Πλατής - Αναστασιάδης
& Συνεργάτες

Η συνεργαζόμενη δικηγορική εταιρία
με την ΕΥ Ελλάδος

Ιανουάριος 2025

Law Alert

Κανονισμός για την κυβερνοανθεκτικότητα (Cyber Resilience Act): Οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία

Ο Κανονισμός για την κυβερνοανθεκτικότητα θεσπίζει κανόνες για την προστασία των καταναλωτών και των επιχειρήσεων που αγοράζουν ή χρησιμοποιούν λογισμικό ή προϊόντα με ψηφιακά στοιχεία. Ο Κανονισμός εισάγει απαιτήσεις κυβερνοασφάλειας για τους οικονομικούς φορείς που εμπλέκονται στην παραγωγή και διάθεση τέτοιων προϊόντων, ενώ οι απαιτήσεις κυβερνοασφάλειας επεκτείνονται σε όλο τον κύκλο ζωής του προϊόντος.

Στις 23 Οκτωβρίου 2024 δημοσιεύτηκε στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης ο Κανονισμός (Ε.Ε.) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Οκτωβρίου 2024 που θεσπίζει οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία («Κανονισμός για την κυβερνοανθεκτικότητα» ή «Κανονισμός»).

Ο Κανονισμός καθορίζει ενιαίες απαιτήσεις κυβερνο-ασφάλειας για τον σχεδιασμό, την ανάπτυξη, την παραγωγή και τη διάθεση στην Ε.Ε. προϊόντων με ψηφιακά στοιχεία.

Με τον Κανονισμό επιβάλλονται υποχρεώσεις για την τήρηση απαιτήσεων κυβερνοασφάλειας στους κατασκευαστές, εισαγωγείς, διανομείς, ή άλλα πρόσωπα που σχετίζονται με την κατασκευή προϊόντων με ψηφιακά στοιχεία ή σε σχέση με τη διάθεση στην αγορά προϊόντων με ψηφιακά στοιχεία. Ο Κανονισμός ανακοινώθηκε το 2020 στο πλαίσιο της Στρατηγικής της Ε.Ε. για την ασφάλεια στον κυβερνοχώρο, η οποία προστατεύει πολίτες, επιχειρήσεις και θεσμικά όργανα από απειλές στον κυβερνοχώρο και προωθεί διεθνή συνεργασία και ένα παγκόσμιο, ανοικτό Διαδίκτυο. Στο πλαίσιο αυτό, ο Κανονισμός λειτουργεί συμπληρωματικά με τη νομοθεσία στον συγκεκριμένο τομέα και ειδικότερα την Οδηγία NIS2.

Σύμφωνα με τον Κανονισμό, καταναλωτές και επιχειρήσεις θα μπορούν στο εξής να προβαίνουν σε πιο τεκμηριωμένες επιλογές, έχοντας εμπιστοσύνη στα διαπιστευτήρια κυβερνοασφάλειας των προϊόντων με σήμανση CE.

1. Αντικείμενο & Πεδίο Εφαρμογής

Ο Κανονισμός εφαρμόζεται σε προϊόντα με ψηφιακά στοιχεία που διατίθενται στην αγορά των οποίων ο σκοπός ή η χρήση περιλαμβάνει λογική ή φυσική σύνδεση δεδομένων με συσκευή ή δίκτυο.

Ως Προϊόν με ψηφιακά στοιχεία ορίζεται στον Κανονισμό κάθε προϊόν λογισμικού ή υλισμικού και οι οικείες λύσεις εξ αποστάσεως επεξεργασίας δεδομένων, συμπεριλαμβανομένων των δομοστοιχείων λογισμικού ή υλισμικού που τίθενται σε κυκλοφορία στην αγορά χωριστά.

Χαρακτηριστικό παράδειγμα τέτοιου είδους προϊόντων αποτελούν τα έξυπνα οικιακά προϊόντα, ατομικές φερόμενες συσκευές καθώς και υλισμικό και λογισμικό που αν και λιγότερο κρίσιμα, θεωρείται ότι μπορούν να διευκολύνουν τη διατάραξη της λειτουργίας μιας συσκευής ή δικτύου.

Στο ουσιαστικό πεδίο του Κανονισμού εμπίπτουν οι κατασκευαστές, διανομείς, εισαγωγείς και λοιποί οικονομικοί φορείς που προμηθεύουν ψηφιακά προϊόντα στην αγορά της Ένωσης.

