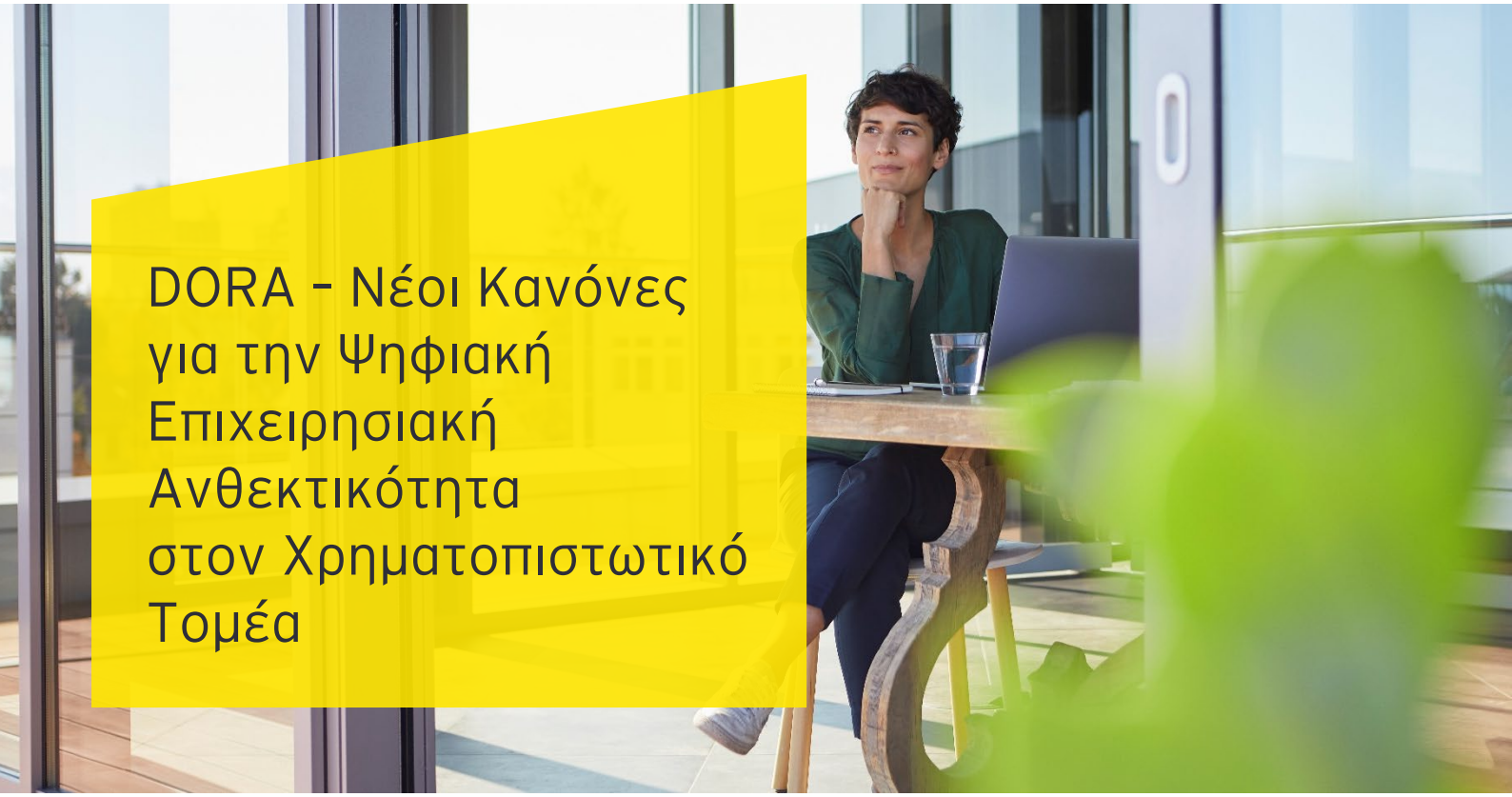
Δεκέμβριος 2022

Law Alert

Πλατής - Αναστασιάδης & Συνεργάτες

Η συνεργαζόμενη δικηγορική εταιρία με την ΕΥ Ελλάδος



DORA – Νέοι Κανόνες για την Ψηφιακή Επιχειρησιακή Ανθεκτικότητα στον Χρηματοπιστωτικό Τομέα

Ο Κανονισμός DORA καθορίζει ενιαίες απαιτήσεις σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών που υποστηρίζουν τις επιχειρηματικές διαδικασίες των χρηματοπιστωτικών οντοτήτων με στόχο την επίτευξη υψηλού κοινού επιπέδου ψηφιακής επιχειρησιακής ανθεκτικότητας του χρηματοπιστωτικού τομέα σε ολόκληρη την Ευρωπαϊκή Ένωση.

