ΕΥΡΩΠΑΪΚΟ
ΕΛΕΓΚΤΙΚΟ
ΣΥΝΕΔΡΙΟ

EL

Γνώμη 02/2023

(υποβαλλόμενη δυνάμει του άρθρου 322, παράγραφος 1, ΣΛΕΕ)

σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας [Διοργανικός φάκελος 2023/0109(COD) της 18ης Απριλίου 2023]

Περιεχόμενα

	Σημείο
Εισαγωγή	01-03
Γενικές παρατηρήσεις	04-05
Ειδικά σχόλια	06-40
Απουσία εκτίμησης επιπτώσεων	06-08
Ελλιπείς πληροφορίες σχετικά με τη χρηματοδότηση	09-12
Ελλιπείς πληροφορίες όσον αφορά τις ανάγκες χρηματοδότησης και σε ανθρώπινους πόρους	09-10
Ελλιπείς πληροφορίες σχετικά με το χρηματοδοτικό σχήμα της ευρωπαϊκής κυβερνοασπίδας	11-12
Κίνδυνοι που σχετίζονται με την ευρωπαϊκή κυβερνοασπίδα	13-26
Αυξημένη πολυπλοκότητα και πρόσθετα επίπεδα	13-20
Ανταλλαγή πληροφοριών	21-26
Κίνδυνοι που σχετίζονται με τον μηχανισμό έκτακτης ανάγκης στον κυβερνοχώρο	27-34
Ανάπτυξη της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας	27-29
Παρέκκλιση από την αρχή της «ετήσιας διάρκειας» του προϋπολογισμού	30-34
Κίνδυνοι σχετικά με τον μηχανισμό εξέτασης περιστατικών κυβερνοασφάλειας	35-36
Παρακολούθηση των επιδόσεων και αξιολόγηση της πολιτικής	37-40
Τελικές παρατηρήσεις	41-43
Παράρτημα – Ο ευρωπαϊκός γαλαξίας κυβερνοασφάλειας	

Εισαγωγή

01 Στις 18 Απριλίου 2023, η Ευρωπαϊκή Επιτροπή δημοσίευσε πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας (εφεξής «η πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο»).

02 Η προτεινόμενη πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο προβλέπει μέτρα για την ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας, ιδίως μέσω:

- της **ευρωπαϊκής κυβερνοασπίδας**, για την οικοδόμηση και την ενίσχυση συντονισμένων ικανοτήτων ανίχνευσης και αντίληψης της κατάστασης·
- του **μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο**, με σκοπό τη στήριξη των κρατών μελών όσον αφορά την προετοιμασία, την αντίδραση και την ανάκαμψη από σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας·
- του **μηχανισμού εξέτασης περιστατικών κυβερνοασφάλειας**, για την εξέταση και την αξιολόγηση σημαντικών ή μεγάλης κλίμακας περιστατικών.

03 Η νομική βάση της πρότασης της Επιτροπής επιβάλλει τη διαβούλευση με το Ευρωπαϊκό Ελεγκτικό Συνέδριο[1]. Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης μας απηύθυναν γραπτό αίτημα στις 2 Ιουνίου 2023 και στις 7 Ιουνίου 2023, αντίστοιχα, ζητώντας σχετική γνωμοδότησή μας. Η παρούσα γνώμη ανταποκρίνεται στην απαίτηση διαβούλευσης.

[1] Άρθρο 322, παράγραφος 1, της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης.

Γενικές παρατηρήσεις

04 Τα κράτη μέλη φέρουν την πρωταρχική ευθύνη για την πρόληψη, την ετοιμότητα και την αντιμετώπιση περιστατικών και κρίσεων κυβερνοασφάλειας που τα επηρεάζουν. Σύμφωνα με το άρθρο 4, παράγραφος 2, της Συνθήκης για την Ευρωπαϊκή Ένωση, η εθνική ασφάλεια παραμένει στην αποκλειστική σφαίρα ευθύνης κάθε κράτους μέλους. Ωστόσο, ο δυνητικός αντίκτυπος σημαντικών ή μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας ενδέχεται να καταστήσει αναγκαία την ανάληψη κοινής δράσης σε επίπεδο ΕΕ.

05 Το ΕΕΣ επιδοκιμάζει τους στόχους της πρότασης για ενίσχυση της συλλογικής κυβερνοανθεκτικότητας της ΕΕ. Στην παρούσα γνώμη, διατυπώνουμε ειδικά σχόλια σχετικά με τις τρεις συνιστώσες της προτεινόμενης πράξης της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο και επισημαίνουμε ορισμένους κινδύνους που εντοπίσαμε σε σχέση με την απουσία εκτίμησης επιπτώσεων, τις οικονομικές πτυχές και τρόπους με τους οποίους θα μπορούσαν να υλοποιηθούν τα μέτρα που προβλέπονται στην πρόταση. Ειδικότερα, τονίζουμε ότι είναι υπαρκτός ο κίνδυνος η πρόταση κανονισμού να καταστήσει πολυπλοκότερο τον συνολικό γαλαξία κυβερνοασφάλειας της ΕΕ και εισηγούμαστε τρόπους για τον μετριασμό του κινδύνου αυτού (βλέπε σημεία ***13***-***20***).

Ειδικά σχόλια

Απουσία εκτίμησης επιπτώσεων

06 Στις κατευθυντήριες γραμμές για τη βελτίωση της νομοθεσίας, η Επιτροπή προτείνει τη χρήση εκτιμήσεων επιπτώσεων και διαβουλεύσεων με τα ενδιαφερόμενα μέρη στο πλαίσιο μιας ολοκληρωμένης ανάλυσης των επιλογών σχεδιασμού και υλοποίησης πολιτικής. Θεωρούμε ότι οι ολοκληρωμένες εκτιμήσεις επιπτώσεων αποτελούν βασικό εργαλείο, προκειμένου να αξιολογείται κατά πόσον υπάρχει ανάγκη για ανάληψη δράσης από την ΕΕ και να αναλύονται οι δυνητικές επιπτώσεις των διαθέσιμων λύσεων, πριν από την έγκριση οποιασδήποτε πρότασης.

