ΑΝΑΛΥΣΗ ΣΥΝΕΠΕΙΩΝ ΡΥΘΜΙΣΗΣ

ΤΙΤΛΟΣ ΑΞΙΟΛΟΓΟΥΜΕΝΗΣ ΡΥΘΜΙΣΗΣ

ΣΧΕΔΙΟ ΝΟΜΟΥ ΤΟΥ ΥΠΟΥΡΓΕΙΟΥ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΜΕ ΤΙΤΛΟ Ενσωμάτωση της Οδηγίας (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) 910/2014 και της Οδηγίας (ΕΕ) 2018/1972, και την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS 2) και άλλες διατάξεις

Επισπεύδον Υπουργείο: Υπουργείο Ψηφιακής Διακυβέρνησης
Στοιχεία επικοινωνίας: Βασιλική Βλάχου, νομική σύμβουλος Υπουργού Ψηφιακής Διακυβέρνησης,210 9098601, email: v.vlachou@mindigital.gr

Επιλέξατε από τον παρακάτω κατάλογο τον τομέα ή τους τομείς νομοθέτησης στους οποίους αφορούν οι βασικές διατάξεις της αξιολογούμενης ρύθμισης:

ΤΟΜΕΙΣ ΝΟΜΟΘΕΤΗΣΗΣ	(X)
ΕΚΠΑΙΔΕΥΣΗ - ΠΟΛΙΤΙΣΜΟΣ[1]	
ΕΘΝΙΚΗ ΑΜΥΝΑ – ΕΞΩΤΕΡΙΚΗ ΠΟΛΙΤΙΚΗ[2]	
ΟΙΚΟΝΟΜΙΚΗ / ΔΗΜΟΣΙΟΝΟΜΙΚΗ / ΦΟΡΟΛΟΓΙΚΗ ΠΟΛΙΤΙΚΗ[3]	
ΚΟΙΝΩΝΙΚΗ ΠΟΛΙΤΙΚΗ[4]	
ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ – ΔΗΜΟΣΙΑ ΤΑΞΗ – ΔΙΚΑΙΟΣΥΝΗ[5]	X
ΑΝΑΠΤΥΞΗ – ΕΠΕΝΔΥΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ[6]	X

[1] Τομέας νομοθέτησης επί θεμάτων Υπουργείου Παιδείας, Θρησκευμάτων και Αθλητισμού και Υπουργείου Πολιτισμού.

[2] Τομέας νομοθέτησης επί θεμάτων Υπουργείου Εθνικής Άμυνας και Υπουργείου Εξωτερικών.

[3] Τομέας νομοθέτησης επί θεμάτων Υπουργείου Εθνικής Οικονομίας και Οικονομικών.

[4] Τομέας νομοθέτησης επί θεμάτων Υπουργείου Εργασίας και Κοινωνικής Ασφάλισης και Υπουργείου Υγείας.

[5] Τομέας νομοθέτησης επί θεμάτων Υπουργείου Εσωτερικών, Υπουργείου Ψηφιακής Διακυβέρνησης, Υπουργείου Προστασίας του Πολίτη και Υπουργείου Δικαιοσύνης.

[6] Τομέας νομοθέτησης επί θεμάτων Υπουργείου Ανάπτυξης, Υπουργείου Περιβάλλοντος και Ενέργειας, Υπουργείου Υποδομών και Μεταφορών, Υπουργείου Ναυτιλίας και Νησιωτικής Πολιτικής, Υπουργείου Αγροτικής Ανάπτυξης και Τροφίμων και Υπουργείου Τουρισμού.

Α. Αιτιολογική έκθεση

	Η «ταυτότητα» της αξιολογούμενης ρύθμισης
1.	Ποιο ζήτημα αντιμετωπίζει η αξιολογούμενη ρύθμιση;
	Με το προτεινόμενο σχέδιο νόμου εναρμονίζεται το εθνικό δίκαιο με την 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) 910/2014 και της Οοδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 (στο εξής «Οδηγία NIS 2» ή «Οδηγία», L 333) ενσωματώνοντας την οδηγία αυτή στην ελληνική εννομη τάξη. Η Οδηγία NIS 2, η οποία καταργεί την Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (στο εξής «Οδηγία NIS 1», L 194), επικαιροποιεί και διευρύνει σημαντικά τις υποχρεώσεις για την ασφάλεια και τη διαχείριση κινδύνων στον κυβερνοχώρο σε ολόκληρη την Ευρωπαϊκή Ένωση. Εισάγει μια ολοκληρωμένη προσέγγιση κυβερνοασφάλειας με βάση τον κίνδυνο, με στόχο την επίτευξη υψηλού κοινού επιπέδου ασφάλειας στον κυβερνοχώρο σε όλα τα κράτη μέλη, ενισχύοντας τη λειτουργία της εσωτερικής αγοράς μέσω βελτιωμένων πρωτοκόλλων ασφαλείας και δυνατοτήτων αντιμετώπισης περιστατικών. Δεδομένης της εντατικοποίησης και της αυξημένης πολυπλοκότητας των απειλών και των κυβερνοεπιθέσεων, ο αριθμός, το μέγεθος, η επινοητικότητα, η συχνότητα και ο αντίκτυπος των περιστατικών στον κυβερνοχώρο αυξάνονται και συνιστούν μείζονα απειλή για τη λειτουργία των συστημάτων δικτύου και πληροφοριών. Το γεγονός αυτό επηρεάζει τη λειτουργία υποδομών ζωτικής σημασίας, η οποία βασίζεται σε πληροφοριακά συστήματα και συχνά διαταράσσει την παροχή κρίσιμων υπηρεσιών για την οικονομική και κοινωνική ζωή. Παράλληλα, το κόστος του κυβερνοεγκλήματος διαρκώς αυξάνεται, ξεπερνώντας σε παγκόσμιο επίπεδο τα δέκα τρισεκατομμύρια δολάρια για το έτος 2023, γεγονός που επηρεάζει αρνητικά την εμπιστοσύνη των πολιτών στην ψηφιακή μετάβαση συνολικά. Την ίδια στιγμή, σειρά ατομικών δικαιωμάτων βρίσκονται αντιμέτωπα με νέες και σύνθετες απειλές στον κυβερνοχώρο. Το προτεινόμενο σχέδιο νόμου καλύπτει κενά, τα οποία διαπιστώθηκαν κατά την περίοδο εφαρμογής της Οδηγίας NIS 1, η οποία μεταφέρθηκε στην ελληνική έννομη τάξη με τον ν. 4577/2018 (Α’ 199), τόσο στον καθορισμό μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας και υποχρεώσεων αναφοράς περιστατικών σε όλους τους διευρυμένους τομείς τους οποίους καλύπτει, όπως η ενέργεια, οι μεταφορές, η υγεία, η δημόσια διοίκηση, η εφοδιαστική αλυσίδα, η παραγωγή τροφίμων, οι τηλεπικοινωνίες και οι ψηφιακές υποδομές κ.ά., όσο και στην ομοιόμορφη αντιμετώπιση των σχετικών ζητημάτων στο σύνολο των κρατών μελών της Ευρωπαϊκής Ένωσης.

	Σε μία εποχή αυξημένης αξιοποίησης των Τεχνολογιών Πληροφορικής και Επικοινωνιών για τον ιδιωτικό τομέα και συνεχιζόμενου ψηφιακού μετασχηματισμού για τον δημόσιο τομέα, η βελτίωση των ικανοτήτων και η ενίσχυση της ανθεκτικότητας του ψηφιακού κράτους και της κρίσιμης ψηφιακής υποδομής που υποστηρίζει την παροχή υπηρεσιών ιδιωτικών επιχειρήσεων, σε σημαντικούς τομείς για την κοινωνική και οικονομική ζωή της χώρας, αποτελούν επιτακτική ανάγκη για την αδιάλειπτη παροχή των αγαθών και υπηρεσιών αυτών, την προστασία των ατομικών δικαιωμάτων στον κυβερνοχώρο και την καλλιέργεια κλίματος εμπιστοσύνης. Με το προτεινόμενο σχέδιο νόμου θεσπίζεται ένα συνεκτικό πλαίσιο για τη διακυβέρνηση της κυβερνοασφάλειας, ως διακριτής, οριζόντιου χαρακτήρα δημόσιας πολιτικής, καθώς και μηχανισμοί αποτελεσματικής συνεργασίας μεταξύ των αρμόδιων αρχών και των οργανισμών που παρέχουν κρίσιμες υπηρεσίες για την οικονομική και κοινωνική ζωή. Με ένα πλέγμα διατάξεων που υπερβαίνουν την ελάχιστη απαιτούμενη ενσωμάτωση των διατάξεων της Οδηγίας NIS 2 δημιουργείται ένα σταθερό πεδίο διασφάλισης υψηλού επιπέδου κυβερνασφάλειας. Ειδικότερα: **ΜΕΡΟΣ Α':** **Κεφάλαιο Α':** Προσδιορίζεται ο σκοπός και οριοθετείται το αντικείμενο του σχεδίου νόμου. **Κεφάλαιο Β':** Καθορίζεται το πεδίο εφαρμογής του σχεδίου νόμου, με τον ορισμό των βασικών και σημαντικών οντοτήτων και προβλέπονται οι αναγκαίοι ορισμοί για τους σκοπούς του νόμου. **Κεφάλαιο Γ':** Θεσπίζονται συντονισμένα κανονιστικά πλαίσια κυβερνοασφάλειας με την εφαρμογή ενός ολοκληρωμένου πλαισίου στρατηγικής, τον ορισμό Εθνικής Αρχής Κυβερνοσφάλειας (ΕΑΚ) ως αρμόδιας Αρχής και ενιαίου σημείου επαφής, τον ορισμό των ομάδων απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών (CSIRTs), τη θέσπιση εθνικού πλαισίου διαχείρισης κυβερνοκρίσεων και τη δημιουργία πλαισίου συνεργασίας μεταξύ της ΕΑΚ και άλλων αρμόδιων αρχών. **Κεφάλαιο Δ':** Θεσπίζεται υποχρέωση λήψης μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας από τις βασικές και σημαντικές οντότητες, καθώς και υποχρεώσεις αναφοράς περιστατικών. **Κεφάλαιο Ε':** Ρυθμίζονται ζητήματα που αφορούν τη δικαιοδοσία και την εδαφικότητα και θεσπίζεται υποχρέωση τήρησης μητρώων οντοτήτων και βάσης δεδομένων καταχώρισης ονομάτων τομέα. **Κεφάλαιο ΣΤ':** Ρυθμίζονται ζητήματα που αφορούν την ανταλλαγή πληροφοριών στον τομέα της κυβερνοασφάλειας.

