

Κανονισμός 2022/2554 (DORA): Αντίστροφη Μέτρηση για Συμμόρφωση

Ο Κανονισμός (Ε.Ε.) 2022/2554 «Πράξη για την Ψηφιακή Επιχειρησιακή Ανθεκτικότητα» (DORA) έχει σχεδιαστεί για να ενισχύσει την ψηφιακή ανθεκτικότητα των φορέων του χρηματοπιστωτικού τομέα σε όλη την Ευρωπαϊκή Ένωση. Ο DORA καθορίζει υποχρεωτικές απαιτήσεις για τη διαχείριση των κινδύνων σχετικά με τις Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ) και την εξασφάλιση της επιχειρησιακής συνέχειας απέναντι σε κυβερνοαπειλές, λειτουργικές διακοπές και ευπάθειες.

Κύριοι Στόχοι του DORA:

- Διαχείριση Κινδύνων ΤΠΕ: Δημιουργία και διατήρηση ισχυρών πλαισίων για την αναγνώριση, παρακολούθηση και διαχείριση των κινδύνων που σχετίζονται με ΤΠΕ.
- Δοκιμές Λειτουργικής Ανθεκτικότητας: Εφαρμογή προηγμένων στρατηγικών δοκιμών, συμπεριλαμβανομένων των δοκιμών διείσδυσης, για να διασφαλιστεί ότι τα συστήματα παραμένουν λειτουργικά υπό πίεση.
- Αναφορά Περιστατικών: Υποχρεωτική και δομημένη αναφορά των περιστατικών που σχετίζονται με το ΤΠΕ στις αρμόδιες ρυθμιστικές αρχές.
- Διαχείριση Κινδύνων Τρίτων: Διασφάλιση ότι οι πάροχοι υπηρεσιών ΤΠΕ συμμορφώνονται με τις απαιτήσεις του DORA μέσω της συμπερίληψης συγκεκριμένων διατάξεων στις συμβάσεις.

- Ανθεκτικότητα του Χρηματοπιστωτικού Τομέα: Ευθυγράμμιση των πρακτικών σε όλο τον κλάδο για μια ενιαία απάντηση στις ψηφιακές και λειτουργικές απειλές.

Αντίστροφη Μέτρηση για Συμμόρφωση

Ο DORA τέθηκε σε ισχύ στις 16 Ιανουαρίου 2023 και θα εφαρμόζεται από τις 17 Ιανουαρίου 2025. Τα χρηματοπιστωτικά ιδρύματα πρέπει να δράσουν γρήγορα για να εφαρμόσουν τις διατάξεις του DORA.

Η αναμονή μέχρι την τελευταία στιγμή ενέχει κινδύνους μη συμμόρφωσης και δημιουργεί σημαντικές λειτουργικές προκλήσεις.

1. Πεδίο Εφαρμογής

Οι υπηρεσίες που εμπίπτουν στο πεδίο εφαρμογής περιλαμβάνουν υπηρεσίες ΤΠΕ, οι οποίες καλύπτουν ένα ευρύ φάσμα υπηρεσιών, επεκτεινόμενες πέρα από τις παραδοσιακές υπηρεσίες IT που τίθενται υπό εξωπορισμό (outsourcing).

Οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής περιλαμβάνουν:

- Φορείς του χρηματοπιστωτικού τομέα (π.χ. πιστωτικά ιδρύματα, ιδρύματα πληρωμών, ασφαλιστικές και αντασφαλιστικές επιχειρήσεις).
- Τρίτους παρόχους υπηρεσιών ΤΠΕ.

2. Οι 'πέντε πυλώνες' του DORA

Πυλώνας 1: Διαχείριση Κινδύνων ΤΠΕ

- Διακυβέρνηση και οργάνωση
- Πλαίσιο διαχείρισης κινδύνων ΤΠΕ
- Διαχείριση συστημάτων, πρωτοκόλλων και εργαλείων ΤΠΕ
- Αναγνώριση και ταξινόμηση συστημάτων ΤΠΕ
- Προστασία, πρόληψη και ανίχνευση συστημάτων ΤΠΕ
- Σχέδια επιχειρησιακής συνέχειας, απόκρισης και ανάκαμψης και επικοινωνίας ΤΠΕ
- Πολιτικές δημιουργίας αντιγράφων ασφαλείας, διαδικασίες αποκατάστασης και ανάκαμψης
- Ανασκοπήσεις μετά από περιστατικά και μαθήματα που αντλήθηκαν