Στις 17 Νοεμβρίου 2022, τα θεσμικά όργανα της ΕΕ ενέκριναν τον Κανονισμό για την Ψηφιακή Επιχειρησιακή Ανθεκτικότητα για τον Χρηματοπιστωτικό Τομέα («DORA» ή «Πράξη»).

Ο Κανονισμός, ο οποίος προτάθηκε από την Επιτροπή στις 24 Σεπτεμβρίου 2020 ως μέρος της Δέσμης Μέτρων για τον Ψηφιακό Οικονομικό Τομέα 2020, αποτελεί την πιο σταθερή πρωτοβουλία της Ευρωπαϊκής Ένωσης ("ΕΕ") για τη διασφάλιση της ασφάλειας και της ανθεκτικότητας του Ευρωπαϊκού Χρηματοπιστωτικού Τομέα σε συνθήκες γρήγορου ψηφιακού μετασχηματισμού.

Το εκτεταμένο πεδίο εφαρμογής της Πράξης περιλαμβάνει, μεταξύ άλλων, πιστωτικά και χρηματοδοτικά ιδρύματα, παρόχους υπηρεσιών κρυπτοστοιχείων, τόπους διαπραγμάτευσης και αρχεία καταγραφής συναλλαγών, παρόχους επενδυτικών υπηρεσιών, οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας, παρόχους υπηρεσιών πληθοχρηματοδότησης και, επίσης, τρίτους παρόχους υπηρεσιών Τεχνολογιών Πληροφορικής & Επικοινωνιών («ΤΠΕ»).

Όσον αφορά τις προαναφερθείσες οντότητες, ο DORA προβλέπει υποχρεώσεις που σχετίζονται με (α) τη διαχείριση κίνδυνων των ΤΠΕ, (β) την αναφορά συμβάντων που σχετίζονται με ΤΠΕ, (γ) τις ψηφιακές δοκιμές επιχειρησιακής ανθεκτικότητας, (δ) την ανταλλαγή στοιχείων και πληροφοριών σε σχέση με απειλές και ευπάθειες στον κυβερνοχώρο και με (ε) τη διαχείριση κινδύνων τρίτων στις ΤΠΕ.

Προκειμένου να προωθηθεί η καινοτομία, η Πράξη επιτρέπει ένα πιο αναλογικό σύνολο υποχρεώσεων για τις χρηματοπιστωτικές οντότητες που χαρακτηρίζονται ως πολύ μικρές επιχειρήσεις έναντι μεγαλύτερων χρηματοπιστωτικών ιδρυμάτων, τα οποία είναι υποχρεωμένα να θεσπίζουν πιο σύνθετες δομές διακυβέρνησης.

Επιπλέον, η Πράξη θεσπίζει ρητά την αρχή της αναλογικότητας τόσο στην εποπτεία όσο και στην τήρηση των διατάξεών της, σύμφωνα με την οποία οι χρηματοοικονομικές οντότητες αναμένεται γενικά να εφαρμόζουν τις απαιτήσεις της Πράξης με αναλογικό τρόπο, λαμβάνοντας υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου τους, καθώς και τη φύση, το μέγεθος και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών τους.

Η DORA θα τεθεί σε εφαρμογή 24 μήνες και είκοσι (20) ημέρες μετά τη δημοσίευσή της στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

1. **Απαιτήσεις Διαχείρισης Κινδύνου ΤΠΕ**
   Η Πράξη θεσπίζει τη γενική υποχρέωση των χρηματοπιστωτικών οντοτήτων να διαθέτουν πλαίσιο εσωτερικής διακυβέρνησης και ελέγχου που διασφαλίζει την αποτελεσματική και συνετή διαχείριση των κινδύνων ΤΠΕ υπό την επίβλεψη και ευθύνη των οργάνων διαχείρισης τους.

   Επιπλέον, οι χρηματοπιστωτικές οντότητες υποχρεούνται να διαθέτουν ένα υγιές, περιεκτικό και καλά τεκμηριωμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ, το οποίο περιλαμβάνει μια ψηφιακή επιχειρησιακή στρατηγική ανθεκτικότητας και κατάλληλες, αξιόπιστες, επαρκείς και τεχνολογικά ανθεκτικές πολιτικές, διαδικασίες, πρωτόκολλα και εργαλεία ΤΠΕ μαζί με μια ανεξάρτητη λειτουργία ελέγχου εντός του οργανισμού τους.