07 Στο πλαίσιο της υπό εξέταση πρότασης κανονισμού, δεν διενεργήθηκε εκτίμηση επιπτώσεων. Στην ενότητα 3 της αιτιολογικής έκθεσης που συνοδεύει την πρόταση, η Επιτροπή αιτιολόγησε την επιλογή της να μην προβεί σε τέτοια εκτίμηση επικαλούμενη τον «*επείγοντα χαρακτήρα της πρότασης*». Ανέφερε επίσης ότι τα μέτρα που θεσπίζονται με την πρόταση κανονισμού θα λάβουν στήριξη από το πρόγραμμα «Ψηφιακή Ευρώπη» (Digital Europe Programme, DEP) και είναι σύμφωνα με τον κανονισμό για το πρόγραμμα αυτό, ο οποίος αποτέλεσε αντικείμενο ειδικής εκτίμησης επιπτώσεων το 2018. Επιπλέον, η Επιτροπή εξήγησε ότι τα προτεινόμενα μέτρα βασίστηκαν σε προηγούμενες δράσεις, εκπονηθείσες σε στενό συντονισμό με τα βασικά ενδιαφερόμενα μέρη και τα κράτη μέλη, και ότι ενσωματώνουν τα σχετικά διδάγματα.

08 Εντούτοις, επισημαίνουμε ότι η εκτίμηση επιπτώσεων σχετικά με το πρόγραμμα «Ψηφιακή Ευρώπη» δεν καλύπτει τα νέα μέτρα που θεσπίζει η πρόταση κανονισμού. Ως εκ τούτου, οι πληροφορίες όσον αφορά τις διαθέσιμες επιλογές πολιτικής και το κόστος που συνεπάγεται η πρόταση είναι περιορισμένες.

Ελλιπείς πληροφορίες σχετικά με τη χρηματοδότηση

Ελλιπείς πληροφορίες όσον αφορά τις ανάγκες χρηματοδότησης και σε ανθρώπινους πόρους

09 Τα μέτρα που προβλέπονται στην πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο θα χρηματοδοτηθούν από το πρόγραμμα «Ψηφιακή Ευρώπη». Η Επιτροπή, στην ενότητα 4 της αιτιολογικής της έκθεσης, ανέφερε ότι 115 εκατομμύρια ευρώ είχαν ήδη διατεθεί για την ευρωπαϊκή κυβερνοασπίδα μέσω της

χρηματοδότησης πιλοτικών έργων την περίοδο 2021-2022. Ανέφερε επίσης ότι η πρόταση θα αυξήσει τον προϋπολογισμό, ύψους 743 εκατομμυρίων ευρώ, που διατίθεται την περίοδο 2023-2027 στον ειδικό στόχο της κυβερνοασφάλειας και εμπιστοσύνης του προγράμματος «Ψηφιακή Ευρώπη» κατά 100 εκατομμύρια ευρώ, μέσω εσωτερικής ανακατανομής χρηματοδότησης.

10 Κατόπιν την ανακατανομής αυτής, η διαθέσιμη ενωσιακή χρηματοδότηση για την κυβερνοασφάλεια, για την περίοδο 2023-2027, θα ανέρχεται σε 843 εκατομμύρια ευρώ. Επισημαίνουμε ότι το ποσό αυτό δεν καλύπτει μόνο δράσεις που καθορίζονται στην πρόταση κανονισμού αλλά και άλλες δράσεις για την κυβερνοασφάλεια που εντάσσονται στο πρόγραμμα «Ψηφιακή Ευρώπη» (όπως η στήριξη του κλάδου ή της τυποποίησης). Στην πρόταση δεν παρέχεται εκτίμηση του συνολικού αναμενόμενου κόστους για τη θέσπιση και την εφαρμογή των προτεινόμενων μέτρων [της ευρωπαϊκής κυβερνοασπίδας, του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο (περιλαμβανομένης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας) και του μηχανισμού εξέτασης περιστατικών κυβερνοασφάλειας]. Δεδομένου ότι η πρόταση δεν συνοδεύεται από εκτίμηση επιπτώσεων, προτείνουμε η Επιτροπή να δημοσιοποιήσει τις εν λόγω εκτιμήσεις κόστους προς ενίσχυση της διαφάνειας.

Ελλιπείς πληροφορίες σχετικά με το χρηματοδοτικό σχήμα της ευρωπαϊκής κυβερνοασπίδας

11 Στο κεφάλαιο II της πρότασης κανονισμού θεσπίζεται η ευρωπαϊκή κυβερνοασπίδα, η οποία αποτελείται από εθνικά κέντρα επιχειρήσεων ασφάλειας (national security operations centres, εφεξής «εθνικά SOC») και διασυνοριακά κέντρα επιχειρήσεων ασφάλειας (cross-border security operations centres, εφεξής «διασυνοριακά SOC»). Βάσει της πρότασης, τα επιλέξιμα εθνικά SOC μπορούν να λάβουν χρηματοδοτική συνεισφορά από την ΕΕ, η οποία να καλύπτει έως και το 50 % του κόστους αγοράς των εργαλείων και των υποδομών και έως το 50 % του κόστους λειτουργίας τους. Όσον αφορά τα διασυνοριακά SOC, η χρηματοδοτική συνεισφορά της ΕΕ καλύπτει έως και το 75 % του κόστους αγοράς των εργαλείων και των υποδομών και έως το 50 % του κόστους λειτουργίας. Η πρόταση κανονισμού δεν διευκρινίζει τους λόγους για τους οποίους τα διασυνοριακά SOC χρειάζονται πρόσθετα εργαλεία και υποδομές, τα οποία συγχρηματοδοτούνται σε υψηλότερο ποσοστό, σε σχέση με τα εργαλεία που έχουν στη διάθεσή τους εθνικά SOC που συμμετέχουν σε κοινοπραξία.

12 Στην πρόταση δεν προσδιορίζεται επίσης για πόσο χρονικό διάστημα το κόστος λειτουργίας των εθνικών και διασυνοριακών SOC θα συγχρηματοδοτείται από την ΕΕ.

Ελλοχεύει, επομένως, ο κίνδυνος η λειτουργία και η βιωσιμότητα της ευρωπαϊκής κυβερνοασπίδας να εξαρτώνται από την ενωσιακή χρηματοδότηση.

