ΕΣΠΔ–ΕΕΠΔ Κοινή γνωμοδότηση [4/2026]

σχετικά με την πρόταση κανονισμού για
την κυβερνοασφάλεια 2
και την πρόταση τροποποίησης της
οδηγίας NIS 2

Εκδόθηκε στις 18 Μαρτίου 2026

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Πίνακας περιεχομένων

Συνοπτική παρουσίαση

Στις 20 Ιανουαρίου 2026 η Ευρωπαϊκή Επιτροπή εξέδωσε πρόταση κανονισμού σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας και την ασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ και την κατάργηση του κανονισμού (ΕΕ) 2019/881 (κανονισμός για την κυβερνοασφάλεια 2) και πρόταση οδηγίας για την τροποποίηση της οδηγίας (ΕΕ) 2022/2555 όσον αφορά τα μέτρα απλούστευσης και την ευθυγράμμιση με την [πρόταση κανονισμού για την κυβερνοασφάλεια 2]. Στις 21 Ιανουαρίου 2026 η Επιτροπή ζήτησε επισήμως τη γνώμη του ΕΣΠΔ και του ΕΕΠΔ σύμφωνα με το άρθρο 42 παράγραφος 2 του κανονισμού (ΕΕ) 2018/1725.

Το ΕΣΠΔ και ο ΕΕΠΔ υπενθυμίζουν ότι η σχέση μεταξύ της προστασίας των δεδομένων και της κυβερνοασφάλειας είναι διττή. Αφενός, η κυβερνοασφάλεια εξυπηρετεί την προστασία των δεδομένων προσωπικού χαρακτήρα περιορίζοντας τους κινδύνους ανεπιθύμητης πρόσβασης, τροποποίησης ή μη διαθεσιμότητας των εν λόγω δεδομένων. Αφετέρου, ορισμένα μέτρα κυβερνοασφάλειας μπορεί να συνιστούν επέμβαση στα δικαιώματα και στις ελευθερίες των ατόμων, ιδίως στα δικαιώματα στην ιδιωτική ζωή και την προστασία των δεδομένων. Ως εκ τούτου, παρότι η αποτελεσματικότητα αποτελεί σημαντικό σημείο εστίασης για τα μέτρα κυβερνοασφάλειας, η αναγκαιότητα και η αναλογικότητα πρέπει επίσης να εξετάζονται.

Το ΕΣΠΔ και ο ΕΕΠΔ υποστηρίζουν τον γενικό στόχο των προτάσεων για ενίσχυση του ρόλου του ENISA και διευκόλυνση της υιοθέτησης πιστοποίησης της κυβερνοασφάλειας, με την επιφύλαξη των ειδικών συστάσεων που παρέχονται στην παρούσα κοινή γνωμοδότηση. Επικροτούν επίσης τον στόχο της θέσπισης μηχανισμών και προϋποθέσεων, με την οδηγία (ΕΕ) 2022/2555, που θα συμβάλουν στη διευκόλυνση της συμμόρφωσης με τις απαιτήσεις κυβερνοασφάλειας και, κατ' αυτόν τον τρόπο, θα καταστήσουν την εφαρμογή τους συνεκτικότερη και αποτελεσματικότερη, καθώς και τον στόχο της περαιτέρω αντιμετώπισης των διαφόρων κινδύνων για τις αλυσίδες εφοδιασμού ΤΠΕ, συμπεριλαμβανομένων των μη τεχνικών κινδύνων. Το ΕΣΠΔ και ο ΕΕΠΔ υποστηρίζουν επίσης σθεναρά τον στόχο της δημιουργίας ενιαίου σημείου εισόδου για την κοινοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα, καθώς θα μειώσει τον διοικητικό φόρτο για τους οργανισμούς χωρίς να επηρεάσει το επίπεδο προστασίας των υποκειμένων των δεδομένων.

Το ΕΣΠΔ και ο ΕΕΠΔ εκφράζουν επίσης την ικανοποίησή τους για τις περαιτέρω διευκρινίσεις που θα παράσχει η πρόταση κανονισμού για την κυβερνοασφάλεια 2 (στο εξής: ΚΚΑ2) σχετικά με τις λεπτομέρειες της παροχής στήριξης από τον ENISA σε διάφορους συμφεροντούχους και συνιστούν να προστεθεί και ο ΕΕΠΔ ως πιθανός αιτών συμβουλές από τον ENISA. Το ΕΣΠΔ και ο ΕΕΠΔ υποστηρίζουν σθεναρά την παροχή των εν λόγω συμβουλών κατόπιν αιτήματος, ώστε να διασφαλίζεται ότι ο συντονισμός και η κατανομή των αρμοδιοτήτων θα είναι σαφείς.

Όσον αφορά τη συνεργασία μεταξύ του ENISA και άλλων οντοτήτων της Ένωσης εν γένει, το ΕΣΠΔ και ο ΕΕΠΔ εκφράζουν την ικανοποίησή τους για τις συνέργειες που μπορεί να επιφέρει η συνεργασία αυτή, σύμφωνα με τα αντίστοιχα καθήκοντα και τις εντολές τους. Συνιστούν να προστεθεί ρητή αναφορά και στον ΕΕΠΔ ως όργανο της Ένωσης με το οποίο θα συνεργάζεται ο ENISA.

Το ΕΣΠΔ και ο ΕΕΠΔ θεωρούν ότι, εάν τα μελλοντικά καθήκοντα του ENISA ως κόμβου πληροφοριών απαιτούν σημαντικό βαθμό επεξεργασίας δεδομένων προσωπικού χαρακτήρα, αυτό θα πρέπει να αναφέρεται ρητά στις διατάξεις της βασικής πράξης που διέπει τα αντίστοιχα καθήκοντα, συμπεριλαμβανομένων των ουσιωδών στοιχείων κάθε επεξεργασίας μεγάλης κλίμακας και των κατάλληλων εγγυήσεων. Αντιστρόφως, εάν ο στόχος είναι να δοθεί στον ENISA η δυνατότητα να συλλέγει και να επεξεργάζεται περαιτέρω κυρίως συγκεντρωτικά δεδομένα μη προσωπικού χαρακτήρα, αυτό θα πρέπει επίσης να αποσαφηνιστεί.

Το ΕΣΠΔ και ο ΕΕΠΔ υπενθυμίζουν ότι, καταρχήν, μόνο οι πολύ τεχνικές (πρακτικές) λεπτομέρειες που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να αποφασίζονται στο πλαίσιο της διοικητικής αυτονομίας του οικείου φορέα της ΕΕ (στην προκειμένη περίπτωση του διοικητικού συμβουλίου αποκεντρωμένου οργανισμού). Επιπλέον, το ΕΣΠΔ και ο ΕΕΠΔ συνιστούν να προβλεφθεί στο άρθρο 66 της πρότασης ΚΚΑ2 να ζητείται η γνώμη του ΕΕΠΔ πριν από τη θέσπιση των σχετικών κανόνων.

Όσον αφορά το ευρωπαϊκό πλαίσιο δεξιοτήτων κυβερνοασφάλειας (ΕΠΔΚ), το ΕΣΠΔ και ο ΕΕΠΔ συνιστούν στους συννομοθέτες να τροποποιήσουν το άρθρο 19 παράγραφος 2 της πρότασης ΚΚΑ2, ώστε το ΕΠΔΚ να μην περιορίζεται αποκλειστικά στους «επαγγελματίες στον τομέα της κυβερνοασφάλειας», αλλά να περιλαμβάνει επίσης προφίλ για το εργατικό δυναμικό εν γένει.

Σχετικά με το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας, το ΕΣΠΔ και ο ΕΕΠΔ συνιστούν να αποσαφηνιστεί περαιτέρω το πεδίο εφαρμογής του άρθρου 80 παράγραφος 1 στοιχείο κγ) του ΚΚΑ2 και η σχέση με την πιστοποίηση βάσει του ΓΚΠΔ. Επιπλέον, το ΕΣΠΔ και ο ΕΕΠΔ συνιστούν να απαιτείται από τον ENISA να διαβουλεύεται με το ΕΣΠΔ πριν από την έγκριση σχημάτων πιστοποίησης βάσει του άρθρου 80 παράγραφος 1 στοιχείο κγ) του ΚΚΑ2, ώστε να διασφαλίζεται η συνοχή.

Το ΕΣΠΔ και ο ΕΕΠΔ τονίζουν την ανάγκη για εξέταση όχι μόνο της αποτελεσματικότητας των μέτρων κυβερνοασφάλειας, αλλά και της αναγκαιότητας και της αναλογικότητάς τους. Το ΕΣΠΔ και ο ΕΕΠΔ συνιστούν να διευκρινιστεί ότι τα σχήματα πιστοποίησης θα πρέπει, στο μέτρο του δυνατού, να λαμβάνουν υπόψη τους ελέγχους ασφάλειας οι οποίοι μπορούν να βοηθήσουν να αποδειχθεί η εκπλήρωση των απαιτήσεων του ΓΚΠΔ, ιδίως όταν τα σχήματα εφαρμόζονται σε προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας που είναι πιθανό να χρησιμοποιηθούν σε πράξεις επεξεργασίας δεδομένων.

Το ΕΣΠΔ και ο ΕΕΠΔ επικροτούν επίσης το προτεινόμενο μέτρο που αποσκοπεί στην εξασφάλιση πλαισίου για αξιόπιστες αλυσίδες εφοδιασμού ΤΠΕ και στην αντιμετώπιση των μη τεχνικών κινδύνων σε τομείς υψηλής κρισιμότητας.

