DATA BREACH.

Η ΑΝΤΙΜΕΤΩΠΙΣΗ ΑΠΟ ΤΗΝ ΑΠΔΠΧ – ΠΡΟΤΑΣΕΙΣ ΣΩΣΤΗΣ ΠΡΟΕΤΟΙΜΑΣΙΑΣ

ΑΛΚΙΒΙΑΔΗΣ ΠΟΥΛΙΑΣ

Η ΥΛΟΠΟΙΗΣΗ ΑΠΟ ΤΗΝ ΑΠΔΠΧ ΤΩΝ ΝΕΩΝ ΑΡΜΟΔΙΟΤΗΤΩΝ ΤΗΣ

- Ο ΓΚΠΔ (GDPR) άλλαξε ριζικά το ρόλο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ενόψει της αρχής της λογοδοσίας.
- Πλέον ο Υπεύθυνος Επεξεργασίας πρέπει να είναι σε θέση να αποδεικνύει τη διαρκή συμμόρφωσή του στον ΓΚΠΔ.
- Η έννοια της άδειας της ΑΠΔΠΧ δεν υφίσταται πλέον, όμως η Αρχή έχει ευρεία εξουσία ελέγχου, όμοια με αυτή της Αρχής Ανταγωνισμού
- Μπορεί να διεξάγει ελέγχους και να ζητά κάθε πληροφορία που κρίνει απαραίτητη για την άσκηση των καθηκόντων της

ΥΠΟΧΡΕΩΣΕΙΣ ΣΕ ΠΕΡΙΠΤΩΣΗ DATA BREACH

- **Παραβίαση δεδομένων** (άρθρο 4 στοιχείο 12 GDPR): Η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή , απώλεια, μεταβολή, άνευ αδείας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα
- **Αρχή της λογοδοσίας:** Υποχρέωση του Υπευθύνου Επεξεργασίας να γνωστοποιεί στην Αρχή την παραβίαση προσωπικών δεδομένων αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη γνώση του περιστατικού.
- Η **καθυστέρηση γνωστοποίησης** θα πρέπει να δικαιολογείται με αντικειμενικό και σοβαρό λόγο.
- Δυνατή η **σταδιακή γνωστοποίηση** παραβάσεων, εάν δεν είναι δυνατόν να παρασχεθούν οι πληροφορίες ταυτόχρονα.
- Εάν διαπιστώνεται υψηλός κίνδυνος για τα δικαιώματα και τις υποχρεώσεις των υποκειμένων, πρέπει να γίνει άμεση και ειδική γνωστοποίηση και στα υποκείμενα των δεδομένων που παραβιάστηκαν

ΤΙ ΠΕΡΙΛΑΜΒΑΝΕΙ Η ΓΝΩΣΤΟΠΟΙΗΣΗ;

- **Φύση της παραβίασης** (κατηγορίες δεδομένων, κατ' εκτίμηση αριθμός των επηρεαζόμενων προσώπων, κατηγορίες και αριθμός κατά προσέγγιση των αρχείων προσωπικών δεδομένων που παραβιάστηκαν)
- **Όνομα και στοιχεία επικοινωνίας** του Υπευθύνου Προστασίας Δεδομένων
- **Ενδεχόμενες συνέπειες** της παραβίασης
- **Ληφθέντα ή προτεινόμενα μέτρα** για την αντιμετώπιση της παραβίασης και των συνεπειών της

Η ΣΤΑΣΗ ΤΗΣ ΑΠΔΠΧ ΣΕ ΠΡΟΣΦΑΤΑ ΠΕΡΙΣΤΑΤΙΚΑ DATA BREACH

- Κατά τους πρώτους 6 μήνες εφαρμογής του **GDPR**, έχουν υποβληθεί στην Αρχή 66 γνωστοποιήσεις περιστατικών παραβίασης (ενημερωτική ανακοίνωση της ΑΠΔΠΧ 20.12.2018)
- Σε 36 περιπτώσεις έγινε και ανακοίνωση του περιστατικού σε επηρεαζόμενα φυσικά πρόσωπα.
- Η Αρχή έχει εκδώσει 3 αποφάσεις για τα ανωτέρω περιστατικά, ενώ είναι υπό εξέταση άλλες 9 περιπτώσεις.

ΟΙ ΤΡΕΙΣ ΑΠΟΦΑΣΕΙΣ ΤΗΣ ΑΠΔΠΧ ΣΕ ΠΡΟΣΦΑΤΑ ΠΕΡΙΣΤΑΤΙΚΑ DATA BREACH

- **Η ΑΠΔΠΧ εξέτασε τρεις περιπτώσεις παραβίασης** δεδομένων: Η μια σχετίζεται με **hacking** ιστοσελίδας ηλεκτρονικών πωλήσεων και οι δύο με ακούσια περιορισμένη διαρροή προσωπικών δεδομένων από Τράπεζες.
- Οι δύο Τράπεζες δεν γνωστοποίησαν την παραβίαση εντός 72 ωρών, αλλά με καθυστέρηση
- Η μία Τράπεζα δεν αιτιολόγησε την καθυστέρηση, ενώ η δεύτερη επικαλέστηκε λόγους διερεύνησης και επιβεβαίωσης των παραβιάσεων.
- Η εταιρεία ηλεκτρονικών πωλήσεων έκανε εμπρόθεσμη αρχική γνωστοποίηση και ακολούθησε συμπληρωματική γνωστοποίηση. Η Αρχή ζήτησε επιπλέον διευκρινίσεις και η εταιρεία έκανε και νέα διευκρινιστική απάντηση.