Πυλώνας 2: Ταξινόμηση και αναφορά περιστατικών ΤΠΕ

- Διαδικασία διαχείρισης περιστατικών που σχετίζονται με το ΤΠΕ
- Ταξινόμηση περιστατικών και κυβερνοαπειλών που σχετίζονται με το ΤΠΕ
- Αναφορά σημαντικών περιστατικών ΤΠΕ και εθελοντική κοινοποίηση σημαντικών κυβερνοαπειλών

Πυλώνας 3: Δοκιμές ψηφιακής λειτουργικής ανθεκτικότητας

- Πρόγραμμα δοκιμών ψηφιακής λειτουργικής ανθεκτικότητας
- Δοκιμές εργαλείων και συστημάτων ΤΠΕ
- Προηγμένες δοκιμές εργαλείων, συστημάτων και διαδικασιών ΤΠΕ βάσει Δοκιμών Διείσδυσης Καθοδηγούμενου Κινδύνου (TLPT)
- Απαιτήσεις για τους δοκιμαστές TLPT

Πυλώνας 4: Διαχείριση κινδύνων τρίτων ΤΠΕ

- Στρατηγική και διαδικασίες διαχείρισης κινδύνων τρίτων ΤΠΕ
- Μητρώο πληροφοριών
- Συμβατικές ρυθμίσεις
- Δικαίωμα ελέγχου
- Στρατηγικές και σχέδια εξόδου
- Κίνδυνοι συγκέντρωσης ΤΠΕ και κίνδυνοι υπεργολαβίας

Πυλώνας 5: Διευθετήσεις ανταλλαγής πληροφοριών

- (Εθελοντική) ανταλλαγή πληροφοριών για κυβερνοαπειλές

3. Πλαίσιο Εποπτείας DORA για τον χρηματοπιστωτικό τομέα

Εξουσίες που χορηγούνται στις ΕΑΑ (Εθνικές Αρμόδιες Αρχές)

- Οι ΕΑΑ πρέπει να διαθέτουν όλες τις εποπτικές, ερευνητικές και κυρωτικές εξουσίες που είναι απαραίτητες για την εκπλήρωση των καθηκόντων τους βάσει του DORA, συμπεριλαμβανομένων τουλάχιστον:
- Πρόσβαση σε οποιοδήποτε έγγραφο ή δεδομένο που κατέχεται σε οποιαδήποτε μορφή και που η ΕΚΑ θεωρεί σχετικό για την εκτέλεση των καθηκόντων της και λήψη ή αντιγραφή αυτού
 - Διενέργεια επιτόπιων επιθεωρήσεων ή ερευνών
 - Απαίτηση διορθωτικών και αποκαταστατικών μέτρων για παραβιάσεις των απαιτήσεων του DORA

Κυρώσεις που μπορούν να επιβάλουν οι ΕΑΑ

- Διοικητικές κυρώσεις
- Αποκαταστατικά μέτρα
- Ποινικές κυρώσεις (εάν η παραβίαση υπόκειται σε ποινικές κυρώσεις βάσει της εθνικής νομοθεσίας των ΚΜ)

Παράγοντες που λαμβάνονται υπόψη κατά τον καθορισμό των κυρώσεων

- Βαθμός στον οποίο η παραβίαση είναι σκόπιμη ή προκύπτει από αμέλεια
- Σημαντικότητα, σοβαρότητα και διάρκεια της παραβίασης
- Ευθύνη
- Επίπεδο συνεργασίας
- Απώλειες για τρίτους
- Οικονομική ισχύς
- Σημαντικότητα των κερδών που αποκτήθηκαν ή των ζημιών που αποφεύχθηκαν

Λειτουργίες των ΕΑΑ

- Εποπτεία σε κρίσιμους τρίτους παρόχους ΤΠΕ
- Συνεργασία και βοήθεια προς τον κύριο εποπτικό φορέα σχετικά με το Πλαίσιο Εποπτείας
- Παρακολούθηση των συστάσεων του Κύριου Εποπτικού Φορέα
- Περιστατικά που σχετίζονται με το ΤΠΕ
- Λήψη αναφορών σημαντικών περιστατικών ΤΠΕ
- Παροχή σχετικής και αναλογικής εποπτικής ανατροφοδότησης
- Δοκιμές διείσδυσης με βάση τις απειλές
- Επικύρωση του πεδίου εφαρμογής TLPT
- Παροχή πιστοποίησης που επιβεβαιώνει το TLPT

