

RegTech - έχει και η συμμόρφωση την τεχνολογία της...

Η συμμόρφωση με τους εθνικούς και ευρωπαϊκούς κανονισμούς ή πλαίσια δεν είναι κάτι εύκολο, όμως αποτελεί αναγκαία προϋπόθεση για τη σωστή λειτουργία επιχειρήσεων και οργανισμών και την αποτροπή κινδύνων που, ειδικά στον χώρο της κυβερνοασφάλειας, μπορούν να επηρεάσουν αρνητικά οικοσυστήματα, αλλά και ολόκληρες χώρες. Η τεχνολογία έρχεται να τείνει χείρα βοηθείας και σ' αυτόν τον τομέα...

ΤΟΥ ΓΙΑΝΝΗ ΡΙΖΟΠΟΥΛΟΥ

Ενα από τα πιο μεγάλα και 'καυτά' θέματα στον κόσμο των επιχειρήσεων και των οργανισμών, ιδιαίτερα εκείνων των οποίων ο ρόλος έχει χαρακτηριστεί 'κρίσιμος' για την οικονομική και κοινωνική ζωή του τόπου, είναι η υποχρέωσή τους να συμμορφώνονται τώρα και στο μέλλον (εφόσον ο ρόλος τους παραμένει

ίδιος) με όσα προβλέπουν για τη λειτουργία τους, εθνικοί και ευρωπαϊκοί κανονισμοί ή πλαίσια. Που είναι, βεβαίως, απαραίτητοι -πολύ περισσότερο στους σημερινούς δύσκολους καιρούς- ψηφίζονται με ευρείες πλειοψηφίες και επιβάλλονται εξ ανάγκης, προκειμένου να ελαχιστοποιηθούν οι κίνδυνοι και οι συχνά απρόβλεπτες συνέπειες για το κοινωνικό σύνολο, σε περίπτωση παραβίασης και αστοχίας.



Οι πηχυαίοι τίτλοι και τα δραματικά ρεπορτάζ μπορεί να δημιουργούν αίσθηση στις κάποιες λίγες περιπτώσεις που, λόγω αμέλειας ή απραξίας, η συμφορά δεν αποτρέπεται και βεβαίως τραβάνε το ενδιαφέρον της κοινής γνώμης, αλλά οι περισσότερες επιχειρήσεις και οργανισμοί σέβονται την υποχρέωσή τους για συμμόρφωση και κάνουν ό,τι μπορούν καλύτερο προς αυτή την κατεύθυνση. Όμως, συχνά οι κανονισμοί και τα πλαίσια είναι πολλά και δυσεφάρμοστα, με αποτέλεσμα η συμμόρφωση για τους «υπόχρεους» να είναι κάθε άλλο παρά απλή υπόθεση. Το κύριο ζητούμενο είναι η λήψη μέτρων για την προστασία των ευαίσθητων δεδομένων και του προσωπικού απορρήτου, αλλά και τη διασφάλιση των ψηφιακών περιουσιακών στοιχείων τους. Κι αυτό όσο εύκολο είναι να το λες, τόσο δύσκολο είναι να το κάνεις.

Από την άλλη πλευρά, η μη-συμμόρφωση λόγω αδυναμίας ανθρώπων και υλικών ή όποιου άλλου λόγου, όχι μόνο βάζει σε κίνδυνο την ίδια την επιχείρηση ή οργανισμό, αλλά ταυτόχρονα επηρεάζει αρνητικά (ανάλογα με τον ρόλο της, στην κοινωνία – σκεφτείτε τι μπορεί να συμβεί αν υπάρξουν τέτοιοι είδους προβλήματα στις τράπεζες, την ενέργεια, τις επικοινωνίες ή τις μεταφορές) τη ζωή μέρους ή και του συνόλου των πολιτών μιας χώρας. Εξ ου και σ' αυτές τις περιπτώσεις γίνονται έρευνες και ανακρίσεις, καταλογίζονται ευθύνες και πέφτει βαρύς ο 'πέλεκυς' των ελεγκτικών αρχών, με πρόστιμα που -μερικές φορές- είναι βαρύτατα.

