www.motive.com.gr

Διαχείριση & Προστασία Προσωπικών Δεδομένων

Νέος Ευρωπαϊκός Κανονισμός GDPR

02/11/2017

Ιωαννίδης Τάσος, Motive Συμβουλευτική

Curriculum Vitae

Ιωαννίδης Τάσος

- ***General Manager Motive Συμβουλευτική,***
- ***MSc in Quality Management, Information Security Management System (ISMS) & GDPR Expert Consultant,***
- ***Information Technology Service Management System (ITSMS) Expert Consultant***


ioannidis@motive.com.gr


6972 50 34 13


ioannidis.tasos


Tasos Ioannidis

Motive Συμβουλευτική

Η Motive Συμβουλευτική συστάθηκε το 2006 με αντικείμενο δραστηριότητας:

- Σχεδιασμός, Ανάπτυξη και Υποστήριξη Διαχειριστικών Συστημάτων βάσει Διεθνών Προτύπων (ISO 9001, ISO 27001, ISO 20000, ISO 14001, ISO 22000 κλπ)
- Υπηρεσίες Εναρμόνισης με τον Νέο Ευρωπαϊκό Κανονισμό GDRP (General Data Protection Regulation) 679/2016
- Υπηρεσίες εκπαίδευσης (σεμινάρια, ενδοεπιχειρησιακά, webinars)
- Σχεδιασμός και Διαχείριση R&D έργων (χρηματοδοτικά εργαλεία)
- Συμβουλευτικές Υπηρεσίες και Διαχείριση Έργων ΕΣΠΑ και άλλων χρηματοδοτικών εργαλείων (Εθνικών ή Ευρωπαϊκών) για Δημόσιους και Ιδιωτικούς Φορείς
- Συμβουλευτικές Υπηρεσίες και Διαχείριση Έργων Οργάνωσης και Διοίκησης επιχειρήσεων-οργανισμών όπως Business Plan, Marketing Plan, Μελέτες Σκοπιμότητας, Μελέτες Βιωσιμότητας κλπ
- Ανάπτυξη, διάθεση και υποστήριξη εξειδικευμένου software Business Process Management Solutions, παρέχοντας καινοτόμες λύσεις σε επιχειρήσεις και οργανισμούς του Δημόσιου και Ιδιωτικού τομέα.
- Δημιουργία υποδομής στη Διοικητική Οργάνωση την διαχείριση και διοίκηση των διαδικασιών (Process Management Solutions) των επιχειρήσεων και οργανισμών του Δημόσιου αλλά και του Ιδιωτικού Τομέα

Κατάλογος Έργων

- Επενδυτικά Προγράμματα
- Business Plans
- Marketing Plans
- Έρευνες Αγοράς
- Business Consulting
- Σχεδιασμός, Ανάπτυξη και Εφαρμογή Συστημάτων Διαχείρισης κατά **ISO 9001, ISO 14001, ISO 220000 και OHSAS 18001**σε **επιχειρήσεις και οργανισμούς**
- Σχεδιασμός, Ανάπτυξη και Εφαρμογή Συστημάτων **Διαχειριστικής Επάρκειας και ΕΛΟΤ 1429 σε οργανισμούς**
- Σχεδιασμός, Ανάπτυξη και Εφαρμογή Συστημάτων Διαχείρισης (ISMS) κατά **ISO 27001, ISO 27002, ISO 27017, ISO 27018, ISO 22301** σε **επιχειρήσεις και οργανισμούς**
- Σχεδιασμός, Ανάπτυξη και Εφαρμογή Συστημάτων Διαχείρισης IT services (ITSMS) κατά **ISO 20000** σε **επιχειρήσεις**
- **Σχεδιασμός, Ανάπτυξη και Εφαρμογή συστημάτων διαχείρισης ασφάλειας προσωπικών δεδομένων κατά GDPR σε επιχειρήσεις -οργανισμούς**

Motive Συμβουλευτική

Φράγκων 12, Θεσσαλονίκη, Τηλ: 2310-541017,Fax: 2310-521402,T.K:54626,

E-mail: info@motive.com.gr Web: www.motive.com.gr

Compliance & Training Services GDPR Pro

www.gdprprofessional.com, www.gdprprofessional.gr

gdpr@motive.com.gr

LinkedIn Group: GDPR Pro

CASE STUDIES

Data Breaches

USA

- Τον Σεπτέμβριο του 2016, η Yahoo ανακοίνωσε την παραβίαση δεδομένων που συνέβαινε από τα τέλη του 2014, σε περισσότερους από 500 εκατομμύρια λογαριασμούς χρηστών αποκαλύπτοντας ορισμένες πληροφορίες λογαριασμού χρήστη, συμπεριλαμβανομένων των ημερομηνιών γεννήσεως, των κωδικών πρόσβασης που έχουν χρεωθεί και, σε ορισμένες περιπτώσεις, κρυπτογραφημένων ή μη κρυπτογραφημένων ερωτήσεων και απαντήσεων σχετικά με την ασφάλεια. Τον Δεκέμβριο του 2016 ανακοίνωσε μια δεύτερη, μεγαλύτερη, παραβίαση σε 1 δισεκατομμύριο λογαριασμούς η οποία συνέβη τον Αύγουστο του 2013, με μη εξουσιοδοτημένα τρίτα πρόσωπα να κλέβουν παρόμοια δεδομένα. Οι εν λόγω παραβιάσεις έχουν πλέον θέσει υπό αμφισβήτηση την εκκρεμούσα εξαγορά της εταιρείας, ύψους 4,8 δισ. Δολαρίων, από την Verizon.

