Issue

Ο νέος **κανονισμός προστασίας των δεδομένων** και η ανάγκη για Data Breach Insurance

Στις 14 Απριλίου 2016, το Ευρωπαϊκό Κοινοβούλιο ενέκρινε το Γενικό Κανονισμό για τα Προσωπικά δεδομένα. Ο κανονισμός αναμένεται να τεθεί σε ισχύ την άνοιξη του 2016 και θα αρχίσει να εφαρμόζεται την άνοιξη του 2018.

Ο νέος κανονισμός που ενέκρινε το Ευρωπαϊκό Κοινοβούλιο για τα προσωπικά δεδομένα, περιγράφει τα δικαιώματα του υποκειμένου των δεδομένων, δηλαδή του ατόμου του οποίου τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία. Αυτά τα ενισχυμένα δικαιώματα παρέχουν στα άτομα μεγαλύτερο έλεγχο επί των προσωπικών τους δεδομένων, μεταξύ άλλων μέσω:

- Της ανάγκης ύπαρξης σαφούς συγκατάθεσης του ενδιαφερομένου για την επεξεργασία των προσωπικών του δεδομένων.
- Της ευκολότερης πρόσβασης του ενδιαφερομένου στα προσωπικά του δεδομένα
- των δικαιωμάτων διόρθωσης, διαγραφής και «λήθης».
- Του δικαιώματος εναντίωσης, μεταξύ άλλων στη χρησιμοποίηση των δεδομένων προσωπικού χαρακτήρα για την «κατάρτιση προφίλ».
- Του δικαιώματος φορητότητας των δεδομένων από πάροχο σε πάροχο

Ο νέος κανονισμός θεσπίζει επίσης, την υποχρέωση των υπεύθυνων επεξεργασίας των δεδομένων να παρέχουν διαφανείς


Νίκος Γεωργόπουλος, *MBA, cyRM*
Cyber Risks Advisor
Cromar Coverholder at Lloyd's

και εύκολα προσβάσιμες πληροφορίες στα υποκείμενα όσον αφορά την επεξεργασία των δεδομένων τους. Επιπλέον, ορίζει αναλυτικά τις γενικές υποχρεώσεις που έχουν οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία των δεδομένων προσωπικού χαρακτήρα για λογαριασμό αυτών. Και οι δύο, έχουν την υποχρέωση τήρησης κατάλληλων μέτρων ασφαλείας ανάλογα με τον κίνδυνο τον οποίον ενέχουν οι πράξεις επεξεργασίας δεδομένων τις οποίες εκτελούν.

Οι υπεύθυνοι επεξεργασίας σε ορισμένες περιπτώσεις, πρέπει να **κοινοποιούν τα περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα εντός 72 ωρών** από την ανακάλυψη του περιστατικού παραβίασης και απώλειας προσωπικών δεδομένων στις αρμόδιες αρχές και στα υποκείμενα των δεδομένων αν η φύση των δεδομένων που χάθηκαν το απαιτεί. Επίσης, για τις εταιρείες και τις δημόσιες αρχές που εκτελούν πράξεις επεξεργασίας δεδομένων που ενέχουν κινδύνους και το προσωπικό τους ξεπερνά τα 250 άτομα θα πρέπει να έχουν ορίσει **υπεύθυνο προστασίας δεδομένων**. Για τους υπεύθυνους επεξεργασίας ή τους εκτελούντες την επεξεργασία δεδομένων οι οποίοι παραβιάζουν τους κανόνες για την προστασία των δεδομένων προβλέπονται πολύ αυστηρές κυρώσεις.

Στους υπευθύνους επεξεργασίας δεδομένων μπορεί να επιβληθεί πρόστιμο που μπορεί να ανέλθει σε 20 εκατ. € ή στο 4% του συνολικού ετήσιου κύκλου εργασιών τους.