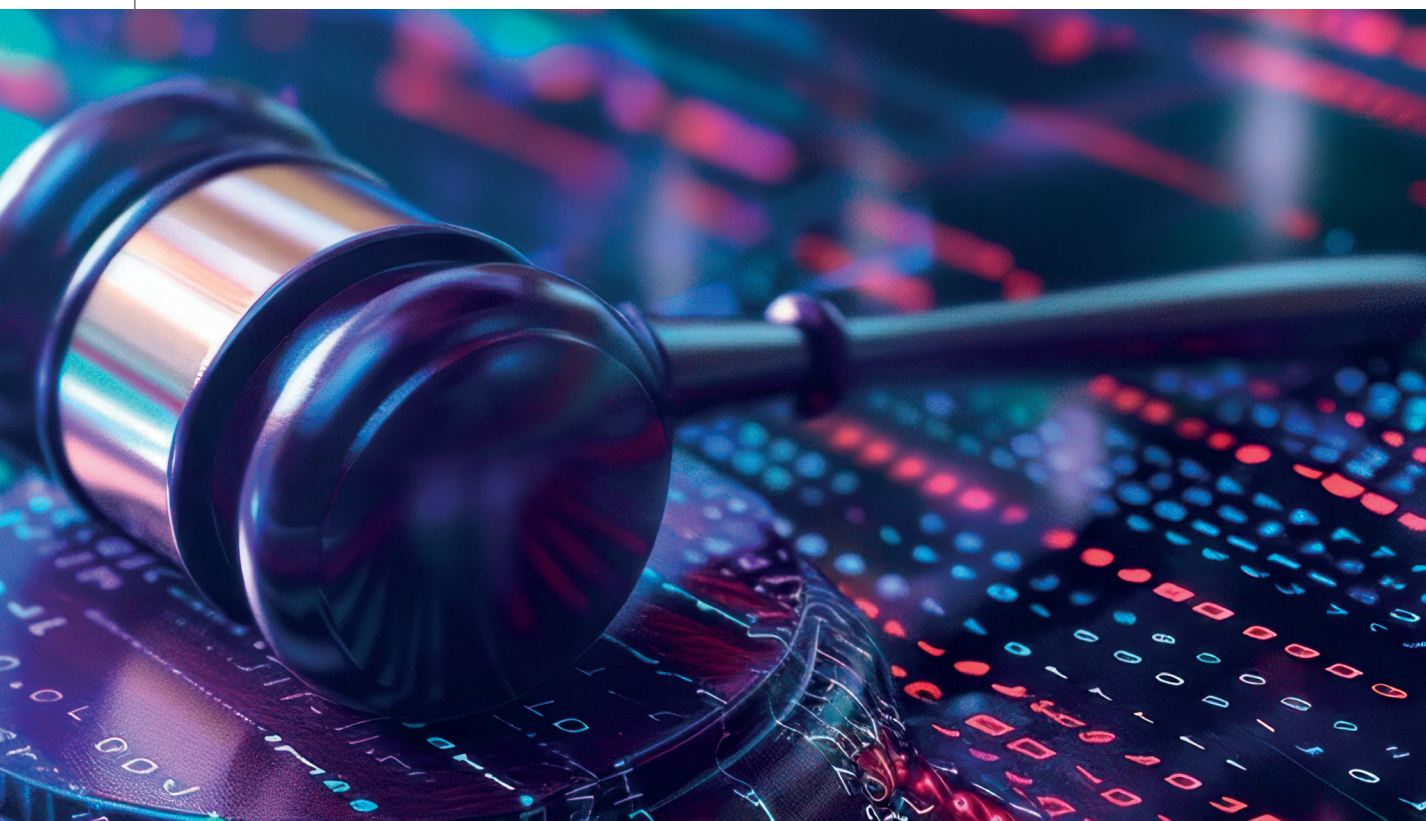
Απειλές και προκλήσεις

Προφανώς, όλα ξεκινούν από την ανάγκη για προστασία των απροστάτευτων δεδομένων (μετά την, λόγω της πανδημίας, κατακόρυφη αύξηση της απομακρυσμένης