Κίνδυνοι που σχετίζονται με την ευρωπαϊκή κυβερνοασπίδα

Αυξημένη πολυπλοκότητα και πρόσθετα επίπεδα

13 Όπως επισημάναμε στην επισκόπηση 02/2019[2], το τοπίο της κυβερνοασφάλειας στην ΕΕ είναι πολύπλοκο και πολυεπίπεδο. Στο μη στρατιωτικό σκέλος συμμετέχει πληθώρα φορέων από τον δημόσιο και τον ιδιωτικό τομέα σε περιφερειακό, εθνικό και ενωσιακό επίπεδο, περιλαμβανομένων φορέων επιβολής του νόμου και μονάδων χρηματοοικονομικών πληροφοριών. Η κυβερνοασφάλεια αποτελεί επίσης βασικό στοιχείο της εθνικής ασφάλειας και άμυνας. Στο ***παράρτημα*** της παρούσας γνώμης παρουσιάζεται χάρτης του νέου γαλαξία κυβερνοασφάλειας στην ΕΕ, όπου παρατίθενται, εντός πλαισίου με σομόν φόντο, όλοι οι μηχανισμοί και οι συνιστώσες που εισήγαγε η πρόταση. Ο χάρτης αποτυπώνει την πρόσθετη πολυπλοκότητα και τα νέα επίπεδα που απορρέουν από τον κανονισμό.

14 Σκοπός της ευρωπαϊκής κυβερνοασπίδας που θεσπίζεται στο κεφάλαιο II της πρότασης κανονισμού είναι η ανάπτυξη προηγμένων ικανοτήτων της ΕΕ όσον αφορά την ανίχνευση, την ανάλυση και την επεξεργασία δεδομένων σχετικά με απειλές και περιστατικά στον κυβερνοχώρο. Πρόκειται για μια διασυνδεδεμένη πανευρωπαϊκή υποδομή εθνικών και διασυνοριακών κέντρων επιχειρήσεων ασφάλειας (SOC).

15 Προκειμένου να συμμετάσχει στην ευρωπαϊκή κυβερνοασπίδα, ένα κράτος μέλος οφείλει να ορίσει τουλάχιστον ένα εθνικό SOC, το οποίο πρέπει να είναι δημόσιος φορέας. Με τη σειρά τους, τα εθνικά SOC οφείλουν να συγκροτήσουν διασυνοριακά SOC, ήτοι κοινοπραξίες αποτελούμενες από SOC τουλάχιστον τριών κρατών μελών που δεσμεύονται να συνεργαστούν και να συντονίζουν τις δραστηριότητές τους για την ανίχνευση περιστατικών κυβερνοασφάλειας και την παρακολούθηση απειλών στον κυβερνοχώρο.

16 Τα τελευταία χρόνια, η ΕΕ έχει ενισχύσει το κανονιστικό της πλαίσιο σχετικά με την κυβερνοασφάλεια. Μέσο καίριας σημασίας του πλαισίου αυτού είναι η οδηγία για την ασφάλεια δικτύων και πληροφοριών (οδηγία NIS) του 2016, καθώς και η οδηγία για την αναθεώρησή της (οδηγία NIS 2) του 2022. Δυνάμει της οδηγίας NIS 2,

[2] Επισκόπηση αριθ. 02/2019, με τίτλο «Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια».

τα κράτη μέλη οφείλουν να συστήσουν σε εθνικό επίπεδο μία ή περισσότερες ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Teams, CSIRT). Σε επίπεδο ΕΕ, η οδηγία NIS 2 θεσπίζει επίσης την ομάδα συνεργασίας NIS, το δίκτυο CSIRT και το ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για κρίσεις στον κυβερνοχώρο (EU-CyCLONe).

17 Το 2021, η ΕΕ δημιούργησε το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας. Εγκαινιασθέν τον Μάιο του 2023, το κέντρο αυτό υποστηρίζεται από δίκτυο 27 εθνικών κέντρων συντονισμού, ένα ανά κράτος μέλος, μερικά από τα οποία είναι και εθνικά SOC. Το κέντρο είναι υπεύθυνο για την υλοποίηση της συνιστώσας της κυβερνοασφάλειας του προγράμματος «Ψηφιακή Ευρώπη», εξαιρουμένης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Η εφεδρεία θα υλοποιηθεί από την Επιτροπή, όμως η αρμοδιότητα για τη λειτουργία και τη διοίκησή της ενδέχεται να ανατεθεί στον ENISA.

18 Η Επιτροπή σύστησε επίσης την Κοινή Κυβερνομονάδα. Η μονάδα αυτή, η δημιουργία της οποίας ανακοινώθηκε το 2020 στο πλαίσιο της στρατηγικής κυβερνοασφάλειας της ΕΕ, προσδιορίστηκε λεπτομερέστερα σε σύσταση που διατύπωσε η Επιτροπή το 2021.

19 Τον Απρίλιο του 2023, η Επιτροπή ανακοίνωσε τη δρομολόγηση της ακαδημίας κυβερνοδεξιοτήτων, μιας νέας πρωτοβουλίας με στόχο την κάλυψη της έλλειψης ταλέντων στον τομέα της κυβερνοασφάλειας και την ενίσχυση του εργατικού δυναμικού της ΕΕ για τον κυβερνοχώρο.

20 Βάσει των ανωτέρω, θεωρούμε ότι ελλοχεύει ο κίνδυνος η πρόταση κανονισμού να καταστήσει πολυπλοκότερο τον συνολικό γαλαξία κυβερνοασφάλειας της ΕΕ. Υπάρχει το ενδεχόμενο αλληλοεπικάλυψης μεταξύ του υφιστάμενου δικτύου CSIRT και των SOC. Μολονότι η Επιτροπή ανέφερε στην ενότητα 1 της αιτιολογικής της έκθεσης ότι οι διασυνοριακές πλατφόρμες SOC θα πρέπει να αποτελέσουν μια νέα ικανότητα που θα συμπληρώνει το δίκτυο CSIRT, διαπιστώνουμε ότι ορισμένα καθήκοντα και στόχοι εθνικών SOC, διασυνοριακών SOC, CSIRT και του σχετικού δικτύου παρουσιάζουν ομοιότητες. Σε αυτά συγκαταλέγονται η ανίχνευση και η αντιμετώπιση απειλών, η συλλογή πληροφοριών σχετικά με τις απειλές στον κυβερνοχώρο και η αντίληψη της κατάστασης. Κατ' αρχήν, ο κίνδυνος αυτός θα μπορούσε να μετριαστεί με τη σταδιακή ενοποίηση των εμπλεκόμενων δομών, ιδίως των εθνικών SOC και των CSIRT, με τα διασυνοριακά SOC. Επιπροσθέτως, η πρόταση θα πρέπει να αποσαφηνίσει τον τρόπο αλληλεπίδρασης των εν λόγω δομών, προβλέποντας σαφείς ρυθμίσεις διακυβέρνησης και αρμοδιότητες, με σκοπό την εξασφάλιση αποτελεσματικού συντονισμού και την επίτευξη συνεργιών.