ΟΙ ΤΡΕΙΣ ΑΠΟΦΑΣΕΙΣ ΤΗΣ ΑΠΔΠΧ ΣΕ ΠΡΟΣΦΑΤΑ ΠΕΡΙΣΤΑΤΙΚΑ DATA BREACH

- Η Αρχή απηύθυνε **και στις τρεις περιπτώσεις επίπληξη** στους Υπευθύνους Επεξεργασίας, με διαφορετική αιτιολόγηση.
- **Οι δύο τράπεζες,** παρά το ότι έλαβαν τα κατάλληλα μέτρα και αντιμετώπισαν σωστά την παραβίαση, η οποία κρίθηκε ως περιορισμένη, δέχθηκαν επίπληξη **γιατί δεν τήρησαν την προειδοποίηση των 72 ωρών**.
- **Η αιτιολόγηση καθυστέρησης της δεύτερης τράπεζας κρίθηκε ανεπαρκής,** δεδομένου ότι η καθυστέρηση των 24 ημερών κρίθηκε υπερβολική σε κάθε περίπτωση.
- **Η εταιρεία ηλεκτρονικού εμπορίου** δέχθηκε επίπληξη **για παραβίαση της αρχής της ασφάλειας των δεδομένων,** καθώς διαπιστώθηκε έλλειψη κατάλληλων μηχανισμών ανίχνευσης επιθέσεων ασφαλείας, έλλειψη τακτικών ενημερώσεων ασφαλείας λογισμικού και τακτικής δοκιμής αποτελεσματικότητας των μέτρων ασφαλείας.

ΟΙ ΤΡΕΙΣ ΑΠΟΦΑΣΕΙΣ ΤΗΣ ΑΠΔΠΧ ΣΕ ΠΡΟΣΦΑΤΑ ΠΕΡΙΣΤΑΤΙΚΑ DATA BREACH

- **Οι δύο αποφάσεις** που απευθύνουν επίπληξη για καθυστέρηση γνωστοποίησης, στην αιτιολόγηση της ποινής **αναφέρουν ότι λήφθηκε υπ' όψη το γεγονός ότι ο ΓΚΠΔ (GDPR) έχει μόλις τεθεί σε εφαρμογή**.
- **Στο μέλλον η αντιμετώπιση** της καθυστέρησης στη γνωστοποίηση **θα είναι αυστηρότερη**.
- **Οι αποφάσεις** αυτές **δίνουν χρήσιμα στοιχεία** για τις κατάλληλες ενέργειες αποφυγής και προετοιμασίας μιας παραβίασης δεδομένων.

ΠΡΟΤΑΣΕΙΣ ΠΡΟΕΤΟΙΜΑΣΙΑΣ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ

Ο ανθρώπινος παράγοντας:

- **Κρίσιμη η εκπαίδευση του προσωπικού,** ώστε να είναι εξοικειωμένοι με τις βασικές αρχές και υποχρεώσεις του GDPR και να αναγνωρίζουν έγκαιρα την παραβίαση
- Εξ αρχής **ορισμός συγκεκριμένων ατόμων, που να υποστηρίζουν τον DPO** τόσο στην αναγνώριση, όσο και στην αντιμετώπιση περίπτωσης παραβίασης δεδομένων
- **Στον Όμιλο ΕΛΠΕ λειτουργεί Συμβούλιο Προστασίας Προσωπικών Δεδομένων**, το οποίο αναλαμβάνει υπό την αποτελεσματικότερη διαχείριση των κρίσεων που τυχόν θα προκύψουν σε περίπτωση σοβαρών περιστατικών Παραβίασης Προσωπικών Δεδομένων, βάσει ειδικής Διαδικασίας
- Επίσης **έχουν οριστεί Υπεύθυνοι Προστασίας Ιδιωτικότητας** για κάθε Γενική Διεύθυνση και Οργανωτική Μονάδα

ΠΡΟΤΑΣΕΙΣ ΠΡΟΕΤΟΙΜΑΣΙΑΣ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ

Τα τεχνικά μέτρα

- Απαραίτητα τα επαρκή και σύγχρονα συστήματα ηλεκτρονικής διαχείρισης δεδομένων
- Έλεγχος και δοκιμές για την σωστή λειτουργία
- Άμεση εφαρμογή ενημερώσεων ασφαλείας
- Κατάλληλοι μηχανισμοί για έγκαιρη διαπίστωση επιθέσεων ασφαλείας