	Κεφάλαιο Ζ': Καθορίζονται τα μέτρα εποπτείας και επιβολής για τις βασικές και σημαντικές οντότητες, ορίζεται η ΕΑΚ ως αρμόδια αρχή εποπτείας και ελέγχου, προβλέπονται οι γενικοί όροι για την επιβολή διοικητικών προστίμων, και καθορίζονται τα διοικητικά πρόστιμα και οι κυρώσεις σε περίπτωση παραβίασης. **Κεφάλαιο Η':** Περιλαμβάνονται οι εξουσιοδοτικές, μεταβατικές, τελικές και καταργούμενες διατάξεις των κεφαλαίων Α' έως Ζ'. **ΜΕΡΟΣ Β':** Περιλαμβάνονται ρυθμίσεις για την τροποποίηση διατάξεων του ν. 5086/2024 (Α' 23) και του ν. 4961/2022 (Α' 146). **ΜΕΡΟΣ Γ':** Καθορίζεται η έναρξη ισχύος των διατάξεων του σχεδίου νόμου.
2.	Γιατί αποτελεί πρόβλημα;
	Η διείσδυση και τα οφέλη των νέων τεχνολογιών στην οικονομική και κοινωνική ζωή αναδεικνύουν την κυβερνοασφάλεια σε στρατηγικής σημασίας ζήτημα. Η παροχή κρίσιμων υπηρεσιών, όπως η ενέργεια, οι μεταφορές, οι υπηρεσίες υγείας, ο χρηματοπιστωτικός τομέας, εξαρτώνται τόσο από φυσικές όσο και - ολοένα και περισσότερο - από ψηφιακές υποδομές, γεγονός το οποίο αυξάνει τις ευπάθειες και την πιθανότητα διατάραξης της παροχής των κρίσιμων αυτών υπηρεσιών. Η κυβερνοασφάλεια, ως ένας ταχέως εξελισσόμενος και ιδιαιτέρως κρίσιμος τομέας για τη χώρα, συνδέεται άρρηκτα τόσο με την εύρυθμη λειτουργία των κρίσιμων υποδομών της όσο και με την ανθεκτικότητα και απόκριση του κράτους σε κυβερνοαπειλές, καθώς επίσης και με την επιχειρησιακή συνέχεια των υπηρεσιών που παρέχει. Δεδομένης της εντατικοποίησης και της αυξημένης πολυπλοκότητας των απειλών και των κυβερνοεπιθέσεων, ο αριθμός, το μέγεθος, η επινοητικότητα, η συχνότητα και ο αντίκτυπος των περιστατικών στον κυβερνοχώρο αυξάνονται και συνιστούν μείζονα απειλή για τη λειτουργία των συστημάτων δικτύου και πληροφοριακών συστημάτων και την παροχή υπηρεσιών που παρέχονται μέσω αυτών. Η επίτευξη υψηλού επιπέδου κυβερνοασφάλειας αποτελεί ζήτημα με εθνική και υπερεθνική διάσταση. Με το προτεινόμενο σχέδιο νόμου εναρμονίζεται το εθνικό δίκαιο με την Οδηγία NIS 2 για την επίτευξη των στόχων που έχουν τεθεί σε ενωσιακό επίπεδο.
3.	Ποιους φορείς ή πληθυσμιακές ομάδες αφορά;
	Άμεσα, οι προτεινόμενες ρυθμίσεις αφορούν οργανισμούς και επιχειρήσεις του δημόσιου και του ιδιωτικού τομέα που δραστηριοποιούνται σε κρίσιμους τομείς για την οικονομική και κοινωνική ζωή της χώρας, καθώς εισάγονται υποχρεώσεις λήψης τεχνικών και οργανωτικών μέτρων κυβερνοασφάλειας, κατά κανόνα σε μεσαίες επιχειρήσεις και άνω, που δραστηριοποιούνται στους τομείς και υπο-τομείς που εμπίπτουν στο πεδίο εφαρμογής του προτεινόμενου σχεδίου νόμου. Συγκεκριμένα, οι προτεινόμενες ρυθμίσεις αφορούν άμεσα την ΕΑΚ, ως κεντρικό φορέα για τη διακυβέρνηση, υλοποίηση και εποπτεία εφαρμογής της

	κυβερνοασφάλειας, ως διακριτής δημόσιας πολιτικής, καθώς και φορείς όπως την αρμόδια οργανική μονάδα του Γενικού Επιτελείου Εθνικής Άμυνας για θέματα κυβερνοασφάλειας / κυβερνοάμυνας, που υποστηρίζει μεταβατικά την ΕΑΚ στην εκτέλεση των καθηκόντων της, και τη Διεύθυνση Κυβερνοχώρου της Εθνικής Υπηρεσίας Πληροφοριών, που ορίζεται ως ομάδα απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών (CSIRT) για τους φορείς του δημόσιου τομέα, καθώς, επίσης, και το σύνολο των Υπουργείων, που αναλαμβάνουν συγκεκριμένους ρόλους και υποχρεώσεις στην υλοποίηση κρίσιμων λειτουργιών. Επιπλέον, οι προτεινόμενες ρυθμίσεις αφοορούν το μερίδιο εκείνο της αγοράς που δραστηριοποιείται στους τομείς και υπο-τομείς που εμπτίπτουν στο πεδίο εφαρμογής του προτεινόμενου σχεδίου νόμου, λόγω της αυξημένης και συνεχώς αυξανόμενης ζήτησης σε υπηρεσίες, προϊόντα και ειδικότητες στον τομέα της κυβερνοασφάλειας και της πληροφορικής, καθώς και σε άλλες ειδικότητες (όπως συμβουλευτικές υπηρεσίες, νομικές υπηρεσίες, εκπαίδευση κυβερνοασφάλειας). Έμμεσα, πλην όμως ουσιαστικά, οι προτεινόμενες ρυθμίσεις αφορούν το σύνολο των πολιτών, για τους οποίους διασφαλίζεται η αδιάλειπτη παροχή υπηρεσιών σε κρίσιμους τομείς, προστατεύοντας και θωρακίζοντας τις ψηφιακές υποδομές με τις οποίες αυτές παρέχονται.

	Η αναγκαιότητα της αξιολογούμενης ρύθμισης	
4.	Το εν λόγω ζήτημα έχει αντιμετωπιστεί με νομοθετική ρύθμιση στο παρελθόν; ΝΑΙ **X** ΟΧΙ ❒ Εάν ΝΑΙ, ποιο είναι το ισχύον νομικό πλαίσιο που ρυθμίζει το ζήτημα;	
	ν. 4577/2018 (Α' 199) και υπ' αρ. 1017/4.10.2019 απόφαση του Υπουργού Επικρατείας (Β' 3739), για την εφαρμογή του νόμου αυτού ν. 4635/2019 (Α' 167) ν. 4961/2022 (Α' 146) ν. 5002/2022 (Α' 228) ν. 5086/2024 (Α΄ 23)	
5.	Γιατί δεν είναι δυνατό να αντιμετωπιστεί στο πλαίσιο της υφιστάμενης νομοθεσίαςκα;	
	i) με αλλαγή προεδρικού διατάγματος, υπουργικής απόφασης ή άλλης κανονιστικής πράξης;	Απαιτείται συνολική και ενιαία νέα ρύθμιση για την επίτευξη των στόχων της Οδηγίας NIS 2, καθώς θεσπίζεται νέο και ενισχυμένο πλαίσιο διακυβέρνησης, με νέους ρόλους για τους φορείς του δημόσιου τομέα και νέες υποχρεώσεις για τους φορείς του ιδιωτικού τομέα, για το οποίο απαιτείται ρύθμιση σε επίπεδο τυπικού νόμου. Οι σκοποί που επιδιώκονται με τις προτεινόμενες ρυθμίσεις δεν είναι δυνατό να επιτευχθούν με αλλαγή προεδρικού διατάγματος, υπουργικής απόφασης ή

	άλλης κανονιστικής πράξης, ελλείψει σχετικής νομοθετικής εξουσιοδότησης. Ταυτόχρονα, τα προς ρύθμιση θέματα αποτελούν αντικείμενο τυπικού νόμου.
ii) με αλλαγή διοικητικής πρακτικής συμπεριλαμβανομένης της δυνατότητας νέας ερμηνευτικής προσέγγισης της υφιστάμενης νομοθεσίας;	Βλ. πεδίο (i)
iii) με διάθεση περισσότερων ανθρώπινων και υλικών πόρων;	Βλ. πεδίο (i)

	Συναφείς πρακτικές	
6.	Έχετε λάβει υπόψη συναφείς πρακτικές; ΝΑΙ **X** ΟΧΙ ❒ Εάν ΝΑΙ, αναφέρατε συγκεκριμένα:	
	i) σε άλλη/ες χώρα/ες της Ε.Ε. ή του ΟΟΣΑ:	Οι προτεινόμενες ρυθμίσεις αξιοποιούν τις βέλτιστες πρακτικές που εφαρμόζονται στον τομέα της κυβερνοασφάλειας από το σύνολο, σχεδόν, των κρατών μελών της Ευρωπαικής Ένωσης. Χαρακτηριστικά παραδείγματα αποτελούν οι πρακτικές που ακολουθούνται στη Γερμανία, στο Βέλγιο, στην Ιταλία και στη Γαλλία. Επιπλέον, οι προτεινόμενες ρυθμίσεις ακολουθούν τις διεθνείς τάσεις που επικρατούν στον τομέα της κυβερνοασφάλειας, ως προς τα ελάχιστα μέτρα ασφάλειας στον κυβερνοχώρο και το μοντέλο διακυβέρνσης της δημόσιας πολιτικής κυβερνοασφάλειας. Χαρακτηριστικό παράδειγμα αποτελούν οι τάσεις που επιρακτούν στις Ηνωμένες Πολιτείες της Αμερικής και στο Ηνωμένο Βασίλειο.
	ii) σε όργανα της Ε.Ε.:	Αξιοποιούνται τα αποτελέσματα της ενισχυμένης συνεργασίας των κρατών μελών της Ευρωπαικής Ένωσης, στο πλαίσιο της «Ομάδας Συνεργασίας» που έχει θεσπιστεί σε ενωσιακό επίπεδο, ήδη με τις διατάξεις της Οδηγίας NIS 1, καθώς και του Κανονισμού (ΕΕ) 2023/2841 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2023, για τον καθορισμό μέτρων για υψηλό κοινό επίπεδο

	κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης.
iii) σε διεθνείς οργανισμούς:	

	Στόχοι αξιολογούμενης ρύθμισης
7.	Σημειώστε ποιοι από τους στόχους βιώσιμης ανάπτυξης των Ηνωμένων Εθνών επιδιώκονται με την αξιολογούμενη ρύθμιση
	❒  ❒   ❒❒  ❒  ❒  ❒  ❒  ☒  ❒  ❒  ❒  ❒  ❒  ❒  ❒  ❒ 
8.	Ποιοι είναι οι στόχοι της αξιολογούμενης ρύθμισης;

i) βραχυπρόθεσμοι:	- Η περαιτέρω ενδυνάμωση του εθνικού συστήματος διακυβέρνησης, των ικανοτήτων της χώρας και των αρμόδιων αρχών στον τομέα της κυβερνοασφάλειας. - Η ενίσχυση του επιπέδου κυβερνοασφάλειας των επιχειρήσεων που παρέχουν κρίσιμες και σημαντικές υπηρεσίες για την κοινωνικοοικονομική ζωή.
ii) μακροπρόθεσμοι:	- Η θεσμική και τεχνολογική θωράκιση έναντι των κυβερνοαπειλών και η συνολική αναβάθμιση του επιπέδου της κυβερνοασφάλειας στη χώρα, που συνιστούν παράμετρο εξέχουσας σημασίας για την προάσπιση της δημόσιας ασφάλειας. - Η ενίσχυση της ανθεκτικότητας του κράτους και των κρίσιμων, βασικών και σημαντικών υποδομών έναντι απειλών και επιθέσεων στον κυβερνοχώρο. - Η ενίσχυση του ψηφιακού οικοσυστήματος στη χώρα, μέσω της διαμόρφωσης ενός περιβάλλοντος με ασφαλείς υποδομές.

	- Η δημιουργία ασφαλούς, ανθεκτικού και ανταγωνιστικού ψηφιακού περιβάλλοντος, που διασφαλίζει χωρίς αποκλίσεις τη συνολική ανθεκτικότητα της χώρας έναντι απειλών και η προώθηση της συνεργασίας και ανταλλαγής πληροφοριών μεταξύ δημόσιων και ιδιωτικών φορέων για την αντιμετώπιση κυβερνοαπειλών. - Η αύξηση της ανταγωνιστικότητας της ψηφιακής οικονομίας, με προώθηση της καινοτομίας και της ανάπτυξης και η ενθάρρυνση της υιοθέτησης νέων τεχνολογιών και πρακτικών ασφάλειας. - Η εμπέδωση εμπιστοσύνης στην ψηφιακή αγορά και στην ασφάλεια των ψηφιακών υπηρεσιών, με στόχο την ενίσχυση των κοινωνικών και οικονομικών δραστηριοτήτων των πολιτών και των επιχειρήσεων. - Η ενίσχυση της εμπιστοσύνης των πολιτών και των επιχειρήσεων στις ψηφιακές υπηρεσίες του κράτους και της αγοράς, η οποία συνιστά ιδιαιτέρως σημαντικό παράγοντα στην προσπάθεια διευκόλυνσης και ενίσχυσης του ψηφιακού μετασχηματισμού της χώρας.

