Grant Thornton

GDPR & Νέες προκλήσεις

Αντιμετωπίζοντας τις διαρκείς και νέες προκλήσεις στη μετά-Brexit & μετά-Shcrems II ψηφιακή εποχή

Ιανουάριος 2022

Διεθνείς διαβιβάσεις προσωπικών δεδομένων υπό το πρίσμα του GDPR & άλλες επίκαιρες προκλήσεις

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) μετρά ήδη **τρία (3) χρόνια εφαρμογής**. Οι επιχειρήσεις στην πλειοψηφία τους έχουν προχωρήσει, ήδη πριν από την έναρξη εφαρμογής του, στην υλοποίηση ισχυρών προγραμμάτων συμμόρφωσης και θωράκισης των διαδικασιών και πολιτικών προστασίας προσωπικών δεδομένων.

Ωστόσο, η εφαρμογή του GDPR στην πράξη, οι σύγχρονες εξελίξεις στην τεχνολογία, όπως άλλωστε και η πανδημία Covid19, **δημιουργούν συνεχώς νέες ανάγκες συμμόρφωσης, ιδίως με τη μορφή της επικαιροποίησης.** Επιπλέον, τόσο η εφαρμογή & ερμηνεία του GDPR από τις αρμόδιες ρυθμιστικές και εποπτικές αρχές όσο και από τη νομολογία ιδίως σε ευρωπαϊκό επίπεδο, δημιουργεί νέες, **διαρκείς & διευρυμένες απαιτήσεις ελέγχου και επικαιροποίησης των υφιστάμενων πολιτικών και διαδικασιών**.

Επίκαιρα ζητήματα Αρχών και Επιχειρήσεων

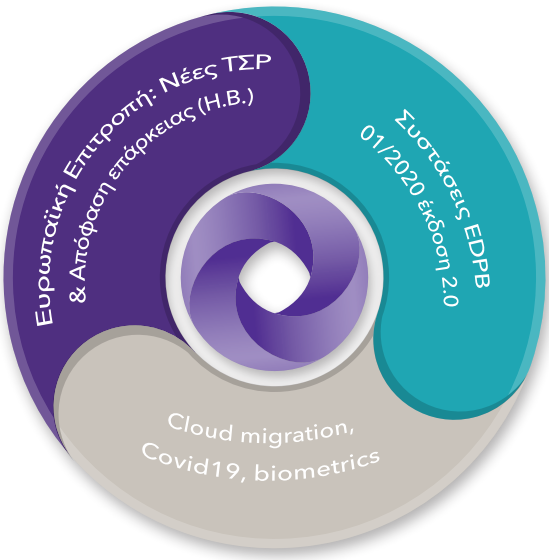
Η **διεθνής διαβίβαση δεδομένων σε τρίτες χώρες**. Το ζήτημα αυτό έλαβε εξαιρετικές διαστάσεις ιδίως σε συνέχεια του **Brexit**, αλλά και της απόφασης **Schrems II** του Δικαστηρίου της Ε.Ε., την ίδια στιγμή που οι τεχνολογικές εξελίξεις οδηγούν όλο και περισσότερες επιχειρήσεις στη διαβίβαση των δεδομένων τους προς διεθνείς παρόχους υπηρεσιών πληροφορικής cloud (**cloud migration**), οι οποίοι συχνά εδρεύουν σε τρίτες χώρες, όπως οι Η.Π.Α. στη μετά-Schrems II εποχή ή το μετά-Brexit Ηνωμένο Βασίλειο.

Η **de facto διαχείριση ειδικών κατηγοριών προσωπικών δεδομένων** από πολλές επιχειρήσεις, ιδίως δεδομένων υγείας & βιομετρικών δεδομένων στα πλαίσια της συνεχιζόμενης **πανδημίας Covid19**.

Η **εισαγωγή νέων τεχνολογιών** ελέγχου ταυτότητας, ψηφιακών (βιομετρικών) υπογραφών κ.ά., με τις ανάλογες προκλήσεις διαχείρισης των δεδομένων αυτών, αλλά και διαχείρισης περιπτώσεων πιθανής εγκληματολογικής διερεύνησης (forensic examination).