   Σύμφωνα με το πλαίσιο αυτό, οι χρηματοπιστωτικές οντότητες οφείλουν, από τη μία πλευρά, να ταξινομούν τις επιχειρηματικές λειτουργίες, τους ρόλους, τις ευθύνες και τα περιουσιακά στοιχεία που υποστηρίζονται από ΤΠΕ, καθώς και τους ρόλους και τις εξαρτήσεις τους σε σχέση με τον κίνδυνο ΤΠΕ.

   Από την άλλη πλευρά, απαιτείται να εντοπίζουν, σε συνεχή βάση, όλες τις πηγές κινδύνου ΤΠΕ, να αξιολογούν τις απειλές στον κυβερνοχώρο και τις ευπάθειες των ΤΠΕ και να προβαίνουν σε αξιολόγηση κινδύνου για κάθε σημαντική αλλαγή στις υποδομές, τις διαδικασίες και τα περιουσιακά τους στοιχεία.

   Επιπλέον, έχουν την υποχρέωση να αναπτύσσουν κατάλληλα εργαλεία, πολιτικές και διαδικασίες για την ασφάλεια των ΤΠΕ, συμπεριλαμβανομένης μιας πολιτικής ασφάλειας πληροφοριών και πολιτικών για ισχυρή επαλήθευση ταυτότητας, διαχείριση αλλαγών, ενημερώσεις κώδικα και επικαιροποιήσεις.

   Επιπρόσθετα, να διαθέτουν (α) μηχανισμούς ανίχνευσης ανώμαλων δραστηριοτήτων, (β) πολιτική αδιάλειπτης λειτουργίας της επιχείρησης και σχέδια αντιμετώπισης και αποκατάστασης των ΤΠΕ, (γ) πολιτικές δημιουργίας αντιγράφων ασφαλείας και μεθόδους αποκατάστασης, διαδικασίες και μεθόδους αποκατάστασης και ανάκτησης και (δ) διαδικασίες ελέγχου μετά από συμβάντα που σχετίζονται με τις ΤΠΕ. Μια καινοτομία που εισήγαγε η πράξη είναι η απαίτηση για τις υπόχρεες οντότητες να διενεργούν αναλύσεις επιχειρηματικών επιπτώσεων («ΑΕΕ») των εκθέσεών τους σε σοβαρές επιχειρηματικές διαταραχές ως μέσο για την ανάπτυξη μεθόδων διαχείρισης σεναρίων κινδύνου.

   Τέλος, ως μέρος του πλαισίου διαχείρισης κινδύνου ΤΠΕ, οι χρηματοπιστωτικές οντότητες οφείλουν να διαθέτουν σχέδια επικοινωνίας σε καταστάσεις κρίσης επιτρέποντας την υπεύθυνη γνωστοποίηση, τουλάχιστον, σημαντικών περιστατικών ή τρωτών σημείων που σχετίζονται με τις ΤΠΕ σε πελάτες και ομολόγους καθώς και στο κοινό, όπως αρμόζει.

2. **Απαιτήσεις Αναφοράς Συμβάντων σε Σχέση με ΤΠΕ**
   Σχετικά με την αναφορά συμβάντων, η DORA επιβάλλει τις ακόλουθες υποχρεώσεις στις χρηματοπιστωτικές οντότητες:

   - Τη δημιουργία και εφαρμογή μιας διαδικασίας διαχείρισης συμβάντων που σχετίζονται με τις ΤΠΕ.
   - Την τήρηση αρχείου για περιστατικά που σχετίζονται με τις ΤΠΕ και απειλές στον κυβερνοχώρο.
   - Τον συνεπή και ολοκληρωμένο έλεγχο, χειρισμό και παρακολούθηση συμβάντων που σχετίζονται με τις ΤΠΕ, ώστε να εξασφαλιστεί ότι τα βαθύτερα αίτια προσδιορίζονται.
   - Την ταξινόμηση των συμβάντων που σχετίζονται με τις ΤΠΕ με βάση την σοβαρότητα των υπηρεσιών που διατρέχουν κίνδυνο και τον προσδιορισμό των επιπτώσεών τους.

Σύμφωνα με την Πράξη, οι χρηματοοικονομικές οντότητες αναφέρουν σημαντικά περιστατικά που σχετίζονται με τις ΤΠΕ στις αρμόδιες εποπτικές αρχές, οι οποίες μπορούν να παρέχουν σχόλια και καθοδήγηση σχετικά με τον χειρισμό τέτοιων συμβάντων. Τα περιστατικά που έχουν ταξινομηθεί ως σημαντικά και προκαλούνται σε πιστωτικά ιδρύματα αναφέρονται από τις εθνικές αρχές στην ΕΚΤ.

