίο εφαρμογής του ευρωπαϊκού σχήματος πιστοποίησης, συμπεριλαμβανομένων του τύπου ή των κατηγοριών των καλυπτόμενων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ και διαχειριζόμενων υπηρεσιών ασφάλειας,»·

β) το στοιχείο ζ) αντικαθίσταται από το ακόλουθο κείμενο:

«ζ) τα ειδικά κριτήρια και τις μεθόδους αξιολόγησης που πρόκειται να χρησιμοποιούνται, συμπεριλαμβανομένων των τύπων αξιολόγησης, προκειμένου να καταδεικνύεται ότι επιτυγχάνονται οι εφαρμοστέοι στόχοι ασφάλειας που αναφέρονται στα άρθρα 51 και 51α,»·

γ) το στοιχείο ι) αντικαθίσταται από το ακόλουθο κείμενο:

«ι) τους κανόνες παρακολούθησης της συμμόρφωσης των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ ή των διαχειριζόμενων υπηρεσιών ασφάλειας με τις απαιτήσεις των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας ή των δηλώσεων συμμόρφωσης ΕΕ, συμπεριλαμβανομένων των μηχανισμών για την κατάδειξη της συνεχούς συμμόρφωσης με τις συγκεκριμένες απαιτήσεις της κυβερνοασφάλειας,»·

δ) το στοιχείο ιβ) αντικαθίσταται από το ακόλουθο κείμενο:

«ιβ) τους κανόνες σχετικά με τις συνέπειες όσον αφορά προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ ή διαχειριζόμενες υπηρεσίες ασφάλειας που έχουν πιστοποιηθεί ή για τα οποία έχει εκδοθεί δήλωση συμμόρφωσης ΕΕ τα οποία όμως δεν συμμορφώνονται προς τις απαιτήσεις του σχήματος,»·

ε) το στοιχείο ιε) αντικαθίσταται από το ακόλουθο κείμενο:

«ιε) τον προσδιορισμό εθνικών ή διεθνών σχημάτων πιστοποίησης της κυβερνοασφάλειας που καλύπτουν τον ίδιο τύπο ή τις ίδιες κατηγορίες προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας απαιτήσεις ασφάλειας, κριτήρια και μεθόδους αξιολόγησης και επίπεδα διασφάλισης,»·

στ) το στοιχείο ιζ) αντικαθίσταται από το ακόλουθο κείμενο:

«ιζ) την περίοδο διαθεσιμότητας της δήλωσης συμμόρφωσης ΕΕ, την τεχνική τεκμηρίωση και όλες τις άλλες σχετικές πληροφορίες που πρέπει να καταστούν διαθέσιμες από τον κατασκευαστή ή τον πάροχο προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας,».

14) Το άρθρο 56 τροποποιείται ως εξής:

α) η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ, οι διαδικασίες ΤΠΕ και οι διαχειριζόμενες υπηρεσίες ασφάλειας που έχουν πιστοποιηθεί στο πλαίσιο ενός ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας που εγκρίνεται δυνάμει του άρθρου 49 τεκμαίρονται ότι πληρούν τις απαιτήσεις ενός τέτοιου σχήματος.»·

β) η παράγραφος 3 τροποποιείται ως εξής:

i) το πρώτο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«Η Επιτροπή αξιολογεί τακτικά την απόδοση και τη χρήση των εγκριθέντων ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας, καθώς και αν συγκεκριμένα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας πρόκειται να καταστούν υποχρεωτικά μέσω συναφούς ενωσιακού δικαίου προκειμένου να διασφαλίζεται επαρκές επίπεδο κυβερνοασφάλειας των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ και, από τις 4 Φεβρουαρίου 2025, των διαχειριζόμενων υπηρεσιών ασφάλειας στην Ένωση και να βελτιωθεί η λειτουργία της εσωτερικής αγοράς. Η πρώτη τέτοια αξιολόγηση διενεργείται έως τις 31 Δεκεμβρίου 2023 και οι ακόλουθες αξιολογήσεις διενεργούνται τουλάχιστον ανά διετία εν συνεχεία. Η Επιτροπή, βασιζόμενη στα αποτελέσματα της εν λόγω αξιολόγησης, προσδιορίζει τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ, τις διαδικασίες ΤΠΕ και τις διαχειριζόμενες υπηρεσίες ασφάλειας που καλύπτονται από ήδη υφιστάμενο σχήμα πιστοποίησης και τα οποία πρέπει να καλυφθούν από υποχρεωτικό σχήμα πιστοποίησης.»·