εργασίας και κατάργηση στην πράξη της ως τότε καλά φυλασσόμενης «περιμέτρου») και πλέον σημαντικά εκτεθειμένων οργανισμών και επιχειρήσεων στις διαθέσεις των κακόβουλων. Ο **Σπύρος Τάσσης**, partner της Ποταμίτης - Βεκρής με μεγάλη εμπειρία σ' αυτά τα θέματα, μίλησε στο netweek για τις σαρωτικές αλλαγές που βιώνουμε τον τελευταίο καιρό στο τοπίο της κυβερνοασφάλειας. Να τι μας είπε: «Το τοπίο της κυβερνοασφάλειας τόσο στην Ελλάδα όσο και στην Ευρωπαϊκή Ένωση εξελίσσεται συνεχώς, με νέες απειλές και προκλήσεις να αναδύονται καθημερινά. Αυτές είναι:

- ▶ Η άνοδος των συμβάντων κυβερνοεπιθέσεων που βασίζονται στην Τεχνητή Νοημοσύνη για πιο στοχευμένες επιθέσεις και κάνουν δυσχερέστερη την άμυνα κατά των απειλών.
- ▶ Οι ολοένα συχνότερες επιθέσεις λυτρισμικού (βλέπε, ransomware) με τους επιτιθέμενους να απαιτούν μεγάλα ποσά σε κρυπτονομίσματα προκειμένου να 'απελευθερώσουν' κρυπτογραφημένα δεδομένα.
- ▶ Η εκρηκτική αύξηση στη χρήση συσκευών IoT, υπολογιστικού νέφους κι άλλων αναδυόμενων τεχνολογιών, που έχει αυξήσει το πεδίο επιθέσεων και τα εύαλτα σημεία για τους οργανισμούς.
- ▶ Η έλλειψη εξειδικευμένων επαγγελματιών στον τομέα της κυβερνοασφάλειας σε παγκόσμια κλίμακα, γεγονός που δυσχεραίνει την επαρκή προστασία των οργανισμών.

Επομένως, η συνεχής ενημέρωση σχετικά με τις τελευταίες απειλές και οι βέλτιστες πρακτικές διαχεί-



ρισης και εποπτείας δεδομένων και συστημάτων (data and system management) είναι ζωτικής σημασίας για τους οργανισμούς όλων των μεγεθών».

Νέοι κανονισμοί και συμμόρφωση

Σχετικά με την πληθώρα των νέων κανονισμών και την εκ του νόμου υποχρέωση συμμόρφωσης όλων των εμπλεκόμενων, ο κ. Τάσσης τονίζει ότι «GDPR, AI Act, NIS2, CRA, DORA κλπ. δημιουργούν ένα στενό ρυθμιστικό πλαίσιο σ' ό,τι αφορά στους οργανισμούς που χειρίζονται δεδομένα (προσωπικά ή μη) κι αυτό είναι εύλογο, αν σκεφτεί κανείς τόσο την αξία τους, όσο και τον κίνδυνο από τα μη-ασφαλή ψηφιακά συστήματα. Η τήρηση ενός δομημένου συστήματος data management, καθώς και αναγνωρισμένων πλαισίων στον χώρο της κυβερνοασφάλειας, πρέπει να αποτελεί πρωταρχικό μέλημα, με την ένταση της εποπτείας των διαδικασιών αυτών να εξαρτάται από τον τομέα δραστηριοποίησης (π.χ. υγειονομική περίθαλψη, χρηματοοικονομικά).

Περαιτέρω, σημαντικός είναι ο έλεγχος της συμμόρφωσης της εφοδιαστικής αλυσίδας, η ύπαρξη σαφώς καθορισμένου σχεδίου αντιμετώπισης περιστατικών και αποκατάστασης των δεδομένων και συστημάτων από επιθέσεις, οι τακτικές αξιολογήσεις των διαδικασιών, καθώς και η συνεχής εκπαίδευση των εργαζομένων. Με την προληπτική δημιουργία πλαισίου συμμόρφωσης, οι οργανισμοί μπορούν να ελαχιστοποιήσουν τον κίνδυνο δαπανηρών παραβιάσεων και να διατηρήσουν τη συμμόρφωση με τους εξελισσόμενους κανονισμούς».