	Ψηφιακή διακυβέρνηση	
10.	Σε περίπτωση που προβλέπεται η χρήση πληροφοριακού συστήματος, ποια θα είναι η συμβολή αυτού στην επίτευξη των στόχων της αξιολογούμενης ρύθμισης: ΑΜΕΣΗ ❒ ή/και ΕΜΜΕΣΗ ❒	
	i) Εάν είναι άμεση, εξηγήστε:	
	ii) Εάν είναι έμμεση, εξηγήστε:	
11.	Το προβλεπόμενο πληροφοριακό σύστημα είναι συμβατό με την εκάστοτε ψηφιακή στρατηγική της χώρας (Βίβλος Ψηφιακού Μετασχηματισμού); ΝΑΙ ❒ ΟΧΙ ❒	
	Εξηγήστε:	
12.	Διασφαλίζεται η διαλειτουργικότητα του εν λόγω πληροφοριακού συστήματος με άλλα υφιστάμενα συστήματα; ΝΑΙ ❒ ΟΧΙ ❒	
	Αναφέρατε ποια είναι αυτά τα συστήματα:	
13.	Έχει προηγηθεί μελέτη βιωσιμότητας του προβλεπόμενου πληροφοριακού συστήματος; ΝΑΙ ❒ ΟΧΙ ❒	

Εξηγήστε:	

	Κατ' άρθρο ανάλυση αξιολογούμενης ρύθμισης	
14.	Σύνοψη στόχων κάθε άρθρου	
	Άρθρο	*Στόχος*
	1	Καθορίζεται ο σκοπός του μέρους Α', ο οποίος συνίσταται στην επίτευξη υψηλού επιπέδου κυβερνοασφάλειας σε εθνικό επίπεδο, με την ενσωμάτωση της Οδηγίας NIS 2 στην εθνική έννομη τάξη.
	2	Οριοθετείται το αντικείμενο του μέρους Α', το οποίο συνίσταται: • στον καθορισμό των αρμόδιων εθνικών αρχών για την εποπτεία εφαρμογής και την εφαρμογή του νόμου, σε επίπεδο τεχνικό, επιχειρησιακό και στρατηγικό, • στην υποχρεωτική λήψη μέτρων ενίσχυσης της κυβερνοσφάλειας κρίσιμων και σημαντικών οργανισμών και επιχειρήσεων, • στην ενίσχυση της συνεργασίας όλων των εμπλεκομένων, • στη θέσπιση ενός αποτελεσματικού, αναλογικού και αποτρεπτικού εποπτικού μηχανισμού για τη διασφάλιση της εφαρμογής των υποχρεώσεων που απορρέουν από το πρτοεινόμενο σχέδιο νόμου.
	3	Καθορίζεται το πεδίο εφαρμογής του μέρους Α', το οποίο καλύπτει τομείς υψηλής κρισιμότητας και το σύνολο των σημαντικών τομέων για τη θωράκιση της κοινωνικοοικονομικής ζωής στον κυβερνοχώρο. Συγκεκριμένα, θεσπίζεται ενιαίο κριτήριο για τον προσδιορισμό των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής του μέρους Α': όλες οι οντότητες που χαρακτηρίζονται μεσαίες επιχειρήσεις σύμφωνα με το άρθρο 2 του παραρτήματος της Σύστασης 2003/361/ΕΚ της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων (L 124) ή υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις και ταυτόχρονα δραστηριοποιούνται στους τομείς και παρέχουν τα είδη υπηρεσιών ή ασκούν τις δραστηριότητες που καλύπτονται από τον παρόντα νόμο, εμπίπτουν στο πεδίο εφαρμογής του. Περαιτέρω, εμπίπτουν στο πεδίο εφαρμογής του μέρους Α' ορισμένες μικρές επιχειρήσεις και πολύ μικρές επιχειρήσεις, που πληρούν ειδικά κριτήρια τα οποία υποδεικνύουν βασικό ρόλο για την κοινωνία, την οικονομία ή για συγκεκριμένους ευαίσθητους τομείς.
	4	Ορίζονται δύο (2) κατηγορίες οντοτήτων με κριτήριο αφενός το μέγεθος και αφετέρου τη σπουδαιότητά τους για την παροχή κρίσιμων

	υπηρεσιών, τη λειτουργία της αγοράς ή την ιδιαίτερη σημασία τους, ανεξαρτήτως μεγέθους. Ειδικότερα, οι οντότητες διακρίνονται ως εξής: 1. Βασικές οντότητες, στις οποίες περιλαμβάνονται: • Κατά κανόνα, κάθε επιχείρηση ή οργανισμός που υπερβαίνει τα ανώτατα όρια για τις μεσαίες επιχειρήσεις (σύμφωνα με την παρ. 1 του άρθρου 2 του παραρτήματος της Σύστασης 2003/361/ΕΚ) και δραστηριοποιείται στους τομείς του παραρτήματος Ι του πρτοεινόμενου σχεδίου νόμου: ενέργεια, μεταφορές, τράπεζες, υποδομές χρηματοπιστωτικών αγορών, υγεία, πόσιμο νερό, λύματα, ψηφιακές υποδομές (μεταξύ των οποίων πλέον και οι πάροχοι τηλεπικοινωνιακών υπηρεσιών, πάροχοι υπηρεσιών cloud, data center κ.ά.), διαχείριση υπηρεσιών Τεχνολογίας Πληροφορικής και Επικοινωνιών (ΤΠΕ) (πάροχοι διαχειριζομένων υπηρεσιών «Managed Service Providers» και πάροχοι διαχειριζομένων υπηρεσιών ασφάλειας «Managed Security Service Providers MSSPs»). • Οντότητες δημόσιας διοίκησης. • Πάροχοι υπηρεσιών DNS, TLD name registries, υπηρεσιών εμπιστοσύνης, ανεξαρτήτως μεγέθους. • Οργανισμοί των παραρτημάτων Ι και ΙΙ του προτεινόμενου σχεδίου νόμου που ορίζονται ως τέτοιοι βάσει ειδικών κριτηρίων. • Οργανισμοί που εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, για την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ του Συμβουλίου για την προστασία των κρίσιμων υποδομών (L 333). • Οργανισμοί που αναγνωρίστηκαν, σύμφωνα με το άρθρο 4 του ν. 4577/2018 και το άρθρο 16 της υπ' αρ. 1027/4.10.2019 απόφασης του Υπουργού Επικρατείας, πριν από τις 16 Ιανουαρίου 2023, ως φορείς εκμετάλλευσης βασικών υπηρεσιών. 2. Σημαντικές οντότητες (παράρτημα ΙΙ), στις οποίες περιλαμβάνονται: • Κάθε επιχείρηση ή οργανισμός που υπερβαίνει τα ανώτατα όρια για τις μεσαίες επιχειρήσεις (σύμφωνα με την παρ. 1 του άρθρου 2 του παραρτήματος της Σύστασης 2003/361/ΕΚ) και δραστηριοποιείται στους τομείς του παραρτήματος ΙΙ του πρτοεινόμενου σχεδίου νόμου: ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών, διαχείριση απορριμμάτων, κατασκευή, παραγωγή και διανομή χημικών ουσιών, παραγωγή, επεξεργασία και διανομή τροφίμων, κατασκευή εξοπλισμού (όπως ιατρικού, ηλεκτρονικού, μηχανολογικού εξοπλισμού κ.ά.), πάροχοι ψηφιακών υπηρεσιών

	(περιλαμβανομένων των πλατφορμών μέσων κοινωνικής δικτύωσης), ερευνητικοί οργανισμοί. • Κάθε επιχείρηση ή οργανισμός των παραρτημάτων I και II που δεν πληροί το κριτήριο του μεγέθους, πλην όμως αναγνωρίζονται ως τέτοιοι από τα κράτη-μέλη βάσει κριτηρίων. Για τον ακριβή προσδιορισμό των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής του προτεινόμενου σχεδίου νόμου, η ΕΑΚ καταρτίζει σχετικό κατάλογο βασικών και σημαντικων οντοτήτων, καθώς και οντοτήτων που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, ο οποίος περιλαμβάνει τα βασικά στοιχεία κάθε οντότητας.
5	Προκειμένου να αποφεύγεται η συρροή διατάξεων και να μην αντίκεινται σε τομεακές ενωσιακές νομικές πράξεις που επιφέρουν τουλάχιστον ισοδύναμα αποτελέσματα στο ίδιο πεδίο, η NIS 2, που ενσωματώνεται στην ελληνική έννομη τάξη με το προτεινόμενο σχέδιο νόμου, λειτουργεί συμπληρωματικά και επικουρικά σε ό, τι έχει ήδη ρυθμιστεί ειδικά ή τομεακά σε ενωσιακό επίπεδο. Οι οντότητες του τραπεζικού τομέα εξαιρούνται από το πεδίο εφαρμογής, καθώς εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των Κανονισμών (ΕΚ) 1060/2009, (ΕΕ) 648/2012, (ΕΕ) 600/2014, (ΕΕ) 909/2014 και (ΕΕ) 2016/1011 (L 333). Ωστόσο, εξακολουθούν να υποχρεούνται σε άμεση και ισοδύναμη αναφορά περιστατικού κυβερνοασφάλειας αλλά και σε άμεση αναφορά στην ΕΑΚ απευθείας, βάσει των υποχρεώσεων αναφοράς περιστατικών του παρόντος. Κατά την εφαρμογή του παρόντος άρθρου λαμβάνονται υπόψη οι κατευθυντήριες γραμμές που έχει θεσπίσει η Ευρωπαϊκή Επιτροπή στις 13.9.2023 [C(2023) 6068/13.09.2023 και C(2023) 6070/13.09.2023], όπως αυτές τροποποιούνται και ισχύουν κάθε φορά, σύμφωνα με την παρ. 3 του άρθρου 4 της Οδηγίας NIS 2.
6	Παρατίθενται οι ορισμοί των εννοιών που περιέχονται στο μέρος Α’ και είναι απαραίτητοι για την εφαρμογή του, σύμφωνα με τους ορισμούς της Οδηγίας NIS 2 αλλά και της αντίστοιχης τομεακής ή ενωσιακής νομοθεσίας, όπου υπάρχει παραπομπή.
7	Προβλέπεται η σύνταξη Εθνικής Στρατηγικής Κυβερνοασφάλειας (Ε.Σ.Κ.), η οποία περιλαμβάνει κατ’ ελάχιστον, μεταξύ άλλων: α) πρόβλεψη στρατηγικών στόχων και προτεραιότητες για την επίτευξη και διατηρηση υψηλού επιπέδου κυβερνοασφάλειας και συνεκτικό πλαίσιο διακυβέρνησης για την επίτευξή τους, β) τους αναγκαίους πόρους για την επίτευξη των εν λόγω στόχων και γ) τα αναγκαία κανονιστικά μέτρα και μέτρα πολιτικής για την κυβερνοασφάλεια.