ii) το τρίτο εδάφιο τροποποιείται ως εξής:

— το στοιχείο α) αντικαθίσταται από το ακόλουθο κείμενο:

«α) λαμβάνει υπόψη τον αντίκτυπο των μέτρων στους κατασκευαστές ή τους παρόχους των εν λόγω προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας και στους χρήστες από άποψη κόστους των εν λόγω μέτρων και τα κοινωνικά ή οικονομικά οφέλη που προκύπτουν από το αναμενόμενο βελτιωμένο επίπεδο ασφάλειας για τα στοχευόμενα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ, τις διαδικασίες ΤΠΕ ή τις διαχειριζόμενες υπηρεσίες ασφάλειας,»,

— το στοιχείο δ) αντικαθίσταται από το ακόλουθο κείμενο:

«δ) λαμβάνει υπόψη τις προθεσμίες εφαρμογής, τα μεταβατικά μέτρα και χρονικά διαστήματα, ιδίως όσον αφορά τις πιθανές συνέπειες του μέτρου για τους κατασκευαστές ή παρόχους προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας, συμπεριλαμβανομένων των συγκεκριμένων συμφερόντων και αναγκών των ΜΜΕ, μεταξύ άλλων και των πολύ μικρών επιχειρήσεων,»·

γ) οι παράγραφοι 7 και 8 αντικαθίστανται από το ακόλουθο κείμενο:

«7. Το φυσικό ή νομικό πρόσωπο που υποβάλλει τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ, τις διαδικασίες ΤΠΕ ή τις διαχειριζόμενες υπηρεσίες ασφάλειας προς πιστοποίηση θέτει στη διάθεση της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας που ορίζεται δυνάμει του άρθρου 58, σε περίπτωση που η εν λόγω αρχή είναι ο οργανισμός που εκδίδει το ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας, ή του οργανισμού αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 60 όλες τις πληροφορίες που απαιτούνται για τη διενέργεια της πιστοποίησης.

8. Ο κάτοχος ευρωπαϊκού πιστοποιητικού κυβερνοασφάλειας ενημερώνει την αρχή ή τον οργανισμό που αναφέρεται στην παράγραφο 7 για τυχόν τρωτά σημεία ή παρατυπίες που εντοπίστηκαν σε μεταγενέστερο στάδιο σχετικά με την ασφάλεια του πιστοποιημένου προϊόντος ΤΠΕ, υπηρεσίας ΤΠΕ, διαδικασίας ΤΠΕ ή διαχειριζόμενης υπηρεσίας ασφάλειας που μπορεί να έχουν αντίκτυπο στη συμμόρφωσή του με τις απαιτήσεις σχετικά με την πιστοποίηση. Η εν λόγω αρχή ή οργανισμός διαβιβάζει τις εν λόγω πληροφορίες χωρίς αδικαιολόγητη καθυστέρηση στην ενδιαφερόμενη εθνική αρχή πιστοποίησης της κυβερνοασφάλειας.».