Ανταλλαγή πληροφοριών

21 Στο πλαίσιο της ειδικής έκθεσης 05/2022[3], διαπιστώσαμε ότι τα θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ δεν αντάλλασσαν συστηματικά μεταξύ τους βασικές πληροφορίες σχετικά με την κυβερνοασφάλεια, ακόμη και όταν υπήρχε σχετική υποχρέωση. Την αποτελεσματική ανταλλαγή πληροφοριών υπονόμευσαν περαιτέρω και προβλήματα διαλειτουργικότητας, τα οποία παρεμπόδιζαν την ασφαλή επικοινωνία. Μολονότι το εύρημά μας αφορούσε τη συγκριτικά μικρή και ομοιογενή ομάδα φορέων της ΕΕ, θεωρούμε ότι η πρόκληση αυτή θα αποκτά όλο και μεγαλύτερη σημασία στον ολοένα πολυπλοκότερο και ανομοιογενή γαλαξία κυβερνοασφάλειας σε επίπεδο κρατών μελών.

22 Σύμφωνα με το άρθρο 4 της πρότασης κανονισμού, το εθνικό SOC πρέπει να λειτουργεί ως «σημείο αναφοράς και πύλη» προς άλλους δημόσιους και ιδιωτικούς οργανισμούς σε εθνικό επίπεδο για τη συλλογή και ανάλυση πληροφοριών σχετικά με απειλές και περιστατικά κυβερνοασφάλειας. Ωστόσο, επί του παρόντος δεν υφίστανται σε επίπεδο ΕΕ απαιτήσεις αναφοράς στοιχείων για δημόσιους και ιδιωτικούς οργανισμούς (περιλαμβανομένων εθνικών CSIRT, ιδιωτικών SOC, και «βασικών και σημαντικών οντοτήτων» όπως ορίζονται στην οδηγία NIS 2) έναντι των εθνικών SOC. Είναι επομένως υπαρκτός ο κίνδυνος τα εθνικά SOC να μην λαμβάνουν επαρκή δεδομένα ή πληροφορίες για την κάλυψη των αναγκών τους.

23 Στην ενότητα 2.2.2 του νομοθετικού δημοσιονομικού δελτίου που συνοδεύει την πρόταση, η Επιτροπή εντοπίζει τον κίνδυνο τα κράτη μέλη να μην ανταλλάσσουν «επαρκή όγκο» σχετικών πληροφοριών για κυβερνοαπειλές είτε εντός των διασυνοριακών πλατφορμών SOC είτε μεταξύ διασυνοριακών πλατφορμών και άλλων σχετικών οντοτήτων σε επίπεδο ΕΕ. Αυτή η ελλιπής ανταλλαγή πληροφοριών θα μπορούσε να υπονομεύσει την αποτελεσματικότητα και την προστιθέμενη αξία της ευρωπαϊκής κυβερνοασπίδας.

24 Ως εκ τούτου, χαιρετίζουμε το γεγονός ότι η πρόταση περιλαμβάνει ειδικές διατάξεις στα άρθρα 4, 5 και 6 για τον μετριασμό των κινδύνων που σχετίζονται με την ελλιπή ανταλλαγή πληροφοριών. Η πρόταση προβλέπει τη διάθεση χρηματοδότησης από την ΕΕ προς τα εθνικά SOC, υπό την προϋπόθεση ότι αυτά δεσμεύονται να συμμετάσχουν σε διασυνοριακό SOC. Ωστόσο, επισημαίνουμε ότι δεν προβλέπεται η επιστροφή της χρηματοδοτικής στήριξης που χορηγήθηκε τα πρώτα δύο χρόνια σε περίπτωση που το εθνικό SOC δεν ενταχθεί σε διασυνοριακό. Η

[3] Ειδική έκθεση 05/2022, με τίτλο «Η κυβερνοασφάλεια στα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ - Ο βαθμός ετοιμότητας συνολικά δεν είναι ανάλογος των απειλών».

πρόταση κανονισμού εισάγει επίσης την υποχρέωση των μελών διασυνοριακών SOC να αναλάβουν τη δέσμευση να ανταλλάσσουν μεταξύ τους «σημαντικό όγκο δεδομένων» και να καθιερώσουν ένα πλαίσιο διακυβέρνησης συνάπτοντας γραπτή συμφωνία κοινοπραξίας.

25 Επιπροσθέτως, το άρθρο 7 της πρότασης προβλέπει την υποχρέωση των διασυνοριακών SOC να παρέχουν πληροφορίες στο EU-CyCLONe, στο δίκτυο CSIRT και στην Επιτροπή σχετικά με δυνητικό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας «χωρίς αδικαιολόγητη καθυστέρηση». Τονίζουμε τη σημασία να διασφαλιστεί η αποτελεσματική εφαρμογή της διάταξης αυτής.

26 Σύμφωνα με το άρθρο 6 της πρότασης κανονισμού, η Επιτροπή μπορεί, με εκτελεστικές πράξεις, να καθορίζει τους όρους της διαλειτουργικότητας μεταξύ των διασυνοριακών SOC. Το άρθρο 8 ορίζει ότι η Επιτροπή δύναται επίσης να εκδίδει εκτελεστικές πράξεις για τον καθορισμό τεχνικών απαιτήσεων ώστε τα κράτη μέλη να διασφαλίζουν υψηλό επίπεδο ασφάλειας των δεδομένων και υλικής ασφάλειας της υποδομής. Οι εν λόγω όροι και απαιτήσεις πρέπει να συμφωνηθούν χωρίς καθυστέρηση, ώστε να αποφευχθεί η παράλληλη ανάπτυξη ασύμβατων συστημάτων και να μειωθεί το κόστος.