2. Απαιτήσεις Κυβερνοασφάλειας

Ο Κανονισμός προβλέπει ότι τα προϊόντα με ψηφιακά στοιχεία καθίσταται διαθέσιμα στην αγορά μόνο εφόσον πληρούν ουσιώδεις απαιτήσεις κυβερνοασφάλειας και οι διαδικασίες που εφαρμόζει ο κατασκευαστής τους συμμορφώνονται με τις απαιτήσεις αυτές.

Βάσει εκτίμησης κινδύνου από τον κατασκευαστή, πρέπει μεταξύ άλλων να διατίθενται με ασφαλή διαμόρφωση, να προστατεύουν από μη εξουσιοδοτημένη πρόσβαση, να διασφαλίζουν την εμπιστευτικότητα και ακεραιότητα των δεδομένων, να προστατεύουν τη διαθεσιμότητα βασικών λειτουργιών και να ελαχιστοποιούν αρνητικές επιπτώσεις.

Περαιτέρω, ως προς τις απαιτήσεις χειρισμού ευπαθειών, οι κατασκευαστές πρέπει να εντοπίζουν και να τεκμηριώνουν τις ευπάθειες των προϊόντων, να τις αντιμετωπίζουν άμεσα, να εφαρμόζουν δοκιμές και αξιολογήσεις ασφαλείας και να έχουν πολιτική για τη γνωστοποίηση ευπαθειών και μηχανισμούς για αυτόματες ενημερώσεις ασφαλείας.

Εξυπακούεται ότι τα προϊόντα με ψηφιακά στοιχεία καθίστανται διαθέσιμα στην αγορά μόνον εφόσον πληρούν τις ανωτέρω απαιτήσεις ασφαλείας, όπως αυτές ειδικότερα ορίζονται στο Παράρτημα I μέρος I & II του Κανονισμού.

3. Διαδικασία Αξιολόγησης

Ο Κανονισμός προβλέπει ειδικές υποχρεώσεις για τους οικονομικούς φορείς όσων προϊόντων χαρακτηρίζονται ως σημαντικά ή κρίσιμα.

Ειδικότερα, ως σημαντικά προϊόντα με ψηφιακά στοιχεία ορίζονται αυτά που απαριθμούνται στο Παράρτημα III του Κανονισμού και υποδιαιρούνται σε Κλάσεις I και II. Πρόκειται ουσιαστικά για τα προϊόντα που παρουσιάζουν υψηλότερο κίνδυνο κυβερνοασφάλειας και θα πρέπει να υποβάλλονται σε αυστηρότερη διαδικασία αξιολόγησης της συμμόρφωσης. Τα προϊόντα αυτά, υπόκεινται στις διαδικασίες αξιολόγησης της συμμόρφωσης που αναφέρονται στο άρθρο 32 παράγραφοι 2 (όσον αφορά την Κλάση I) και 3 (όσον αφορά την κρισιμότερη Κλάση II) του Κανονισμού. Επισημαίνεται ότι όσον αφορά τα προϊόντα που εντάσσονται στην Κλάση II, θεωρούνται υψηλότερης κρισιμότητας και άρα υπόκεινται σε αυστηρότερες διαδικασίες αξιολόγησης συμμόρφωσης, συμπεριλαμβανομένης της αξιολόγησης από εξωτερικά τρίτα μέρη.

Περαιτέρω, ως κρίσιμα προϊόντα με ψηφιακά στοιχεία ορίζονται όσα απαριθμούνται στο Παράρτημα IV του Κανονισμού. Τα κρίσιμα προϊόντα, υπόκεινται σε αυστηρότερες απαιτήσεις αξιολόγησης της συμμόρφωσης, καθώς απαιτείται να λαμβάνουν ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας ή/και υπόκεινται σε αξιολόγηση από εξωτερικό τρίτο μέρος.

Κατά τα λοιπά, για τα προϊόντα με ψηφιακά στοιχεία που δεν αναφέρονται ως σημαντικά ή κρίσιμα προϊόντα βάσει του Κανονισμού, θεσπίζεται διαδικασία αυτοαξιολόγησης της συμμόρφωσης που διενεργείται από τον κατασκευαστή με δική του ευθύνη.