15) Στο άρθρο 57, οι παράγραφοι 1 και 2 αντικαθίστανται από το ακόλουθο κείμενο:

«1. Με την επιφύλαξη της παραγράφου 3 του παρόντος άρθρου, τα εθνικά σχήματα πιστοποίησης της κυβερνοασφάλειας και οι σχετικές διαδικασίες για τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ, τις διαδικασίες ΤΠΕ και τις διαχειριζόμενες υπηρεσίες ασφάλειας που καλύπτονται από ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας παύουν να παράγουν αποτελέσματα από την ημερομηνία που ορίζεται στην εκτελεστική πράξη που εκδίδεται σύμφωνα με το άρθρο 49 παράγραφος 7. Τα εθνικά σχήματα πιστοποίησης της κυβερνοασφάλειας και οι σχετικές διαδικασίες για τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ, τις διαδικασίες ΤΠΕ και τις διαχειριζόμενες υπηρεσίες ασφάλειας που δεν καλύπτονται από ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας εξακολουθούν να παράγουν αποτελέσματα.

2. Τα κράτη μέλη δεν θεσπίζουν νέα εθνικά σχήματα πιστοποίησης της κυβερνοασφάλειας για τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ, τις διαδικασίες ΤΠΕ και τις διαχειριζόμενες υπηρεσίες ασφάλειας που καλύπτονται ήδη από ισχύον ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας.».

16) Το άρθρο 58 τροποποιείται ως εξής:

α) η παράγραφος 7 τροποποιείται ως εξής:

i) τα στοιχεία α) και β) αντικαθίστανται από το ακόλουθο κείμενο:

«α) εποπτεύουν και μεριμνούν για την εφαρμογή των κανόνων που περιλαμβάνονται στα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας σύμφωνα με το άρθρο 54 παράγραφος 1 στοιχείο ι) για την παρακολούθηση της συμμόρφωσης των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας προς τις απαιτήσεις των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας που έχουν εκδοθεί στα αντίστοιχα εδάφη τους, σε συνεργασία με άλλες αρμόδιες αρχές εποπτείας της αγοράς,

β) παρακολουθούν τη συμμόρφωση με τις υποχρεώσεις των κατασκευαστών ή των παρόχων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας που είναι εγκατεστημένοι στα αντίστοιχα εδάφη τους και που διενεργούν αυτοαξιολόγηση συμμόρφωσης και επιβάλλουν την εφαρμογή των εν λόγω υποχρεώσεων και παρακολουθούν ιδίως τη συμμόρφωση με τις υποχρεώσεις των εν λόγω κατασκευαστών ή παρόχων που προβλέπονται στο άρθρο 53 παράγραφοι 2 και 3 και στο αντίστοιχο ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας και επιβάλλουν την εφαρμογή των εν λόγω υποχρεώσεων,»·

ii) το στοιχείο η) αντικαθίσταται από το ακόλουθο κείμενο:

«η) συνεργάζονται με άλλες εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας ή άλλες δημόσιες αρχές, μεταξύ άλλων ανταλλάσσοντας πληροφορίες σχετικά με την πιθανή μη συμμόρφωση προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας με τις απαιτήσεις του παρόντος κανονισμού ή με τις απαιτήσεις συγκεκριμένων ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας, και»·

β) η παράγραφος 9 αντικαθίσταται από το ακόλουθο κείμενο:

«9. Οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας συνεργάζονται μεταξύ τους και με την Επιτροπή, ιδίως ανταλλάσσοντας πληροφορίες, εμπειρίες και ορθές πρακτικές όσον αφορά την πιστοποίηση της κυβερνοασφάλειας και τα τεχνικά ζητήματα που αφορούν την κυβερνοασφάλεια των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας.».

17) Στο άρθρο 59 παράγραφος 3, τα στοιχεία β) και γ) αντικαθίστανται από το ακόλουθο κείμενο:

«β) τις διαδικασίες για την εποπτεία και την επιβολή των κανόνων παρακολούθησης της συμμόρφωσης των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας με ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας δυνάμει του άρθρου 58 παράγραφος 7 στοιχείο α),

γ) τις διαδικασίες για την παρακολούθηση και την τήρηση των υποχρεώσεων των κατασκευαστών ή των παρόχων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας δυνάμει του άρθρου 58 παράγραφος 7 στοιχείο β),».