Αβεβαιότητες και κόστος

Μια άλλη, πρακτική και ιδιαίτερως ενδιαφέρουσα πτυχή της υποχρέωσης για συμμόρφωση θίγει η επίσης νομικός, **Πέννη Κοντογεώργου**, Partner στην εταιρία Ζούλοβιτς – Κοντογεώργου, που τονίζει ότι «λόγω της διεύρυνσης των υποχρεών επιχειρήσεων, ορισμένες κατηγορίες εξ αυτών ενδέχεται να μην είναι βέβαιες αν εμπίπτουν στη NIS2, με αποτέλεσμα να παρατηρείται καθυστερημένη συμμόρφωση, με νομικό ρίσκο. Για παράδειγμα, αυτό συμβαίνει με εταιρίες Fintech / Startup οι οποίες δραστηριοποιούνται μεν σε ρυθμιζόμενους τομείς, αλλά δεν πληρούν τα κριτήρια μεγέθους, εταιρίες logistics που μπορεί μεν να επηρεάζουν κρίσιμες υπηρεσίες, αλλά δεν είναι σαφές αν εμπίπτουν ή, τέλος, υπηρεσίες AI που -ανάλογα με τη χρήση τους- ενέχεται να θεωρηθούν κρίσιμες, όσον αφορά στον τομέα της κυβερνοασφάλειας.

Η συμμόρφωση με τη NIS2 συνεπάγεται σημαντικό οικονομικό κόστος, καθώς οι επιχειρήσεις καλούνται να επενδύσουν σε τεχνολογικές αναβαθμίσεις, εξειδικευμένους συμβούλους (π.χ. CISO, DPO, Risk Management Officers κ.ά.), και εκπαίδευση προσωπικού. Βεβαίως, το αυξημένο κόστος συμμόρφωσης οι επιχειρήσεις μπορούν να το μετακυλήσουν στις τιμές των προϊόντων ή υπηρεσιών τους, όμως οι μικρομεσαίες επιχειρήσεις (ΜμΕ) που έχουν περιορισμένους πόρους, ενδέχεται να αποκλειστούν από αλυσίδες εφοδιασμού, παραχωρώντας



έμμεσα ανταγωνιστικό πλεονέκτημα στους μεγαλύτερους οργανισμούς, οι οποίες έχουν ήδη ανεπτυγμένα συστήματα κυβερνοασφάλειας. Η NIS2 απαιτεί από τις επιχειρήσεις αυξημένο έλεγχο συμμόρφωσης (audit) των third-party providers (cloud, SaaS κτλ.), διότι τις καθιστά υπεύθυνες για τη συνολική αλυσίδα εφοδιασμού. Άρα, εδώ υπάρχει ανάγκη για συμβατικές ρήτρες ασφαλείας, διαρκή αξιολόγηση κινδύνων, επιπλέον πιστοποιήσεις και συμβατικές δεσμεύσεις και εγγυήσεις των τρίτων, υποχρεώσεις που αυξάνουν τη ρυθμιστική πολυπλοκότητα και το κόστος συμμόρφωσης».