Όσον αφορά την πρόταση για τροποποίηση της οδηγίας NIS 2, το ΕΣΠΔ και ο ΕΕΠΔ εκφράζουν την ικανοποίησή τους για τον ορισμό των παρόχων ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας και ευρωπαϊκών πορτοφολιών επιχειρήσεων ως «βασικών οντοτήτων» και υποστηρίζουν πλήρως τον σημαντικό στόχο της πρόληψης μελλοντικών επιθέσεων λυτρισμικού και της παρεμπόδισης και εξάρθρωσης των εγκληματικών οργανώσεων που βρίσκονται πίσω από αυτές.

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων

Έχοντας υπόψη το άρθρο 42 παράγραφος 2 του κανονισμού (ΕΕ) 2018/1725, 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,

Εξέδωσαν την ακόλουθη κοινή γνωμοδότηση (στο εξής: γνωμοδότηση)

1 ΙΣΤΟΡΙΚΟ

1. Στις 20 Ιανουαρίου 2026 η Ευρωπαϊκή Επιτροπή (στο εξής: Επιτροπή) εξέδωσε πρόταση κανονισμού σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας και την ασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ και την κατάργηση του κανονισμού (ΕΕ) 2019/881 (κανονισμός για την κυβερνοασφάλεια 2)[1] και πρόταση οδηγίας για την τροποποίηση της οδηγίας (ΕΕ) 2022/2555 όσον αφορά τα μέτρα απλούστευσης και την ευθυγράμμιση με την [πρόταση κανονισμού για την κυβερνοασφάλεια 2] [2] (στο εξής: «πρόταση ΚΚΑ2», «πρόταση τροποποίησης της NIS 2» και από κοινού «προτάσεις»). Στις 21 Νοεμβρίου 2026 η Επιτροπή ζήτησε επισήμως τη γνώμη του ΕΣΠΔ και του ΕΕΠΔ σύμφωνα με το άρθρο 42 παράγραφος 2 του κανονισμού (ΕΕ) 2018/1725 (EUDPR)[3].
2. Η πρόταση ΚΚΑ2 αποσκοπεί στην αντικατάσταση της ισχύουσας πράξης για την κυβερνοασφάλεια[4] προκειμένου 1) να ενισχυθεί ο ρόλος του ENISA, με έμφαση στις ανάγκες των συμφεροντούχων σε ένα όλο και πιο εχθρικό τοπίο απειλών, 2) να δοθεί νέα ώθηση στην εφαρμογή του ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας (ΕΠΠΚ), 3) να μειωθούν η πολυπλοκότητα και η πολυμορφία των πολιτικών που σχετίζονται με την κυβερνοασφάλεια, και 4) να αντιμετωπιστούν περαιτέρω οι κίνδυνοι για την ασφάλεια των αλυσίδων εφοδιασμού ΤΠΕ[5].
3. Η πρόταση τροποποίησης της NIS 2 επικεντρώνεται ιδίως στον τρίτο στόχο, με την εισαγωγή διευκρινίσεων και τη διευκόλυνση της συμμόρφωσης των ρυθμιζόμενων οντοτήτων[6].

[1] COM(2026) 11 final.
[2] COM(2026) 13 final.
[3] 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).
[4] 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, ELI: http://data.europa.eu/eli/reg/2019/881/oj), όπως τροποποιήθηκε με τον κανονισμό (ΕΕ) 2025/37 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Δεκεμβρίου 2024, για την τροποποίηση του κανονισμού (ΕΕ) 2019/881 όσον αφορά τις διαχειριζόμενες υπηρεσίες ασφάλειας (ΕΕ L, 2025/37, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/37/oj).
[5] COM(2026) 11 final, σ. 1, αιτιολογική έκθεση.
[6] COM(2026) 13 final.

4. Στόχος της παρούσας κοινής γνωμοδότησης είναι να εξετάσει τις σχετικές πτυχές των προτάσεων που έχουν ιδιαίτερη σημασία για την προστασία των δικαιωμάτων και των ελευθεριών των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

2 ΓΕΝΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ

5. Η πρόταση ΚΚΑ2 αποσκοπεί στην επέκταση της εντολής του ENISA και στην ενίσχυση της επιχειρησιακής του ικανότητας. Το ΕΣΠΔ και ο ΕΕΠΔ υποστηρίζουν την ενίσχυση του ρόλου του ENISA και τον στόχο για διευκόλυνση της υιοθέτησης πιστοποίησης της κυβερνοασφάλειας, με την επιφύλαξη των ειδικών συστάσεων που παρέχονται κατωτέρω.

6. Το ΕΣΠΔ και ο ΕΕΠΔ επικροτούν επίσης τον στόχο της θέσπισης μηχανισμών και προϋποθέσεων, με την οδηγία (ΕΕ) 2022/2555[7] (στο εξής: οδηγία NIS 2), που θα συμβάλουν στη διευκόλυνση της συμμόρφωσης με τις απαιτήσεις κυβερνοασφάλειας και, κατ' αυτόν τον τρόπο, θα καταστήσουν την εφαρμογή τους συνεκτικότερη και αποτελεσματικότερη, καθώς και τον στόχο της περαιτέρω αντιμετώπισης των διαφόρων κινδύνων για τις αλυσίδες εφοδιασμού ΤΠΕ, συμπεριλαμβανομένων μη τεχνικών κινδύνων.

7. Όπως δήλωσαν ήδη στην κοινή τους γνωμοδότηση σχετικά με την πρόταση της δέσμης μέτρων Omnibus για τον ψηφιακό τομέα[8], το ΕΣΠΔ και ο ΕΕΠΔ υποστηρίζουν επίσης σθεναρά τον στόχο της δημιουργίας ενιαίου σημείου εισόδου για την κοινοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα, καθώς θα μειώσει τον διοικητικό φόρτο για τους οργανισμούς χωρίς να επηρεάσει το επίπεδο προστασίας των υποκειμένων των δεδομένων.

8. Στο άρθρο 5 παράγραφος 1 στοιχείο στ) του κανονισμού (ΕΕ) 2016/679 (ΓΚΠΔ), η ασφάλεια ορίζεται ως μία από τις βασικές αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Στο άρθρο 32 του ΓΚΠΔ, προσδιορίζεται περαιτέρω η υποχρέωση αυτή, η οποία ισχύει τόσο για τους υπευθύνους επεξεργασίας όσο και για τους εκτελούντες την επεξεργασία, προκειμένου να διασφαλίζεται κατάλληλο επίπεδο ασφάλειας. Και οι δύο διατάξεις καθιστούν σαφές ότι η ασφάλεια της επεξεργασίας δεδομένων προσωπικού χαρακτήρα είναι απαραίτητη για τη συμμόρφωση με τη νομοθεσία της ΕΕ για την προστασία των δεδομένων.

9. Η σχέση μεταξύ της προστασίας των δεδομένων και της κυβερνοασφάλειας είναι διττή. Αφενός, η κυβερνοασφάλεια εξυπηρετεί την προστασία των δεδομένων προσωπικού χαρακτήρα περιορίζοντας τους κινδύνους ανεπιθύμητης πρόσβασης, τροποποίησης ή μη διαθεσιμότητας των εν λόγω δεδομένων. Αφετέρου, ορισμένα μέτρα κυβερνοασφάλειας μπορεί να συνιστούν επέμβαση στα δικαιώματα και στις ελευθερίες των ατόμων, ιδίως στα δικαιώματα στην ιδιωτική ζωή και την προστασία των δεδομένων[9].

[7] 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).

[8] EDPB-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus) [ΕΣΠΔ–ΕΕΠΔ Κοινή γνωμοδότηση 2/2026 σχετικά με την πρόταση κανονισμού όσον αφορά την απλούστευση του νομοθετικού πλαισίου για τον ψηφιακό τομέα (δέσμη μέτρων Omnibus για τον ψηφιακό τομέα), εκδόθηκε στις 10 Φεβρουαρίου 2026].

[9] Πρβλ. ΕΕΠΔ Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive (Γνωμοδότηση 5/2021 σχετικά με τη στρατηγική κυβερνοασφάλειας και την οδηγία NIS 2.0), 11 Μαρτίου 2021, παράγραφοι 10-11, ΕΕΠΔ Opinion 7/2022 on the Proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union (Γνωμοδότηση 7/2022 για την πρόταση κανονισμού σχετικά με την ασφάλεια των πληροφοριών στα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης), 17 Μαΐου 2022, παράγραφοι 9-10, και ΕΕΠΔ Opinion 2/2024 on the Proposal for a Regulation amending the Cybersecurity Act as regards managed security services (Γνωμοδότηση 2/2024 σχετικά με την πρόταση κανονισμού για την τροποποίηση της πράξης για την κυβερνοασφάλεια όσον αφορά τις διαχειριζόμενες υπηρεσίες ασφάλειας), 10 Ιανουαρίου 2024, παράγραφος 5.

10. Το ΕΣΠΔ και ο ΕΕΠΔ υπενθυμίζουν ότι, στην αιτιολογική σκέψη 49 του ΓΚΠΔ, αναγνωρίζεται ότι τα μέτρα κυβερνοασφάλειας που περιλαμβάνουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα συνιστούν έννομο συμφέρον του ενδιαφερόμενου υπευθύνου επεξεργασίας δεδομένων, ενώ παράλληλα υπογραμμίζεται ότι τα μέτρα θα πρέπει να είναι αυστηρά αναγκαία και αναλογικά για τους σκοπούς της διασφάλισης της ασφάλειας δικτύων και πληροφοριών. Ως εκ τούτου, τα μέτρα κυβερνοασφάλειας δεν θα πρέπει να έχουν ως γνώμονα μόνο την αποτελεσματικότητα, αλλά και να εξετάζουν αν ο αντίκτυπός τους στα θεμελιώδη δικαιώματα παραμένει εντός των ορίων του αναγκαίου και αναλογικού.