Η προμήθεια **εξειδικευμένων υπηρεσιών υπευθύνου προστασίας (DPO as a service)**, με σκοπό την αποτελεσματική **διακυβέρνηση προσωπικών δεδομένων υπό το πρίσμα των παραπάνω προκλήσεων.**

Νέες απαιτήσεις κανονιστικής συμμόρφωσης



- Στις 18/6/2021, υιοθετήθηκε η**Έκδοση 2.0 των Συστάσεων 01/2020** του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ ή EDPB) σχετικά με τα **μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ.**
- Στις 4/6/2021 εκδόθηκε η εκτελεστική απόφαση της Ευρωπαϊκής Επιτροπής, η οποία επικύρωσε τις **νέες τυποποιημένες συμβατικές ρήτρες (ΤΣΡ ή SCCs)** για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες.
- Στις 28/6/2021 εκδόθηκε η εκτελεστική απόφαση της Ευρωπαϊκής Επιτροπής που επικύρωσε την **απόφαση επάρκειας προστασίας προσωπικών δεδομένων στο Ηνωμένο Βασίλειο (UK adequacy decision).**

Η Κίνα πέρασε για πρώτη φορά έναν ειδικό νόμο για την προστασία των προσωπικών πληροφοριών (PIPL) στις 20/08/2021, με ισχύ από 01/11/2021. Ο νόμος αυτός έχει αρκετές ομοιότητες με τον GDPR, εισάγει ωστόσο σειρά από υποχρεώσεις που ενδέχεται να διαφέρουν σημαντικά από αυτόν ως προς την ερμηνεία τους και τις συνεπακόλουθες ουσιαστικές υποχρεώσεις των μερών, ενώ κάποιες υποχρεώσεις που περιλαμβάνονται στον GDPR δεν περιλαμβάνονται στον PIPL. Οι επιχειρήσεις που επεξεργάζονται προσωπικά δεδομένα υποκειμένων της Κίνας, πρέπει άμεσα να προσαρμοστούν λειτουργικά στις νέες απαιτήσεις.

Τα βήματα προς τη συμμόρφωση της επιχείρησής σας

Δημιουργείται επομένως ένας χάρτης με τα βήματα που οφείλει να ακολουθεί κάθε επιχείρηση, είτε ως υπεύθυνος επεξεργασίας είτε ως εκτελών την επεξεργασία, προκειμένου να εξασφαλίσει ότι ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας με εκείνο που είναι εγγυημένο εντός της Ε.Ε. συνοδεύει μόνιμα τα προσωπικά δεδομένα σε περίπτωση διεθνών διαβιβάσεων.

1. Καταγραφή διαβιβάσεων (Know your tranfers):

Η χαρτογράφηση όλων των διαβιβάσεων δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ενδέχεται να συνιστά δύσκολο εγχείρημα. Η ενημέρωση όσον αφορά τον προορισμό των δεδομένων προσωπικού χαρακτήρα είναι ωστόσο απαραίτητη, ώστε να διασφαλίζεται ότι παρέχεται ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας οπουδήποτε και αν πραγματοποιείται επεξεργασία. Πρέπει επίσης να επαληθεύεται ότι τα δεδομένα που διαβιβάζονται είναι κατάλληλα, συναφή και περιορίζονται στα απολύτως αναγκαία για τους σκοπούς για τους οποίους διαβιβάζονται και υποβάλλονται σε επεξεργασία στην τρίτη χώρα.

2. Επαλήθευση εργαλείου διαβίβασης:

Αναγκαία παράμετρος η επιλογή του καταλληλότερου εργαλείου μεταξύ εκείνων που απαριθμούνται στο κεφάλαιο V του GDPR (π.χ. απόφαση περί επάρκειας, κατάλληλες εγγυήσεις), λαμβάνοντας υπόψη τις νέες εξελίξεις στις ΤΣΡ και τις αποφάσεις επάρκειας της Ε.Ε.