Μέγα εύρος αναγκών - εφαρμογών

Με δεδομένο το τεράστιο εύρος των αναγκών κυβερνοασφάλειας -αλλά και των εφαρμογών που καλούνται να τις καλύψουν- η ύπαρξη των αντίστοιχων κανονισμών και πλαισίων είναι προφανώς επιβεβλημένη και μάλιστα με υψηλό βαθμό αυστηρότητας, όπως απαιτεί και η κοινή γνώμη. Όταν τομείς ευαίσθητοι όπως η υγεία, η εκπαίδευση, οι χρηματοοικονομικές υπηρεσίες συμπεριλαμβανομένου και του ασφαλιστικού κλάδου, η εύρυθμη λειτουργία του κράτους, ο χώρος της ενέργειας και των τηλεπικοινωνιών, ο αντίστοιχος της λιανικής με την ηλεκτρονική έκφασή του (βλέπε, eCommerce) και, προφανώς, η άμυνα (έστω κι αν ειδικά εκεί, λαμβάνονται σοβαρότατα μέτρα εκ των έσω, από τις αρμόδιες στρατιωτικές υπηρεσίες) αντιμετωπίζουν οριζόντια περίπου τις ίδιες απειλές, τότε είναι εύλογος ο αριθμός των περίπου 2000 φορέων και επιχειρήσεων που έχουν μπει από φέτος στη χορεία όσων ελέγχονται σε συνεχή βάση από την Εθνική Αρχή Κυβερνοασφάλειας και τους συνεργάτες της, σ' ό,τι αφορά στη συμμόρφωσή τους με όσα επιβάλλονται από κανονισμούς και πλαίσια.

Όπως έχουν δηλώσει επανειλημμένα ηγετικά στελέχη της ΕΑΚ, στόχος τους δεν είναι η επιβολή μικρών ή



μεγάλων προστίμων, αλλά -ειδικά τώρα, στην αρχή της εποχής του NIS2- η παραίνεση, η καθοδήγηση και η παροχή συμβουλών ή διευκρινίσεων προς όλο το οικοσύστημα, ώστε η επιβεβλημένη σε πανευρωπαϊκό επίπεδο συμμόρφωση να αποδώσει καρπούς και να 'θωρακίσει', όσο είναι δυνατό τους εμπλεκόμενους, αλλά και την ίδια τη χώρα.

Δυσχερής η διαχείριση

Ακόμα κι αν υπάρχει καλή θέληση και επιθυμία για συμμόρφωση, όμως, τα πράγματα στην πράξη δεν είναι εύκολα, πολύ περισσότερο για τις μικρότερες σε μέγεθος (πλην κρίσιμες ως προς το αντικείμενό τους) επιχειρήσεις. Συχνά δεν έχουν ούτε τους ανθρώπινους πόρους, οι οποίες μπορούν να προχωρήσουν ευκολότερα σε ένα ευρύτερο πρόγραμμα συμμόρφωσης. Η Πέννυ Κοντογεώργου, αναλύει τους λόγους: «Σχεδόν πάντα, η συμμόρφωση συνεπάγεται διαχειριστικές δυσκολίες, καθώς απαιτούνται ανασχεδιασμοί στη διακυβέρνηση των πληροφοριακών συστημάτων, καταμερισμός αρμοδιοτήτων, υιοθέτηση μηχανισμών ανίχνευσης και διαδικασίες αναφορών περιστατικών και reporting.

Επιπλέον, οι επιχειρήσεις έχουν να αντιμετωπίσουν κατακερματισμό των ροών συμμόρφωσης, λόγω παράλληλων υποχρεώσεων για NIS2, GDPR, DORA, MiCAR και CER, καθώς απαιτούνται ξεχωριστές διαδικασίες διαχείρισης κινδύνων και αναφοράς περιστατικών. Η ανάγκη για πολλαπλούς εξειδικευμένους ρόλους, όπως αυτοί του Data Protection Officer (για θέματα GDPR), Chief Information Security Officer (για το NIS2), AI Compliance Officer (λόγω του AI Act) αυξάνει το λειτουργικό κόστος και περιπλέκει τον εσωτερικό συντονισμό. Ο κίνδυνος αντικρουόμενων απαιτήσεων και επικάλυψης ευθυνών μπορεί να οδηγήσει τον οργανισμό σε γραφειοκρατική επιβάρυνση, με αποτέλεσμα σημαντικές καθυστερήσεις στη λήψη αποφάσεων, ενώ τα διαφορετικά χρονοδιαγράμματα και υποχρεώσεις αναφοράς ενδέχεται να προκαλέσουν νομικές και λειτουργικές δυσκολίες».