Κίνδυνοι που σχετίζονται με τον μηχανισμό έκτακτης ανάγκης στον κυβερνοχώρο

Ανάπτυξη της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας

27 Στην ειδική έκθεσή μας 05/2022 επισημάναμε ότι, κατά τον χρόνο του ελέγχου μας, η CERT-ΕΕ, η ομάδα της ΕΕ για την αντιμετώπιση έκτακτων αναγκών στην πληροφορική, που παρέχει υποστήριξη στα θεσμικά και λοιπά όργανα και στους οργανισμούς της ΕΕ για την αντιμετώπιση σχετικών συμβάντων, δεν λειτουργούσε όλο το 24ωρο επί 7 ημέρες την εβδομάδα.

28 Στο άρθρο 14 της πρότασης κανονισμού προβλέπεται ότι τα αιτήματα για υποστήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας αξιολογούνται από την Επιτροπή, με την υποστήριξη του ENISA, και η απάντηση διαβιβάζεται «χωρίς καθυστέρηση». Καθώς, σε περίπτωση πολλαπλών παράλληλων αιτημάτων, ενδέχεται να είναι απαραίτητη η ιεράρχησή τους, η πρόταση κανονισμού καθορίζει ορισμένα κριτήρια για τη λήψη των σχετικών αποφάσεων. Το άρθρο 13 προβλέπει ότι η Επιτροπή μπορεί, με εκτελεστικές πράξεις, να προσδιορίζει περαιτέρω τις λεπτομερείς ρυθμίσεις για την κατανομή της εφεδρείας.

29 Θεωρούμε άκρως σημαντικό το διάστημα που μεσολαβεί μεταξύ της υποβολής του αιτήματος για υπηρεσίες υποστήριξης από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας και της απάντησης της Επιτροπής να μην εξαρτάται από τη χρονική στιγμή υποβολής του αιτήματος. Ωστόσο, η πρόταση δεν καθορίζει συγκεκριμένη προθεσμία, ούτε προβλέπει τη λήψη μέτρων σε οργανωτικό επίπεδο για την τήρηση της προθεσμίας αυτής.

Παρέκκλιση από την αρχή της «ετήσιας διάρκειας» του προϋπολογισμού

30 Μία από τις βασικές αρχές που διέπει τον προϋπολογισμό της ΕΕ είναι η ετήσια διάρκειά του, κάτι που σημαίνει ότι οι πιστώσεις που εγγράφονται στον προϋπολογισμό εγκρίνονται για ένα οικονομικό έτος έως τις 31 Δεκεμβρίου. Οι μη χρησιμοποιηθείσες αναλήψεις υποχρεώσεων και πιστώσεις πληρωμών δεν μεταφέρονται αυτόματα στο επόμενο οικονομικό έτος. Η αρχή αυτή ορίζεται στο κεφάλαιο 2 του δημοσιονομικού κανονισμού.

31 Η διάταξη του άρθρου 19 της πρότασης κανονισμού παρεκκλίνει από την εν λόγω αρχή όσον αφορά τη χρηματοδότηση δράσεων στο πλαίσιο του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο. Συγκεκριμένα, προβλέπει ότι οι μη χρησιμοποιηθείσες πιστώσεις ανάληψης υποχρεώσεων και πληρωμών για δράσεις που αφορούν την ετοιμότητα, την αντίδραση και την αμοιβαία συνδρομή μεταφέρονται αυτόματα και μπορούν να δεσμευθούν και να καταβληθούν έως τις 31 Δεκεμβρίου του επόμενου οικονομικού έτους. Στην ενότητα 2 της αιτιολογικής έκθεσής της, η Επιτροπή αιτιολόγησε την ανάγκη για ευελιξία ως προς τη διαχείριση του προϋπολογισμού επικαλούμενη τον «*απρόβλεπτο, έκτακτο και ειδικό χαρακτήρα του τοπίου της κυβερνοασφάλειας και των κυβερνοαπειλών*».

32 Όσον αφορά την ετοιμότητα, θεωρούμε ότι οι συντονισμένες δοκιμασίες της ετοιμότητας των οντοτήτων πρέπει να αποτελούν προγραμματισμένες δραστηριότητες και, επομένως, κατά κανόνα δεν είναι ούτε απρόβλεπτες ούτε έκτακτες. Κατά την άποψή μας, τέτοιες προγραμματισμένες δραστηριότητες δεν καθιστούν αναγκαία την παρέκκλιση από τη βασική αρχή της ετήσιας διάρκειας του προϋπολογισμού.

33 Ωστόσο, δεδομένου ότι η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας και η αμοιβαία συνδρομή θα αξιοποιηθούν μόνο για την απόκριση σε απρόβλεπτα γεγονότα, θεωρούμε ότι μόνο στην περίπτωση αυτή είναι βάσιμο το σκεπτικό της εν λόγω παρέκκλισης.

34 Χάριν σαφήνειας και σύμφωνα με τη διατύπωση άλλων κανονισμών, όπως ο κανονισμός περί μηχανισμού πολιτικής προστασίας της Ένωσης ή ο κανονισμός για τη θέσπιση Μηχανισμού Γειτονίας, Ανάπτυξης και Διεθνούς Συνεργασίας – Παγκόσμια Ευρώπη, θεωρούμε επίσης ότι πρέπει να διευκρινίζεται στην πρόταση κανονισμού ότι η αυτόματη μεταφορά μη χρησιμοποιηθεισών αναλήψεων υποχρεώσεων πρέπει να γίνεται στο επόμενο οικονομικό έτος και μόνο.

Κίνδυνοι σχετικά με τον μηχανισμό εξέτασης περιστατικών κυβερνοασφάλειας

35 Στο άρθρο 18 της πρότασης κανονισμού προβλέπεται ότι, κατόπιν αιτήματος της Επιτροπής, του EU-CyCLONe ή του δικτύου CSIRT, ο ENISA εξετάζει και αξιολογεί απειλές, τρωτά σημεία και δράσεις μετριασμού σε σχέση με συγκεκριμένο σημαντικό ή μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας. Ο ENISA συνεργάζεται με όλα τα σχετικά ενδιαφερόμενα μέρη και, εν συνεχεία, υποβάλλει έκθεση εξέτασης περιστατικού που καλύπτει τα κύρια αίτια, τα τρωτά σημεία και τα αντληθέντα διδάγματα.

