PAPATRIANTAFYLLOU & THANASENARI

Compliance

Overview

Papatriantafyllou & Thanasenari
217 Alexandras Av., Athens, tel. +302106440368
web:https://www.pathlawfirm.gr/

Πεδίο Εφαρμογής

Η NIS2 είναι Οδηγία της Ευρωπαϊκής ένωσης και έρχεται για να επεκτείνει κατά πολύ το πεδίο εφαρμογής της NIS1 Οδηγίας, η οποία έχει μεταφερθεί στην Ελληνική Έννομη τάξη με τον νόμο 4577/2018. Στις 28 Νοεμβρίου 2024, υιοθετήθηκε και **τέθηκε σε άμεση ισχύ*** ο Ν.5160/2024 μου μεταφέρει τη NIS 2 στην Ελλάδα.

Η νέα νομοθεσία θέτει, μεταξύ άλλων

- Αυστηρότερες απαιτήσεις για τις επιχειρήσεις, τη δημόσια διοίκηση, τις υποδομές.
- Αυστηρότερες υποχρεώσεις κυβερνοασφάλειας για τη διαχείριση κινδύνων, τις υποχρεώσεις υποβολής εκθέσεων και την ανταλλαγή πληροφοριών.

Οι απαιτήσεις καλύπτουν, μεταξύ άλλων διατάξεων, την αντιμετώπιση συμβάντων, την ασφάλεια της αλυσίδας εφοδιασμού, την κρυπτογράφηση και τη δημοσιοποίηση τρωτών σημείων.

Περισσότερα νομικά πρόσωπα και τομείς θα πρέπει να λάβουν μέτρα για την προστασία τους. Ακόμη, «βασικοί τομείς», όπως της ενέργειας, των μεταφορών, των τροφίμων, των τραπεζών, της υγείας, των ψηφιακών υποδομών, της δημόσιας διοίκησης και του διαστήματος, θα καλύπτονται από τις νέες διατάξεις.

*Για τους οργανισμούς τοπικής αυτοδιοίκησης, οι διατάξεις του Ν.5160/2024 θα τεθούν σε ισχύ από 28.11.2025

Ο τομέας της παραγωγής, μεταποίησης και διανομής τροφίμων αποτελεί έναν από τους νέους τομείς, οι οποίοι προστίθενται στο πεδίο εφαρμογής την NIS 2.

Συγκεκριμένα, η Οδηγία NIS2 (Άρθρο 2) και ο Ν. 5160/2024 (Άρθρο 3) εφαρμόζονται και σε ιδιωτικές οντότητες στον τομέα της παραγωγής, μεταποίησης και διανομής τροφίμων, οι οποίες χαρακτηρίζονται ως μεσαίες επιχειρήσεις ή υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις και ασκούν τις δραστηριότητές τους εντός της ΕΕ. Τα ακριβή κριτήρια για την ένταξη στη βαθμίδα “μεσαίες επιχειρήσεις” ή σε ανώτερη βαθμίδα τα ορίζει το άρθρο 2 του παραρτήματος της Σύστασης 2003/361/ΕΚ. Ειδικότερα, ως μεσαίες χαρακτηρίζονται επιχειρήσεις με περισσότετρους από 50 εργαζομένους, των οποίων ο ετήσιος κύκλος εργασιών ή το σύνολο του ετήσιου ισολογισμού υπερβαίνει τα 10 εκατομμύρια ευρώ

Η Οδηγία NIS2 και ο Ν.5160/2024 αφορούν, μεταξύ άλλων:

- Όλες τις μεσαίες επιχειρήσεις (απασχολούν περισσότερους από 50 εργαζομένους και έχουν κύκλο εργασιών που υπερβαίνει τα 10 εκατομύρια ευρώ) ή και μεγάλες επιχειρήσεις που δραστηριοποιούνται ενδεικτικά στους τομείς της Ενέργειας, των Μεταφορών, της Υγείας, Υπηρεσιών Cloud και Data Centers, Τηλεπικοινωνιών, **Παραγωγής και Διανομής Τροφίμων**, Παραγωγής Χημικών Προϊόντων, Φαρμακευτικών Προϊόντων, Διαχείρισης Λυμάτων και Αποβλήτων & Εταιριών Ταχυμεταφορών.