Ειδικά για τις (άγνωστες, ακόμα, σε βάθος χρόνου) επιπτώσεις των εφαρμογών Τεχνητής Νοημοσύνης, που

σμό με το σωστό πλαίσιο διακυβέρνησης των (καλών και ποιοτικών) δεδομένων.

Γενικά, η πλεύση σε «αχαρτογράφητα νερά» δεν είναι εύκολη υπόθεση, όμως, σε σχέση με το άναρχο παρελθόν και με δεδομένη τη διαρκή αύξηση των κυβερνοεπιθέσεων, η συμμόρφωση με κανονισμούς και πλαίσια και η συντεταγμένη πορεία απ' όλους τους εμπλεκόμενους μάλλον αποτελεί τη μόνη συνταγή επιβίωσης και την επόμενη ημέρα.

Η από μηχανής τεχνολογία

Κι εδώ έρχεται να προσφέρει χείρα βοηθείας -για πολυποστή φορά- η τεχνολογία που, στη συγκεκριμένη περίπτωση έχει τόσο ιδιαίτερο όνομα -RegTech (Regulation Technology)- όσο και ιδιαίτερη αποστολή, τη βέλτιστη διαχείριση των κανονιστικών διαδικασιών με τη βοήθεια της τεχνολογίας, η οποία έρχεται αρωγός μας στον έλεγχο, στην αναφορά συμβάντων και βεβαίως στη συμμόρφωση με ένα ή περισσότερα κανονιστικά πλαίσια. Καθώς η αποτελεσματική συμμόρφωση με τόσους πολλούς κανονισμούς, μόνο απλή δεν είναι, η τεχνολογία -κυρίως αυτοματισμοί, Μηχανική Μάθηση (ML), εφαρμογές blockchain και βεβαίως Τεχνητή Νοημοσύνη (AI)- έρχεται να βοηθήσει στην αποδοτική διαχείριση μεγάλου όγκου δεδομένων, με τον σωστό τρόπο και στον σωστό χρόνο, ξεπερνώντας την πολυπλοκότητα του περιβάλλοντος. Μεγάλα πλεονεκτήματα, εκτός από την αποτελεσματικότητα που προαναφέραμε, η ακρίβεια στις μετρήσεις, οι ολοκληρωμένες εκτιμήσεις και αναφορές σε πραγματικό χρόνο σε περιβάλλον διαφάνειας και εμπιστοσύνης για όποια αλλαγή συμβεί, όπως και η δυνατότητα άμεσης προσαρμογής στους διαρκώς εξελισσόμενους κανονισμούς με τη χρήση κατάλληλων εργαλείων, ώστε να μην υπάρξει ο παραμικρός κίνδυνος από αστοχία κατά την εφαρμογή τους.

Έτσι, η υιοθέτηση και υλοποίηση τέτοιων τεχνολογιών στο πλαίσιο μιας επιχείρησης ή ενός οργανισμού αποκτά ξεχωριστή σπουδαιότητα, καθώς -πέρα από την ευκολία και την ευελιξία που την ακολουθεί- εξοικονομεί πόρους και χρόνο, 'κτίζοντας' σταδιακά ανταγωνιστικό

Η τεχνολογία έρχεται να βοηθήσει στη διαχείριση μεγάλου όγκου δεδομένων, με τον σωστό τρόπο και χρόνο ώστε να επιτευχθεί η συμμόρφωση

έχουν ήδη αρχίσει να αξιοποιούνται και στον χώρο της κυβερνοασφάλειας, οι ρυθμιστικές αρχές θέλουν να διασφαλίσουν ότι αυτά τα συστήματα αναπτύσσονται και χρησιμοποιούνται με υπεύθυνο τρόπο, ενώ παράλληλα υφίστανται οι αναγκαίες δικλίδες ασφαλείας, που θα εμποδίσουν την προβληματική λειτουργία και θα ορίσουν 'ποιος έχει να δώσει λόγο'. Προφανώς, στο νέο περιβάλλον που δημιουργείται, η διαφάνεια είναι εκ των ων ουκ άνευ σε όλο το εύρος των δραστηριοτήτων, πάντα σε συνδυα-