3. Αξιολόγηση νομοθεσίας/πρακτικής τρίτης χώρας:

Κρίσιμη είναι η νομοθεσία/πρακτική που θα μπορούσε να επηρεάσει την αποτελεσματικότητα των κατάλληλων εγγυήσεων των εργαλείων διαβίβασης στα οποία βασίζεται μία επιχείρηση, στο πλαίσιο της συγκεκριμένης διαβίβασης. Η αξιολόγηση αυτή θα πρέπει να εστιάζει πρωτίστως στη νομοθεσία της τρίτης χώρας που σχετίζεται με τη διαβίβαση και το εργαλείο διαβίβασης στο οποίο βασίζεται η επιχείρηση και το οποίο ενδέχεται να θέσει σε κίνδυνο το επίπεδο προστασίας του.

4. Προσδιορισμός και θέσπιση πρόσθετων μέτρων:

Θεσπίζονται πρόσθετα μέτρα προκειμένου το επίπεδο προστασίας των διαβιβαζόμενων δεδομένων να προσεγγίσει το επίπεδο του προτύπου της ΕΕ όσον αφορά την ουσιαστική ισοδυναμία. Αυτό το βήμα είναι απαραίτητο μόνο εάν από την αξιολόγηση (του προηγούμενου βήματος) προκύψει ότι η νομοθεσία τρίτων χωρών επηρεάζει την αποτελεσματικότητα του εργαλείου διαβίβασης στο οποίο βασίζεται η επιχείρηση στο πλαίσιο της διαβίβασης δεδομένων σε τρίτη χώρα.

5. Τυπικές διαδικαστικές ενέργειες:

Μπορεί να απαιτούνται από την έγκριση των πρόσθετων μέτρων, ανάλογα με το εργαλείο διαβίβασης και ιδίως σε περιπτώσεις που δεν υπάρχει απόφαση επάρκειας της Ε.Ε.
για το επίπεδο προστασίας της τρίτης χώρας.

6. Επανεκτίμηση επιπέδου προστασίας:

Ανά τακτά χρονικά διαστήματα απαιτείται επανεκτίμηση του επιπέδου προστασίας των δεδομένων που διαβιβάζονται σε τρίτες χώρες και παρακολούθηση για το εάν υπήρξαν ή εάν υπάρξουν εξελίξεις είτε στη χώρα αυτή είτε σε επίπεδο Ε.Ε., που μπορεί να επηρεάσουν το επίπεδο προστασίας. Η αρχή της λογοδοσίας απαιτεί συνεχή επαγρύπνηση του επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα, αλλά και συνεχή συνεργασία με τους αποδέκτες των δεδομένων σε τρίτες χώρες.

Η επικαιροποίηση της συμμόρφωσης της επιχείρησής σας είναι η απάντηση στις νέες προκλήσεις

Κατά τη μετάβασή σας στο cloud

Η μετάβασή σας σε περιβάλλον πληροφορικής cloud προϋποθέτει ανοικτό δίαυλο ανταλλαγής σαφών πληροφοριών με τον πάροχο των υπηρεσιών (που συχνά θα δρα ως εκτελών επεξεργασία για λογαριασμό σας), ιδίως όταν πρόκειται για πάροχο με ισχυρή παρουσία στις μετά-Schrems II Η.Π.Α. & το μετά-Brexit Η.Β. Ταυτόχρονα, απαιτεί επιλογή & ενσωμάτωση του κατάλληλου GDPR εργαλείου & διαδικασιών, εφόσον διαπιστωθεί περίπτωση μεταβιβάσεων προσωπικών δεδομένων σε τρίτες χώρες. Ο **έλεγχος της συμμόρφωσης** με τις νεότερες συστάσεις του EDPB, η χρήση των SCCs στις αντίστοιχες συμβάσεις & της απόφασης επάρκειας για το ΗΒ, η πρόβλεψη ειδικών μέτρων ασφάλειας και η αντίστοιχη επικαιροποίηση των πολιτικών/διαδικασιών σας είναι μονόδρομος.