Ημερομηνία Εαρμογής

Το άρθρο 41 της Οδηγίας ορίζει οτι έως τις 17 Οκτωβρίου 2024, τα κράτη μέλη θεσπίζουν και δημοσιεύουν τα μέτρα που απαιτούνται προκειμένου να συμμορφωθούν προς αυτήν, Η Ελλάδα καθυστέρησε λίγους μήνες την υιοθέτηση του Ν.5160/2024, ωστόσο αυτός έχει **πλέον άμεση ισχύ** ήδη από την ημερομηνία έκδοσής του (28.11.2024). Εντός 3 μηνών από την ημερομηνία ισχύος του, δηλαδή έως τις 28.02.2025, θα πρέπει οι δημόσιοι και οι ιδιωτικοί φορείς που δεσμεύονται από τις διατάξεις του Ν.5160/2024 να ανακοινώσουν και να λάβουν τα κατάλληλα μέτρα συμμόρφωσης, προκειμένου να μην βρίσκονται αντιμέτωποι με αυστηρά διοικητικά πρόστιμα

Κυρώσεις

Για να διασφαλιστεί ότι οι απαιτήσεις της NIS2 και του Ν.5160/2024 μπορούν να εφαρμοστούν αποτελεσματικά, ο Ν.5160/2024 εισάγει ένα σύνολο ελέγχων (Άρθρα 14 έως 17), συμπεριλαμβανομένων προστίμων και άλλων διοικητικών κυρώσεων (Άρθρα 26 έως 27):

- Όταν παραβιάζουν τις υποχρεώσεις των άρθρων 21 ή 23, οι σημαντικές οντότητες υπόκεινται σε διοικητικά πρόστιμα ύψους κατ' ανώτατο όριο **7.000.000,00 Ευρώ ή κατ' ανώτατο όριο 1,4 % του κατά το προηγούμενο οικονομικό έτος συνολικού παγκόσμιου ετήσιου κύκλου εργασιών τους**.
- Κατά περίπτωση **περιορίζεται** ή και **αναστέλλεται** η λειτουργία της επιχείρησης.

Η Οδηγία NIS 2 και ο Ν. 5160/2024 επιβάλλουν αυστηρές κυρώσεις για τη μη συμμόρφωση, οι οποίες καθορίζονται από την αρμόδια αρχή του κάθε Κράτους Μέλους της ΕΕ, ήτοι την Εθνική Αρχή Κυβερνοασφάλειας στην Ελλάδα.

Η Ομάδα μας

Τα μέλη της ομάδας μας διαθέτουν τις πλέον αναγνωρισμένες πιστοποιήσεις στον τομέα διεθνώς, όπως CIPP/E, CIPM, CIPT και FIP πιστοποιήσεις από την International Association of Privacy Professionals (IAPP), ενώ αποτελούν μέλη σε ομάδες ειδικών σε επίπεδο Ευρωπαϊκής Ένωσης, όπως η δεξαμενή ειδικών του Ευρωπαϊκού Συμβουλίου Προστασίας Προσωπικών Δεδομένων (EDPB), του Internet Privacy Engineering Network (IPEN) του Ευρωπαίου Επόπτη Προστασίας Δεδομένων (EDPS), καθώς και του Δικτύου Εμπειρογνωμόνων Προστασίας Δεδομένων της Europol (EDEN). Συχνά, αποτελούν ομιλητές σε κορυφαία συνέδρια στην Ελλάδα και στο εξωτερικό, αρθρογραφούν σε διεθνώς καταξιωμένα νομικά περιοδικά για σχετικές θεματικές, και συμμετέχουν ως εξωτερικοί σύμβουλοι σε ερευνητικά προγράμματα της Ευρωπαϊκής Ένωσης ή μέλη σε σχετικές ακαδημαϊκές ερευνητικές ομάδες και think tank. Τέλος, έχουν λάβει βραβεία και αναγνώριση, όπως η συμπερίληψή τους στη λίστα 20 Under 40 Compliance του περιοδικού LAWYER.

Η πολυετής εμπειρία και εξειδίκευσή τους εγγυάται την παροχή αξιόπιστων συμβουλών και υπηρεσιών συμμόρφωσης σε σύνθετα ζητήματα που σχετίζονται με την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) , καθώς επίσης και άλλων νομικών ζητημάτων που αφορούν τις νέες τεχνολογίες και την κυβερνοασφάλεια.