36 Θεωρούμε ότι πρόκειται για σημαντικό μηχανισμό αναπληροφόρησης που θα ενισχύει διαρκώς τις ικανότητες ανίχνευσης, ετοιμότητας και αντιμετώπισης απειλών και περιστατικών στον τομέα της κυβερνοασφάλειας. Ωστόσο, προτείνουμε η πρόταση κανονισμού να ορίζει μέγιστη προθεσμία για την κατάρτιση της έκθεσης του ENISA μετά από ένα περιστατικό, προκειμένου να διασφαλίζεται η έγκαιρη παροχή αναπληροφόρησης. Επιπλέον, σύμφωνα με την πρόταση, στην έκθεση πρέπει να διατυπώνονται συστάσεις, εφόσον κρίνεται σκόπιμο, για τη βελτίωση της κατάστασης κυβερνοασφάλειας στην Ένωση. Όμως δεν διευκρινίζεται ο τρόπος μεταπαρακολούθησης των εν λόγω συστάσεων.

Παρακολούθηση των επιδόσεων και αξιολόγηση της πολιτικής

37 Το άρθρο 19 της πρότασης κανονισμού τροποποιεί το παράρτημα II του κανονισμού για το πρόγραμμα «Ψηφιακή Ευρώπη», θεσπίζοντας έναν νέο μετρήσιμο δείκτη, και συγκεκριμένα «*[τον] αριθμό των δράσεων που στηρίζουν την ετοιμότητα και την αντιμετώπιση περιστατικών κυβερνοασφάλειας στο πλαίσιο του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο*». Ο δείκτης αυτός συμπληρώνει δύο υφιστάμενους δείκτες που αποσκοπούν στην παρακολούθηση της προόδου ως προς την επίτευξη του ειδικού στόχου της κυβερνοασφάλειας και εμπιστοσύνης του προγράμματος «Ψηφιακή Ευρώπη», ήτοι «*[τον] αριθμό υποδομών ή εργαλείων*

κυβερνοασφάλειας, ή και τα δύο, που αποκτώνται με κοινές συμβάσεις» και «*[τον] αριθμό χρηστών και κοινοτήτων χρηστών που αποκτούν πρόσβαση σε ευρωπαϊκά μέσα κυβερνοασφάλειας*», και στην αναφορά σχετικών στοιχείων.

38 Είμαστε της άποψης ότι ο προτεινόμενος νέος δείκτης μετρά μόνο εκροές και θα παρέχει περιορισμένες μόνο πληροφορίες σχετικά με τη χρήση και τα αποτελέσματα της ευρωπαϊκής κυβερνοασπίδας και του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο.

39 Σύμφωνα με το άρθρο 20 της πρότασης, η Επιτροπή οφείλει να υποβάλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο έκθεση σχετικά με την αξιολόγηση και την επανεξέταση του εν προκειμένω κανονισμού τέσσερα χρόνια μετά την ημερομηνία εφαρμογής του.

40 Αν και θεωρούμε ότι η αξιολόγηση πρέπει να βασίζεται σε επαρκή και αξιόπιστα δεδομένα, το ταχέως μεταβαλλόμενο τοπίο των απειλών απαιτεί διαρκή προσαρμογή και καινοτομία από μέρους της ΕΕ και των κρατών μελών της. Ως εκ τούτου, κατά την άποψή μας, υπάρχει το ενδεχόμενο η αξιολόγηση, όπως προτείνεται επί του παρόντος, να διενεργείται πολύ αργά για να αξιοποιηθεί κατά τη νέα περίοδο προγραμματισμού. Επιπλέον, μέχρι το τέλος του 2027 θα έχουν αναληφθεί υποχρεώσεις για το σύνολο του προϋπολογισθέντος ποσού για τον ειδικό στόχο της κυβερνοασφάλειας και εμπιστοσύνης του προγράμματος «Ψηφιακή Ευρώπη».

Τελικές παρατηρήσεις

41 Η προτεινόμενη πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο προβλέπει μέτρα για την ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας. Το ΕΕΣ επιδοκιμάζει τους στόχους της πρότασης για ενίσχυση της συλλογικής κυβερνοανθεκτικότητας στην ΕΕ.

42 Στην παρούσα γνώμη αναδεικνύουμε ορισμένους κινδύνους που εντοπίσαμε, καθώς και τρόπους με τους οποίους θα μπορούσαν να υλοποιηθούν τα μέτρα που προβλέπονται στην πρόταση. Ειδικότερα, επισημαίνουμε τον κίνδυνο η λειτουργία και η βιωσιμότητα της ευρωπαϊκής κυβερνοασπίδας να εξαρτώνται από την ενωσιακή χρηματοδότηση και η ελλιπής ανταλλαγή πληροφοριών να παρεμποδίζει τη λειτουργία της, καθώς και τον κίνδυνο τα θεσπιζόμενα με την πρόταση μέτρα να καθιστούν πολυπλοκότερο τον συνολικό γαλαξία κυβερνοασφάλειας της ΕΕ.

43 Κατόπιν της από μέρους μας εξέτασης της νομοθετικής πρότασης, εισηγούμαστε στην **Επιτροπή και τους νομοθέτες να εξετάσουν το ενδεχόμενο**:

— να δημοσιοποιήσουν τις εκτιμήσεις κόστους για τη θέσπιση και την εφαρμογή των προτεινόμενων μέτρων, προς ενίσχυση της διαφάνειας (σημείο ***10***)·

— να αποσαφηνίσουν τον τρόπο αλληλεπίδρασης των εθνικών και των διασυνοριακών SOC, των CSIRT και του σχετικού δικτύου, προβλέποντας σαφείς ρυθμίσεις διακυβέρνησης και αρμοδιότητες, με σκοπό την εξασφάλιση αποτελεσματικού συντονισμού και την επίτευξη συνεργιών (σημείο ***20***)·