Κατά τη διαχείριση βιομετρικών δεδομένων με την εισαγωγή νέων τεχνολογιών στη δραστηριότητά σας

Η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων του άρθρου 9 του GDPR, όπως είναι για παράδειγμα τα βιομετρικά δεδομένα που συλλέγονται από την ένταξη ψηφιακών υπογραφών στις διαδικασίες & τη λειτουργία σας, επιτρέπονται μόνο υπό πολύ αυστηρές προϋποθέσεις. Όσο πληθαίνουν οι περιπτώσεις αμφισβήτησης τέτοιων υπογραφών, αυξάνονται οι ανάγκες σας για παράδειγμα σε ενδεχόμενες περιπτώσεις διερεύνσης απάτης ή αμφισβήτησης μιας συμφωνίας. Η συμμόρφωσή σας περιλαμβάνει την ένταξη των νέων κατηγοριών σε ειδικές διαδικασίες προστασίας προσωπικών δεδομένων της Εταιρείας σας, εκτιμήσεις αντικτύπου (DPIAs), σχεδιασμό νέων διαδικασιών & ειδικών πολιτικών διατήρησης & ασφαλούς καταστροφής, όπως και προβλέψεις για ειδικά μέτρα ασφάλειας που περιλαμβάνουν κρυπτογράφηση & ανωνυμοποίηση.

Κατά τη διαχείριση προσωπικών δεδομένων υγείας στο πλαίσιο των μέτρων κατά της πανδημίας Covid19

Οι επιχειρήσεις έχουν κληθεί να συμβάλλουν στην καταπολέμηση της πανδημίας Covid19, εφαρμόζοντας μέτρα & διαδικασίες για την ασφάλεια του προσωπικού τους και για την προστασία της δημόσιας υγείας. Υπό αυτό το πρίσμα, είναι πολύ πιθανό να διαχειρίζεστε de facto προσωπικά δεδομένα ειδικών κατηγοριών, όπως τα δεδομένα υγείας του προσωπικού σας, ακόμη και αν δεν ήσασταν πραγματικά έτοιμοι για τη σύννομη επεξεργασία μιας τέτοιας κατηγορίας προσωπικών δεδομένων. Ωστόσο, με βάση την αρχή της λογοδοσίας, είστε υποχρεωμένοι να συμμορφωθείτε με τις αρχές & προϋποθέσεις νόμιμης επεξεργασίας των ειδικών αυτών κατηγοριών προσωπικών δεδομένων & να αναπτύξετε πλάνο ενεργειών & επικαιροποίησης συμμόρφωσης που περιλαμβάνει εκτιμήσεις αντικτύπου (DPIAs), ειδικές πολιτικές & διαδικασίες διατήρησης και προβλέψεις για ειδικά μέτρα ασφάλειας.

Η ανάγκη για εξειδικευμένους συμβούλους data privacy & DPO as a service providers

Οι νέες προκλήσεις εφαρμογής του νομοθετικού πλαισίου υπό το πρίσμα της πανδημίας Covid19 δημιουργούν μια ακόμη πρόκληση για τις Εταιρείες: ν` αναζητήσουν και να εξεύρουν συμβούλους προστασίας προσωπικών δεδομένων με εξειδίκευση & ειδικές γνώσεις, οι οποίοι να είναι σε θέση όχι μόνο να παρέχουν ολοκληρωμένες υπηρεσίες DPO, αλλά και να διαβλέπουν τις προκλήσεις & να προετοιμάζουν με ευελιξία την ετοιμότητα της Εταιρείας να ανταποκρίνεται σε διαρκείς ανάγκες συμμόρφωση.

Η Grant Thornton είναι δίπλα σας στην διαδικασία ενίσχυσης της προστασίας προσωπικών δεδομένων στον Οργανισμό σας και διασφάλιση/επικαιροποίηση της Κανονιστικής σας Συμμόρφωσης

Τα **εξειδικευμένα και έμπειρα στελέχη** του **Business Risk Services** της Grant Thornton, συνεργάζονται μαζί σας με σκοπό την **ανάπτυξη εξειδικευμένων λύσεων**, οι οποίες **ενισχύουν την προστασία προσωπικών δεδομένων** και διασφαλίζουν **την επικαιροποίηση της κανονιστικής συμμόρφωσης** με το ισχύον πλαίσιο του GDPR και την απάντηση στις νέες προκλήσεις του. Πιο αναλυτικά, οι υπηρεσίες που σας προσφέρουμε περιλαμβάνουν:

Υποστήριξη στη διαδικασία μετάβασης στο cloud & μεταβιβάσεων δεδομένων σε τρίτες χώρες

Στα πλαίσια μεταβιβάσεων προσωπικών δεδομένων σε τρίτες χώρες ή/και στη διάρκεια της μετάβασής σας σε περιβάλλον υπηρεσιών cloud πληροφορικής, όπως και για τις ανάγκες διαχείρισης των προκλήσεων της τεχνολογίας & της πανδημίας, σας προσφέρουμε συμβουλευτικές υπηρεσίες επισκόπησης πλήρωσης των προαπαιτούμενων & υπηρεσίες προετοιμασίας για μεταβιβάσεις ή εισαγωγή ειδικών κατηγοριών δεδομένων προς επεξεργασία, ιδίως με:

- Επιλογή & ενσωμάτωση κατάλληλου εργαλείου/ διαδικασίας διαβίβασης
- Ενσωμάτωση ρητρών επεξεργασίας και ΤΣΡ
- DPIAs ειδικών κατηγοριών
- Ανάπτυξη ειδικών διαδικασιών διαχείρισης βιομετρικών δεδομένων & δεδομένων υγείας

Υπηρεσίες επικαιροποίησης κανονιστικής συμμόρφωσης & υποστήριξης στη διαδικασία διαχείρισης ειδικών κατηγοριών

Καθ΄ όλη τη διάρκεια λειτουργίας της Εταιρείας, αλλά και κατά την εισαγωγή επεξεργασίας ειδικών κατηγοριών προσωπικών δεδομένων, σας προσφέρουμε εξειδικευμένες υπηρεσίες κανονιστικής συμμόρφωσης & επικαιροποίησης συμμόρφωσης σύμφωνα με το πλαίσιο προστασίας προσωπικών δεδομένων του GDPR, υπό το πλαίσιο συνεργασίας ή εξωτερικής ανάθεσης. Ειδικότερα παρέχουμε ολοκληρωμένες υπηρεσίες:

- Συμβουλευτικής για την προστασία προσωπικών δεδομένων
- Ανάλυσης κενών & πλάνου ενεργειών
- Σχεδιασμού & ανάπτυξης επικαιροποίησης ολοκληρωμένου πλαισίου διακυβέρνησης προσωπικών δεδομένων
- Παρακολούθησης & επικαιροποίησης συμμόρφωσης με το πλαίσιο του GDPR
- Εκτίμησης αντικτύπου (DPIA)

Υπηρεσίες DPO & εξειδικευμένες συμβουλευτικές υπηρεσίες data privacy

Οι υπηρεσίες του DPO είναι ιδανικό & βέλτιστο να συνδυάζουν εξειδικευμένη γνώση, εμπειρία & ευελιξία καθ` όλο τον κύκλο επεξεργασίας & προστασίας προσωπικών δεδομένων της Εταιρείας σας.

Εμείς ειδικότερα σας παρέχουμε ολοκληρωμένες υπηρεσίες (DPO as a service):

- Συμβουλευτικές υπηρεσίες data privacy
- Διαχείρισης παραβιάσεων
- Αναφοράς περιστατικών
- Παρακολούθησης & επικαιροποίησης πολιτικών και διαδικασιών προστασίας προσωπικών δεδομένων
- Συνεργασίας & επαφής με την εποπτική αρχή (ΑΠΔΠΧ)
- Παρακολούθησης συμμόρφωσης & ενημέρωσης
- Σχεδιασμού εκπαίδευσης & εγχειριδίων για το προσωπικό

Στο τρέχον επιχειρηματικό περιβάλλον, το οποίο καταγράφει συνεχή ανάπτυξη, η Grant Thornton βρίσκεται δίπλα σας σε κάθε βήμα της διαδικασίας συμμόρφωσης με τις νέες απαιτήσεις που προκύπτουν στον τομέα της προστασίας δεδομένων προσωπικού χαρακτήρα.

Ξεχωρίζουμε στο σήμερα. Καθορίζουμε το αύριο.