Ακόμη, παρέχουμε συμβουλευτικές υπηρεσίες και υπηρεσίες συμμόρφωσης σε υποθέσεις που σχετίζονται με την Οδηγία για τις πληρωμές (Payment Services Directive 2 – PSD2), που ενσωματώθηκε στην ελληνική νομοθεσία με τον νόμο 4537/2018, ή την Οδηγία για το υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών (NIS Directive και πλέον NIS2), και τον Κανονισμό 2022/2554 για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα (DORA).

Οκτώ γραμμές υπηρεσιών

- Συμβουλές Συμόρφωσης
- Έκπαίδευση
- Audit Report / Maturity Scan
- Certification Counseling
- Incident Response Plan
- Risk Assessment Report
- Δικαστικές διαφορές
- Έλεγχος Εποπτικών Αρχών

1. Συμβουλές Συμμόρφωσης

Παρέχουμε υποστήριξη συμμόρφωσης για να βοηθήσουμε τους πελάτες μας να συμβαδίζουν με το μεταβαλλόμενο κανονιστικό τοπίο και να συμμορφωθούν με τα κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια συστημάτων δικτύου και πληροφοριακών συστημάτων που χρησιμοποιούν για τις δραστηριότητές τους ή για την παροχή των υπηρεσιών τους, όπως ορίζονται στις διατάξεις του Κεφαλαίου Δ του Ν.5160/2024.

Συγκεκριμένα, όπως ορίζει το Άρθρο 14 του Ν.5160/2024, εντός 3 μηνών από την ημερομηνία ισχύος του, δηλαδή έως τις 28.02.2025, τα όργανα διοίκησης των οντοτήτων που δεσμεύουν οι διατάξεις του νόμου θα πρέπει να εγκρίνουν τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, να επιβλέπουν ήδη την εφαρμογή τους, καθώς και να είναι υπεύθυνα για την εκ μέρους τους παραβίαση των υποχρεώσεων που ανακύπτουν από τη νομοθεσία. Οπότε, από τον Μάρτιο του 2025, όλες οι οντότητες θα έχουν να αντιμετωπίσουν κυρώσεις.

Αναλαμβάνουμε την παροχή δημιουργικών και πρακτικών συμβουλών προκειμένου να βοηθήσουμε τους πελάτες μας να συμμορφωθούν με τις διατάξεις των Άρθρων 15 και 16 του Ν.5160/2024 προκειμένου να λάβουν τα αναγκαία μέτρα διαχείρισης κινδύνων αλλά και να συμμορφωθούν με τις υποχρεώσεις τους αναφοράς περιστατικών ασφάλειας υπολογιστών στις αρμόδιες αρχές.

Βοηθάμε τους πελάτες μας με τον εντοπισμό και τη διερεύνηση περιστατικών ασφαλείας, παρέχουμε συμβουλές για τις σχετικές υποχρεώσεις, και συνδράμουμε στην προετοιμασία των αναγκαίων επικοινωνιών στις αρμόδιες αρχές.

2. Εκπαίδευση

Το άρθρο 20 της NIS2 και το άρθρο 14 του Ν. 5160/2024 ορίζουν ότι τα μέλη της ανώτατης διοίκησης των σημαντικών οντοτήτων υποχρεούνται να παρακολουθούν εκπαίδευση, ενώ παρόμοια κατάρτιση θα πρέπει να προσφέρεται και στους υπαλλήλους τους σε τακτική βάση, προκειμένου να αποκτούν επαρκείς γνώσεις και δεξιότητες που θα τους επιτρέπουν να εντοπίζουν τους κινδύνους και να αξιολογούν τις πρακτικές διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τον αντίκτυπό τους στις υπηρεσίες που παρέχει η κάθε οντότητα.

Αναλαμβάνουμε σχετικές εκπαιδευτικές δράσεις. Έχουμε αναπτύξει μία εύληπτη, διαδραστική και περιεκτική παρουσίαση για την κάθε ομάδα στόχο (ανώτατη διοίκηση και υπάλληλοι), οι οποία μπορεί να προσαρμοστεί στις ανάγκες της δικής σας επιχείρησης.