3 ΣΤΗΡΙΞΗ ΑΠΟ ΤΟΝ ENISA ΓΙΑ ΤΗΝ ΕΦΑΡΜΟΓΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΚΑΙ ΤΟΥ ΔΙΚΑΙΟΥ ΤΗΣ ΈΝΩΣΗΣ ΚΑΙ ΤΗ ΣΥΝΕΡΓΑΣΙΑ ΜΕ ΑΛΛΕΣ ΟΝΤΟΤΗΤΕΣ ΤΗΣ ΈΝΩΣΗΣ

11. Σύμφωνα με το άρθρο 5 παράγραφος 1 της πρότασης ΚΚΑ2, ο ENISA συμβάλλει στην εφαρμογή της πολιτικής και του δικαίου της Ένωσης σε διάφορους τομείς, παρέχοντας στήριξη σε διάφορους συμφεροντούχους, όπως παρατίθενται στο εν λόγω άρθρο.

12. Μεταξύ αυτών, σύμφωνα με το άρθρο 5 παράγραφος 1 στοιχείο η) της πρότασης ΚΚΑ2, ο ENISA θα παρέχει, κατόπιν αιτήματος του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, συμβουλές σχετικά με την εφαρμογή συγκεκριμένων πτυχών κυβερνοασφάλειας της πολιτικής και του δικαίου της Ένωσης που σχετίζονται με την προστασία των δεδομένων και της ιδιωτικής ζωής. Το ΕΣΠΔ και ο ΕΕΠΔ επισημαίνουν ότι το άρθρο 5 παράγραφος 1 στοιχείο η) της πρότασης ΚΚΑ2 δεν αποτελεί εντελώς νέα διάταξη. Το άρθρο 5 σημείο 5) στοιχείο γ) της ισχύουσας πράξης για την κυβερνοασφάλεια προβλέπει ήδη ότι ο ENISA μπορεί να στηρίζει «τα κράτη μέλη στην εφαρμογή των ειδικών πτυχών κυβερνοασφάλειας της πολιτικής και του δικαίου της Ένωσης σχετικά με την προστασία των δεδομένων και της ιδιωτικής ζωής, παρέχοντας συμβουλευτική γνώμη στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων κατόπιν αιτήματος».

13. Το ΕΣΠΔ και ο ΕΕΠΔ εκφράζουν την ικανοποίησή τους για τις περαιτέρω διευκρινίσεις που θα παράσχει η πρόταση ΚΚΑ2 σχετικά με τις λεπτομέρειες της συνεργασίας, διατηρώντας παράλληλα τα βασικά στοιχεία του άρθρου 5 σημείο 5) στοιχείο γ) της πράξης για την κυβερνοασφάλεια. Στο νέο άρθρο 5 παράγραφος 1 στοιχείο η), θα διευκρινίζεται ότι το ΕΣΠΔ, ως όργανο της Ένωσης, έχει το δικαίωμα να ζητεί απευθείας τις συμβουλές του ENISA (χωρίς αυτό να συνδέεται με την εφαρμογή συγκεκριμένων πτυχών κυβερνοασφάλειας της πολιτικής και του δικαίου της Ένωσης που σχετίζονται με την προστασία των δεδομένων και της ιδιωτικής ζωής από τα κράτη μέλη).

14. Ταυτόχρονα, το ΕΣΠΔ και ο ΕΕΠΔ συνιστούν να προστεθεί και ο ΕΕΠΔ στο άρθρο 5 παράγραφος 1 στοιχείο η) του ΚΚΑ2 ως πιθανός αιτών, δεδομένου του ρόλου του ως εποπτικής αρχής για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ευρωπαϊκής Ένωσης. Η παροχή της δυνατότητας τόσο στο ΕΣΠΔ όσο και στον ΕΕΠΔ να αξιοποιούν την τεχνική επάρκεια του ENISA στον τομέα της κυβερνοασφάλειας μπορεί να συμβάλει στη διασφάλιση ότι η καθοδήγηση και οι αποφάσεις τους στον τομέα της προστασίας των δεδομένων βασίζονται στις πλέον σύγχρονες γνώσεις κυβερνοασφάλειας. Οι συμβουλές και η συνεργασία μπορεί να είναι επωφελείς σε διάφορα θέματα, συμπεριλαμβανομένων των προτύπων κυβερνοασφάλειας και των επιχειρησιακών πρακτικών, καθώς και της χρήσης τεχνολογιών για τη βελτίωση της προστασίας της ιδιωτικής ζωής στο πλαίσιο της κυβερνοασφάλειας.

15. Το ΕΣΠΔ και ο ΕΕΠΔ υποστηρίζουν σθεναρά ότι οι συμβουλές που αναφέρονται στο άρθρο 5 παράγραφος 1 στοιχείο η) του ΚΚΑ2 παρέχονται μόνο κατόπιν αιτήματος του ΕΣΠΔ ή, όπως προτείνεται στην παρούσα γνωμοδότηση, του ΕΕΠΔ. Προβλέποντας ότι ο ENISA ενεργεί μόνο κατόπιν αιτήματος του ΕΣΠΔ ή του ΕΕΠΔ, το άρθρο 5 παράγραφος 1 στοιχείο η) θα διασφαλίσει ότι ο συντονισμός και η κατανομή των αρμοδιοτήτων θα είναι σαφείς[10].

16. Το ΕΣΠΔ και ο ΕΕΠΔ επισημαίνουν ότι το άρθρο 5 παράγραφος 1 στοιχείο η) της πρότασης ΚΚΑ2 φαίνεται ότι αποτελεί συγκεκριμένη έκφανση μιας γενικότερης υποχρέωσης συνεργασίας που κατοχυρώνεται στο άρθρο 68 της πρότασης ΚΚΑ2, στο οποίο ρυθμίζεται η συνεργασία του ENISA με άλλες οντότητες της Ένωσης. Σύμφωνα με το άρθρο 68, ο ENISA συνεργάζεται σε θέματα που σχετίζονται με την κυβερνοασφάλεια με άλλα όργανα της ΕΕ, συμπεριλαμβανομένου του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, για τη διασφάλιση της συνέπειας, τη δημιουργία συνεργειών και την αντιμετώπιση ζητημάτων κοινού ενδιαφέροντος. Η συνεργασία αυτή μπορεί να εξασφαλίζεται μέσω της ανταλλαγής τεχνογνωσίας και βέλτιστων πρακτικών· της παροχής συμβουλών και της έκδοσης κατευθυντήριων γραμμών για θέματα σχετικά με την κυβερνοασφάλεια· και της θέσπισης πρακτικών ρυθμίσεων για την εκτέλεση συγκεκριμένων καθηκόντων κατόπιν διαβούλευσης με την Επιτροπή.

17. Το ΕΣΠΔ και ο ΕΕΠΔ επικροτούν τη συνεργασία και τις συνέργειες μεταξύ του ENISA και άλλων οντοτήτων της Ένωσης, σύμφωνα με τα αντίστοιχα καθήκοντα και τις εντολές τους. Στο πλαίσιο αυτό, για λόγους νομικής σαφήνειας, το ΕΣΠΔ και ο ΕΕΠΔ συνιστούν την τροποποίηση του άρθρου 68 της πρότασης ΚΚΑ2, με την προσθήκη ρητής αναφοράς και στον ΕΕΠΔ ως όργανο της Ένωσης με το οποίο θα συνεργάζεται ο ENISA[11].

4 ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΥΝΕΡΓΑΣΙΑ, ΚΟΙΝΗ ΕΠΙΓΝΩΣΗ ΤΗΣ ΚΑΤΑΣΤΑΣΗΣ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

[10] Με το αίτημα των εποπτικών αρχών ως αναγκαία προϋπόθεση για τη συμμετοχή του ENISA, τηρείται διαρθρωμένη διαδικασία διαβούλευσης, στο πλαίσιο της οποίας ο ENISA παρέχει τεχνική εμπειρογνωσία, ενώ οι εποπτικές αρχές διατηρούν τον πλήρη έλεγχο των αποφάσεων που σχετίζονται με την προστασία των δεδομένων. Διασφαλίζεται επίσης ο συντονισμός κάθε παρέμβασης του ENISA, καθώς το ΕΣΠΔ ή ο ΕΕΠΔ αναλαμβάνει πρωτοβουλίες και καθορίζει τις ενδεδειγμένες ενέργειες. Αυτός ο σεβασμός των καθιερωμένων ρόλων προωθεί τη συνοχή, αποτρέπει τον κανονιστικό κατακερματισμό και ενισχύει τη λογοδοσία των φορέων προστασίας δεδομένων στο πλαίσιο του εποπτικού τους ρόλου.

[11] Το ΕΣΠΔ και ο ΕΕΠΔ θεωρούν ότι το άρθρο 7 παράγραφος 2 της ισχύουσας πράξης για την κυβερνοασφάλεια, βάσει του οποίου υποχρεώνεται ο ENISA να συνεργάζεται σε επιχειρησιακό επίπεδο και να αναπτύσσει συνέργειες με τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, μεταξύ άλλων με τις εποπτικές αρχές που ασχολούνται με την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα, με σκοπό την αντιμετώπιση κοινών προβλημάτων, καλύπτει ήδη τον ΕΕΠΔ.