	Η Ε.Σ.Κ. τελεί σε αρμονία με τη Στρατηγική Εθνικής Ασφάλειας που διαμορφώνεται από το Κυβερνητικό Συμβούλιο Εθνικής Ασφάλειας, σύμφωνα με την παρ. 5 του άρθρου 7 του ν. 4622/2019 (Α' 133).
8	Η ΕΑΚ ορίζεται ως αρμόδια αρχή για την κυβερνοασφάλεια, παρακολουθεί την εφαρμογή του νόμου και αποτελεί το ενιαίο σημείο επαφής, για τη διευκόλυνση της διασυνοριακής συνεργασίας. Με τον ορισμό της ΕΑΚ ως ενιαίου σημείου επαφής και αρμόδιας εποπτικής αρχής διασφαλίζεται ο αναγκαίος συντονισμός για την αναγνώριση και τον μετριασμό των κινδύνων στον κυβερνοχώρο σε εθνικό επίπεδο και καθιερώνεται ένας εποπτικός μηχανισμός ικανός να επιτελεί τον ρόλο του αποτελεσματικά και με την αναγκαία λειτουργική ανεξαρτησία έναντι των εποπτευόμενων φορέων. Η ΕΑΚ έχει κεντρικό ρόλο στη δημόσια πολιτική κυβερνοασφάλειας, όπως ορίζεται ήδη στον ν. 5086/2024 (Α' 23), και δύναται να κινητοποιεί, να συντονίζει και να κατευθύνει τη δράση του συνόλου των φορέων του δημόσιου και ιδιωτικού τομέα για την εφαρμογή του πλαισίου κυβερνοασφάλειας σε στρατηγικό και κανονιστικό επίπεδο, καθώς και σε επιχειρησιακές και τεχνικές λειτουργίες, μέσω του αναγκαίου ελέγχου συμμόρφωσης. Στο πλαίσιο των αρμοδιοτήτων της, η ΕΑΚ ασκεί καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών της Ελλάδας με τις αρμόδιες αρχές άλλων κρατών μελών και, κατά περίπτωση, με την Ευρωπαϊκή Επιτροπή και τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), καθώς και για τη διασφάλιση διατομεακής, οριζόντιας συνεργασίας με άλλες αρμόδιες αρχές εντός της Ελλάδας, όπως την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας κ.ά.. Η ΕΑΚ κοινοποιεί αμελλητί στην Ευρωπαϊκή Επιτροπή τον ορισμό της ως αρμόδιας αρχής και ενιαίου σημείου επαφής, τα καθήκοντά της, καθώς και κάθε μεταγενέστερη τροποποίηση των στοιχείων αυτών.
9	Η ΕΑΚ ορίζεται ως υπεύθυνη για τη διαχείριση περιστατικών μεγάλης κλίμακας και κρίσεων στον τομέα της κυβερνοασφάλειας (αρχή διαχείρισης κυβερνοκρίσεων), διασφαλίζει τη συνοχή με το υφιστάμενο πλαίσιο για τη γενική εθνική διαχείριση κρίσεων, ενώ συμμετέχει από πλευράς Ελλάδας στο Ευρωπαϊκό Δίκτυο οργανώσεων διασύνδεσης για κρίσεις στον κυβερνοχώρο (EU-CyCLONe), ως οργανισμός CyCLO. Στο πλαίσιο αυτό, εντός έξι (6) μηνών από την έναρξη ισχύος του μέρους Α', εκδίδεται απόφαση του Διοικητή της ΕΑΚ, η οποία εγκρίνεται εντός ενός (1) μηνός από την Επιτροπή Συντονισμού για θέματα Κυβερνοασφάλειας του άρθρου 23 του ν. 5002/2022 (Α' 228), με την οποία καταρτίζεται εθνικό σχέδιο αντιμετώπισης περιστατικών μεγάλης κλίμακας και κρίσεων στον τομέα της κυβερνοασφάλειας, στο οποίο καθορίζονται οι στόχοι και οι ρυθμίσεις για τη διαχείριση περιστατικών μεγάλης κλίμακας και κρίσεων. Τέλος, προβλέπεται η κοινοποίηση στην Ευρωπαϊκή Επιτροπή και το ευρωπαϊκό δίκτυο οργανισμών

	διασύνδεσης για κυβερνοκρίσεις (EU-CyCLONe) των αντίστοιχων πληροφοριών.
10	Τα κράτη μέλη, σύμφωνα με την Οδηγία NIS 2, πρέπει να είναι επαρκώς εξοπλισμένα όσον αφορά τόσο τις τεχνικές όσο και τις οργανωτικές ικανότητες για την πρόληψη, τον εντοπισμό και την αντιμετώπιση περιστατικών και κινδύνων, καθώς και για τον μετριασμό των επιπτώσεών τους. Στο πλαίσιο αυτό, η ΕΑΚ ορίζεται ως αρμόδια ομάδα απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών (Computer Security Incident Response Team- CSIRT), ενώ ειδικά για τους οργανισμούς της δημόσιας διοίκησης, ως CSIRT ορίζεται η Διεύθυνση Κυβερνοχώρου της Εθνικής Υπηρεσίας Πληροφοριών. Ταυτόχρονα, για την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας δύναται να καθορίζονται και έτερες CSIRTs. Οι έτερες CSIRTs επιλαμβάνονται συμβάντων που αφορούν στην ασφάλεια υπολογιστών του οικείου τομέα, εφόσον ζητηθεί η συνδρομή τους από την ΕΑΚ, και έχουν υποχρέωση να ενημερώνουν την ΕΑΚ αμελλητί για συμβάν που διαπιστώνουν. Επίσης, η ΕΑΚ ως ενιαίο σημείο επαφής και οι τυχόν έτερες CSIRTs, συνεργάζονται μεταξύ τους για τους σκοπούς της τήρησης των υποχρεώσεων που προβλέπονται στο μέρος Α'. Προβλέπεται η συνεργασία της ΕΑΚ και άλλων CSIRTs και η ανταλλαγή πληροφοριών σχετικών, σύμφωνα με το άρθρο 21, με τομεακές ή διατομεακές κοινότητες βασικών και σημαντικών οντοτήτων, καθώς και η συμμετοχή σε αξιολογήσεις από ομοτίμους στο πλαίσιο της συνεργασίας τους εντός του δικτύου CSIRT. Για να διευκολυνθεί εξάλλου η άντληση διδαγμάτων από τις κοινές εμπειρίες, να ενισχυθεί η αμοιβαία εμπιστοσύνη και να επιτευχθεί κοινό επίπεδο κυβερνοασφάλειας, προβλέπεται η αξιολόγηση των CSIRT από ομοτίμους του δικτύου CSIRT της Ένωσης. Προβλέπεται ακόμη η σύσταση ειδικών ομάδων απόκρισης οι οποίες δεν ασκούν καθήκοντα ελέγχου, αλλά συστήνονται για παροχή συνδρομής σε περίπτωση εκδήλωσης περιστατικού.
11	Καθορίζονται οι απαιτήσεις, οι τεχνικές ικανότητες και τα καθήκοντα των CSIRTs, ώστε να εξασφαλίζεται ότι είναι επαρκώς εξοπλισμένες, όσον αφορά τόσο τις τεχνικές όσο και τις οργανωτικές τους ικανότητες, για την πρόληψη, τον εντοπισμό, την αντιμετώπιση περιστατικών και κινδύνων, τον μετριασμό των επιπτώσεών τους, καθώς και τη διασφάλιση της αποτελεσματικής συνεργασίας στο επίπεδο της Ευρωπαϊκής Ένωσης. Ρητά προβλέπεται, στο πλαίσιο ενίσχυσης των ικανοτήτων της χώρας και της διευρωπαϊκής συνεργασίας σε τεχνικό επίπεδο, ότι η ΕΑΚ, επικουρούμενη κατά περίπτωση από τις λοιπές CSIRTs, μπορεί να συμμετέχει σε διεθνή δίκτυα συνεργασίας, ενώ συμμετέχει και στο δίκτυο CSIRT του άρθρου 15 της Οδηγίας NIS 2.
12	Δεδομένου ότι οι ευπάθειες συχνά εντοπίζονται και γνωστοποιούνται από τρίτους, ο κατασκευαστής ή ο πάροχος προϊόντων ή υπηρεσιών

	Τεχνολογίας Πληροφορικής και Επικοινωνιών πρέπει να θεσπίσει τις αναγκαίες διαδικασίες για τη λήψη πληροφοριών από τρίτους σχετικά με ευπάθειες. Στο νέο πλαίσιο για τη συντονισμένη γνωστοποίηση ευπαθειών σε έμπιστες οντότητες, και προκειμένου οι ευπάθειες που εντοπίζονται κυρίως σε προϊόντα αλλά και σε υπηρεσίες να αντιμετωπίζονται το συντομότερο δυνατόν και με συστηματικό και συντονισμένο τρόπο, ανατίθεται συντονιστικός ρόλος για τους σκοπούς της συντονισμένης γνωστοποίησης ευπαθειών στην ΕΑΚ, ως CSIRT, ενεργώντας ως αξιόπιστος ενδιάμεσος φορέας που θα διευκολύνει την επικοινωνία μεταξύ των αναφερουσών οντοτήτων και των κατασκευαστών ή παρόχων προϊόντων και υπηρεσιών Τεχνολογίας Πληροφορικής και Επικοινωνιών.
13	Διασφαλίζεται η αναγκαία συνεργασία μεταξύ της ΕΑΚ, έτερων CSIRT και ενός συνόλου άλλων φορέων με συναφείς αρμοδιότητες, προκειμένου να επιτυγχάνεται ο αναγκαίος συντονισμός στην εφαρμογή της οριζόντιας δημόσιας πολιτικής κυβερνοασφάλειας. Στο πλαίσιο αυτό, προβλέπεται και συστηματοποιείται η συνεργασία της ΕΑΚ και των CSIRTs, με τις αρμόδιες αρχές επιβολής του μέρους Α', ιδίως τις εισαγγελικές αρχές, την Ελληνική Αστυνομία, φορείς όπως η Αρχή Πολιτικής Αεροπορίας και η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, τους εποπτικούς φορείς που ορίζονται σύμφωνα με τον Κανονισμό (ΕΕ) 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της Οδηγίας 1999/93/ΕΚ (L 257), την Τράπεζα της Ελλάδος, την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων και τις αρμόδιες αρχές που ορίζονται σύμφωνα με την Οδηγία (ΕΕ) 2022/2557. Η ΕΑΚ, ως αρμόδια εθνική αρχή σύμφωνα με την Οδηγία NIS 2, και οι λοιπές αρμόδιες εθνικές αρχές σύμφωνα με την Οδηγία (ΕΕ) 2022/2557, συνεργάζονται και ανταλλάσσουν πληροφορίες, σε τακτική βάση, όσον αφορά τον προσδιορισμό των κρίσιμων οντοτήτων, τους κινδύνους, τις κυβερνοαπειλές και τα περιστατικά, καθώς και τους κινδύνους, τις απειλές και τα περιστατικά εκτός του κυβερνοχώρου, που επηρεάζουν βασικές οντότητες που προσδιορίζονται ως κρίσιμες οντότητες βάσει της Οδηγίας (ΕΕ) 2022/2557. Παράλληλα, προβλέπεται πλέγμα ρυθμίσεων για την περαιτέρω ενίσχυση της συνεργασίας και την επίτευξη οριζόντιου συντονισμού μεταξύ όλων των υπηρεσιών και φορέων που έχουν συναφή ρόλο και αρμοδιότητες. Τέλος, ο ορισμός τομεακών σημείων επαφής και συνεργασίας σύμφωνα με την παρ. 11 του άρθρου 29 του σχεδίου νόμου, τίθεται αποκλειστικά με γνώμονα την ενίσχυση του συντονισμού και του πλαισίου συνεργασίας μεταξύ της ΕΑΚ και των επιμέρους αρμόδιων για θέματα κυβερνοασφάλειας αρχών, φορέων, υπηρεσιών και οργανικών