Κριτήρια επιβολής προστίμου

Για την επιβολή διοικητικού προστίμου, καθώς και σχετικά με το ύψος του διοικητικού προστίμου για κάθε μεμονωμένη περίπτωση, λαμβάνονται υπόψη ενδεικτικά τα ακόλουθα:

- Η φύση, η βαρύτητα και η διάρκεια της παράβασης, λαμβάνοντας υπόψη τη φύση, την έκταση ή το σκοπό της σχετικής επεξεργασίας, καθώς και τον αριθμό των υποκειμένων των δεδομένων που έθιξε η παράβαση και το βαθμό ζημίας που υπέστησαν.
- Ο δόλος ή η αμέλεια που προκάλεσε την παράβαση.
- Οποιεσδήποτε ενέργειες στις οποίες προέβη ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία για να μετριάσει τη ζημία που υπέστησαν τα υποκείμενα των δεδομένων.
- Ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα που εφαρμόζουν.
- Τυχόν σχετικές προηγούμενες παραβάσεις του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.
- Ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των πιθανών δυσμενών επιπτώσεών της.
- Οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει η παράβαση.
- Ο τρόπος με τον οποίο η εποπτική αρχή πληροφορήθηκε την παράβαση, ειδικότερα εάν και κατά πόσο ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία κοινοποίησε την παράβαση.
- Σε περίπτωση που διατάχθηκε προηγουμένως η λήψη των μέτρων που αναφέρονται κατά του εμπλεκόμενου υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σχετικά με το ίδιο αντικείμενο, η συμμόρφωση με τα εν λόγω μέτρα.
- Η τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης σύμφωνα.
- Κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο που προκύπτει από τις περιστάσεις της συγκεκριμένης περίπτωσης, όπως τα οικονομικά οφέλη που αποκομίστηκαν ή ζημιών που αποφεύχθηκαν, άμεσα ή έμμεσα, από την παράβαση.

Η απαίτηση για Data Breach Insurance

Ο κανονισμός αναγνωρίζει το δικαίωμα των υποκειμένων των δεδομένων να υποβάλλουν καταγγελία σε εποπτική αρχή καθώς και το δικαίωμά τους για δικαστική προσφυγή και αποζημίωση. Έτσι, οι εταιρείες είναι εκτεθειμένες σε αγωγές από τρίτους των οποίων χάθηκαν τα προσωπικά τους δεδομένα. Η συμμόρφωση των εταιρειών με τον Νέο Γενικό Κανονισμό δεν σημαίνει ότι δε θα έχουμε περιστατικά παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών, για το λόγο αυτό οι εταιρείες που θέλουν να τα διαχειριστούν αποτελεσματικά και να προστατεύουν τον Ισολογισμό τους θα πρέπει να χρησιμοποιήσουν την ασφάλιση **Data Breach Insurance.**

Λαμβάνοντας υπόψη τα νέα δεδομένα που θα προκύψουν από την εφαρμογή του κανονισμού η Cromar προσφέρει στην Ελληνική αγορά σε συνεργασία με τους Beazley, ηγετικό συνδικάτο των Lloyd's στην ασφάλιση περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων, μία από τις καλύτερες ασφαλιστικές λύσεις το "Beazley Global Breach Solution". Το "Beazley Global Breach Solution" προσφέρει εκτός από τις χρηματικές αποζημιώσεις πρόσβαση στην Ομάδα Διαχείρισης Περιστατικών του η οποία έχει αντιμετωπίσει πάνω από 3.000 περιστατικά παγκοσμίως και έχει βραβευθεί από την Advisen ως η καλύτερη ομάδα διαχείρισης για το 2015. Περισσότερες πληροφορίες μπορείτε να βρείτε στα **www.cyberinsurancegreece.com, www.privacyrisksadvisors.com** και **www.cyberinsurancequote.gr**. Επίσης μπορείτε να δείτε την παρουσίαση του συνεδρίου Infocom Security 2016 με τίτλο "Not if but When". ITSecurity