18. Σύμφωνα με τα άρθρα 10 και 11 της πρότασης ΚΚΑ2, τα οποία θα αποτελέσουν περαιτέρω ανάπτυξη του ισχύοντος άρθρου 7 της πράξης για την κυβερνοασφάλεια, ο ENISA θα επεκτείνει τον ρόλο του ως κεντρικού κόμβου επιχειρησιακής συνεργασίας, συμπεριλαμβανομένης της επεξεργασίας σημαντικού όγκου πληροφοριών σχετικά με απειλές[12]. Ως εκ τούτου, θα μπορούσε να συναχθεί το συμπέρασμα ότι οι πληροφορίες που θα επεξεργάζεται ο ENISA στο πλαίσιο του ρόλου του μπορούν να περιλαμβάνουν δεδομένα προσωπικού χαρακτήρα, όπως διευθύνσεις IP, διαπιστευτήρια χρήστη, αρχεία καταγραφής δραστηριότητας χρήστη, χρηματοοικονομικές συναλλαγές ή στοιχεία λογαριασμών που έχουν παραβιαστεί.

19. Μετά τις διευκρινίσεις που παρασχέθηκαν από την Ευρωπαϊκή Επιτροπή[13], το ΕΣΠΔ και ο ΕΕΠΔ κατανοούν ότι, στο πλαίσιο του ΚΚΑ2, δεν πρόκειται να ανατεθεί στον ENISA και να εγκριθεί μεγάλης κλίμακας επεξεργασία δεδομένων προσωπικού χαρακτήρα[14].

    Παρότι λαμβάνουν υπόψη το γεγονός ότι ο ENISA θα συλλέγει και θα επεξεργάζεται περαιτέρω κυρίως συγκεντρωτικά δεδομένα μη προσωπικού χαρακτήρα, το ΕΣΠΔ και ο ΕΕΠΔ υπενθυμίζουν ότι, εάν τα μελλοντικά καθήκοντα του ENISA ως κόμβου πληροφοριών απαιτούν σημαντικό βαθμό επεξεργασίας δεδομένων προσωπικού χαρακτήρα, αυτό θα πρέπει να αναφέρεται ρητά στις διατάξεις της βασικής πράξης που διέπει τα αντίστοιχα καθήκοντα, συμπεριλαμβανομένων των ουσιωδών στοιχείων κάθε επεξεργασίας μεγάλης κλίμακας και των κατάλληλων εγγυήσεων. Αντιστρόφως, εάν ο στόχος είναι να δοθεί στον ENISA η δυνατότητα να συλλέγει και να επεξεργάζεται περαιτέρω κυρίως συγκεντρωτικά δεδομένα μη προσωπικού χαρακτήρα, αυτό θα πρέπει επίσης να αποσαφηνιστεί, τουλάχιστον με αιτιολογική σκέψη.

20. Το ΕΣΠΔ και ο ΕΕΠΔ επισημαίνουν ότι ο ENISA θα συνεχίσει να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για διοικητικούς σκοπούς[15]. Το άρθρο 66 παράγραφος 1 της πρότασης ΚΚΑ2, ομοίως με τον ισχύοντα κανονισμό ΚΚΑ[16], περιέχει γενική αναφορά στην ισχύουσα νομοθεσία για την προστασία των δεδομένων, δηλαδή τον EUDPR, χωρίς να προβλέπει περαιτέρω ειδικούς κανόνες.

[12] Πρβλ. COM(2026) 11 final, νομοθετικό δημοσιονομικό και ψηφιακό δελτίο, σ. 23: «Τα νέα στοιχεία/καθήκοντα της πρότασης θα προσδώσουν προστιθέμενη αξία στους Ευρωπαίους συμφεροντούχους, οι οποίοι θα επωφεληθούν από το γεγονός ότι ο ENISA θα είναι κόμβος πληροφοριών, συμβάλλοντας στην ανταλλαγή πληροφοριών και κοινοποιώντας προειδοποιήσεις στις ομάδες ή τις οντότητες που εκπροσωπούν.» και σ. 109: «Τα τελευταία χρόνια ο ENISA έχει μετατραπεί σε κόμβο πληροφοριών, ο οποίος κατέχει πληροφορίες από διάφορες πηγές. Υπό την έννοια αυτή, πολλά από τα καθήκοντα του ENISA συνδέονται με την επαναχρησιμοποίηση και την ανακύκλωση πληροφοριών για τους σκοπούς διαφόρων αναλύσεων.».

[13] Οι οποίες παρασχέθηκαν κατά την ad hoc συνεδρίαση της υποομάδας εμπειρογνωμόνων σε θέματα τεχνολογίας του ΕΣΠΔ στις 27 Φεβρουαρίου 2026.

[14] Η Επιτροπή έχει διευκρινίσει ότι ο ENISA δεν έχει εντολή να διενεργεί επιχειρησιακή ανάλυση περιστατικών ούτε έχει πρόσβαση σε δεδομένα από τα ίδια τα περιστατικά. Αντιθέτως, τα δεδομένα που θα υποβάλλονται σε επεξεργασία θα είναι συγκεντρωτικά. Οι προειδοποιήσεις από τις εθνικές CSIRT συνήθως δεν περιλαμβάνουν επιχειρησιακά δεδομένα προσωπικού χαρακτήρα, αλλά διοικητικά δεδομένα, όπως στοιχεία επικοινωνίας. Στο ίδιο πνεύμα, οι εταιρείες που εγγράφονται για να λαμβάνουν έγκαιρες προειδοποιήσεις μπορεί επίσης να παρέχουν τα στοιχεία επικοινωνίας τους. Σύμφωνα με την Ευρωπαϊκή Επιτροπή, στη σπάνια περίπτωση που οι συγκεντρωτικές πληροφορίες για απειλές ή περιστατικά οι οποίες παρέχονται στον ENISA περιέχουν διευθύνσεις IP, ο ENISA δεν θα έχει επιχειρησιακή ανάγκη και, κατά συνέπεια, δεν θα έχει καμία νομική και πραγματική δυνατότητα έρευνας σχετικά με τον συνδρομητή που βρίσκεται πίσω από τη διεύθυνση IP. Η Ευρωπαϊκή Επιτροπή διευκρίνισε περαιτέρω ότι το γραφείο υποστήριξης που προβλέπεται στο άρθρο 13 έχει συμβουλευτικό χαρακτήρα και παρέχει, για παράδειγμα, πληροφορίες σχετικά με την αρμόδια αρχή του κράτους μέλους με την οποία πρέπει να υπάρξει επαφή.

[15] Για παράδειγμα, κατά τη διαδικασία εξέτασης αιτήσεων αδειοδότησης ως παρόχου βεβαιώσεων στο πλαίσιο του σχήματος ευρωπαϊκής ατομικής βεβαίωσης δεξιοτήτων κυβερνοασφάλειας (άρθρο 22), κατά τη διαδικασία προσφυγής κατά των αποφάσεων που λαμβάνονται (άρθρα 36 και επόμενα), κατά τη διεκπεραίωση καταγγελιών από φυσικά ή νομικά πρόσωπα σε σχέση με πιστοποίηση ή δηλώσεις συμμόρφωσης ΕΕ [άρθρο 88 παράγραφος 6 στοιχείο η)] ή σε σχέση με πιστοποιήσεις κυβερνοασφάλειας (άρθρο 96).

[16] Βλ. άρθρο 41 παράγραφος 1 του κανονισμού (ΕΕ) 2019/881.

21. Στο ίδιο πνεύμα, το άρθρο 66 παράγραφος 2 της πρότασης ΚΚΑ2 αναπαράγει το ισχύον άρθρο 41 παράγραφος 2 της ΚΚΑ, το οποίο προβλέπει τη δυνατότητα του διοικητικού συμβουλίου του ENISA να θεσπίζει «τις πρόσθετες διατάξεις που απαιτούνται για την εφαρμογή του κανονισμού (ΕΕ) 2018/1725» από τον Οργανισμό[17], χωρίς υποχρέωση του διοικητικού συμβουλίου να λαμβάνει συγκεκριμένα μέτρα. Η διάταξη του άρθρου 66 παράγραφος 2 της πρότασης ΚΚΑ2 δεν προσδιορίζει το πεδίο εφαρμογής και το είδος των εν λόγω πρόσθετων διατάξεων για την προστασία των δεδομένων ούτε την εφαρμοστέα διαδικασία θέσπισης. Επίσης, δεν διευκρινίζει τον ρόλο του ΕΕΠΔ στη διαδικασία[18].

22. Το ΕΣΠΔ και ο ΕΕΠΔ αντιλαμβάνονται ότι, εάν το διοικητικό συμβούλιο του ENISA προχωρήσει στην εφαρμογή του άρθρου 66 παράγραφος 2 της πρότασης ΚΚΑ2, οι αποφάσεις του θα πρέπει να περιλαμβάνουν επιπλέον λεπτομέρειες όσον αφορά τον τρόπο με τον οποίο διενεργεί την επεξεργασία δεδομένων προσωπικού χαρακτήρα ο ENISA.

23. Το ΕΣΠΔ και ο ΕΕΠΔ υπενθυμίζουν ότι, καταρχήν, μόνο οι πολύ τεχνικές (πρακτικές) λεπτομέρειες που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να αποφασίζονται στο πλαίσιο της διοικητικής αυτονομίας του οικείου φορέα της ΕΕ, στην προκειμένη περίπτωση, του διοικητικού συμβουλίου αποκεντρωμένου οργανισμού. Ο λόγος είναι ότι η έγκριση παρεμβάσεων στα θεμελιώδη δικαιώματα θα είναι καλύτερο να επαφίεται στον νομοθέτη και, το πολύ, στην Επιτροπή μέσω εκτελεστικών ή κατ' εξουσιοδότηση πράξεων[19]. Ως εκ τούτου, η ακριβής έννοια της φράσης στη δεύτερη περίοδο του σχεδίου άρθρου 66 παράγραφος 2 «τις πρόσθετες διατάξεις που απαιτούνται για την εφαρμογή του κανονισμού (ΕΕ) 2018/1725 από τον ENISA» θα πρέπει να αποσαφηνιστεί ρητά στο διατακτικό του κανονισμού.