	μονάδων και δεν θίγει τις θεσπισμένες με άλλες διατάξεις αρμοδιότητες της ΕΑΚ ή των λοιπών υπηρεσιών.
14	Επιφορτίζεται η διοίκηση των βασικών και σημαντικών οντοτήτων με την ευθύνη για τη λήψη των οργανωτικών και τεχνικών μέτρων κυβερνοασφάλειας. Στο πλαίσιο αυτό, τα όργανα διοίκησης είναι υπεύθυνα για την έγκριση των αναγκαίων μέτρων, την αποτελεσματική εφαρμογή τους και τη διαρκή ανατροφοδότηση αυτών με βάση περιοδικά αποτελέσματα εφαρμογής, καθώς και για την εκπαίδευση και καλλιέργεια κουλτούρας κυβερνοασφάλειας σε κάθε οργανισμό. Με τον τρόπο αυτό, διασφαλίζεται η συμμόρφωση εκ μέρους των υπόχρεων οντοτήτων προς τις σχετικές υποχρεώσεις τόσο για τη λήψη των αναγκαίων μέτρων όσο και για την έγκαιρη γνωστοποίηση περιστατικών κυβερνοασφάλειας στην αρμόδια CSIRT. Ειδικά για το δημόσιο τομέα, το Εθνικό Κέντρο Δημόσιας Διοίκησης και Αυτοδιοίκησης σε συνεργασία με την ΕΑΚ και τη Γενική Γραμματεία Δημόσιας Διοίκησης του Υπουργείου Εσωτερικών οργανώνει ειδικό πρόγραμμα πιστοποίησης επάρκειας στον τομέα της κυβερνοασφάλειας για το προσωπικό του δημοσίου.
15	Προβλέπονται τα μέτρα που πρέπει να λαμβάνουν οι βασικές και σημαντικές οντότητες, έχοντας υπόψη και την αντιμετώπιση κινδύνων που απορρέουν από την αλυσίδα εφοδιασμού τους και τη σχέση με τους προμηθευτές τους, ενώ περιλαμβάνονται, μεταξύ άλλων υποχρεώσεις για το προσωπικό τους. Ειδικότερα, επιβάλλεται υποχρέωση για τις βασικές και σημαντικές οντότητες να λαμβάνουν κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν για τις δραστηριότητές τους ή για την παροχή των υπηρεσιών τους, καθώς και για την πρόληψη ή ελαχιστοποίηση των επιπτώσεων των περιστατικών στους αποδέκτες των υπηρεσιών τους ή σε άλλες υπηρεσίες και οργανισμούς. Τα μέτρα αυτά πρέπει να είναι αναλογικά με τον βαθμό έκθεσης της οντότητας σε κινδύνους και με τον κοινωνικό αντίκτυπο που θα είχε ένα περιστατικό, καθώς, επίσης, και κατάλληλα ανάλογα με την κατηγορία της οντότητας. Περαιτέρω, οι βασικές και σημαντικές οντότητες υποχρεούνται να ορίζουν ένα αρμόδιο στέλεχός τους, ανάλογων προσόντων και εμπειρογνωμοσύνης, ως Υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (ΥΑΣΠΕ). Τα καθήκοντα του ΥΑΣΠΕ είναι ασυμβίβαστα με αυτά του Υπευθύνου Προστασίας Δεδομένων (ΥΠΔ) του άρθρου 37 του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων, Γ.Κ.Π.Δ., L 119) και των άρθρων 7 και 8 του ν. 4624/2019 (Α’ 137).

	Ο ΥΑΣΠΕ, στο πλαίσιο της αποτελεσματικής άσκησης των καθηκόντων του και σύμφωνα με τις διεθνείς καλές πρακτικές, πρέπει να διαθέτει κατάλληλο επίπεδο αυτονομίας στη λήψη αποφάσεων, δυνατότητα εφαρμογής τους από τις επιμέρους οργανικές μονάδες της οντότητας, απευθείας ενημέρωση των ανώτατων οργάνων διοίκησης, συντονισμό της διαχείρισης περιστατικών ασφαλείας, καθώς και των διαδικασιών εφαρμογής των σχεδίων επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή.
16	Εξορθολογίζεται και αυστηροποιείται η υποχρέωση υποβολής αναφοράς περιστατικών, η οποία υποβάλλεται στην ΕΑΚ [24ωρη προθεσμία για αρχική γνωστοποίηση περιστατικού – «early warning», πληρέστερη ενημέρωση για το περιστατικό εντός 72 ωρών, ακολουθούμενη από ενδιάμεση πληροφόρηση εάν ζητηθεί από την ΕΑΚ και, τέλος, υποβολή τελικής, πλήρους αναφοράς το αργότερο εντός ενός (1) μήνα. Αυτή η προσέγγιση πολλαπλών σταδίων ως προς την αναφορά σοβαρών περιστατικών επιτυγχάνει ταχεία αναφορά και ενημέρωση της αρμόδιας CSIRT, που συμβάλλει στον μετριασμό της πιθανής εξάπλωσης σοβαρών περιστατικών και στην έγκαιρη επίγνωση της κατάστασης σε εθνικό επίπεδο και, επιπλέον, επιτρέπει στις βασικές και σημαντικές οντότητες να αναζητούν στήριξη ώστε να ανακάμπτουν από περιστατικά κυβερνοασφάλειας. Ταυτόχρονα, διασφαλίζει τον κατάλληλο συντονισμό σε ενωσιακό και εθνικό επίπεδο, όπου κατά περίπτωση απαιτείται.
17	Ενθαρρύνεται η χρήση ευρωπαϊκών και διεθνώς αποδεκτών προτύπων και τεχνικών προδιαγραφών σχετικών με την ασφάλεια συστημάτων δικτύου και πληροφοριών, στο πλαίσιο της αποτελεσματικής εφαρμογής των μέτρων διαχείρισης κινδύνων. Τα μέτρα ενθάρρυνσης ορίζονται με απόφαση του Διοικητή της ΕΑΚ.
18	Αποσαφηνίζονται ζητήματα δικαιοδοσίας και εδαφικότητας, αίροντας ασάφειες που έχουν διαπιστωθεί κατά το παρελθόν, λόγω του διασυνοριακού χαρακτήρα του ίδιου του διαδικτύου και συνεπώς της ασφάλειας στον κυβερνοχώρο.
19	Λαμβάνεται ειδική μέριμνα για την ενημέρωση της ΕΑΚ με βασικά στοιχεία ψηφιακών υποδομών, οι οποίες είναι ιδιαιτέρως κρίσιμες για την ασφάλεια στον κυβερνοχώρο [όπως οι πάροχοι υπηρεσιών Domain Name System (DNS), τα μητρώα ονομάτων top-level domain (TLD), οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, οι πάροχοι υπηρεσιών υπολογιστικού νέφους, οι πάροχοι υπηρεσιών κέντρων δεδομένων, οι πάροχοι δικτύων διανομής περιεχομένου, οι πάροχοι διαχειριζομένων υπηρεσιών, οι πάροχοι διαχειριζομένων υπηρεσιών ασφάλειας, οι πάροχοι επιγραμμικών αγορών ή επιγραμμικών μηχανών αναζήτησης]. Παράλληλα, λόγω της σημασίας τους σε ευρωπαϊκό επίπεδο, οι πληροφορίες αυτές διαβιβάζονται από την ΕΑΚ στον ENISA, ο οποίος

	είναι επιφορτισμένος με την υποχρέωση τήρησης σχετικού μητρώου σε ενωσιακό επίπεδο.
20	Λαμβάνεται ειδική μέριμνα για την ασφάλεια, τη σταθερότητα και την ανθεκτικότητα του Domain Name System (DNS) και των μητρώων ονομάτων [top-level domain (TLD)], λόγω της ιδιαίτερης κρισιμότητάς τους στην κυβερνοασφάλεια.
21	Εισάγεται ρύθμιση για την ενθάρρυνση ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας μεταξύ οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής του μέρους Α του προτεινόμενου σχεδίου νόμου και, κατά περίπτωση, άλλων οντοτήτων που δεν εμπίπτουν στο πεδίο εφαρμογής του, με στόχο την ενίσχυση του επιπέδου κυβερνοασφάλειας. Επιδιώκεται η συστηματοποίση της ανταλλαγής πληροφοριών μέσω «κοινοτήτων» βασικών και σημαντικών οντοτήτων, των προμηθευτών τους ή παρόχων υπηρεσιών κυβερνοασφάλειας με στόχο την ευρύτερη καλλιέργεια κουλτούρας ασφάλειας στον κυβερνοχώρο.
22	Προβλέπεται η κοινοποίηση πληροφοριών στην ΕΑΚ, οι οποίες αφορούν σε περιστατικά, κυβερνοαπειλές και παρ' ολίγον περιστατικά, σε εθελοντική βάση, πέραν της υποχρεωτικής κοινοποίησης περιστατικών του παρόντος νόμου. Η κοινοποίηση αυτή επιτρέπει στην ΕΑΚ να σχηματίζει εγκαίρως πληρέστερη αντίληψη για την ασφάλεια του κυβερνοχώρου σε εθνικό επίπεδο, δρώντας όχι μόνο κατασταλτικά αλλά και προληπτικά.
23	Προβλέπεται μηχανισμός εποπτείας και επιβολής ο οποίος ενεργεί με λειτουργική ανεξαρτησία κυρίως ως προς την ικανότητά του να ελέγχει και να επιβάλλει κυρώσεις τόσο σε οντότητες του ιδιωτικού τομέα, όσο και σε φορείς της δημόσιας διοίκησης που εμπίπτουν στο πεδίο εφαρμογής του μέρους Α του πρτοεινόμενου σχεδίου νόμου. Με βάση τον Κανονισμό Ελέγχου και Εποπτείας της ΕΑΚ, διασφαλίζονται η εμπειρογνωμοσύνη και η επάρκεια των αρμόδιων ελεγκτών του δημόσιου και του ιδιωτικού τομέα, καθώς και η άντληση εμπειρογνωμοσύνης από πιστοποιημένους από την ίδια, τεχνικούς εμπειρογνώμονες. Για την προστασία του δημοσίου συμφέροντος, και ιδίως των κρατικών φορέων, η εποπτεία αυτών ασκείται αποκλειστικά από τους επιθεωρητές της ΕΑΚ και από πιστοποιημένους από αυτήν επιθεωρητές του δημοσίου, οι οποίοι κατά περίπτωση μπορούν να επικουρούνται από πιστοποιημένο από την ΕΑΚ τεχνικό εμπειρογνώμονα (Subject Matter Experts, SMEs) σύμφωνα με τα ειδικότερα οριζόμενα στον Κανονισμό Ελέγχου και Εποπτείας της ΕΑΚ. Τα έσοδα από τις χρηματικές κυρώσεις που επιβάλλονται σε βάρος φυσικών ή νομικών προσώπων καθώς και τα τέλη εποπτείας και ελέγχου που καταβάλλονται από την οφελούμενη οντότητα, αποτελούν πόρους της ΕΑΚ και διατίθενται αποκλειστικώς για την κάλυψη των λειτουργικών δαπανών της.