4. Υποχρεώσεις κατασκευαστών

Πριν από τη διάθεση των προϊόντων με ψηφιακά στοιχεία στην αγορά της Ένωσης, οι κατασκευαστές υποχρεούνται να:

- Αξιολογούν πιθανούς κινδύνους βάσει της χρήσης και της διάρκειας ζωής του προϊόντος,
- Ενσωματώνουν ασφαλή εξαρτήματα και ασκούν επιμέλεια κατά την προμήθεια αυτών από τρίτους,
- Εφαρμόζουν πολιτικές για την αντιμετώπιση ευπαθειών και τη γνωστοποίησή τους,
- Προετοιμάζουν τεχνική τεκμηρίωση και διεξάγουν αξιολόγηση συμμόρφωσης,
- Εκδίδουν δήλωση συμμόρφωσης ΕΕ και τοποθετούν τη σήμανση CE,
- Περιλαμβάνουν πληροφορίες αναγνώρισης και στοιχεία κατασκευαστή στο προϊόν ή τη συσκευασία,
- Παρέχουν υποστήριξη για τουλάχιστον 5 χρόνια ή για τη διάρκεια ζωής του προϊόντος,
- Διασφαλίζουν ότι οι ενημερώσεις ασφαλείας παραμένουν διαθέσιμες για τουλάχιστον 10 χρόνια ή κατά την περίοδο παροχής υποστήριξης.

Επιπρόσθετα, σύμφωνα με τον Κανονισμό, οι κατασκευαστές πρέπει να πληρούν τις ακόλουθες υποχρεωτικές απαιτήσεις τεκμηρίωσης:

- Τεχνικό φάκελο, ο οποίος μεταξύ άλλων περιλαμβάνει τις σχετικές πτυχές κυβερνοασφάλειας, συμπεριλαμβανομένων των ευπαθειών, σχετικές πληροφορίες που παρέχονται από τρίτους και επικαιροποιήσεις της εκτίμησης κινδύνων κυβερνοασφάλειας των προϊόντων. Ο τεχνικός φάκελος θα πρέπει να διατηρείται για 10 χρόνια ή για την περίοδο υποστήριξης.
- Δήλωση συμμόρφωσης ΕΕ, η οποία αποδεικνύει τη συμμόρφωση με βασικές απαιτήσεις του Κανονισμού και πρέπει να διατηρείται για 10 χρόνια ή για την περίοδο υποστήριξης.
- Πληροφορίες και οδηγίες χρήστη, σε κατανοητή γλώσσα, για ασφαλή εγκατάσταση, λειτουργία και χρήση. Οι πληροφορίες αυτές πρέπει να είναι προσβάσιμες για 10 χρόνια ή για την περίοδο υποστήριξης, είτε διαδικτυακά είτε σε φυσική μορφή.

Τέλος, στους κατασκευαστές επιβάλλονται ορισμένες υποχρεώσεις αναφοράς και ειδικότερα υποχρεούνται να:

- Ενημερώνουν την ΟΑΠΑΥ εντός 24 ωρών για ευπάθειες στα προϊόντα τους,
- Ειδοποιούν την ΟΑΠΑΥ εντός 24 ωρών για περιστατικά που επηρεάζουν την ασφάλεια του προϊόντος,
- Ενημερώνουν εγκαίρως τους χρήστες για περιστατικά και παρέχουν μέτρα μετριασμού,
- Αναφέρουν ευπάθειες σε ενσωματωμένα εξαρτήματα στους αντίστοιχους συντηρητές.

5. Υποχρεώσεις εισαγωγέων, διανομέων και λοιπών τρίτων μερών

Ως προς τους εισαγωγείς, ο Κανονισμός προβλέπει την υποχρέωση να διασφαλίζουν τη συμμόρφωση με τις βασικές απαιτήσεις κυβερνοασφάλειας που ορίζονται στο Παράρτημα Ι του Κανονισμού, να ελέγχουν ότι ο κατασκευαστής έχει διεξάγει αξιολόγηση συμμόρφωσης, να επιβεβαιώνουν ότι η τεχνική τεκμηρίωση είναι διαθέσιμη και το προϊόν με ψηφιακά στοιχεία φέρει τη σήμανση CE, να παρέχουν τα απαραίτητα στοιχεία επικοινωνίας και να περιλαμβάνουν φιλικές προς τον χρήστη οδηγίες και πληροφορίες του προϊόντος.