3. Audit Report / Maturity Scan

Με βάση το άρθρο 21 της NIS2 και το Άρθρο 15 του Ν.5160/2024 υπάρχουν συγκεκριμένα διαχειριστικά μέτρα στα οποία οι σημαντικές οντότητες θα πρέπει να υιοθετήσουν (από πολιτικές για την ανάλυση κινδύνου και την ασφάλεια των πληροφοριακών συστημάτων και τον χειρισμό περιστατικών, μέχρι διαχείριση αντιγράφων ασφαλείας, πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, βασικές πρακτικές κυβερνοϋγιεινής, πολιτικές και διαδικασίες σχετικά με τη χρήση κρυπτογραφίας και, κατά περίπτωση, κρυπτογράφησης κοκ).

Αναλαμβάνουμε να ελέγχουμε σε τι βαθμό συμμόρφωσης βρίσκεται ο κάθε πελάτης (τι έχει από αυτά τα μέτρα ήδη υιοθετήσει, ποια κενά υπάρχουν, κλπ), και να καταρτίζουμε μία μελέτη που να τους ενημερώνουμε για το επίπεδο συμμόρφωση που βρίσκονται ήδη και για τα αναγκαία μέτρα που οφείλουν να υιοθετήσουν.

4. Certification Counseling

Με την NIS2 υιοθετείται μία σειρά από Ευρωπαϊκά Πιστοποιητικά, όπως ορίζεται στο άρθρο 24, τα οποία πιστοποιούν ότι τα μέσα και τα εργαλεία που χρησιμοποιεί μία εταιρεία είναι σε υψηλό επίπεδο και πληρούν τις προϋποθέσεις κυβερνοασφάλειας. Αντίστοιχες προβλέψεις περιέχονται και στο Άρθρο 15 του Ν.5160/2024.

Αναλαμβάνουμε την ενημέρωση και την έκδοση των κατάλληλων κατά περίπτωση Ευρωπαϊκών Πιστοποιητικών που είναι διαθέσιμα.

5. Incident Response Plan

Στο άρθρο 23 της Οδηγίας NIS2 και στο Άρθρο 16 του Ν.5160/2024 προβλέπεται οτι οι σημαντικές οντότητες έχουν συγκεκριμένες υποχρεώσεις επικοινωνίας περιστατικών κυβερνοεπιθέσεων σε διαφορετικές οντότητες (ανάλογα με την περίσταση από τις εθνικές Ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT), τις εθνικές αρμόδιες αρχές, τους αποδέκτες των υπηρεσιών τους κοκ).

Αν σε αυτά τα περιστατικά υφίσταντο και απώλειες προσωπικών δεδομένων ή γενικότερη παραβίαση της νομοθεσίας για προστασία προσωπικών δεδομένων (data breach notifications), τότε προστίθενται στις υποχρεώσεις επικοινωνίας και άλλες αρχές ή κατά περίπτωση ακόμα και υποκείμενα δεδομένων.

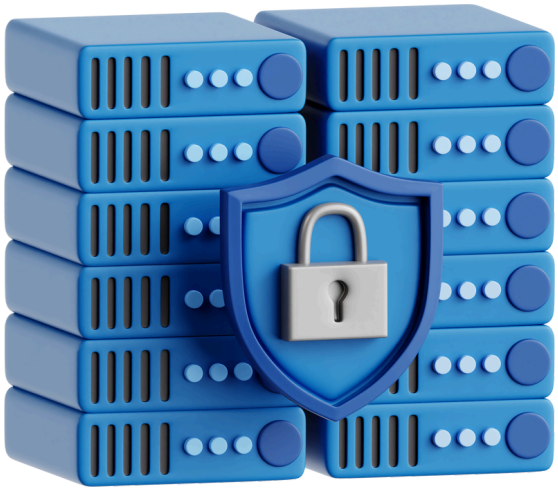
Καταρτίζουμε πολιτικές διαχείρισης περιστατικών, προκειμένου ανάλογα με το κάθε περισταστικό κυβερνοασφάλειας οι πελάτες μας να γνωρίζουν σε πρώτη φάση με ποιον, πως και μέχρι πότε οφείλουν να το επικοινωνήσουν. Η πολιτική αυτή έχει ως στόχο να δημιουργήσει εσωτερικά στην κάθε επιχείρηση ένα μοντέλο απόκρισης και επικοινωνίας τέτοιων συμβάντων, ανάλογα με τον χαρακτήρα τους, ενώ επιπλέον αναλάβουμε συμβουλευτικές υπηρεσίες επί εκάστοτε περιστατικού.