πλεονέκτημα και ενισχύοντας τις αγαθές σχέσεις με τους πελάτες, κάτι ιδιαίτερα χρήσιμο στο σημερινό σκληρό περιβάλλον της αγοράς. Σύμφωνα με πρόσφατη έρευνα της Juniper Research, οι επενδύσεις των χρηματοοικονομικών οργανισμών, αλλά και της βιομηχανίας σε RegTech θα σημειώσουν αύξηση 124% στη διάρκεια της πενταετίας 2023-2028... Ποιος θα πίστευε σ' αυτή την εξέλιξη, όταν είδαμε τα πρώτα 'ψήγματα' τέτοιων τεχνολογιών, μετά την χρηματοοικονομική κρίση του 2006-7;

Πολλές οι προκλήσεις

Τα πλεονεκτήματα σίγουρα είναι πολλά, αλλά και οι προκλήσεις δεν πάνε πίσω... Σε πρώτη ανάγνωση και ανάλογα με το είδος του οργανισμού ή της επιχείρησης, αυτά μπορεί να έχουν σχέση με την προσπάθεια ενσωμάτωσης των νέων συστημάτων και της συνεργασίας τους με τα παλιά (βλέπε, legacy systems), τις διαφορετικές αρχιτεκτονικές τόσο στο ίδιο το IT, όσο και στη διαχείριση των δεδομένων που συχνά εμποδίζουν κάτι τέτοιο, με την ποιότητα των δεδομένων τα οποία τροφοδοτούν τα νέα συστήματα, ενδεχομένως με την πολυπλοκότητα των (εθνικών ή ευρωπαϊκών) πλαισίων και την εξειδίκευση η οποία μπορεί να απαιτείται, αλλά και με την ανάγκη για εκπαίδευση ή έστω επιμόρφωση των ατόμων που θα αναλάβουν να 'τρέξουν' τόσο το project της υλοποίησης, όσο και τη λειτουργία των σχετικών με το RegTech συστημάτων.

Αυτό, ειδικά στον δημόσιο τομέα στη χώρα μας, αποτελεί μεγάλη και ξεχωριστή πρόκληση, όπως υπογραμμίζει ο **Αθανάσιος Κοσμοπούλος**, νομικός ο ίδιος, Υπεύθυνος Προστασίας Δεδομένων στο υπουργείο Ψηφιακής Διακυβέρνησης, αλλά και πρόεδρος της Επιτροπής των ομολόγων του από εννιά κρίσιμα υπουργεία, η οποία συστάθηκε στα τέλη του περασμένου χρόνου, με στόχο τον καλύτερο συντονισμό του κοινού έργου τους. Να τι δήλωσε στο netweek, στο πλαίσιο αυτού του Special Report:

«Η διαρκής συμμόρφωση με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR) αποτελεί μια σύνθετη και πολυεπίπεδη πρόκληση για τον δημόσιο τομέα και τους οργανισμούς του ευρύτερου δημόσιου τομέα. Η δυσκολία έγκειται κυρίως στον τεράστιο όγκο προσωπικών δεδο-



εποπτικές αρχές. Η ενσωμάτωση τεχνολογιών Τεχνητής Νοημοσύνης και Μηχανικής Μάθησης συμβάλλει περαιτέρω, επιτρέποντας την αυτοματοποιημένη αναγνώριση κινδύνων, την κατάταξη δεδομένων και την αποφυγή ανθρωπίνων λαθών.

Ένα ενδεικτικό επιτυχημένο παράδειγμα είναι η εφαρμογή εργαλείων αυτοματοποιημένης διαχείρισης DPIAs (εκτιμήσεις αντικτύπου προστασίας δεδομένων) σε ευρωπαϊκούς δημόσιους φορείς, τα οποία όχι μόνο επιτάχυναν τη διαδικασία, αλλά επέτρεψαν και την ενίσχυση της λογοδοσίας. Η χρήση dashboards συμμόρφωσης, εργαλείων διαχείρισης συγκατάθεσης και αυτοματοποιημένων ειδοποιήσεων για παραβιάσεις έχει ήδη αρχίσει να μεταμορφώνει τον τρόπο με τον οποίο οι οργανισμοί αντιμετωπίζουν τις υποχρεώσεις τους βάσει του GDPR, σε αρκετά κράτη-μέλη της ΕΕ.