Για την εισαγωγή προϊόντων με ψηφιακά στοιχεία στην αγορά της Ένωσης, θα πρέπει να εξασφαλίζεται τεχνική τεκμηρίωση, σήμανση CE πληροφορίες, οδηγίες χρήσης, στοιχεία επικοινωνίας του εισαγωγέα καθώς και δήλωση συμμόρφωσης ΕΕ του κατασκευαστή. Σε περίπτωση που ο εισαγωγές υποψιάζεται έλλειψη συμμόρφωσης του προϊόντος θα πρέπει να αποφεύγει τη διάθεσή του στην αγορά, ενώ σε περίπτωση κινδύνου κυβερνοασφάλειας ενημερώνει τον κατασκευαστή και τις αρχές εποπτείας της αγοράς.

Αντίστοιχες υποχρεώσεις βαρύνουν και τους διανομείς, οι οποίοι πρέπει να ενεργούν με δέουσα προσοχή και να ελέγχουν ότι το προϊόν με ψηφιακά στοιχεία φέρει τη σήμανση CE και ότι κατασκευαστές και εισαγωγείς έχουν εκπληρώσει τις υποχρεώσεις συμμόρφωσής τους. Πρέπει επίσης να αποφεύγουν τη διάθεση μη συμμορφούμενων προϊόντων στην αγορά και να ενημερώνουν τον κατασκευαστή και τις αρχές εποπτείας της αγοράς για οποιουσδήποτε κινδύνους κυβερνοασφάλειας.

Τέλος, φυσικό ή νομικό πρόσωπο που πραγματοποιεί ουσιαστική τροποποίηση σε προϊόν με ψηφιακά στοιχεία και το διαθέτει στην αγορά, θεωρείται κατασκευαστής και υπόκειται στις αντίστοιχες υποχρεώσεις.

6. Υποχρεώσεις για τους φορείς ανάπτυξης λογισμικού

Ο Κανονισμός εφαρμόζεται και στα συνδέσιμα προϊόντα λογισμικού, επιβάλλοντας υποχρεώσεις στους φορείς ανάπτυξης λογισμικού.

Στο πλαίσιο αυτό, οι εν λόγω φορείς πρέπει να διασφαλίζουν τη συμμόρφωση με τις απαιτήσεις κυβερνοασφάλειας εφαρμόζοντας σύγχρονα μέτρα ασφαλείας και βέλτιστες πρακτικές για την αντιμετώπιση των εντοπισμένων κινδύνων, παρέχοντας προϊόντα με ασφαλείς προεπιλεγμένες ρυθμίσεις και επιτρέποντας στους χρήστες να τα επαναφέρουν σε ασφαλή κατάσταση αν χρειαστεί. Περαιτέρω, οι φορείς ανάπτυξης λογισμικού, πρέπει να εντοπίζουν και να εξαλείφουν ευπάθειες, να αποτρέπουν μη εξουσιοδοτημένη πρόσβαση και να αναφέρουν παραβιάσεις καθώς και να επεξεργάζονται μόνο τα απαραίτητα δεδομένα, διασφαλίζοντας την εμπιστευτικότητα και ακεραιότητα των δεδομένων. Επιπλέον, πρέπει να διασφαλίζουν ότι οι βασικές λειτουργίες παραμένουν ενεργές μετά από περιστατικά, μετριάζοντας κινδύνους όπως επιθέσεις άρνησης υπηρεσίας, και να παρέχουν ασφαλείς επιλογές για διαγραφή και μεταφορά δεδομένων μεταξύ προϊόντων ή συστημάτων.

Ως προς την τεχνική τεκμηρίωση, οι φορείς ανάπτυξης λογισμικού οφείλουν να τηρούν κατάλογο υλικών λογισμικού και δήλωση συμμόρφωσης ΕΕ η οποία πρέπει να είναι προσβάσιμη στους χρήστες και να περιλαμβάνει πληροφορίες συμμόρφωσης του λογισμικού. Τέλος, οι φορείς ανάπτυξης λογισμικού πρέπει να παρέχουν στις εποπτικές αρχές τα στοιχεία οποιοδήποτε οικονομικού φορέα στον οποίο έχουν προμηθεύσει λογισμικό, αλλά και να τηρούν την εν λόγω πληροφορία για 10 έτη.