18) Στο άρθρο 67, οι παράγραφοι 2 και 3 αντικαθίστανται από το ακόλουθο κείμενο:

«2. Η αξιολόγηση εξετάζει επίσης τον αντίκτυπο, την αποτελεσματικότητα και την απόδοση των διατάξεων του τίτλου III του παρόντος κανονισμού, συμπεριλαμβανομένων των διαδικασιών που οδηγούν στη θέσπιση ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας και των βάσεων τεκμηρίωσής τους, σε σχέση με τους στόχους αφενός της διασφάλισης επαρκούς επιπέδου κυβερνοασφάλειας των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας στην Ένωση και αφετέρου της βελτίωσης της λειτουργίας της εσωτερικής αγοράς.

3. Η αξιολόγηση εκτιμά κατά πόσον είναι απαραίτητες βασικές απαιτήσεις κυβερνοασφάλειας για την πρόσβαση στην εσωτερική αγορά, ώστε να αποφευχθεί η είσοδος προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ και διαχειριζόμενων υπηρεσιών ασφάλειας που δεν πληρούν τις βασικές απαιτήσεις κυβερνοασφάλειας στην εσωτερική αγορά.».

19) Το παράρτημα τροποποιείται σύμφωνα με το παράρτημα του παρόντος κανονισμού.

Άρθρο 2

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

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

Βρυξέλλες, 19 Δεκεμβρίου 2024.

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Η Πρόεδρος	*Ο Πρόεδρος*
R. METSOLA	BÓKA J.

ΠΑΡΑΡΤΗΜΑ

Το παράρτημα του κανονισμού (ΕΕ) 2019/881 τροποποιείται ως εξής:

1) Τα σημεία 2 έως 5 αντικαθίστανται από το ακόλουθο κείμενο:

«2. Ο οργανισμός αξιολόγησης της συμμόρφωσης είναι τρίτος φορέας, ανεξάρτητος από τον οργανισμό ή τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ, τις διαδικασίες ΤΠΕ ή τις υπηρεσίες διαχειριζόμενης ασφάλειας που αξιολογεί.

3. Ένας οργανισμός που ανήκει σε ένωση επιχειρήσεων ή επαγγελματική ομοσπονδία που εκπροσωπεί επιχειρήσεις οι οποίες συμμετέχουν στον σχεδιασμό, την κατασκευή, την παροχή, τη συναρμολόγηση, τη χρήση ή τη συντήρηση προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσίες ασφάλειας που αξιολογεί, μπορεί να θεωρείται οργανισμός αξιολόγησης της συμμόρφωσης, υπό την προϋπόθεση ότι η ανεξαρτησία του και η απουσία σύγκρουσης συμφερόντων είναι αποδεδειγμένες.

4. Οι οργανισμοί αξιολόγησης της συμμόρφωσης, τα διευθυντικά τους στελέχη και τα πρόσωπα που είναι αρμόδια για την εκτέλεση των καθηκόντων αξιολόγησης της συμμόρφωσης δεν είναι ο σχεδιαστής, ο κατασκευαστής, ο προμηθευτής, ο εγκαταστάτης, ο αγοραστής, ο ιδιοκτήτης, ο χρήστης ή ο συντηρητής του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ, της διαδικασίας ΤΠΕ ή της διαχειριζόμενης υπηρεσίας ασφάλειας που αξιολογείται, ούτε ο εξουσιοδοτημένος αντιπρόσωπος των ανωτέρω. Η εν λόγω απαγόρευση δεν αποκλείει τη χρήση των αξιολογημένων προϊόντων ΤΠΕ που είναι αναγκαία για τις λειτουργίες του οργανισμού αξιολόγησης της συμμόρφωσης ή τη χρήση των εν λόγω προϊόντων ΤΠΕ για προσωπικούς σκοπούς.