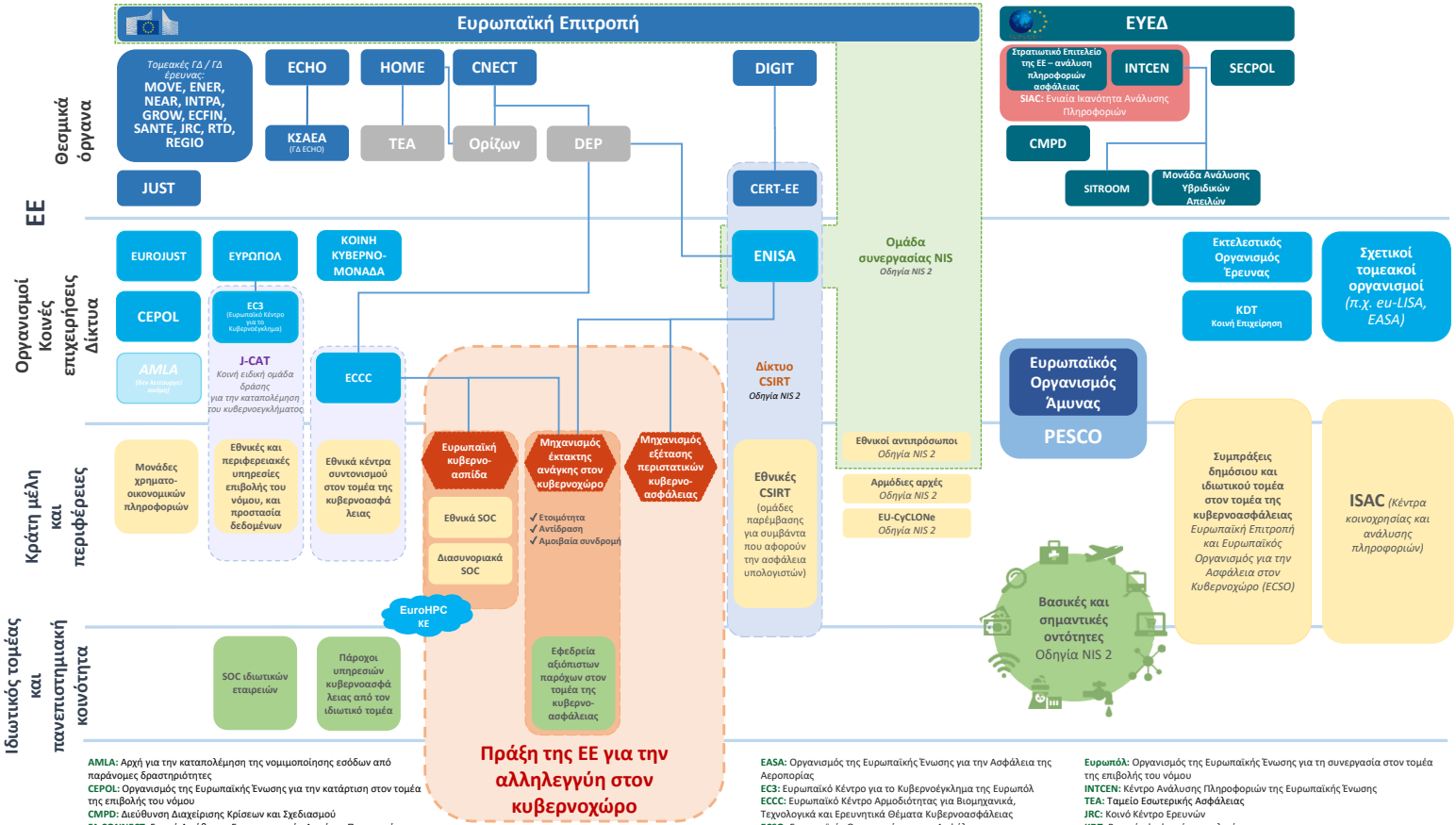
— να διασφαλίσουν ότι ο χρόνος που μεσολαβεί μεταξύ της υποβολής του αιτήματος για υπηρεσίες υποστήριξης από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας και της απάντησης της Επιτροπής δεν εξαρτάται από τη χρονική στιγμή υποβολής του αιτήματος (σημείο ***29***)·

— να περιορίσουν την απόκλιση από την αρχή της ετήσιας διάρκειας του προϋπολογισμού στην περίπτωση δράσεων που αφορούν την αντίδραση και την αμοιβαία συνδρομή, και να διευκρινίσουν ότι η αυτόματη μεταφορά μη χρησιμοποιηθεισών αναλήψεων υποχρεώσεων πρέπει να γίνεται στο επόμενο οικονομικό έτος και μόνο (σημεία ***32***-***34***)·

— να ορίσουν μέγιστη προθεσμία για την υποβολή της έκθεσης του ENISA μετά από ένα περιστατικό, προκειμένου να διασφαλίζεται η έγκαιρη παροχή αναπληροφόρησης (σημείο ***36***)·

— να συντμήσουν την προθεσμία για την κατάρτιση της έκθεσης της Επιτροπής σχετικά με την αξιολόγηση και την επανεξέταση του εν προκειμένω κανονισμού (σημείο ***40***).

