ΣΤΡΑΤΗΓΙΚΗ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η μεθοδολογία ολιστικής στρατηγικής GDPR της SYNTAX θέτει τους πελάτες και τα δεδομένα τους σε ύψιστη προτεραιότητα, προστατεύει τη φήμη και ενισχύει την ανταγωνιστικότητα του οργανισμού.

Του **Καλαντζή Παναγιώτη**, ISGRC & Data Privacy Manager, SYNTAX Πληροφορική Α.Β.Ε.Ε.

Στη SYNTAX, με βάση την μακροχρόνια εμπειρία μας σε θέματα προστασίας της ιδιωτικότητας των πληροφοριών, έχουμε σχεδιάσει μια ολιστική προσέγγιση που εξασφαλίζει τη συμμόρφωση των οργανισμών με τον Γενικό Κανονισμό Προστασίας Δεδομένων και επιτρέπει τον αξιόπιστο επιχειρηματικό έλεγχο της πληροφορίας. Μόλις επτά μήνες απομένουν μέχρι τον Μάιο του 2018 που τίθεται σε πλήρη ισχύ ο ΓΚΠΔ, που αφορά στα δικαιώματα των υποκειμένων, όπως στη λήθη και στη φορητότητα των δεδομένων τους καθώς και στις υποχρεώσεις των εταιρειών και τις συνέπειες που πηγάζουν από τη μη συμμόρφωση τους με τον κανονισμό. Πρόκειται για μια πολύ σημαντική αλλαγή στην προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής των πολιτών της ΕΕ που έρχεται να εναρμονίσει το πλαίσιο λειτουργίας σε όλα τα κράτη- μέλη της Ε.Ε.

Ο ΓΚΠΔ είναι μια επιχειρηματική πρόκληση η οποία προϋποθέτει στρατηγική αντιμετώπιση

Η συμμόρφωση με τον ΓΚΠΔ είναι πρωτίστως μια στρατηγική επιχειρηματική πρόκληση προκειμένου να ανταποκριθεί ο οργανισμός στην πραγματικότητα της αγοράς και να συνεχίσει την εύρυθμη λειτουργία του μέσα από όλα τα κανάλια επικοινωνίας με το εξωτερικό περιβάλλον. Ως εκ τούτου, μπορεί να ληφθεί ως θετική επιχειρησιακή πρόκληση και να συμβάλει στη βελτιστοποίηση των διαδικασιών του οργανισμού με τα γνωστά οφέλη στην τυποποίηση, την αποδοτικότητα και στην κερδοφορία. Επιπρόσθετα, η θέσπιση στρατηγικής διαχείρισης των δεδομένων θέτει τους πελάτες- και τα δεδομένα τους – σε ύψιστη προτεραιότητα, βελτιώνει τη φήμη του οργανισμού και κατ' επέκταση ενισχύει την ανταγωνιστικότητα του. Ο Γενικός Κανονισμός απαιτεί ουσιαστικά οι οργανισμοί να μπορούν να αποδείξουν αποτελεσματικά ότι έκαναν ό, τι χρειάζεται για την ορθή επεξεργασία των προσωπικών δεδομένων που έχουν στην κατοχή τους. Προκειμένου ο οργανισμός να αποδείξει ότι εφαρμόζει μέτρα με τη δέουσα επιμέλεια και μεριμνά για την αντιμετώπιση θεμάτων που άπτονται του Κανονισμού, χρειάζεται ένα δομημένο στρατηγικό σχέδιο που εξετάζει τις περιοχές με τους υψηλότερους κινδύνους και συμβάλει στον προσδιορισμό και την ιεράρχηση των δράσεων για τη συμμόρφωση με τον Κανονισμό.

Ενδεικτικές λύσεις GDPR

Με αυτή την προοπτική στη SYNTAX διευκολύνουμε τους οργανισμούς στη σωστή διαχείριση των πληροφοριών σε όλο τον κύκλο ζωής τους εφαρμόζοντας μια στρατηγική προσέγγιση συμμόρφωσης με τον Γενικό Κανονισμό σε τέσσερα στάδια.

Ενημέρωση των εργαζομένων για θέματα συμμόρφωσης με τον Κανονισμό.