Όταν συμβαίνει ένα σημαντικό περιστατικό που σχετίζεται με τις ΤΠΕ και έχει αντίκτυπο στα οικονομικά συμφέροντα των πελατών, οι χρηματοπιστωτικές οντότητες θα πρέπει, αδικαιολόγητη καθυστέρηση, αμέσως μόλις λάβουν γνώση του περιστατικού, να προβαίνουν σε σχετική ειδοποίηση στους πελάτες τους και επίσης να τους ενημερώνουν για μέτρα μετριασμού του.

3. **Απαιτήσεις Δοκιμών Ψηφιακής Επιχειρησιακής Ανθεκτικότητας**
Οι χρηματοπιστωτικές οντότητες, εκτός από τις πολύ μικρές επιχειρήσεις, υποχρεούνται επίσης να καθιερώσουν, να διατηρούν και να επανεξετάζουν ένα υγιές και περιεκτικό ψηφιακό πρόγραμμα δοκιμών επιχειρησιακής ανθεκτικότητας ως αναπόσπαστο μέρος του πλαισίου διαχείρισης των κινδύνων από ΤΠΕ.

Οι σχετικές δοκιμές, όπως αξιολογήσεις και σαρώσεις ευπάθειας, αναλύσεις λογισμικών ανοικτής πηγής («open source»), αξιολογήσεις ασφάλειας δικτύου, αναλύσεις ελλείψεων, επισκοπήσεις φυσικής ασφάλειας, λύσεις λογισμικού ερωτηματολογίων και σάρωσης, επανεξετάσεις κωδίκων πηγής, όπου αυτό είναι εφικτό, δοκιμές βάσει σεναρίων, δοκιμές συμβατότητας, δοκιμές επιδόσεων, διατερματικές δοκιμές και δοκιμές διείσδυσης θα πραγματοποιούνται από ανεξάρτητα μέρη, είτε εσωτερικά ή εξωτερικά.

Τουλάχιστον κάθε τρία (3) έτη, οι χρηματοπιστωτικές οντότητες υποχρεούνται επίσης να διενεργούν αναβαθμισμένους δοκιμές διείσδυσης βάσει απειλών σε πολλές ή όλες τις κρίσιμες ή σημαντικές λειτουργίες, που εκτελούνται σε συστήματα παραγωγής εν πλήρη λειτουργία.

Στο τέλος κάθε τέτοιας δοκιμής, η χρηματοπιστωτική οντότητα και, κατά περίπτωση, οι εξωτερικοί ελεγκτές θα παρέχουν στην αρμόδια αρχή μία περίληψη των αποτελεσμάτων της δοκιμής και η Αρχή με τη σειρά της θα παρέχει βεβαίωση ότι η δοκιμή πραγματοποιήθηκε σύμφωνα με τις απαιτήσεις του DORA.

4. **Ανταλλαγή Πληροφοριών για Απειλές και Ευπάθειες**
Οι χρηματοπιστωτικές οντότητες αποκτούν το δικαίωμα να ανταλλάσσουν μεταξύ τους στοιχεία και πληροφορίες για απειλές στον κυβερνοχώρο, συμπεριλαμβανομένων των δεικτών έκθεσης σε κίνδυνο, τακτικών, τεχνικών και διαδικασιών, προειδοποιήσεων κυβερνοασφάλειας και εργαλείων παραμετροποίησης, στον βαθμό που η εν λόγω ανταλλαγή στοιχείων και πραγματοποιείται στο πλαίσιο αξιόπιστων ενώσεων χρηματοπιστωτικών οντοτήτων μέσω ρυθμίσεων ανταλλαγής πληροφοριών που προστατεύουν τον δυνητικά ευαίσθητο χαρακτήρα των ανταλλασσόμενων πληροφοριών.