Ένα τέτοιο σύστημα εγκαθιστούμε αυτές τις ημέρες στη Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης, στο πλαίσιο της συμμόρφωσής της με τον GDPR, και ειδικά στο γραφείο DPO, με το οποίο οι συνεργάτες μου και εγώ θα παρακολουθούμε καθημερινά τις σχετικές δραστηριότητες και θα δρομολογούμε την επίλυση των θεμάτων που ανακύπτουν, τόσο στις τρέχουσες εφαρμογές και συστήματα, όσο και στα σχεδιαζόμενα νέα, προκειμένου να εξασφαλίζουμε την by default και by design συμμόρφωση με τον GDPR».

Το μέλλον... προβλέψιμο!

Συνηθίζουμε να λέμε πως το μέλλον είναι αόρατο. Στην περίπτωση του RegTech, όμως, αυτό μάλλον είναι προβλέψιμο: όσο το πλέγμα των κανονισμών και διατάξεων γίνεται περισσότερο περίπλοκο, τόσο θα έχουμε μεγαλύτερη ανάγκη τις συγκεκριμένες τεχνολογίες. Κι όσο προοδεύουν τεχνολογικά η Τεχνητή Νοημοσύνη, η Μη-

Όσο το πλέγμα των κανονισμών και διατάξεων γίνεται περισσότερο περίπλοκο, τόσο θα έχουμε μεγαλύτερη ανάγκη τις συγκεκριμένες RegTech λύσεις

μένων που διαχειρίζονται οι οργανισμοί, την εκτεταμένη γεωγραφική διασπορά σε όλη τη Χώρα, τη σύνθετη φύση των εφαρμογών και συστημάτων, τη συνεχή μεταβολή των τεχνολογιών και των κανονιστικών απαιτήσεων, καθώς και στην ανάγκη ύπαρξης κουλτούρας προστασίας δεδομένων σε όλα τα επίπεδα της διοικητικής πυραμίδας».

Εργαλεία και αποτελεσματικότητα

«Η αυτοματοποίηση αναφορών, ελέγχων και διαδικασιών αποτελεί καταλυτικό παράγοντα τόσο για τη μείωση του λειτουργικού κόστους, όσο και του χρόνου συμμόρφωσης. Ειδικά εργαλεία λογισμικού επιτρέπουν τη συστηματική παρακολούθηση της συμμόρφωσης, την έγκαιρη ανίχνευση παραβάσεων και την παραγωγή τεκμηριωμένων εκθέσεων για τη διοίκηση, αλλά και για τις

χανική Μάθηση και η ανάλυση των μεγάλων δεδομένων (που κι αυτά γίνονται καθημερινά ακόμα 'μεγαλύτερα'), τόσο περισσότερο θα συντρέχει στις προσπάθειές μας ο συνδυασμός τους, προκειμένου να αντιμετωπίσουμε τις αυξανόμενες δυσκολίες σ' αυτόν τον τομέα. Μάλιστα, όσο πυκνώνουν τα σύννεφα στον ορίζοντα της ηπείρου μας, λόγω της διεθνούς γεωπολιτικής κατάστασης, τόσο περισσότερο θα πλησιάζουμε στον στόχο της (όχι μόνο κατ' όνομα, αλλά στην πραγματικότητα) Ευρωπαϊκής Ένωσης. Και δεν αποκλείεται τα ήδη κοινά κανονιστικά πλαίσια να ισχυροποιηθούν ακόμα περισσότερο, τα επόμενα χρόνια, με την πλήρη εναρμόνιση των διαδικασιών συμμόρφωσης, άρα και με καθολική χρήση των ίδιων εφαρμογών RegTech.

Το μέλλον γι' αυτή την τεχνολογία, λοιπόν, είναι όχι μόνο προδιαγεγραμμένο, αλλά και λαμπρό... **nw**