Το πρώτο βήμα προς τη συμμόρφωση με τις απαιτήσεις του Κανονισμού είναι η ευαισθητοποίηση του προσωπικού, έτσι ώστε σταδιακά να διαμορφωθεί η απαραίτητη κουλτούρα για την προστασία των προσωπικών και επιχειρηματικών δεδομένων. Η Διοίκηση καλείται να διασφαλίσει ότι όλοι οι εργαζόμενοι γνωρίζουν για τον Κανονισμό και να εξηγήσει τις αλλαγές που θα επιφέρει στη δουλειά τους. Επιπλέον, πρέπει να σχεδιαστεί και να επικοινωνηθεί αποτελεσματικά τι θα πρέπει να γίνει σε περίπτωση κάποιου περιστατικού παραβίασης της ιδιωτικότητας, δεδομένου των στενών χρονικών περιθωρίων της υποχρέωσης αναφοράς των περιστατικών εντός 72 ωρών.

Το στάδιο ενημέρωσης είναι ένα μικρό αλλά πολύ σημαντικό πρώτο βήμα- μια «γρήγορη νίκη». Ακόμα και αν υπάρχουν συστήματα ασφάλειας και διαχείρισης πληροφοριών τελευταίας τεχνολογίας για την προστασία των προσωπικών δεδομένων, οι άνθρωποι είναι συχνά ο ασθενέστερος σύνδεσμος. Η SYNTAX υποστηρίζει τους οργανισμούς στο σχεδιασμό της σωστής ενημέρωσης του προσωπικού, υλοποιώντας ολιστικά προγράμματα ενημέρωσης που περιλαμβάνουν την αξιολόγηση των αναγκών, το σχεδιασμό εκπαιδευτικού και υποστηρικτικού υλικού, και την υλοποί-

Τα τέσσερα στάδια στρατηγικής προσέγγισης συμμόρφωσης με τον GDPR

1. **Ανακάλυψη (Discover)** και ενημέρωση, όπου «ανακαλύπτονται» τα δεδομένα του οργανισμού, αντιστοιχούνται σε ιδιοκτήτες και κατηγοριοποιούνται ανάλογα με την αξία τους και το βαθμό ευαισθησίας τους
2. **Προστασία (Protect),** όπου υλοποιούνται μηχανισμοί προστασίας των δεδομένων τόσο αναφορικά με την διατήρηση της εμπιστευτικότητα και ακεραιότητας, όσο και από μη εξουσιοδοτημένη πρόσβαση
3. **Έλεγχος (Control),** όπου υλοποιούνται μηχανισμοί ελέγχου της πρόσβασης στην πληροφορία και της αποτροπής διαρροών και μη χρηστής χρήσης
4. **Αναζήτηση (Investigate),** όπου υλοποιούνται μηχανισμοί παρακολούθησης των παραπάνω, καθώς και αναζήτησης πληροφοριών

ηση της εκπαίδευσης είτε κατά πρόσωπο, είτε με την χρήση απομακρυσμένων μεθόδων.

Ανάλυση κινδύνου: από την ευαισθητοποίηση στην αποδεδειγμένη δράση συμμόρφωσης με το GDPR

Σε αυτό το στάδιο, διεξάγεται εμπεριστατωμένη ανάλυση κινδύνου που περιλαμβάνει διαδικασίες διαχείρισης επεξεργασίας και αποθήκευσης πληροφοριών, τις τεχνολογίες επεξεργασίας και προστασίας της ιδιωτικότητας των δεδομένων, και τους ανθρώπους που εμπλέκονται. Η ανάλυση κινδύνου αναδεικνύει τι έχει υλοποιηθεί και τι εκκρεμεί, πού βρίσκεται κάθε πληροφορία και πού πρέπει να βρίσκεται, πού ανιχνεύονται τα κύρια κενά και ποια κενά αποτελούν τον υψηλότερο κίνδυνο. Μόλις εντοπιστούν τα προβλήματα και οι περιοχές με κενά, είτε πρόκειται για τις ανωτέρω διαδικασίες, τα εμπεκόμενα άτομα ή τις τεχνολογίες ασφάλειας κλπ, πρέπει να δημιουργηθεί ένας πίνακας όπου ο βαθμός κινδύνου ορίζεται για κάθε πρόβλημα ή περιοχή με κενά, και δίνει τη δυνατότητα σταδιακής, και τεκμηριωμένης προσέγγισης, η οποία οδηγεί σε δράσεις και σχέδια με βάση τον βαθμό κινδύνου. Στη SYNTAX έχουμε σχεδιάσει μια μεθοδολογία αξιολόγησης ρίσκου και επίπτωσης στην ιδιωτικότητα της πληροφορίας, βασισμένη στο πρότυπο ISO/IEC 29134:2017, η οποία δίνει την δυνατότητα να τεκμηριωθεί η υπάρχουσα κατάσταση, να ανιχνευτούν οι περιοχές που υπάρχει αυξημένο ρίσκο και να σχεδιαστούν οι απαραίτητες ενέργειες για να ελαχιστοποιήσουν το ρίσκο. Το επόμενο στάδιο περιλαμβάνει το σχεδιασμό και την υλοποίηση των έργων που ορίστηκαν στο σχέδιο αντιμετώπισης. Στο στάδιο της υλοποίησης παρακολουθείται και αξιολογείται ο βαθμός επίτευξης των στόχων, οι τρόποι βελτιστοποίησης και η ακολουθία των επόμενων έργων. Η SYNTAX παρέχει στους οργανισμούς τις αναγκαίες κορυφαίες τεχνολογικές λύσεις, μέγιστο όφελος στην αποτελεσματική συμμόρφωση με τις απαιτήσεις του Κανονισμού.