5. **Διαχείριση Κινδύνων Τρίτων στις ΤΠΕ**
Σύμφωνα με τις διατάξεις του DORA, οι χρηματοπιστωτικές οντότητες υποχρεούνται να διαχειρίζονται τον κίνδυνο τρίτων στις ΤΠΕ ως αναπόσπαστο στοιχείο του πλαισίου διαχείρισης κινδύνων ΤΠΕ που εφαρμόζουν, μεταξύ άλλων, σύμφωνα με τις ακόλουθες προϋποθέσεις:

- Τη θέσπιση στρατηγικής για τον κίνδυνο τρίτων παρόχων ΤΠΕ, εφαρμόζοντας μια στρατηγική πολλαπλότητας προμηθευτών. Η στρατηγική αυτή για τον κίνδυνο τρίτων παρόχων ΤΠΕ περιλαμβάνει την πολιτική για τη χρήση υπηρεσιών ΤΠΕ που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ που υποστηρίζει κρίσιμες ή σημαντικές λειτουργίες.
- Την τήρηση μητρώου πληροφοριών όσον αφορά το σύνολο των συμβατικών ρυθμίσεων σχετικά με τη χρήση υπηρεσιών ΤΠΕ που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ.
- Την ετήσια αναφορά στην αρμόδια αρχή των νέων συμβατικών ρυθμίσεων με τρίτους παρόχους υπηρεσιών ΤΠΕ και των παρεχόμενων από αυτούς υπηρεσιών και λειτουργιών ΤΠΕ.
- Την αξιολόγηση των υπηρεσιών ΤΠΕ που ανατίθενται σε εξωτερικούς συνεργάτες, τη συγκέντρωση των κινδύνων και την ανάληψη κάθε δέουσας επιμέλειας των υποψήφιων τρίτων παρόχων υπηρεσιών ΤΠΕ πριν από τη σύναψη συμβατικών ρυθμίσεων.
- Την συμπερίληψη, εάν εμπλέκεται η υποστήριξη κρίσιμων ή σημαντικών λειτουργιών, ενός συνόλου όρων στις συμβάσεις με τρίτους παρόχους υπηρεσιών ΤΠΕ. Κατά τη διαπραγμάτευση των συμβατικών ρυθμίσεων, οι χρηματοπιστωτικές οντότητες και οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ λαμβάνουν υπόψη τη χρήση τυποποιημένων συμβατικών ρητρών που έχουν εκδοθεί από τις αρμόδιες Αρχές.

6. Πλαίσιο Εποπτείας & Εποπτικές Εξουσίες

Η DORA παραχωρεί νέες ευρείες εξουσίες σε εθνικές και ευρωπαϊκές εποπτικές αρχές για την εποπτεία κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ.

Ειδικότερα, οι ESAs έχουν την εξουσία να ορίζουν τους τρίτους παρόχους υπηρεσιών ΤΠΕ που είναι κρίσιμοι για τις χρηματοπιστωτικές οντότητες.

Οι αρμόδιες αρχές έχουν επίσης την εξουσία να διενεργούν επιθεωρήσεις σε μεμονωμένους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ και να εκδίδουν συστάσεις.

Όσον αφορά την εποπτεία, οι αρμόδιες αρχές διαθέτουν όλες τις εξουσίες εποπτείας, διερεύνησης και επιβολής κυρώσεων που απαιτούνται για την εκπλήρωση των καθηκόντων τους βάσει της πράξης, συμπεριλαμβανομένης της διενέργειας επιτόπιων ελέγχων, της εντολής για διορθωτικά μέτρα και μέτρα αποκατάστασης, και της επιβολής αποτελεσματικών, αναλογικών και αποτρεπτικών διοικητικών ποινών.

7. Δευτερογενές Ρυθμιστικό Πλαίσιο

Βασική πτυχή του DORA είναι η παραχώρηση ευρείων εξουσιών στις Ευρωπαϊκές Εποπτικές Αρχές («ESAs»), δηλαδή στην EBA, ESMA και EIOPA, για τη θέσπιση των δευτερογενών κανόνων που θα καταστήσουν δυνατή τη λειτουργία του πλαισίου κανόνων του Κανονισμού.

Ως εκ τούτου, εντός 24 μηνών από την έναρξη ισχύος της Πράξης, οι ESAs θα εκδίδουν από κοινού Ρυθμιστικά Τεχνικά Πρότυπα ("RTS") και Εκτελεστικά Τεχνικά Πρότυπα ("ITS") σχετικά με την εφαρμογή των απαιτήσεων του DORA, τα οποία θα είναι υποχρεωτικά για τις χρηματοπιστωτικές οντότητες.

Επιπλέον, η Ευρωπαϊκή Επιτροπή θα εγκρίνει επίσης δύο κατ' εξουσιοδότηση Πράξεις για τη θέσπιση του πλαισίου εποπτείας των τρίτων Παρόχων ΤΠΕ, που χαρακτηρίζονται ως κρίσιμοι.

Ο Κανονισμός DORA 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 39 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 δικαίου και τεχνολογίας, 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
Email: platisanastassiadis@gr.ey.com

ey.com