24	Αναλύονται τα μέτρα εποπτείας για τις βασικές οντότητες (όπως τακτικοί και στοχευμένοι έλεγχοι ασφάλειας, έκτακτοι ειδικοί έλεγχοι, επιτόπιες επιθεωρήσεις και εποπτεία εκτός των εγκαταστάσεων, συμπεριλαμβανομένων δειγματοληπτικών ελέγχων, σαρώσεις ασφαλείας), καθώς και τα διαθέσιμα μέσα για τις αρμόδιες αρχές (αίτημα παροχής πληροφοριών – πρόσβαση σε στοιχεία, έκδοση δεσμευτικών οδηγιών κ.ά) τα οποία αποσκοπούν στη διασφάλιση τήρησης των υποχρεώσεών τους, λαμβάνοντας ειδική μέριμνα για φορείς της δημόσιας διοίκησης, λόγω του ειδικού καθεστώτος που τους διέπει.
25	Αναλύονται τα μέτρα εποπτείας για τις σημαντικές οντότητες (όπως κατασταλτική εποπτεία εντός και εκτός των εγκαταστάσεων, στοχευμένοι έλεγχοι ασφαλείας, επιτόπιες επιθεωρήσεις και εποπτεία εκτός των εγκαταστάσεων, συμπεριλαμβανομένων δειγματοληπτικών ελέγχων, σαρώσεις ασφαλείας), καθώς και τα διαθέσιμα μέσα για τις αρμόδιες αρχές (όπως αίτημα παροχής πληροφοριών, πρόσβαση σε στοιχεία, έκδοση δεσμευτικών οδηγιών κ.α.). Επιτυγχάνονται με τον τρόπο αυτό η αναγκαία ασφάλεια δικαίου και η διασφάλιση της τήρησης των σχετικών υποχρεώσεων εκ μέρους των υπόχρεων οντοτήτων.
26	Τίθενται γενικοί όροι για την επιβολή διοικητικών προστίμων και κυρώσεων σε βασικές και σημαντικές οντότητες, με στόχο τη θέσπιση ενός αποτελεσματικού, αναλογικού και αποτρεπτικού κυρωτικού πλαισίου, ενώ λαμβάνεται ειδική μέριμνα, αναφορικά με τις οντότητες δημόσιας διοίκησης που εμπίπτουν στο πεδίο εφαρμογής του μέρους Α’ του προτεινόμενου σχεδίου νόμου. Επίσης, θεσπίζεται πλέγμα κυρωτικών ρυθμίσεων σε βάρος φυσικών ή νομικών προσώπων για την παραβίαση των διατάξεων του μέρους Α’ του προτεινόμενου σχεδίου νόμου διασφαλίζοντας την αναλογικότητα, αποτελεσματικότητα και αποτρεπτικότητα του κυρωτικού πλαισίου.
27	Προβλέπεται υποχρέωση ενημέρωσης, χωρίς αδικαιολόγητη καθυστέρηση, της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σε περίπτωση που διαπιστώνεται παραβίαση προσωπικών δεδομένων, στο πλαίσιο της εποπτείας ή της επιβολής κυρώσεων από την ΕΑΚ και ρυθμίζονται ζητήματα που προκύπτουν κατά την επιβολή προστίμων σε αυτήν την περίπτωση.
28	Εισάγεται υποχρέωση της ΕΑΚ, ως αρμόδιας αρχής της Ελλάδας, για παροχή αμοιβαίας συνδρομής σε άλλα κράτη μέλη της Ευρωπαϊκής Ένωσης, σε περίπτωση που μία οντότητα, η οποία εμπίπτει στο πεδίο εφαρμογής του παρόντος, παρέχει υπηρεσίες σε περισσότερα από ένα κράτη μέλη, ένα εκ των οποίων είναι η Ελλάδα, ή παρέχει υπηρεσίες σε ένα ή περισσότερα κράτη μέλη και έχει εγκατάσταση σε έτερο κράτος μέλος και ένα από ως άνω κράτη είναι η Ελλάδα.
29	Περιλαμβάνει εξουσιοδοτικές διατάξεις για τη ρύθμιση συναφών, ειδικότερων τεχνικών και λεπτομερειακών ζητημάτων με κανονιστικές

	αποφάσεις που εκδίδνται από τη διοίκηση κατ' εξουσιοδότηση του νόμου. Η έκδοση κανονιστικών αποφάσεων για την εφαρμογή των αξιολογούμενων ρυθμίσεων του μέρους Α' του προτεινόμενου σχεδίου νόμου κρίνεται αναγκαία λόγω της έντονα τεχνικής διάστασης της κυβερνοασφάλειας και του συνήθως ραγδαίου ρυθμού της τεχνολογικής εξέλιξης. Μέσω των εξουσιοδοτικών διατάξεων διασφαλίζονται η τεχνική ουδετερότητα της αξιολογούμενης ρύθμισης, η διάρκειά της στον χρόνο και η εφαρμογή της σε ένα περιβάλλον διαρκώς μεταβαλλόμενων τεχνικών δεδομένων.
30	Περιλαμβάνει μεταβατικές και τελικές διατάξεις, ώστε να διασφαλιστεί η ομαλή μετάβαση από το υφιστάμενο στο νέο ρυθμιστικό πλαίσιο και να μην υπάρξει κενό στην εφαρμογή των διατάξεων που αφορούν την κυβερνασφάλεια. Ιδίως, διασφαλίζεται η αδιάλειπτη λειτουργία CSIRT μέχρι την έκδοση διαπιστωτικής πράξης του Διοικητή της ΕΑΚ, σχετικά με την επάρκεια των μέσων και πόρων της CSIRT της ΕΑΚ για την αποτελεσματική άσκηση του κρίσιμου ρόλου της και προβλέπεται ότι όπου στην κείμενη νομοθεσία γίνεται αναφορά στον ν. 4577/2018, για ζητήματα σχετικά με την ασφάλεια συστημάτων δικτύου και πληροφοριών, νοείται αναφορά στις αντίστοιχες διατάξεις του πρτοεινόμενου σχεδίου νόμου
31	Περιλαμβάνονται καταργούμενες διατάξεις.
32	Τροποποιείται το άρθρο 21 του ν. 5086/2024 (Α' 23), προκειμένου να διασφαλίζεται ότι η ΕΑΚ επιτελεί αποτελεσματικά τον ενισχυμένο ρόλο της.
33	Τροποποιείται το άρθρο 18 του ν. 4961/2022 (Α' 146), ώστε ελλείψει υπαλλήλου κατηγορίας ΠΕ ή ΤΕ Πληροφορικής να δύναται να ορίζεται ως ΥΑΣΠΕ υπάλληλος οποιουδήποτε κλάδου κατηγορίας ΠΕ ή ΤΕ, διασφαλίζοντας μεθοδολογική αρτιότητα κατά την κάλυψη του κρίσιμου αυτού ρόλου.
34	Ορίζεται η έναρξη ισχύος του πρτοεινόμενου σχεδίου νόμου.

Δ. Έκθεση γενικών συνεπειών

18.	Οφέλη αξιολογούμενης ρύθμισης

			ΘΕΣΜΟΙ, ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ, ΔΙΑΦΑΝΕΙΑ	ΑΓΟΡΑ, ΟΙΚΟΝΟΜΙΑ, ΑΝΤΑΓΩΝΙΣΜΟΣ	ΚΟΙΝΩΝΙΑ & ΚΟΙΝΩΝΙΚΕΣ ΟΜΑΔΕΣ	ΦΥΣΙΚΟ, ΑΣΤΙΚΟ ΚΑΙ ΠΟΛΙΤΙΣΤΙΚΟ ΠΕΡΙΒΑΛΛΟΝ	ΝΗΣΙΩΤΙΚΟΤΗΤΑ
ΟΦΕΛΗ ΡΥΘΜΙΣΗΣ	ΑΜΕΣΑ	Αύξηση εσόδων	**X**	**X**			
		Μείωση δαπανών	**X**	**X**			

		Εξοικονόμηση χρόνου	**x**	**x**	**x**		
		Μεγαλύτερη αποδοτικότητα / αποτελεσματικότητα	**x**	**x**	**x**		
		Άλλο: Ανθεκτικότητα υποδομών	**x**	**x**	**x**	**x**	**x**
	ΕΜΜΕΣΑ	Βελτίωση παρεχόμενων υπηρεσιών	**x**	**x**	**x**		
		Δίκαιη μεταχείριση πολιτών	**x**	**x**	**x**		
		Αυξημένη αξιοπιστία / διαφάνεια θεσμών	**x**	**x**	**x**		
		Βελτιωμένη διαχείριση κινδύνων	**x**	**x**	**x**	**x**	**x**
		Άλλο					

Σχολιασμός / ποιοτική αποτίμηση:

Οι ρυθμίσεις του προτεινόμενου σχεδίου νόμου αναμένεται ότι θα συμβάλλουν στην ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων και δικτύων και στη μείωση του αριθμού και της έκτασης των κυβερνοεπιθέσεων, που μπορούν να έχουν σοβαρές οικονομικές επιπτώσεις τόσο για τον δημόσιο όσο και για τον ιδιωτικό τομέα, καθώς εκτιμάται ότι θα επιτρέψουν την ταχύτερη και αποτελεσματικότερη αντιμετώπιση περιστατικών στον κυβερνοχώρο, προστατεύοντας κρίσιμες υποδομές και υπηρεσίες για τους πολίτες, σε τομείς όπως η υγεία, η ενέργεια και οι μεταφορές. Επίσης, οι ρυθμίσεις του προτεινόμενου σχεδίου νόμου αναμένεται ότι θα ενισχύσουν την εμπιστοσύνη των πολιτών και των επιχειρήσεων στις ψηφιακές υπηρεσίες, αυξάνοντας τη χρήση τους και προωθώντας την ψηφιακή οικονομία, καλλιεργώντας μια κουλτούρα ασφάλειας στον κυβερνοχώρο μέσω της εκπαίδευσης και της ευαισθητοποίησης για τους συνακόλουθους κινδύνους. Περαιτέρω, τα αυξημένα μέτρα ασφαλείας εκτιμάται ότι θα βοηθήσουν τις εγχώριες επιχειρήσεις να παραμείνουν ανταγωνιστικές στην αγορά και να μειώσουν το κόστος από κυβερνοεπιθέσεις και περιστατικά κυβερνοασφάλειας και ότι, επιπλέον, θα συμβάλλουν στην αποτελεσματικότερη προστασία των προσωπικών δεδομένων των πολιτών, μειώνοντας τις πιθανότητες παραβίασης και κατάχρησης των δεδομένων αυτών από κυβερνοεγκληματίες. Επιπρόσθετα, με τις ρυθμίσεις του πρτοεινόμενου σχεδίου νόμου εκτιμάται ότι διασφαλίζεται η παροχή κρίσιμων υπηρεσιών με απομακρυσμένο τρόπο, η οποία πραγματοποιείται με χρήση διαδικτυακών υπηρεσιών.

19.	Κόστος αξιολογούμενης ρύθμισης

			ΘΕΣΜΟΙ, ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ, ΔΙΑΦΑΝΕΙΑ	ΑΓΟΡΑ, ΟΙΚΟΝΟΜΙΑ, ΑΝΤΑΓΩΝΙΣΜΟΣ	ΚΟΙΝΩΝΙΑ & ΚΟΙΝΩΝΙΚΕΣ ΟΜΑΔΕΣ	ΦΥΣΙΚΟ, ΑΣΤΙΚΟ ΚΑΙ ΠΟΛΙΤΙΣΤΙΚΟ ΠΕΡΙΒΑΛΛΟΝ	ΝΗΣΙΩΤΙΚΟΤΗΤΑ
ΚΟΣΤΟΣ ΡΥΘΜΙΣΗΣ	ΓΙΑ ΤΗΝ ΕΝΑΡΞΗ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΡΥΘΜΙΣΗΣ	Σχεδιασμός / προετοιμασία	X	X			
		Υποδομή / εξοπλισμός	X	X			
		Προσλήψεις / κινητικότητα	X	X			
		Ενημέρωση εκπαίδευση εμπλεκομένων	X	X			
		Άλλο					
	ΓΙΑ ΤΗ ΛΕΙΤΟΥΡΓΙΑ & ΑΠΟΔΟΣΗ ΤΗΣ ΡΥΘΜΙΣΗΣ	Στήριξη και λειτουργία διαχείρισης	X	X			
		Διαχείριση αλλαγών κατά την εκτέλεση	X	X			
		Κόστος συμμετοχής στη νέα ρύθμιση		X			
		Άλλο					

Σχολιασμός / ποιοτική αποτίμηση:

Για την αποτελεσματική και αποδοτική εφαρμογή των ρυθμίσεων του προτεινόμενου σχεδίου νόμου, απαιτείται η ενίσχυση, σε επίπεδο υποδομής και στελέχωσης, τόσο του δημόσιου όσο και του ιδιωτικού τομέα και, συνακόλουθα, η εκπαίδευση των στελεχών του, για τη συμμόρφωση με τις ποικίλες απαιτήσεις της Οδηγίας NIS 2. Έτι περαιτέρω, είναι αναγκαία η ενίσχυση της ΕΑΚ, ως αρμόδιας εθνικής αρχής, δεδομένης της αποστολής που καλείται να επιτελέσει, σε συνάρτηση με τις αυξημένες υποχρεώσεις με βάση το εθνικό και ενωσιακό δίκαιο. Πολυάριθμες σχετικές μελέτες, άλλωστε, αναδεικνύουν το έλλειμμα σε εξειδικευμένο ανθρώπινο δυναμικό, ενώ το γεγονός αυτό έχει οδηγήσει τον Ευρωπαϊκό Οργανισμό Κυβερνοασφάλειας να συμπεριλάβει την έλλειψη επιστημονικά καταρτισμένου ανθρώπινου δυναμικού ως μια από τις δέκα (10) βασικές απειλές στον κυβερνοχώρο που αντιμετωπίζουν το σύνολο των κρατών μελών της Ευρωπαϊκής Ένωσης κατά την τρέχουσα δεκαετία.