7. Εποπτεία, κυρώσεις & εφαρμογή

Ο Κανονισμός προβλέπει ότι κάθε κράτος μέλος ορίζει μία ή περισσότερες αρχές εποπτείας της αγοράς για τη διασφάλιση της αποτελεσματικής εφαρμογής του. Ως προς τις κυρώσεις, προβλέπονται πρόστιμα που κυμαίνονται από €5.000.000 έως €15.000.000 και από 1% έως 2,5% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του φορέα, ανάλογα με τη φύση της παραβίασης. Εναπόκειται στα κράτη μέλη να καθορίσουν τους ειδικότερους κανόνες για τις κυρώσεις που επιβάλλονται σε περίπτωση παραβιάσεων των διατάξεων του Κανονισμού.

Ο Κανονισμός τίθεται σε εφαρμογή την 11η Δεκεμβρίου 2027. Παρά ταύτα οι υποχρεώσεις αναφοράς των κατασκευαστών τίθενται σε εφαρμογή από την 11η Σεπτεμβρίου 2026 ενώ οι προβλέψεις σχετικά με την κοινοποίηση των οργανισμών αξιολόγησης της συμμόρφωσης, εφαρμόζονται από την 11η Ιουνίου 2026.

Ο Κανονισμός για την Κυβερνοανθεκτικότητα είναι διαθέσιμος εδώ.

Πλατής - Αναστασιάδης και Συνεργάτες, Δικηγορική Εταιρεία

Η Δικηγορική Εταιρεία Πλατής - Αναστασιάδης και Συνεργάτες είναι μέλος του δικτύου EY Law με παρουσία σε 90 χώρες παγκοσμίως και αποτελείται από δυναμικό 3.500+ συνεργατών.

Πιο συγκεκριμένα, είμαστε μία ανεξάρτητη δικηγορική εταιρεία που στελεχώνεται από 45 δικηγόρους. Η Εταιρεία μας παρέχει νομικές υπηρεσίες υψηλής ποιότητας σε ένα ευρύ πλαίσιο εμπορικών και χρηματοοικονομικών συναλλαγών.

Ιδιαίτερα στη γεωγραφική μας περιφέρεια, έχουμε διαρκή συνεργασία με τις αντίστοιχες δικηγορικές εταιρείες συνεργαζόμενες με την EY, προκειμένου να προσφέρουμε με επαγγελματισμό και συνέπεια υπηρεσίες στους πελάτες μας με διασυνοριακές συναλλαγές.

Η εμπειρία μας, μας επιτρέπει να αντιλαμβανόμαστε καλύτερα τις ανάγκες των πελατών μας και να τους προσφέρουμε ολοκληρωμένες λύσεις που λαμβάνουν υπόψιν τους τομείς της λογιστικής, της φορολογίας και των χρηματοοικονομικών συμβουλευτικών υπηρεσιών.

Η πρακτική που υιοθετείται από τη Δικηγορική Εταιρεία Πλατής - Αναστασιάδης και Συνεργάτες είναι η έμφαση στην εξεύρεση λύσεων. Συνεργαζόμαστε στενά με τους πελάτες μας προκειμένου να υιοθετήσουμε καινοτόμους και πρακτικούς τρόπους αντιμετώπισης των θεμάτων που τους απασχολούν. Βασική προτεραιότητά μας είναι να βοηθήσουμε τους πελάτες μας να επιτύχουν τους επαγγελματικούς τους στόχους. Η πείρα, η αφοσίωση και ο ενθουσιασμός που μας διακρίνει έχουν σαν αποτέλεσμα τη δημιουργία ενός ισχυρού πελατολογίου στο οποίο περιλαμβάνονται εγχώριες και διεθνείς εισηγμένες εταιρείες, εταιρείες Δημοσίου και Ιδιωτικού τομέα και χρηματοπιστωτικά ιδρύματα.

Για περισσότερες πληροφορίες σχετικά με θέματα ψηφιακού δικαίου, μπορείτε να επικοινωνείτε με τους:

Ειρηνικό Πλατή
Partner
eirinikos.platis@gr.ey.com

Αντώνιο Μπρούμα
Senior Manager
antonios.broumas@gr.ey.com

στη δικηγορική εταιρεία
Πλατής - Αναστασιάδης και Συνεργάτες
Τηλ.: +30 210 2886 512
legaloffice@gr.ey.com

ey.com

EY EY Greece eygreece @EY_Greece EY Greece