5. Οι οργανισμοί αξιολόγησης της συμμόρφωσης, τα διευθυντικά του στελέχη και τα πρόσωπα που είναι αρμόδια για την εκτέλεση των καθηκόντων αξιολόγησης της συμμόρφωσης δεν εμπλέκονται άμεσα στο σχεδιασμό, την παραγωγή ή την κατασκευή, την παροχή, την εμπορία, την εγκατάσταση, τη χρήση ή τη συντήρηση των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ ή των διαχειριζόμενων υπηρεσιών ασφάλειας που αξιολογούνται, ούτε εκπροσωπούν μέρη που εμπλέκονται στις εν λόγω δραστηριότητες. Οι οργανισμοί αξιολόγησης της συμμόρφωσης, τα διευθυντικά του στελέχη και τα πρόσωπα που είναι αρμόδια για την εκτέλεση των καθηκόντων αξιολόγησης της συμμόρφωσης δεν αναλαμβάνουν καμιά δραστηριότητα που μπορεί να έλθει σε σύγκρουση με την ανεξάρτητη κρίση ή την ακεραιότητά τους σε σχέση με τις οικείες δραστηριότητες αξιολόγησης της συμμόρφωσης. Η εν λόγω απαγόρευση ισχύει ιδίως για συμβουλευτικές υπηρεσίες.».

2) Το σημείο 10 τροποποιείται ως εξής:

α) το εισαγωγικό μέρος αντικαθίστανται από το ακόλουθο κείμενο:

«10. Ανά πάσα στιγμή και για κάθε διαδικασία αξιολόγησης της συμμόρφωσης και κάθε τύπο, κατηγορία ή υποκατηγορία προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας, ο οργανισμός αξιολόγησης της συμμόρφωσης έχει στη διάθεσή του τα εξής απαραίτητα:»·

β) το στοιχείο γ) αντικαθίστανται από το ακόλουθο κείμενο:

«γ) διαδικασίες για την άσκηση δραστηριοτήτων που λαμβάνουν υπόψη το μέγεθος μιας επιχείρησης, τον κλάδο στον οποίο δραστηριοποιείται, τη δομή της, τον βαθμό πολυπλοκότητας της τεχνολογίας του εν λόγω προϊόντος ΤΠΕ, υπηρεσίας ΤΠΕ, διαδικασίας ΤΠΕ ή διαχειριζόμενης υπηρεσίας ασφάλειας και τον μαζικό ή εν σειρά χαρακτήρα της παραγωγικής διαδικασίας.».

3) Τα σημεία 19 και 20 αντικαθίστανται από το ακόλουθο κείμενο:

«19. Οι οργανισμοί αξιολόγησης της συμμόρφωσης πληρούν τις απαιτήσεις του σχετικού εναρμονισμένου προτύπου όπως ορίζεται στο άρθρο 2 σημείο 9) του κανονισμού (ΕΚ) αριθ. 765/2008 για τη διαπίστευση των οργανισμών αξιολόγησης της συμμόρφωσης που διενεργούν την πιστοποίηση προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας.

20. Οι οργανισμοί αξιολόγησης της συμμόρφωσης εξασφαλίζουν ότι τα εργαστήρια δοκιμών που χρησιμοποιούνται για σκοπούς αξιολόγησης της συμμόρφωσης πληρούν τις απαιτήσεις του σχετικού εναρμονισμένου προτύπου όπως ορίζεται στο άρθρο 2 σημείο 9) του κανονισμού (ΕΚ) αριθ. 765/2008 για τη διαπίστευση των εργαστηρίων που πραγματοποιούν δοκιμές.».

Έχει γίνει δήλωση σχετικά με τον παρόντα κανονισμό η οποία βρίσκεται στην ΕΕ C, C/2025/307, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/307/oj.