- Αναγνώριση των χρηματοπιστωτικών οντοτήτων που απαιτείται να εκτελέσουν TLPT
- Έγκριση της χρήσης εσωτερικών δοκιμαστών
- Ανασκόπηση των συμβατικών ρυθμίσεων για τη χρήση τρίτων παρόχων ΤΠΕ από χρηματοπιστωτικές οντότητες

4. Εφαρμογή του DORA στον οργανισμό σας

Βάσει του DORA, το διοικητικό σώμα (αυτοί που διοικούν ουσιαστικά την οντότητα ή κατέχουν βασικές λειτουργίες σύμφωνα με την ενωσιακή ή εθνική νομοθεσία) του χρηματοπιστωτικού ιδρύματος είναι υπεύθυνο και υπόλογο για την ορθή εφαρμογή των νομικών απαιτήσεων.

Οι αρμόδιες αρχές έχουν την ρητή εξουσία να επιβάλλουν διοικητικές κυρώσεις (π.χ., πρόστιμα) στα μέλη αυτού του διοικητικού σώματος. Επομένως, είναι κρίσιμο το διοικητικό σώμα να συμμετέχει ενεργά στην εφαρμογή και παρακολούθηση των απαιτήσεων του DORA.

Ορισμένες νέες και δεσμευτικές απαιτήσεις του DORA είναι εξαιρετικά συγκεκριμένες, απαιτώντας λεπτομερή ανάλυση ωριμότητας για την επίτευξη αποτελεσματικής εφαρμογής. Αυτό περιλαμβάνει, αλλά δεν περιορίζεται σε, συμβόλαιο τρίτων και πιθανές επαναδιαπραγματεύσεις.

Οι απαιτήσεις του DORA αναλύονται περαιτέρω στα Ρυθμιστικά Τεχνικά Πρότυπα (RTS) των ΕΑΑ. Αν και τα RTS δεν εισάγουν νέες υποχρεώσεις, παρέχουν προδιαγραφές που απαιτούν εφαρμογή.

Ο Ελληνικός συμπληρωματικός νόμος του DORA, που μεταξύ άλλων θα διορίζει τις εποπτικές αρχές του Κανονισμού, ακόμη εκκρεμεί προς ψήφιση.

Ο Κανονισμός DORA 2022/2554 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 ΕΥ, προκειμένου να προσφέρουμε με επαγγελματισμό και συνέπεια υπηρεσίες στους πελάτες μας με διασυστοριακές 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 Μπούμα

Senior Manager
antonios.broumas@gr.ey.com

στη δικηγορική εταιρεία

Πλατής - Αναστασιάδης και Συνεργάτες

Τηλ.: +30 210 2886 512
legaloffice@gr.ey.com

© 2025

All rights reserved

ey.com



EY



EY Greece



eygreece



@EY_Greece



EY Greece

Η Δικηγορική Εταιρεία Πλατής - Αναστασιάδης και Συνεργάτες συνεργάζεται με την ΕΥ.

Εταίροι: Ε. Πλατής και Α. Αναστασιάδης

Ο αριθμός μητρώου της Δικηγορικής Εταιρείας είναι 80240.

Συγκεντρωτικός κατάλογος με όλους τους συνεργάτες μας αποστέλλεται κατόπιν σχετικού αιτήματος.

Η παρούσα έκδοση περιέχει πληροφορίες σε περιληπτική μορφή και κατά συνέπεια προορίζεται μόνο για γενική πληροφόρηση και καθοδήγηση. Δεν προορίζεται να χρησιμοποιηθεί ως υποκατάστατο μιας λεπτομερούς έρευνας ή της άσκησης επαγγελματικής κρίσης. Ούτε η EYGM Limited, αλλά ούτε κάποιο άλλο μέλος του παγκόσμιου οργανισμού της ΕΥ αναλαμβάνει την ευθύνη για οποιαδήποτε τυχόν ζημία σε οποιοδήποτε πρόσωπο ενεργεί ή απέχει από κάποια ενέργεια, ως αποτέλεσμα χρήσης οποιοδήποτε υλικού αυτής της έκδοσης. Για οποιοδήποτε συγκεκριμένο θέμα, θα πρέπει να απευθύνεστε στον κατάλληλο σύμβουλο.