Παράρτημα – Ο ευρωπαϊκός γαλαξίας κυβερνοασφάλειας



AMLA: Αρχή για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες
CEPOL: Οργανισμός της Ευρωπαϊκής Ένωσης για την κατάρτιση στον τομέα της επιβολής του νόμου
CMPD: Διεύθυνση Διαχείρισης Κρίσεων και Σχεδιασμού
ΓΔ CONNECT: Γενική Διεύθυνση Επικοινωνιακών Δικτύων, Περιεχομένου και Τεχνολογιών
ΓΔ ECFIN: Γενική Διεύθυνση Οικονομικών και Χρηματοδοτικών Υποθέσεων
ΓΔ ECHO: Γενική Διεύθυνση Ευρωπαϊκής Πολιτικής Προστασίας και Επιχειρήσεων Ανθρωπιστικής Βοήθειας
ΓΔ ENER: Γενική Διεύθυνση Ενέργειας
ΓΔ GROW: Γενική Διεύθυνση Εσωτερικής Αγοράς, Βιομηχανίας, Επιχειρηματικότητας και ΜΜΕ
ΓΔ HOME: Γενική Διεύθυνση Μετανάστευσης και Εσωτερικών Υποθέσεων
ΓΔ INTPA: Γενική Διεύθυνση Διεθνών Εταιρικών Σχέσεων
ΓΔ JUST: Γενική Διεύθυνση Δικαιοσύνης και Καταναλωτών
ΓΔ MOVE: Γενική Διεύθυνση Κινητικότητας και Μεταφορών
ΓΔ NEAR: Γενική Διεύθυνση Γειτονίας και Διαπραγματεύσεων για τη Διεύρυνση
ΓΔ REGIO: Γενική Διεύθυνση Περιφερειακής Πολιτικής και Αστικής Ανάπτυξης
ΓΔ RTD: Γενική Διεύθυνση Έρευνας και Καινοτομίας
ΓΔ SANTE: Γενική Διεύθυνση Υγείας και Ασφάλειας των Τροφίμων
DIGIT: Γενική Διεύθυνση Πληροφορικής
EASA: Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια της Αεροπορίας
EC3: Ευρωπαϊκό Κέντρο για το Κυβερνοέγκλημα της Ευρωπόλ
ECCC: Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας
ECSO: Ευρωπαϊκός Οργανισμός για την Ασφάλεια στον Κυβερνοχώρο
ΕΟΑ: Ευρωπαϊκός Οργανισμός Άμυνας
ΕΥΕΔ: Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης
ΚΣΑΕΑ: Κέντρο Συντονισμού Αντιμετώπισης Εκτάκτων Αναγκών
EU-CyCLONe: Ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για τις κρίσεις στον κυβερνοχώρο
EuroHPC: Ευρωπαϊκή υπολογιστική υψηλών επιδόσεων
Eurojust: Οργανισμός της Ευρωπαϊκής Ένωσης για τη συνεργασία στον τομέα της ποινικής δικαιοσύνης
Ευρωπόλ: Οργανισμός της Ευρωπαϊκής Ένωσης για τη συνεργασία στον τομέα της επιβολής του νόμου
INTCEN: Κέντρο Ανάλυσης Πληροφοριών της Ευρωπαϊκής Ένωσης
ΤΕΑ: Ταμείο Εσωτερικής Ασφάλειας
JRC: Κοινό Κέντρο Ερευνών
ΚΔΤ: Βασικές ψηφιακές τεχνολογίες
Οδηγία NIS: Οδηγία για την ασφάλεια δικτύων και πληροφοριών
PESCO: Πλαίσιο μόνιμης διαρθρωμένης συνεργασίας
SECPOL: Διεύθυνση πρόληψης των συγκρούσεων και πολιτικής ασφάλειας
SITROOM: Αίθουσα διαχείρισης κρίσεων
SOC: Κέντρο επιχειρήσεων ασφάλειας

Πηγή: ΕΕΣ.

Η παρούσα γνώμη εγκρίθηκε από το Τμήμα III, του οποίου προεδρεύει η Bettina Jakobsen, Μέλος του Ελεγκτικού Συνεδρίου, στο Λουξεμβούργο, κατά τη συνεδρίασή του της 26ης Σεπτεμβρίου 2023.

Για το Ελεγκτικό Συνέδριο

Tony Murphy
Πρόεδρος

ΔΙΚΑΙΩΜΑΤΑ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

Η πολιτική για την περαιτέρω χρήση εγγράφων του Ευρωπαϊκού Ελεγκτικού Συνεδρίου (ΕΕΣ) ορίζεται στην απόφαση αριθ. 6-2019 του ΕΕΣ για την πολιτική ανοικτών δεδομένων και την περαιτέρω χρήση εγγράφων.

Με εξαίρεση τις περιπτώσεις όπου ορίζεται διαφορετικά (π.χ. σε χωριστές ανακοινώσεις περί πνευματικής ιδιοκτησίας), το περιεχόμενο του ΕΕΣ που ανήκει στην ΕΕ παραχωρείται βάσει της άδειας Creative Commons Attribution 4.0 International (CC BY 4.0). Ισχύει, επομένως, ως γενικός κανόνας ότι η περαιτέρω χρήση επιτρέπεται υπό τον όρο ότι αναφέρεται η πηγή και επισημαίνονται οι αλλαγές. Κατά την περαιτέρω χρήση απαγορεύεται η διαστρέβλωση του αρχικού νοήματος ή μηνύματος των εγγράφων. Το ΕΕΣ δεν φέρει ευθύνη για οποιαδήποτε συνέπεια προερχόμενη από την περαιτέρω χρήση εγγράφων.

Εάν συγκεκριμένο περιεχόμενο αναφέρεται σε ταυτοποιήσιμα φυσικά πρόσωπα, π.χ. φωτογραφίες υπαλλήλων του ΕΕΣ, ή περιλαμβάνει έργα τρίτων, απαιτείται πρόσθετη έγκριση.

Όταν παραχωρείται η έγκριση, αυτή ακυρώνει και αντικαθιστά την ανωτέρω γενική έγκριση και αναφέρει σαφώς τυχόν περιορισμούς στη χρήση.

Για τη χρήση ή την αναπαραγωγή περιεχομένου που δεν ανήκει στην ΕΕ, μπορεί να χρειάζεται να ζητήσετε άδεια απευθείας από τους κατόχους των δικαιωμάτων πνευματικής ιδιοκτησίας.

Το λογισμικό ή τα έγγραφα που καλύπτονται από δικαιώματα βιομηχανικής ιδιοκτησίας, όπως τα διπλώματα ευρεσιτεχνίας, τα εμπορικά σήματα, τα καταχωρισμένα σχέδια, οι λογότυποι και οι επωνυμίες/ονομασίες, εξαιρούνται από την πολιτική του ΕΕΣ για την περαιτέρω χρήση.

Το σύνολο των ιστότοπων των θεσμικών οργάνων της Ευρωπαϊκής Ένωσης εντός του ονόματος χώρου «europa.eu» παρέχει συνδέσμους προς ιστότοπους τρίτων. Δεδομένου ότι το ΕΕΣ δεν έχει έλεγχο επ’ αυτών, σας συνιστούμε να εξετάζετε τις πολιτικές τους για την προστασία του ιδιωτικού απορρήτου και της πνευματικής ιδιοκτησίας.

Χρήση του λογότυπου του ΕΕΣ

Δεν επιτρέπεται η χρήση του λογότυπου του ΕΕΣ χωρίς την προηγούμενη σύμφωνη γνώμη του οργάνου.