Privacy by Design και διαχείριση πληροφοριών στα πλαίσια του Κανονισμού

Η έννοια του Privacy by Design αποτελεί βασικό στοιχείο του Κανονισμού, καθώς ο κανονισμός αναφέρει ρητά ότι τα συστήματα και οι εφαρμογές πρέπει να το υποστηρίζουν εξ ορισμού. Στην πράξη, οι πλατφόρμες και τα συστήματα διαχείρισης πληροφοριών, πρέπει να υποστηρίζουν ένα μοντέλο ασφάλειας, σύμφωνα με το οποίο μόνο τα άτομα που χρειάζονται πρόσβαση σε προσωπικά δεδομένα για την εκτέλεση της εργασίας τους επιτρέπεται να έχουν την απαραίτητη πρόσβαση και μόνο αυτή. Παραδοσιακά πολλοί οργανισμοί υλοποιούν μια αρχιτεκτονική πρόσβασης «ανοικτή εκτός αν». στη βάση πνεύματος διαφάνειας και ενίσχυσης της συνεργασίας. Στην πράξη διαπιστώνεται ότι όλα είναι ανοικτά επειδή κανείς δεν ξέρει πραγματικά ποιο είναι το μοντέλο ασφαλείας. Πρέπει να σχεδιαστεί ένα ολιστικό σύστημα προσβάσεων / εξουσιοδοτήσεων και να αναθεωρηθούν οι υπάρχουσες προσβάσεις στη βάση ενός μοντέλου εξουσιοδότησης «κλειστή εκτός αν» και να χορηγούνται δικαιώματα πρόσβασης μόνο στην βάση επιχειρησιακών αναγκών. Η SYNTAX βοηθά στον επανασχεδιασμό του μοντέλου προσβάσεων και εξουσιοδότησης, υποστηρίζοντας αντίστοιχα τον οργανισμό με τις κατάλληλες λύσεις που έχουν τη δυνατότητα αυτοματοποίησης της διαδικασίας έγκρισης εξουσιοδοτήσεων και κεντρικής παρακολούθησης της επάρκειας και ακρίβειας του σχετικού μοντέλου.

Το δικαίωμα στη λήθη. Γενικός Κανονισμός, Διατήρηση Αρχείων και Εγγραφών

Σύμφωνα με τον Κανονισμό, οι οργανισμοί πρέπει να διακρατούν μόνο τις απαραίτητες για την επιχειρησιακή τους λειτουργία πληροφορίες, που σημαίνει ότι πρέπει να έχουν ένα πλάνο διατήρησης, που καθορίζει τον σκοπό διατήρησης από νομική και ιστορική άποψη αλλά και επιχειρηματική προοπτική. Ως εκ τούτου ο οργανισμός πρέπει να έχει προβλέψει διαδικασία διαγραφής ή αποταυτοποίησης των δεδομένων, και βέβαια αν ένα υποκείμενο των δεδομένων ασκήσει το δικαίωμά του στην λήθη. Αυτό το πλάνο διατήρησης και ταξινόμησης της πληροφορίας θα εξετάζει τους τύπους εγγράφων και τα συστήματα διατήρησης, όπως ορίζονται από το εκάστοτε νομικό πλαίσιο και από το εθνικό δίκαιο που καθορίζει συγκεκριμένες απαιτήσεις διατήρησης, διότι το εθνικό δίκαιο επικρατεί έναντι του GDPR. Η SYNTAX προσφέρει λύσεις σχεδιασμού του πλάνου διατήρησης, καθώς και μηχανισμούς αρχειοθέτησης ώστε να βοηθήσουν τον οργανισμό στην αποδοτική διατήρηση αρχείων και εγγράφων.

INFO

SYNTAX Πληροφορική ΑΒΕΕ
Μεσογείων 216, Χολαργός 15561
T: 210 6543100
E: isgrc@syntax.gr
S: www.syntax.gr