24. Εάν, ωστόσο, κριθεί αναγκαίο το διοικητικό συμβούλιο να θεσπίσει διατάξεις οι οποίες υπερβαίνουν τις τεχνικές (πρακτικές) λεπτομέρειες της επεξεργασίας που προβλέπονται ήδη στη νομοθεσία ή σε κατ' εξουσιοδότηση ή εκτελεστικές πράξεις, πέραν του σαφέστερου καθορισμού του πεδίου εφαρμογής τους, οι διατάξεις που θα θεσπίσει το διοικητικό συμβούλιο θα πρέπει να είναι σαφείς και ακριβείς και η εφαρμογή τους θα πρέπει να είναι προβλέψιμη για τα ενδιαφερόμενα πρόσωπα. Αυτό περιλαμβάνει την κατάλληλη δημοσιοποίηση των σχετικών κανόνων. Επιπλέον, οι διατάξεις θα πρέπει να προβλέπουν τις αναγκαίες εγγυήσεις για τη διασφάλιση της συμμόρφωσης με τις βασικές αρχές και εγγυήσεις προστασίας των δεδομένων, όπως ο περιορισμός του σκοπού, ο περιορισμός της περιόδου αποθήκευσης και η προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού. Επίσης, ως σημαντική πρόσθετη εγγύηση σε τέτοιες περιπτώσεις, το ΕΣΠΔ και ο ΕΕΠΔ συνιστούν να προβλεφθεί στο άρθρο 66 της πρότασης ΚΚΑ2 να ζητείται η γνώμη του ΕΕΠΔ πριν από τη θέσπιση των εν λόγω κανόνων[20].

[17] Στις 21 Νοεμβρίου 2019 το διοικητικό συμβούλιο του ENISA εξέδωσε απόφαση σχετικά με τους εσωτερικούς κανόνες που αφορούν περιορισμούς ορισμένων δικαιωμάτων των υποκειμένων των δεδομένων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της λειτουργίας του ENISA, σύμφωνα με το άρθρο 25 του EUDPR.

[18] Για παράδειγμα, το άρθρο 18α παράγραφος 5 του κανονισμού (ΕΕ) 2016/794 (κανονισμός για την Ευρωπόλ) προβλέπει ότι το διοικητικό συμβούλιο της Ευρωπόλ, ενεργώντας κατόπιν πρότασης του εκτελεστικού διευθυντή και **έπειτα από διαβούλευση με τον ΕΕΠΔ**, διευκρινίζει τους όρους σχετικά με την παροχή και επεξεργασία δεδομένων προσωπικού χαρακτήρα [...] (η επισήμανση του συντάκτη).

[19] Βλ. ΕΕΠΔ «Guidance for co-legislators on key elements of legislative proposals» (Κατευθυντήριες γραμμές για τους συννομοθέτες σχετικά με τα βασικά στοιχεία των νομοθετικών προτάσεων), διατίθεται στη διεύθυνση https://www.edps.europa.eu/system/files/2025-05/EDPS_Publication_Guidance_for_co-legislators_EN.pdf, παράγραφος 76.

[20] Όπως προβλέπεται και στο άρθρο 18α παράγραφος 5 του κανονισμού (ΕΕ) 2016/794 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαΐου 2016, για τον Οργανισμό της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της Επιβολής του Νόμου (Ευρωπόλ) και την αντικατάσταση και κατάργηση των αποφάσεων του Συμβουλίου 2009/371/ΔΕΥ, 2009/934/ΔΕΥ, 2009/935/ΔΕΥ, 2009/936/ΔΕΥ και 2009/968/ΔΕΥ (κανονισμός για την Ευρωπόλ) (ΕΕ L 135 της 24.5.2016), σ. 53.

5 ΕΝΙΑΙΟ ΣΗΜΕΙΟ ΕΙΣΟΔΟΥ ΓΙΑ ΤΗΝ ΑΝΑΦΟΡΑ ΠΕΡΙΣΤΑΤΙΚΩΝ (ΑΡΘΡΟ 15 ΤΟΥ ΚΚΑ2)

25. Σύμφωνα με το άρθρο 15 της πρότασης ΚΚΑ2, ο ENISA πρέπει να δημιουργήσει, να παρέχει, να διαχειρίζεται, να συντηρεί και να επικαιροποιεί, ανάλογα με τις ανάγκες, μεταξύ άλλων, την ενιαία πλατφόρμα αναφοράς που θεσπίστηκε σύμφωνα με το άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2024/2847 και το ενιαίο σημείο εισόδου για την αναφορά περιστατικών που θεσπίστηκε σύμφωνα με το άρθρο 23α της οδηγίας (ΕΕ) 2022/2555. Τα εργαλεία αυτά αποσκοπούν στην απλούστευση των διαφόρων υποχρεώσεων αναφοράς που σχετίζονται με την κυβερνοασφάλεια[21].

26. Όπως δήλωσαν ήδη στην κοινή τους γνωμοδότηση σχετικά με την πρόταση της δέσμης μέτρων Omnibus για τον ψηφιακό τομέα[22], το ΕΣΠΔ και ο ΕΕΠΔ υποστηρίζουν επίσης σθεναρά τον στόχο της δημιουργίας ενιαίου σημείου εισόδου για την κοινοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα, καθώς θα μειώσει τον διοικητικό φόρτο για τους οργανισμούς χωρίς να επηρεάσει το επίπεδο προστασίας των υποκειμένων των δεδομένων. Στη δήλωση του Ελσίνκι του ΕΣΠΔ[23], το ΕΣΠΔ έχει ήδη υπογραμμίσει την υποστήριξή του σε μια πιθανή δικανονιστική ευρωπαϊκή λύση κοινοποίησης, καθώς αυτή θα συμβάλει στη διευκόλυνση της συμμόρφωσης με τον ΓΚΠΔ. Το ΕΣΠΔ και ο ΕΕΠΔ υπενθυμίζουν επίσης τη σημασία της κατοχύρωσης της ασφάλειας των κοινοποιήσεων που υποβάλλονται και διαβιβάζονται μέσω του ενιαίου σημείου εισόδου, καθώς οι κοινοποιήσεις παραβιάσεων δεδομένων συχνά περιλαμβάνουν ευαίσθητες πληροφορίες[24].

6 ΕΥΡΩΠΑΪΚΟ ΠΛΑΙΣΙΟ ΔΕΞΙΟΤΗΤΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ (ΕΠΔΚ) (ΑΡΘΡΟ 19 ΤΟΥ ΚΚΑ2)

[21] Βλ. άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2024/2847 και COM(2025) 837 final, σ. 8.
[22] EDPB-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus) [ΕΣΠΔ–ΕΕΠΔ Κοινή γνωμοδότηση 2/2026 σχετικά με την πρόταση κανονισμού όσον αφορά την απλούστευση του νομοθετικού πλαισίου για τον ψηφιακό τομέα (δέσμη μέτρων Omnibus για τον ψηφιακό τομέα), εκδόθηκε στις 10 Φεβρουαρίου 2026].
[23] ΕΣΠΔ, Η δήλωση του Ελσίνκι σχετικά με την ενίσχυση της σαφήνειας, της στήριξης και της δέσμευσης, Προσέγγιση της καινοτομίας και της ανταγωνιστικότητας με γνώμονα τα θεμελιώδη δικαιώματα, εγκρίθηκε στις 2 Ιουλίου 2025.
[24] Βλ. κεφάλαιο 8.3, EDPB-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus) [ΕΣΠΔ–ΕΕΠΔ Κοινή γνωμοδότηση 2/2026 σχετικά με την πρόταση κανονισμού όσον αφορά την απλούστευση του νομοθετικού πλαισίου για τον ψηφιακό τομέα (δέσμη μέτρων Omnibus για τον ψηφιακό τομέα), εκδόθηκε στις 10 Φεβρουαρίου 2026].

27. Σύμφωνα με το άρθρο 19 της πρότασης ΚΚΑ2, ο ENISA αναπτύσσει και δημοσιοποιεί ευρωπαϊκό πλαίσιο δεξιοτήτων κυβερνοασφάλειας (ΕΠΔΚ). Το ΕΠΔΚ θα συμβάλει στη διασφάλιση ότι οι επαγγελματίες, οι εργοδότες και οι πάροχοι κατάρτισης στον τομέα της κυβερνοασφάλειας, καθώς και οι δημόσιες αρχές, σε όλα τα κράτη μέλη, βασίζονται σε κοινή αντίληψη σχετικά με τις απαιτήσεις συγκεκριμένων θέσεων εργασίας στον τομέα της κυβερνοασφάλειας. Θα στηρίξει τα σαφή προφίλ εργασίας, τις διαφανείς απαιτήσεις προσόντων και την καλύτερη ευθυγράμμιση μεταξύ της εκπαίδευσης και των αναγκών της αγοράς εργασίας. Ο ENISA θα χρησιμοποιεί το ΕΠΔΚ ως βάση για την παροχή κατάρτισης, ιδίως όσον αφορά την υποστήριξη της εφαρμογής της ενωσιακής νομοθεσίας για την κυβερνοασφάλεια, της επιχειρησιακής συνεργασίας μεταξύ των κρατών μελών και των δραστηριοτήτων ευαισθητοποίησης. Αυτό σημαίνει ότι το ΕΠΔΚ λειτουργεί ως βάση για διαρθρωμένα προγράμματα κατάρτισης στον τομέα της κυβερνοασφάλειας, ιδίως για τις δημόσιες αρχές και τις οντότητες που καλύπτονται από τη νομοθεσία της ΕΕ για την κυβερνοασφάλεια.