20.	Κίνδυνοι αξιολογούμενης ρύθμισης

ΘΕΣΜΟΙ, ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ, ΔΙΑΦΑΝΕΙΑ	ΑΓΟΡΑ, ΟΙΚΟΝΟΜΙΑ, ΑΝΤΑΓΩΝΙΣΜΟΣ	ΚΟΙΝΩΝΙΑ & ΚΟΙΝΩΝΙΚΕΣ ΟΜΑΔΕΣ	ΦΥΣΙΚΟ, ΑΣΤΙΚΟ ΚΑΙ ΠΟΛΙΤΙΣΤΙΚΟ ΠΕΡΙΒΑΛΛΟΝ	ΝΗΣΙΩΤΙΚΟΤΗΤΑ

ΚΙΝΔΥΝΟΙ ΡΥΘΜΙΣΗΣ	ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ	Αναγνώριση / εντοπισμός κινδύνου	**X**	**X**			
		Διαπίστωση συνεπειών κινδύνων στους στόχους	**X**	**X**			
		Σχεδιασμός αποτροπής / αντιστάθμισης κινδύνων	**X**	**X**			
		Άλλο					
	ΜΕΙΩΣΗ ΚΙΝΔΥΝΩΝ	Πιλοτική εφαρμογή					
		Ανάδειξη καλών πρακτικών κατά την υλοποίηση της ρύθμισης	**X**	**X**			
		Συνεχής αξιολόγηση διαδικασιών διαχείρισης κινδύνων	**X**	**X**			
		Άλλο					

Σχολιασμός / ποιοτική αποτίμηση:

Η πολυπλοκότητα και κρισιμότητα του τομέα της κυβερνοασφάλειας απαιτεί διαρκή ετοιμότητα, ισχυρό οριζόντιο υπηρεσιακό συντονισμό και συνεργασία. Ο σχετικός κίνδυνος αμβλύνεται λόγω της παρουσίας εθνικών εποπτικών αρχών με υψηλού επιπέδου τεχνογνωσία, σε συνδυασμό με την καθιέρωση μιας ολιστικής προσέγγισης στη διακυβέρνηση της πολιτικής κυβερνοασφάλειας. Σε κάθε περίπτωση, από την εφαρμογή του προτεινόμενου σχεδίου νόμου, υπολογίζεται ότι θα επέλθουν:

Επιβάρυνση της ΕΑΚ με αυξημένο όγκο εργασιών και απαιτήσεων, υπό συνθήκες δυσκολίας προσέλκυσης εξειδικευμένου προσωπικού.

Επιβάρυνση των φορέων του δημόσιου και του ιδιωτικού τομέα, που εμπίπτουν στο πεδίο εφαρμογής του προτεινόμενου σχεδίου νόμου, με υποχρεώσεις λήψης μέτρων κυβερνοασφάλειας. Εντούτοις, επισημαίονεται, ότι η επιβάρυνση είναι αναλογική και δικαιολογημένη, αφορά μεσαίες επιχειρήσεις και άνω και κυμαίνεται ανάλογα με τον βαθμό υφιστάμενης ωριμότητάς τους αναφορικά με την κυβερνοασφάλεια, ενώ αντισταθμίζεται από τη μειωμένη έκθεση σε κινδύνους στον κυβερνοχώρο, την ενίσχυση της ανταγωνιστικότητάς τους, το μειωμένο κόστος ασφάλισης έναντι κινδύνων στον κυβερνοχώρο και τη συνολική ενίσχυση της ανθεκτικότητάς τους. Η ΕΑΚ θα παρέχει καθοδήγηση και τεχνογνωσία στους φορείς για να ανταπεξέλθουν στις έννομες υποχρεώσεις τους, ενώ τα οφέλη από το ενισχυμένο επίπεδο ασφάλειας των δικτύων και πληροφοριακών συστημάτων τους, θα υπερκεράσουν το αρχικό κόστος συμμόρφωσης.

21.	Γνώμες ή πορίσματα αρμόδιων υπηρεσιών και ανεξάρτητων αρχών *(ηλεκτρονική επισύναψη).* Ειδική αιτιολογία σε περίπτωση σημαντικής απόκλισης μεταξύ της γνωμοδότησης και της αξιολογούμενης ρύθμισης.

Ε. Έκθεση διαβούλευσης

22.	Διαβούλευση κατά τη διάρκεια της νομοπαρασκευαστικής διαδικασίας από την έναρξη κατάρτισης της αξιολογούμενης ρύθμισης μέχρι την υπογραφή από τους συναρμόδιους Υπουργούς	
❒	Συνεργασία με άλλα υπουργεία / υπηρεσίες	Έλαβε χώρα διαβούλευση με καθ' ύλην αρμόδια υπουργεία και υπηρεσίες, ιδίως με την Εθνική Υπηρεσία Πληροφοριών, το Γενικό Επιτελείο Εθνικής Άμυνας και τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, για κρίσιμα, συναφή με τις προτεινόμενες ρυθμίσεις, ζητήματα.
❒	Συνεργασία με κοινωνικούς φορείς / Ανεξάρτητες Αρχές	
❒	Διεθνής διαβούλευση	
23.	Σχόλια στο πλαίσιο της διαβούλευσης μέσω της ηλεκτρονικής πλατφόρμας www.opengov.gr *(ηλεκτρονική επισύναψη της έκθεσης)*	

Επί των γενικών αρχών («επί της αρχής») της αξιολογούμενης ρύθμισης	Αριθμός συμμετασχόντων	

	Σχόλια που υιοθετήθηκαν	
	Σχόλια που δεν υιοθετήθηκαν (συμπεριλαμβανομένης επαρκούς αιτιολόγησης)	
Επί των άρθρων της αξιολογούμενης ρύθμισης	Σχόλια που υιοθετήθηκαν	
	Σχόλια που δεν υιοθετήθηκαν (συμπεριλαμβανομένης επαρκούς αιτιολόγησης)	

Στ. Έκθεση νομιμότητας

24.	Συναφείς συνταγματικές διατάξεις	
	Άρθρα 5, 5Α, 9Α, 10, 19, 25, και 106 του Συντάγματος	
25.	Ενωσιακό δίκαιο	
❒	Πρωτογενές ενωσιακό δίκαιο *(συμπεριλαμβανομένου*	1) Άρθρα 8, 11, 16, 17 Χάρτη Θεμελιωδών Δικαιωμάτων Ευρωπαϊκής Ένωσης 2) Άρθρο 346 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ)

	του Χάρτη Θεμελιωδών Δικαιωμάτων)	3) Άρθρο 117 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ)
❒	Κανονισμός	
❒	Οδηγία	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) 910/2014 και της Οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) [L333] .
❒	Απόφαση	
26.	Συναφείς διατάξεις διεθνών συνθηκών ή συμφωνιών	
❒	Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου	Άρθρα 8 και 10 της Ευρωπαικής Σύμβασης Δικαιωμάτων του Ανθρώπου.
❒	Διεθνείς συμβάσεις	

27.	Συναφής νομολογία των ανωτάτων και άλλων εθνικών δικαστηρίων, καθώς και αποφάσεις των Ανεξάρτητων Αρχών	
		Στοιχεία & βασικό περιεχόμενο απόφασης
❒	Ανώτατο ή άλλο εθνικό δικαστήριο (αναφέρατε)	
❒	Ανεξάρτητη Αρχή (αναφέρατε)	
28.	Συναφής ευρωπαϊκή και διεθνής νομολογία	
		Στοιχεία & βασικό περιεχόμενο απόφασης
❒	Νομολογία Δικαστηρίου Ε.Ε.	

❒	Νομολογία Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου	
❒	Άλλα ευρωπαϊκά ή διεθνή δικαστήρια ή διαιτητικά όργανα	

Ζ. Πίνακας τροποποιούμενων ή καταργούμενων διατάξεων

29.	Τροποποίηση – αντικατάσταση – συμπλήρωση διατάξεων	
	Διατάξεις αξιολογούμενης ρύθμισης	*Υφιστάμενες διατάξεις*
	ΤΡΟΠΟΠΟΙΟΥΜΕΝΕΣ ΔΙΑΤΑΞΕΙΣ	
	Άρθρο 32 **Ρυθμίσεις προσωπικού που υπηρετεί στην Εθνική Αρχή Κυβερνοασφάλειας - Τροποποίηση άρθρου 21 του ν. 5086/2024** Στην παρ. 4 του άρθρου 21 του ν. 5086/2024 (Α΄ 23) , περί των μεταβατικών διατάξεων του μέρους Α' του νόμου αυτού, επέρχονται οι ακόλουθες τροποποιήσεις: α) στο πρώτο εδάφιο, η ημερομηνία «31η Δεκεμβρίου 2024» αντικαθίσταται από την ημερομηνία «31η Δεκεμβρίου 2025», β) στο δεύτερο εδάφιο, η ημερομηνία «1η Ιανουαρίου 2025» αντικαθίσταται από την ημερομηνία «1η Ιανουαρίου 2026» και η παρ. 4 διαμορφώνεται ως εξής: «4. Μέχρι την 31η Δεκεμβρίου 2025, το συνολικό κόστος μισθοδοσίας, καθώς και κάθε είδους αποδοχών, περιλαμβανόμενης και της μισθολογικής διαφοράς που προκύπτει από την εφαρμογή του παρόντος βαρύνουν τον προϋπολογισμό του Υπουργείου Ψηφιακής Διακυβέρνησης και καταβάλλονται από αυτό. Με την επιφύλαξη της περ. β) της παρ. 3 του άρθρου 13, από την 1η Ιανουαρίου 2026, το συνολικό κόστος	Η παρ. 4 του άρθρου 21 του ν. 5086/2024 (Α' 23) έχει ως εξής: «4. Μέχρι την 31η Δεκεμβρίου 2024, το συνολικό κόστος μισθοδοσίας, καθώς και κάθε είδους αποδοχών, περιλαμβανόμενης και της μισθολογικής διαφοράς που προκύπτει από την εφαρμογή του παρόντος βαρύνουν τον προϋπολογισμό του Υπουργείου Ψηφιακής Διακυβέρνησης και καταβάλλονται από αυτό. Με την επιφύλαξη της περ. β) της παρ. 3 του άρθρου 13, από την 1η Ιανουαρίου 2025, το συνολικό κόστος μισθοδοσίας, καθώς