6. Risk Assessment Report

Όταν παραβιάζουν τις υποχρεώσεις της Οδηγίας, οι επιχειρήσεις υπόκεινται σε διοικητικά πρόστιμα ύψους κατ' ανώτατο όριο τουλάχιστον 7 000 000 EUR ή κατ' ανώτατο όριο τουλάχιστον 1,4 % του κατά το προηγούμενο οικονομικό έτος συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκει η σημαντική οντότητα, ανάλογα με το ποιο είναι υψηλότερο.

Επιπλέον, κατά περίπτωση δύναται να περιορίζεται ή και αναστέλλεται η λειτουργεία της επιχείρησης.

Πραγματοποιούμε ανάλυση των εκτιμώμενων κινδύνων τόσο για τις πιθανότητες ελέγχου όσο και για την επιβολή τυχόν προστίμων.



7. Δικαστικές Διαφορές

Παρέχουμε συμβουλές και εκπροσωπούμε οργανισμούς σε όλο το φάσμα των καταγγελιών, αξιώσεων και διαφορών που σχετίζονται με την προστασία δεδομένων, την κυβερνοασφάλεια και την ιδιωτικότητα.

Η ομάδα μας για την προστασία των δεδομένων και την κυβερνοασφάλεια υποστηρίζεται από τους συνεργάτες μας που ειδικεύονται στην επίλυση διαφορών, με απαράμιλλης εμπειρίας, η οποία έχει αποκτηθεί σε δικαστήρια όλων των βαθμίδων δικαιοδοσίας.

Ανάλογα με τα χαρακτηριστικά κάθε υπόθεσης δικαστικής διαμάχης, συγκροτούμε μια ομάδα εξειδικευμένων συνεργατών, οι οποίοι συνεργάζονται στενά μαζί σας.

8. 'Ελεγχος από Ρυθμιστικές Αρχές

Η ομάδα μας διαθέτει εκτεταμένη εμπειρία σε διαδικασίες ελέγχων από τις ρυθμιστικές αρχές. Προετοιμάζουμε οργανισμούς για την αντιμετώπιση αυριανών ελέγχων από τις αρμόδιες Αρχές και τους συμβουλεύουμε και τους υποστηρίζουμε καθ' όλη τη διάρκεια της διαδικασίας.

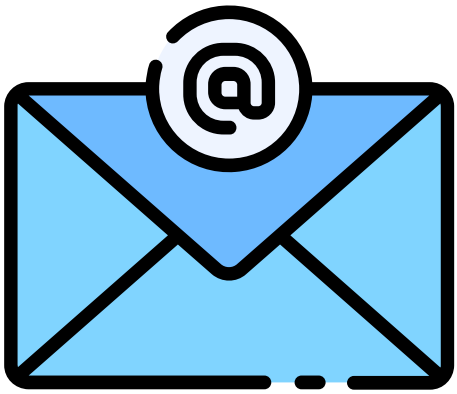
Πριν από τον έλεγχο, παρέχουμε εκπαιδεύσεις στους υπαλλήλους και προετοιμάζουμε σχετικές εσωτερικές πολιτικές.

Κατά τη διάρκεια του ελέγχου, η ομάδα μας υποστηρίζει τον οργανισμό, ώστε να προστατεύονται τα δικαιώματά του καθ' όλη τη διάρκεια της διαδικασίας, διασφαλίζοντας σημαντικά ότι ο έλεγχος παραμένει εντός του νομικού πλαισίου.

Μετά από τον έλεγχο, συμβουλεύουμε σχετικά με τα επόμενα βήματα και προσφέρουμε υποστήριξη σχετικά με τις διαδικασίες παρακολούθησης και επιβολής από τις εποπτικές αρχές.

Εκπροσώπηση

Εκπροσωπήσουμε τους πελάτες μας ενώπιον των δημοσίων αρχών, εστιάζοντας στην προστασία των δικαιωμάτων και των συμφερόντων τους. Παρέχουμε επίσης υπηρεσίες που σχετίζονται με τη νομοθετική διαδικασία - νομοθετική παρακολούθηση, ανάλυση επιπτώσεων και στρατηγικό σχεδιασμό και επικοινωνία με τις δημόσιες αρχές για την προώθηση των συμφερόντων του οργανισμού σας.



Για περισσότερες πληροφορίες μην διστάζετε να επικοινωνήσετε μαζί μας

Papatriantafyllou & Thanasenari
217 Alexandras Avenue,
Athens Greece
tel. +302106440368
web:https://www.pathlawfirm.gr/