28. Το ΕΣΠΔ και ο ΕΕΠΔ επικροτούν τον στόχο της ενίσχυσης του εργατικού δυναμικού της ΕΕ στον τομέα της κυβερνοασφάλειας και υπογραμμίζουν ότι η αύξηση της δυνατότητας μεταφοράς και αναγνώρισης των δεξιοτήτων σε διασυνοριακό επίπεδο είναι σημαντική για τη λειτουργία της ψηφιακής ενιαίας αγοράς.

29. Ταυτόχρονα, διαπιστώνουν ότι τα προφίλ που προσδιορίζονται στο άρθρο 19 παράγραφος 2 της πρότασης ΚΚΑ2 περιορίζονται επί του παρόντος σε επαγγελματίες του τομέα της κυβερνοασφάλειας. Η πρόταση δεν περιλαμβάνει προφίλ των απαραίτητων δεξιοτήτων για τους πολίτες, τους δημόσιους υπαλλήλους ή τα μη εξειδικευμένα μέλη του εργατικού δυναμικού. Όπως αναγνωρίζεται στην αιτιολογική σκέψη 21 της πρότασης ΚΚΑ2, ο ψηφιακός γραμματισμός είναι απαραίτητος για την ενδυνάμωση της ανθεκτικότητας των πολιτών, ωστόσο, σχεδόν το ήμισυ του ενήλικου πληθυσμού δεν διαθέτει βασικές ψηφιακές δεξιότητες, παρά το γεγονός ότι αυτές απαιτούνται σε πάνω από το 90 % των θέσεων εργασίας. Ως εκ τούτου, το ΕΠΔΚ θα πρέπει να περιλαμβάνει ένα προφίλ «κυβερνοασφάλειας για γενικούς υπαλλήλους», το οποίο θα καλύπτει τις ελάχιστες δεξιότητες που θα πρέπει να διαθέτει κάθε κάτοικος της ΕΕ σε ηλικία εργασίας για να αλληλεπιδρά με ασφάλεια εντός της ψηφιακής ενιαίας αγοράς, προστατεύοντας όχι μόνο τον εαυτό του αλλά και τον οργανισμό του και τους άλλους, ιδίως από το ηλεκτρονικό ψάρεμα με τη βοήθεια ΤΝ, τα προϊόντα βαθυπαραποίησης (deepfake), την πλαστοπροσωπία και τις επιθέσεις κοινωνικής μηχανικής. Το προφίλ αυτό θα μπορούσε να χρησιμοποιείται από δημόσιους ή ιδιωτικούς οργανισμούς για την κατάρτιση του προσωπικού τους, ώστε να ελαχιστοποιηθούν οι κίνδυνοι από τον ανθρώπινο παράγοντα και, κατά συνέπεια, να μειωθεί ο συνολικός κίνδυνος παραβιάσεων δεδομένων.

30. Το ΕΣΠΔ και ο ΕΕΠΔ επισημαίνουν ότι, στην αιτιολογική σκέψη 45 της πρότασης, γίνεται ρητή διάκριση μεταξύ του ΕΠΔΚ και του ευρωπαϊκού πλαισίου ψηφιακών ικανοτήτων (DigComp 3.0), καθώς διευκρινίζεται ότι το DigComp αφορά την καθημερινή ζωή, τη συμμετοχή στην κοινωνία, την εργασία και τη μάθηση, και μπορεί να χρησιμοποιηθεί τόσο από ενήλικες όσο και από παιδιά[25], ενώ το ΕΠΔΚ απευθύνεται σε εξειδικευμένο κοινό, αποτελώντας ένα απλό πλαίσιο που προσδιορίζει τους ρόλους κυβερνοασφάλειας και τα συναφή καθήκοντα, τις γνώσεις και τις δεξιότητες που απαιτούνται για την εκτέλεσή τους.

[25] Το ΕΣΠΔ και ο ΕΕΠΔ υπενθυμίζουν ακόμη ότι, μεταξύ του 2022 και του 2024, η Ευρωπαϊκή Επιτροπή διερεύνησε τις δυνατότητες ανάπτυξης ευρωπαϊκού πιστοποιητικού ψηφιακών δεξιοτήτων (EDSC), με βάση το DigComp. Το πιστοποιητικό θα μπορούσε να συμβάλει στη γρήγορη και εύκολη αναγνώριση των ψηφιακών δεξιοτήτων των ατόμων από τους εργοδότες, τους παρόχους κατάρτισης και άλλους. Η πρωτοβουλία αυτή είχε ως στόχο να προσφέρει ένα σήμα ποιότητας για την πιστοποίηση

31. Το ΕΣΠΔ και ο ΕΕΠΔ υποστηρίζουν όλες τις προαναφερθείσες πρωτοβουλίες, είτε εκτελούνται από τον ENISA είτε, στην περίπτωση του DigComp, από το Κοινό Κέντρο Ερευνών (JRC) της Ευρωπαϊκής Επιτροπής, καθώς θα μειώσουν τον κίνδυνο παραβιάσεων δεδομένων, υπό την προϋπόθεση ότι θα υιοθετηθούν επαρκώς. Ως εκ τούτου, ενθαρρύνουν όλα τα μέρη που συμμετέχουν να διερευνήσουν τρόπους για την αύξηση του αντικτύπου των πλαισίων.

32. Ταυτόχρονα, το ΕΣΠΔ και ο ΕΕΠΔ θεωρούν ότι το DigComp δεν υποκαθιστά ένα ειδικό πρόγραμμα κυβερνοασφάλειας για γενικούς υπαλλήλους [26] και συνιστούν στους συννομοθέτες να τροποποιήσουν το άρθρο 19 παράγραφος 2 της πρότασης ΚΚΑ2, ώστε το ΕΠΔΚ να μην περιορίζεται αποκλειστικά στους «επαγγελματίες στον τομέα της κυβερνοασφάλειας», αλλά να περιλαμβάνει και προφίλ για το εργατικό δυναμικό εν γένει ή για τους πολίτες. Αυτό θα πρέπει να συνοδευθεί από αντίστοιχη τροποποίηση της αιτιολογικής σκέψης 45.

33. Επιπλέον, το ΕΣΠΔ και ο ΕΕΠΔ θεωρούν ότι απαιτείται να ενσωματωθεί στα επαγγελματικά προφίλ του ΕΠΔΚ ενότητα σχετικά με την ανάγκη διασφάλισης της συμμόρφωσης των μέτρων κυβερνοασφάλειας με τη νομοθεσία της ΕΕ για την προστασία των δεδομένων, ιδίως όσον αφορά την πρακτική εφαρμογή της αρχής της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού (άρθρο 25 του ΓΚΠΔ), και καλούν τον συννομοθέτη να προσθέσει αιτιολογική σκέψη για τον σκοπό αυτόν.

7 ΕΥΡΩΠΑΪΚΟ ΠΛΑΙΣΙΟ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ (ΤΙΤΛΟΣ ΙΙΙ)

34. Το άρθρο 71 και το άρθρο 80 παράγραφος 1 στοιχείο κγ) της πρότασης ΚΚΑ2 ρυθμίζουν το πεδίο εφαρμογής της πιστοποίησης της κυβερνοασφάλειας. Το άρθρο 80 παράγραφος 1 στοιχείο κγ) προσθέτει, ως στόχο ασφάλειας για κάθε ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας, να «διασφαλίζει ότι η οντότητα είναι σε θέση να εγγυάται την ασφάλεια της επεξεργασίας δεδομένων προσωπικού χαρακτήρα».

των ψηφιακών δεξιοτήτων σε ολόκληρη την Ευρώπη. Κατόπιν μελέτης σκοπιμότητας {βλ. CENTENO, C., COSGROVE, J., CACHIA, R., MORA, T., DI LEGGE, A., VIVARELLI, S., BULIAN, G., MOYES PRELLEZO, N., PIÑA DE SANTISTEBAN, P., SCHULZ, C., HÜSING, T., CUARTAS-ACOSTA, A. και TROIA, S., European Digital Skills Certificate (EDSC) Feasibility Study [Μελέτη σκοπιμότητας σχετικά με το ευρωπαϊκό πιστοποιητικό ψηφιακών δεξιοτήτων (EDSC)], Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης, Λουξεμβούργο, 2024, doi:10.2760/958195, JRC138344, https://publications.jrc.ec.europa.eu/repository/handle/JRC138344} και πιλοτικού έργου με τη συμμετοχή διαφόρων χωρών της ΕΕ, η Ευρωπαϊκή Επιτροπή κατέληξε στο συμπέρασμα ότι αυτό το σήμα ποιότητας δεν θα προσέφερε επαρκή προστιθέμενη αξία στους Ευρωπαίους πολίτες. Ωστόσο, το DigComp, το οποίο δημοσιεύθηκε για πρώτη φορά το 2013, εξακολουθεί να υπάρχει [COSGROVE, J. και CACHIA, R., DigComp 3.0: European Digital Competence Framework (DigComp 3.0: Ευρωπαϊκό πλαίσιο ψηφιακών ικανοτήτων) — Πέμπτη έκδοση, Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης, Λουξεμβούργο, 2025, https://data.europa.eu/doi/10.2760/0001149, JRC144121]. Περιγράφει τα απαιτούμενα για να διαθέτει κανείς ψηφιακή ικανότητα στη σημερινή κοινωνία και στηρίζει την ανάπτυξη ψηφιακών ικανοτήτων σε άτομα όλων των ηλικιών. Καλύπτει ευρύ φάσμα επιπέδων δεξιοτήτων, από βασικές έως εξαιρετικά προηγμένες. Αρκετές ικανότητες του DigComp αναφέρονται ρητά στην κυβερνοασφάλεια, όπως 4.1 Προστασία συσκευών, 4.2 Προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής και ακόμα 4.4 Προστασία του περιβάλλοντος (πρόληψη της διαρροής δεδομένων από απορριπτόμενο εξοπλισμό). Άλλοι τομείς αφορούν επίσης τις σχετικές δεξιότητες, οι οποίες περιλαμβάνουν τις δεξιότητες του τομέα 1 που είναι ζωτικής σημασίας για την άμυνα έναντι της κοινωνικής μηχανικής, μειώνουν τους κινδύνους απειλών εκ των έσω στον τομέα 2 και αποτρέπουν την τυχαία δημοσιοποίηση πληροφοριών, ενώ βελτιώνουν την ταχύτητα εντοπισμού περιστατικών στον τομέα 5.