μισθοδοσίας, καθώς και κάθε είδους αποδοχών βαρύνουν την Αρχή και καταβάλλονται από αυτήν.».	και κάθε είδους αποδοχών βαρύνουν την Αρχή και καταβάλλονται από αυτήν.».
Άρθρο 33 **Ρυθμίσεις για τον ορισμό Υπεύθυνου Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών - Τροποποίηση παρ. 1 άρθρου 18 ν. 4961/2022** Στην παρ. 1 του άρθρου 18 του ν. 4961/2022 (Α' 146), περί του Υπεύθυνου Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών, επέρχονται οι ακόλουθες τροποποιήσεις: α) στο πρώτο εδάφιο, οι λέξεις «ΠΕ ή ΤΕ Πληροφορικής» αντικαθίστανται από τις λέξεις «ΠΕ κλάδου Πληροφορικής οποιασδήποτε ειδικότητας ή υπάλληλος κατηγορίας ΤΕ κλάδου Πληροφορικής ειδικότητας Πληροφορικής (SOFTWARE ή HARDWARE)», β) προστίθεται νέο, δεύτερο, εδάφιο και η παρ. 1 διαμορφώνεται ως εξής: «1. Σε κάθε φορέα κεντρικής Κυβέρνησης κατά την έννοια της περ. γ` της παρ. 1 του άρθρου 14 του ν. 4270/2014 (Α` 143) ορίζεται, με απόφαση του αρμόδιου Υπουργού ή του οργάνου διοίκησης του φορέα, ένας (1) υπάλληλος κατηγορίας ΠΕ κλάδου Πληροφορικής οποιασδήποτε ειδικότητας ή υπάλληλος κατηγορίας ΤΕ κλάδου Πληροφορικής ειδικότητας Πληροφορικής (SOFTWARE ή HARDWARE) ως Ρ (Υ.Α.Σ.Π.Ε.) με τον αναπληρωτή του. Ελλείψει υπαλλήλου κατηγορίας ΠΕ ή ΤΕ κλάδου Πληροφορικής, με την απόφαση του πρώτου εδαφίου ορίζεται υπάλληλος οποιουδήποτε κλάδου κατηγορίας ΠΕ ή ΤΕ. Ο Υ.Α.Σ.Π.Ε. ορίζεται βάσει της εμπειρίας που διαθέτει στον τομέα της κυβερνοασφάλειας.».	Η παρ. 1 του άρθρου 18 του ν. 4961/2022 (Α' 146) έχει ως εξής: «1. Σε κάθε φορέα κεντρικής Κυβέρνησης κατά την έννοια της περ. γ` της παρ. 1 του άρθρου 14 του ν. 4270/2014 (Α` 143) ορίζεται, με απόφαση του αρμόδιου Υπουργού ή του οργάνου διοίκησης του φορέα, ένας (1) υπάλληλος κατηγορίας ΠΕ ή ΤΕ Πληροφορικής ως Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.) με τον αναπληρωτή του. Ο Υ.Α.Σ.Π.Ε. ορίζεται βάσει της εμπειρίας που διαθέτει στον τομέα της κυβερνοασφάλειας.».
ΚΑΤΑΡΓΟΥΜΕΝΕΣ ΔΙΑΤΑΞΕΙΣ	
Άρθρο 31 περ α'	Άρθρο 148 ν. 4727/2020

Τα άρθρα 148 και 149 του ν. 4727/2020 (Α' 184), καταργούνται.	Ασφάλεια δικτύων και υπηρεσιών (άρθρο 40 της Οδηγίας (ΕΕ) 2018/1972) 1. Οι πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών λαμβάνουν πρόσφορα και αναλογικά τεχνικά και οργανωτικά μέτρα για την κατάλληλη διαχείριση του κινδύνου όσον αφορά την ασφάλεια των δικτύων και υπηρεσιών. Τα μέτρα αυτά, λαμβάνοντας υπόψη τις πλέον προηγμένες τεχνικές δυνατότητες, πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τον υπάρχοντα κίνδυνο. 2. Ειδικότερα, οι πάροχοι λαμβάνουν μέτρα, συμπεριλαμβανομένης της κρυπτογράφησης, όπου κρίνεται σκόπιμο, για την αποτροπή και ελαχιστοποίηση των επιπτώσεων από συμβάντα ασφάλειας που επηρεάζουν τους χρήστες και άλλα δίκτυα και υπηρεσίες. Οι πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών κοινοποιούν αμελλητί στην Α.Δ.Α.Ε. κάθε συμβάν ασφάλειας που είχε σημαντικό αντίκτυπο στη λειτουργία των δικτύων και υπηρεσιών. Η Α.Δ.Α.Ε. με τη σειρά της: α) κοινοποιεί αμελλητί κάθε συμβάν, του οποίου λαμβάνει γνώση σύμφωνα με το προηγούμενο εδάφιο, στην Εθνική Αρχή Κυβερνοασφάλειας που έχει οριστεί σύμφωνα με τις διατάξεις του ν. 4577/2018 (Α` 199) και β) κοινοποιεί τα συμβάντα που έχουν αντίκτυπο στη διαθεσιμότητα ή στην ακεραιότητα δικτύων ή υπηρεσιών στην Ε.Ε.Τ.Τ. Για να προσδιοριστεί η σοβαρότητα του αντίκτυπου ενός συμβάντος ασφάλειας, λαμβάνονται υπόψη ιδίως, οι ακόλουθες παράμετροι όπου είναι διαθέσιμες: α) ο αριθμός των χρηστών που επηρεάζονται από το συμβάν ασφάλειας,

	β) η διάρκεια του συμβάντος ασφάλειας, γ) το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν ασφάλειας, δ) ο βαθμός στον οποίο επηρεάζεται η ασφάλεια ή/και η λειτουργία του δικτύου ή της υπηρεσίας, ε) η έκταση του αντίκτυπου στις οικονομικές και κοινωνικές δραστηριότητες. Κατά περίπτωση, η Α.Δ.Α.Ε. ενημερώνει τις αρμόδιες αρχές στα άλλα κράτη - μέλη, καθώς και τον Οργανισμό της Ε.Ε. για την Ασφάλεια Δικτύων και Πληροφοριών («ENISA»). Η Α.Δ.Α.Ε. μπορεί να ενημερώσει το κοινό ή να απαιτήσει την ενημέρωση αυτή από τους παρόχους, εφόσον κρίνει ότι η αποκάλυψη του συμβάντος ασφάλειας είναι προς το δημόσιο συμφέρον. Η Α.Δ.Α.Ε. υποβάλλει κατ` έτος στην Ευρωπαϊκή Επιτροπή και στον ENISA συνοπτική έκθεση σχετικά με τις κοινοποιήσεις που έχει παραλάβει και τη δράση που έχει αναλάβει σύμφωνα με την παρούσα παράγραφο. Η έκθεση του προηγούμενου εδαφίου κοινοποιείται και στην Εθνική Αρχή Κυβερνοασφάλειας. 3. Σε περίπτωση ιδιαίτερης και σημαντικής απειλής για συμβάν ασφάλειας σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών ή διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών, οι πάροχοι των εν λόγω δικτύων ή υπηρεσιών ενημερώνουν τους χρήστες τους, που θα μπορούσαν να επηρεαστούν από μια τέτοια απειλή, σχετικά με τυχόν πιθανά προστατευτικά ή διορθωτικά μέτρα τα οποία μπορούν να ληφθούν από τους χρήστες. Κατά περίπτωση, οι πάροχοι ενημερώνουν επίσης τους χρήστες τους για την ίδια την απειλή. 4. Το παρόν άρθρο ισχύει με την επιφύλαξη του Κανονισμού (ΕΕ)

	2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (L 119), του ν. 4624/2019 (Α` 137) και του ν. 3471/2006 (Α` 133). Άρθρο 149 ν. 4727/2020 Εφαρμογή και επιβολή (άρθρο 41 της Οδηγίας (ΕΕ) 2918/1972) 1. Η Α.Δ.Α.Ε., σε εφαρμογή του άρθρου 148, εκδίδει κανονιστικές πράξεις, συμπεριλαμβανομένων εκείνων που αφορούν τα μέτρα που απαιτούνται για την αντιμετώπιση συμβάντων ασφάλειας ή για την αποτροπή τους, όταν εντοπιστεί σημαντική απειλή, καθώς και τις προθεσμίες εφαρμογής τους, προς τους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών. 2. Η Α.Δ.Α.Ε. απαιτεί από τους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών: α) να παρέχουν πληροφορίες απαραίτητες για την εκτίμηση της ασφάλειας των δικτύων και υπηρεσιών τους, περιλαμβανομένων τεκμηριωμένων πολιτικών ασφάλειας, και β) να υποβάλονται στον έλεγχό της ως προς την ασφάλεια. Το κόστος του ελέγχου επιβαρύνει τον πάροχο. Η πληροφόρηση για την εκτίμηση ασφάλειας δικτύων και υπηρεσιών, περιλαμβανομένων των πολιτικών ασφαλείας, σύμφωνα με την περ. α`, καθώς και τα αποτελέσματα των ελέγχων, σύμφωνα με τα οριζόμενα στην περ. β``, κοινοποιούνται από την Α.Δ.Α.Ε.

	στην Εθνική Αρχή Κυβερνοασφάλειας, όποτε αυτό απαιτηθεί από τη δεύτερη. 3. Η Α.Δ.Α.Ε. διαθέτει όλες τις απαραίτητες εξουσίες για τη διενέργεια ελέγχων για τη διερεύνηση της συμμόρφωσης προς το τεθέν κανονιστικό πλαίσιο, καθώς και για τη διερεύνηση περιπτώσεων μη συμμόρφωσης με αυτό και των επιπτώσεών τους στην ασφάλεια των δικτύων και υπηρεσιών. 4. Όταν παραβιάζονται οι υποχρεώσεις του παρόντος άρθρου, επιβάλλεται από την Α.Δ.Α.Ε. για κάθε παράβαση στους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, ανάλογα με τη βαρύτητα της παράβασης, τον βαθμό υπαιτιότητας και την περίπτωση υποτροπής, μία από τις παρακάτω κυρώσεις: α) σύσταση για συμμόρφωση μέσα στα χρονικά όρια της τασσόμενης προθεσμίας με προειδοποίηση επιβολής προστίμου σε περίπτωση παράλειψης συμμόρφωσης, β) πρόστιμο από δεκαπέντε χιλιάδες ευρώ (15.000 €) έως ένα εκατομμύριο πεντακόσιες χιλιάδες ευρώ (1.500.000 €). Οι εν λόγω κυρώσεις επιβάλλονται με αιτιολογημένη απόφαση της Α.Δ.Α.Ε. ύστερα από προηγούμενη κλήση του ενδιαφερομένου για παροχή εξηγήσεων. Οι αποφάσεις που εκδίδονται κατ` εφαρμογή των διατάξεων του παρόντος άρθρου, υπόκεινται σε προσφυγή ουσίας ενώπιον του Διοικητικού Εφετείου Αθηνών. 5. Για την εφαρμογή του άρθρου 148, η Α.Δ.Α.Ε. επι-κουρείται από Ομάδα Απόκρισης για συμβάντα που αφορούν την Ασφάλεια Υπολογιστών («Computer Security Incident Response Team», «CSIRT»), η οποία ορίζεται σύμφωνα με

	την παρ. 1 του άρθρου 8 του ν. 4577/2018. 6. Η Α.Δ.Α.Ε. συνεργάζεται κατά περίπτωση, σύμφωνα με τις διατάξεις της κείμενης νομοθεσίας, με τις αρμόδιες αρχές επιβολής του νόμου, με την Εθνική Αρχή Κυβερνοασφάλειας, και με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.).
Άρθρο 31 περ β' Τα άρθρα 1 έως 16 του ν. 4577/2018 (Α΄ 199) καταργούνται.	