Η Grant Thornton αποτελεί έναν παγκόσμιο οργανισμό παροχής ελεγκτικών, φορολογικών και συμβουλευτικών υπηρεσιών, με περισσότερα από 58.000 στελέχη σε πάνω από 140 χώρες. Στόχος μας διεθνώς είναι να δημιουργήσουμε σχέσεις εμπιστοσύνης και να βοηθήσουμε δυναμικές επιχειρήσεις να εξελιχθούν, όπου κι αν αυτές δραστηριοποιούνται. Η Grant Thornton στην Ελλάδα αποτελεί έναν από τους μεγαλύτερους παρόχους ελεγκτικών, φορολογικών και συμβουλευτικών υπηρεσιών. Με παρουσία σε 4 πόλεις (Αθήνα, Θεσσαλονίκη, Ηράκλειο Κρήτης και Ιωάννινα) και περισσότερα από 850 εξειδικευμένα στελέχη, διαθέτουμε γνώση, εξειδίκευση και εμπειρία, διασφαλίζοντας μία ουσιαστική σχέση συνεργασίας με τους πελάτες μας, παρέχοντας τους μια προσωποποιημένη εμπειρία.

Βασικοί πυλώνες της προσέγγισής μας, μέσα στο ιδιαίτερο και συνεχώς μεταβαλλόμενο περιβάλλον στο οποίο δραστηριοποιούνται οι πελάτες μας, είναι το αυθεντικό ενδιαφέρον, η κατανόηση των ξεχωριστών προκλήσεων που αντιμετωπίζουν και η αφοσίωση στις φιλοδοξίες και στη στρατηγική τόσο της βιωσιμότητας όσο και της ανάπτυξής τους. Με την προσέγγισή μας, συνθέτουμε τις κατάλληλες ομάδες στελεχών, προκειμένου να προσφέρουμε ένα ευρύ φάσμα υπηρεσιών και λύσεων, που ως στόχο έχουν να εντοπίσουν αλλά και να αξιοποιήσουν όλες εκείνες τις ευκαιρίες που θα οδηγήσουν στην περαιτέρω εξέλιξη των πελατών μας.

Ως αποτέλεσμα, οι πελάτες μάς επιβραβεύουν επιδεικνύοντας υψηλό επίπεδο ικανοποίησης και αφοσίωσης, με το NPS (Net Promoter Score) να αγγίζει το 79%, ένα τα υψηλότερα ανάμεσα στις 140 χώρες που δραστηριοποιούνται οι εταιρείες-μέλη του δικτύου της Grant Thornton. Παράλληλα, η δέσμευσή μας να παρέχουμε την καλύτερη δυνατή εμπειρία στους πελάτες μας, έχει συμβάλλει σημαντικά στο να θεωρούμαστε ως η ταχύτερα αναπτυσσόμενη εταιρεία επαγγελματικών υπηρεσιών.

Επικοινωνήστε με τα εξειδικευμένα στελέχη μας

Τα **εξειδικευμένα και έμπειρα στελέχη** του **Business Risk Services** της Grant Thornton, συνεργάζονται μαζί σας με σκοπό την ανάπτυξη εξειδικευμένων λύσεων που θωρακίζουν τη δραστηριότητα της επιχείρησής σας και ιδίως κατά τη διαβίβαση προσωπικών δεδομένων σε τρίτες χώρες, κατά τη μετάβασή σας στο cloud, όπως και κατά την επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων. Λαμβάνοντας υπόψη το ισχύον νομοθετικό πλαίσιο, τις συστάσεις και τις κατευθυντήριες οδηγίες που έχουν εκδοθεί, καταγράφουμε τις προκλήσεις και προχωράμε στη διασφάλιση της κανονιστικής σας συμμόρφωσης.

Αθηνά Μουστάκη
Partner, Head of Environmental, Social, Governance, Risk & Compliance

E athina.moustaki@gr.gt.com

Ελευθερία Σπυρίδωνος, CIA
Director, Governance, Risk & Compliance

E eleftheria.spyridonos@gr.gt.com

Λένα Λέσση
Senior Manager, Governance, Risk & Compliance

E eleni.lessi@gr.gt.com

Ξανθίππη Ζώταλη
Supervisor, Legal Consultant, Governance, Risk & Compliance

E xanthippi.zotali@gr.gt.com

Grant Thornton

grant-thornton.gr