[26] Στο DigComp, το περιεχόμενο για την ασφάλεια εκτείνεται σε 21 ικανότητες, δεν διαθέτει σαφή μοντέλα απειλών, δεν βασίζει τη λειτουργία σε οργανωτικούς κινδύνους για την ασφάλεια, δεν χαρτογραφεί άμεσα τις υποχρεώσεις συμμόρφωσης. Παρότι το ΕΠΔΚ στην τρέχουσα μορφή του θα μπορούσε να εφαμοστεί στις δεξιότητες των επαγγελματιών στον τομέα της κυβερνοασφάλειας, δεν υπάρχει διαρθρωμένο πλαίσιο σε επίπεδο ΕΕ για τους εργαζομένους εκτός του τομέα της κυβερνοασφάλειας. Το ΕΣΠΔ και ο ΕΕΠΔ υπενθυμίζουν ότι οι περισσότερες παραβιάσεις προέρχονται από το ηλεκτρονικό ψάρεμα, την κοινωνική μηχανική, την κατάχρηση διαπιστευτηρίων, την εσφαλμένη παραμετροποίηση και τη χρήση «σκιώδους ΤΠ», συμπεριφορές οι οποίες σχετίζονται με γενικούς υπαλλήλους. Ένα πλαίσιο κυβερνοασφάλειας για γενικούς υπαλλήλους θα μπορούσε να καταστήσει σαφείς τους κινδύνους, να θέσει προσδοκίες ανάλογες με τους ρόλους (π.χ. για τους ανθρώπινους πόρους, τα οικονομικά) και να στηρίξει την επίτευξη μετρήσιμων αποτελεσμάτων.

35. Το ΕΣΠΔ και ο ΕΕΠΔ επισημαίνουν ότι η διατύπωση του άρθρου 80 παράγραφος 1 στοιχείο κγ) της πρότασης ΚΚΑ2 προσεγγίζει πολύ τις απαιτήσεις του ΓΚΠΔ για την ασφάλεια της επεξεργασίας[27]. Υπό την έννοια αυτή, θα μπορούσε να εκληφθεί ότι το πεδίο εφαρμογής του νέου σχήματος πιστοποίησης περιλαμβάνει απαιτήσεις βάσει του ΓΚΠΔ. Ωστόσο, το νομικό και το επιχειρησιακό πεδίο εφαρμογής δεν είναι απολύτως σαφή, καθώς η διάταξη δεν παραπέμπει σε διατάξεις του ΓΚΠΔ [π.χ. άρθρο 5 παράγραφος 1 στοιχείο στ), άρθρο 32, άρθρο 25 του ΓΚΠΔ] και περιλαμβάνεται σε κατάλογο «στόχων ασφάλειας» (άρθρο 80 παράγραφος 1 πρώτη περίοδος).

36. Το ΕΣΠΔ και ο ΕΕΠΔ υπενθυμίζουν ότι η ασφάλεια βάσει του ΓΚΠΔ σχετίζεται με κινδύνους για τα θεμελιώδη δικαιώματα και τις ελευθερίες των προσώπων. Παρότι ο νομικός ορισμός της κυβερνοασφάλειας βάσει του δικαίου της Ένωσης περιλαμβάνει γενικά την προστασία των χρηστών και άλλων προσώπων[28], το πεδίο εφαρμογής των μέτρων κυβερνοασφάλειας περιλαμβάνει συνήθως κινδύνους κάθε είδους για τον οικείο οργανισμό. Ωστόσο, υπάρχει η ευκαιρία να δημιουργηθούν συνέργειες ώστε να μπορέσει να ενσωματωθεί στην εκτίμηση κινδύνου η προστασία των δικαιωμάτων και των ελευθεριών των προσώπων.

37. Το ΕΣΠΔ και ο ΕΕΠΔ υπενθυμίζουν ακόμα ότι ο ΓΚΠΔ διαθέτει δικό του μηχανισμό πιστοποίησης (άρθρα 42-43 του ΓΚΠΔ) και θεωρούν ότι η πιστοποίηση της κυβερνοασφάλειας είναι διαφορετική από την πιστοποίηση της προστασίας των δεδομένων σύμφωνα με το άρθρο 42 του ΓΚΠΔ.

38. Παρά ταύτα, το ΕΣΠΔ και ο ΕΕΠΔ θεωρούν ότι μπορούν να υπάρξουν συνέργειες μεταξύ της πιστοποίησης της κυβερνοασφάλειας και της πιστοποίησης της προστασίας των δεδομένων. Για παράδειγμα, η πιστοποίηση βάσει του ΚΚΑ2 θα μπορούσε να χρησιμοποιηθεί ως στοιχείο για να αποδειχθεί ότι πληρούνται ορισμένες απαιτήσεις της πιστοποίησης βάσει του ΓΚΠΔ, όσον αφορά την κυβερνοασφάλεια. Ωστόσο, το ΕΣΠΔ και ο ΕΕΠΔ επισημαίνουν ότι, στο άρθρο 80 παράγραφος 1 στοιχείο κγ) της πρότασης ΚΚΑ2, δεν διατυπώνεται με σαφήνεια η σχέση με την πιστοποίηση βάσει των άρθρων 42-43 του ΓΚΠΔ. Για λόγους ασφάλειας δικαίου, το ΕΣΠΔ και ο ΕΕΠΔ συνιστούν να αποσαφηνιστεί περαιτέρω το πεδίο εφαρμογής του άρθρου 80 παράγραφος 1 στοιχείο κγ) του ΚΚΑ2 και η σχέση με την πιστοποίηση βάσει του ΓΚΠΔ. Επιπλέον, το ΕΣΠΔ και ο ΕΕΠΔ συνιστούν να απαιτείται από τον ENISA να διαβουλεύεται με το ΕΣΠΔ πριν από την έγκριση σχημάτων πιστοποίησης βάσει του άρθρου 80 παράγραφος 1 στοιχείο κγ) του ΚΚΑ2, ώστε να διασφαλίζεται η συνοχή.

[27] Βλ. άρθρο 5 παράγραφος 1 στοιχείο στ) και άρθρο 32 του ΓΚΠΔ.

28 Βλ. άρθρο 2 σημείο 1) της πρότασης ΚΚΑ2, το οποίο αποτελεί διάταξη που έχει διατηρηθεί από προηγούμενη νομοθεσία και έχει ως εξής: «κυβερνοασφάλεια»: οι δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων προσώπων που επηρεάζονται από κυβερνοαπειλές.

39. Το ΕΣΠΔ και ο ΕΕΠΔ τονίζουν την ανάγκη για εξέταση όχι μόνο της αποτελεσματικότητας των μέτρων κυβερνοασφάλειας, αλλά και της αναγκαιότητας και της αναλογικότητάς τους. Από ορισμένους ελέγχους κυβερνοασφάλειας, προκύπτουν συγκεκριμένοι κίνδυνοι για την προστασία των δεδομένων. Αυτό μπορεί να συμβαίνει κατά την παρακολούθηση και την καταγραφή, τον έλεγχο πακέτων σε βάθος ή την ανάλυση της συμπεριφοράς των χρηστών. Ένα καλά σχεδιασμένο σχήμα πιστοποίησης για την ασφάλεια της επεξεργασίας θα μπορούσε να περιλαμβάνει ελέγχους με τους οποίους θα διασφαλίζεται ότι τα μέτρα ασφάλειας μπορούν να εφαρμόζονται κατά τρόπο σύμφωνο με τους κανόνες προστασίας των δεδομένων (π.χ. ορισμένες πτυχές θα πρέπει να είναι προσαρμόσιμες· αυτό θα μπορούσε να ισχύει, για παράδειγμα, στην περίπτωση του βαθμού λεπτομέρειας των δεδομένων που καταγράφονται για σκοπούς ασφάλειας —καθώς αυτό μπορεί να καταστήσει δυνατή ή να διευκολύνει τη συμμόρφωση του υπευθύνου επεξεργασίας με τις αρχές ασφάλειας και ελαχιστοποίησης των δεδομένων του ΓΚΠΔ· στο ίδιο πνεύμα, οι περίοδοι αποθήκευσης θα πρέπει να είναι προσαρμόσιμες, ώστε ο υπεύθυνος επεξεργασίας να μπορεί να αποφασίζει, στο πλαίσιο της επεξεργασίας που πραγματοποιεί, για πόσο χρονικό διάστημα θα πρέπει να διατηρηθούν τα δεδομένα προσωπικού χαρακτήρα προτού διαγραφούν ή ανωνυμοποιηθούν με τη χρήση πιστοποιημένων τεχνικών).

40. Ως εκ τούτου, το ΕΣΠΔ και ο ΕΕΠΔ συνιστούν να επεξηγηθεί σε αιτιολογική σκέψη ότι τα σχήματα πιστοποίησης θα πρέπει, στο μέτρο του δυνατού, να σχεδιάζονται, να εφαρμόζονται και να τηρούνται κατά τρόπον ώστε να λαμβάνουν υπόψη τους ελέγχους ασφάλειας οι οποίοι μπορούν να βοηθήσουν να αποδειχθεί η εκπλήρωση των απαιτήσεων του ΓΚΠΔ, όταν τα σχήματα εφαρμόζονται σε προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας που είναι πιθανό να χρησιμοποιηθούν σε πράξεις επεξεργασίας δεδομένων. Θα πρέπει επίσης να σημειωθεί ότι ορισμένοι έλεγχοι μπορούν να αποτελέσουν παράγοντες διευκόλυνσης της προστασίας της ιδιωτικής ζωής και των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού.

8 ΠΛΑΙΣΙΟ ΓΙΑ ΑΞΙΟΠΙΣΤΕΣ ΑΛΥΣΙΔΕΣ ΕΦΟΔΙΑΣΜΟΥ ΤΠΕ (ΤΙΤΛΟΣ IV)

41. Με την πρόταση ΚΚΑ2, προστίθενται μέτρα για την ασφάλεια των αλυσίδων εφοδιασμού ΤΠΕ, με σκοπό ιδίως την αντιμετώπιση μη τεχνικών κινδύνων, όπως οι γεωπολιτικοί, νομικοί και ιδιοκτησιακοί παράγοντες, καθώς και οι παράγοντες εξάρτησης και στρατηγικών παρεμβάσεων, που επηρεάζουν τις αλυσίδες εφοδιασμού ΤΠΕ σε τομείς υψηλής κρισιμότητας και άλλους κρίσιμους τομείς. Μολονότι τα εν λόγω μέτρα ασφάλειας της αλυσίδας εφοδιασμού αποσκοπούν πρωτίστως στην αντιμετώπιση κινδύνων που δεν σχετίζονται άμεσα με την προστασία των δεδομένων, μπορούν επίσης να έχουν ευεργετικό αντίκτυπο στην προστασία των θεμελιωδών δικαιωμάτων, περιορίζοντας τις εξωτερικές παρεμβάσεις σε δεδομένα των υποκειμένων δεδομένων της ΕΕ μέσω δραστηριοτήτων όπως η κατασκοπεία και η παρακολούθηση.

42. Το ΕΣΠΔ και ο ΕΕΠΔ επικροτούν το προτεινόμενο μέτρο που αποσκοπεί στην εξασφάλιση πλαισίου για αξιόπιστες αλυσίδες εφοδιασμού ΤΠΕ και στην αντιμετώπιση των μη τεχνικών κινδύνων σε τομείς υψηλής κρισιμότητας.

9 ΠΡΟΣΘΕΤΕΣ ΒΑΣΙΚΕΣ ΟΝΤΟΤΗΤΕΣ ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ ΓΙΑ ΤΗ NIS 2

43. Με την πρόταση για τροποποίηση της οδηγίας NIS 2, θα συμπεριληφθούν οι πάροχοι ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας και ευρωπαϊκών πορτοφολιών επιχειρήσεων, ανεξαρτήτως μεγέθους, στις «βασικές οντότητες». Οι οντότητες που ταξινομούνται ως «βασικές» υπόκεινται πλήρως στις υποχρεώσεις διαχείρισης κινδύνων κυβερνοασφάλειας που ορίζονται στη NIS 2 και πρέπει να εφαρμόζουν τα μέτρα ασφάλειας που απαιτούνται βάσει του άρθρου 21 της NIS 2, συμπεριλαμβανομένων των πολιτικών για την ανάλυση κινδύνου και την ασφάλεια, του χειρισμού περιστατικών, της επιχειρησιακής συνέχειας και της διαχείρισης κρίσεων, της ασφάλειας της αλυσίδας εφοδιασμού, του χειρισμού ευπαθειών, των πολιτικών για την κρυπτογραφία και την κρυπτογράφηση, καθώς και του ελέγχου πρόσβασης και της διαχείρισης πάγιων στοιχείων.

44. Το ΕΣΠΔ και ο ΕΕΠΔ εκφράζουν την ικανοποίησή τους για τον ορισμό των παρόχων ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας και ευρωπαϊκών πορτοφολιών επιχειρήσεων ως «βασικών οντοτήτων». Το ΕΣΠΔ και ο ΕΕΠΔ θεωρούν ότι τα πορτοφόλια ψηφιακής ταυτότητας αποτελούν βασική συνιστώσα των ψηφιακών υποδομών της ΕΕ, συνεπώς, τα περιστατικά που τα επηρεάζουν μπορούν να έχουν ευρύ διασυνοριακό αντίκτυπο. Υποστηρίζουν την ασφαλή ταυτοποίηση, την επαλήθευση ταυτότητας και τις ηλεκτρονικές βεβαιώσεις. Όσον αφορά την ψηφιακή οικονομία, τα πορτοφόλια επιχειρήσεων είναι εξίσου κρίσιμα με τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας. Κατά συνέπεια, και τα δύο είδη παρόχων πορτοφολιών αντιμετωπίζονται ομοίως με τους παρόχους υπηρεσιών εμπιστοσύνης, οι οποίοι έχουν ήδη οριστεί ως «βασικές οντότητες» στο πλαίσιο της NIS 2, και άλλους φορείς εκμετάλλευσης εξαιρετικά κρίσιμων υποδομών.

10 ΣΥΛΛΟΓΗ ΔΕΔΟΜΕΝΩΝ ΣΧΕΤΙΚΑ ΜΕ ΕΠΙΘΕΣΕΙΣ ΛΥΤΡΙΣΜΙΚΟΥ

45. Σύμφωνα με το άρθρο 5 σημείο 8) της πρότασης τροποποίησης της NIS 2, με το οποίο προτείνεται η προσθήκη των νέων παραγράφων 12 και 13 στο άρθρο 23 της NIS 2, σε περίπτωση επίθεσης λυτρισμικού, μπορεί να ζητηθεί από τις ενδιαφερόμενες οντότητες να υποβάλουν ορισμένες πληροφορίες σχετικά με τα περιστατικά λυτρισμικού στις ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT), μεταξύ άλλων αν μια οντότητα έχει καταβάλει λύτρα και, εάν ναι, τι ποσό και σε ποιον (κρυπτοστοιχεία / πάροχοι υπηρεσιών) και την ταυτότητα του προσώπου που ενεργεί ως σημείο επαφής.

46. Σύμφωνα με το άρθρο 23 παράγραφος 11 της NIS 2, ανατίθεται στην Επιτροπή η εξουσία να εκδίδει εκτελεστικές πράξεις για τον περαιτέρω προσδιορισμό του είδους των πληροφοριών, του μορφότυπου και της διαδικασίας των υποχρεώσεων αναφοράς. Το πεδίο εφαρμογής της εν λόγω εκτελεστικής πράξης θα επεκταθεί ώστε να καλύπτει επίσης τις νέες υποχρεώσεις αναφοράς σε περίπτωση επιθέσεων λυτρισμικού.

47. Το ΕΣΠΔ και ο ΕΕΠΔ υποστηρίζουν πλήρως τον σημαντικό στόχο της πρόληψης μελλοντικών επιθέσεων λυτρισμικού και της παρεμπόδισης και εξάρθρωσης των εγκληματικών οργανώσεων που βρίσκονται πίσω από αυτές. Το ΕΣΠΔ και ο ΕΕΠΔ επισημαίνουν ότι οι πληροφορίες που πρέπει να ανταλλάσσονται σχετικά με επιθέσεις λυτρισμικού θα μπορούσαν να είναι δυνητικά ευαίσθητου χαρακτήρα, όπως εξηγεί περαιτέρω η Επιτροπή στην αιτιολογική σκέψη 10 της πρότασης τροποποίησης της NIS 2. Επιπλέον, η εν λόγω αναφορά μπορεί να συνεπάγεται την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Το ΕΣΠΔ και ο ΕΕΠΔ εκφράζουν την ικανοποίησή τους για την κλιμακωτή προσέγγιση που επιλέχθηκε στις παραγράφους 12 και 13, σύμφωνα με την οποία οι πιο ευαίσθητες πληροφορίες της παραγράφου 13 θα αναφέρονται μόνο κατόπιν αιτήματος.

48. Ταυτόχρονα, λόγω του ευαίσθητου χαρακτήρα των αναφερόμενων δεδομένων και σύμφωνα με τις αρχές της αναγκαιότητας και της αναλογικότητας, σε περίπτωση που η αναφορά επιθέσεων λυτρισμικού περιλαμβάνει την επεξεργασία δεδομένων προσωπικού χαρακτήρα, το ΕΣΠΔ και ο ΕΕΠΔ συνιστούν να προσδιορίζονται στην εκτελεστική πράξη δυνάμει του άρθρου 23 παράγραφος 11 της οδηγίας NIS2 οι εφαρμοστέες εγγυήσεις για την προστασία των δεδομένων. Στο πλαίσιο αυτό, υπενθυμίζουν επίσης την απαίτηση να διαβουλεύεται η Επιτροπή με τον ΕΕΠΔ, σύμφωνα με το άρθρο 42 παράγραφος 1 του EUDPR, σχετικά με τα σχέδια εκτελεστικών και κατ' εξουσιοδότηση πράξεων όταν υπάρχει αντίκτυπος στην προστασία των δικαιωμάτων και των ελευθεριών των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.