Πηγή: http://www.crn.com/slide-shows/security/300083246/the-10-biggest-data-breaches-of-2016.htm/pgno/0/10

USA

- Τον Οκτώβριο του 2016, κατά το τέλος της προεκλογικής εκστρατείας των Αμερικανικών εκλογών, χιλιάδες διαρρεύσαντα μηνύματα ηλεκτρονικού ταχυδρομείου της Δημοκρατικής Εθνικής Επιτροπής (DNC) δημοσιεύθηκαν στο Wikileaks, επηρεάζοντας αρνητικά τους Δημοκρατικούς και βοηθώντας στη διαμόρφωση του εκλογικού αποτελέσματος. Σύμφωνα με τις ΗΠΑ, πίσω από την πειρατεία της DNC βρισκόταν η Ρωσία, υποστηρίζοντας μάλιστα πως έγινε εν γνώση του υποψηφίου προέδρου Ντόναλντ Τραμπ. Σχετική έκθεση αναφέρει την αποτυχημένη προσπάθεια της Ρωσίας να διεισδύσει και στην Εθνική Επιτροπή των Ρεπουμπλικάνων.
- Το Myspace ανακοίνωσε τον Μάιο του 2016 παραβίαση σε πάνω από 360 εκατομμύρια λογαριασμούς. Συγκεκριμένα, ανακάλυψε ότι οι διευθύνσεις ηλεκτρονικού ταχυδρομείου, τα ονόματα χρηστών και οι κωδικοί πρόσβασης για λογαριασμούς που δημιουργήθηκαν πριν από τις 11 Ιουνίου 2013 είχαν αναρτηθεί σε ένα online φόρουμ χάκερ. Το Myspace που είχε ενημερώσει την πλατφόρμα του το 2013, περιλαμβάνοντας ενίσχυση της ασφάλειας του λογαριασμού, απέδωσε το γεγονός στο Ρωσικό Χάκερ «Peace».

Πηγή: http://www.crn.com/slide-shows/security/300083246/the-10-biggest-data-breaches-of-2016.htm/pgno/0/10

USA

Παρόμοια με το MySpace, η Tumblr ανακοίνωσε ότι 65 εκατομμύρια λογαριασμοί, από μια παραβίαση του 2013, είχαν αναρτηθεί στον σκοτεινό ιστό. Η LinkedIn ανακοίνωσε επίσης, ότι ανακάλυψε 117 εκατομμύρια συνδυασμούς ηλεκτρονικού ταχυδρομείου και κωδικούς πρόσβασης προς πώληση στο σκοτεινό ιστό, φέτος, από την παραβίαση του 2012. Το Foursquare επίσης φέρεται να έχει πληγεί από παραβίαση που πλήττει 22,5 εκατομμύρια πελάτες, αν και η εταιρεία αρνείται την παραβίαση.

- Τον Απρίλιο του 2016, ένας φορητός υπολογιστής και φορητοί σκληροί δίσκοι που περιείχαν προσωπικές πληροφορίες 5 εκατομμυρίων ατόμων, εκλάπηκαν από το Γραφείο Επιβολής Παιδικής Υποστήριξης στην Ουάσινγκτον, τμήμα του Υπουργείου Υγείας και Ανθρωπίνων Υπηρεσιών των ΗΠΑ. Το γεγονός αποδώθηκε σε πρώην δυσαρεστημένο υπάλληλο. Η παράβαση ήρθε ένα χρόνο μετά από όταν η ομοσπονδιακή κυβέρνηση ανακοίνωσε μια τεράστια παραβίαση δεδομένων που έπληξε το Γραφείο Διαχείρισης Προσωπικού που εξέθεσε τις προσωπικές πληροφορίες περισσότερων από 21 εκατομμυρίων ομοσπονδιακών εργαζομένων και εργολάβων.
- Η Verizon Enterprise Services ανακοίνωσε την παραβίαση δεδομένων και συλλογή πληροφοριών από χάκερ για περίπου 1,5 εκατομμύριο επιχειρήσεις, συμπεριλαμβανομένων των βασικών πληροφοριών επικοινωνίας. Η Verizon ανέφερε ότι δεν απέκτησαν πρόσβαση σε πληροφορίες που αφορούν αποκλειστικά τους πελάτες του δικτύου ή άλλα δεδομένα. Βέβαια, η ακριβής αιτία της παραβίασης δεν είναι σαφής. Η Verizon στρέφει την προσοχή της στους παρόχους τηλεπικοινωνιών καθώς κατέχουν μεγάλο αριθμό πληροφοριών για τους πελάτες, γεγονός που τους καθιστά εκλυστικό στόχο για τους χάκερς.

Πηγή: http://www.crn.com/slide-shows/security/300083246/the-10-biggest-data-breaches-of-2016.htm/pgno/0/10

USA

- Τον Αύγουστο του 2016, τα συστήματα πληροφορικής της Oracle είχαν πειραχτεί, με επιθέσεις σε συστήματα πληρωμών με πιστωτικές κάρτες της Micros Systems (η Oracle εξαγόρασε τη Micros Systems τον Σεπτέμβριο του 2014 για $ 5,3 δισ.). Ανακοινώθηκε, μάλιστα, ότι μια ρωσική οργανωμένη ομάδα εγκληματικότητας στον κυβερνοχώρο «γνωστή για πειρατεία σε τράπεζες και λιανοπωλητές» φαίνεται να βρίσκεται πίσω από την επίθεση που «παραβίαζε εκατοντάδες συστήματα υπολογιστών» στην Oracle. Για αποτροπή της επανάληψης μιας τέτοιας παραβίασης, η εταιρεία ζήτησε από όλους τους πελάτες της Micros να αλλάξουν τους κωδικούς τους για όλους τους λογαριασμούς Micros.
- Η υπηρεσία φιλοξενίας ιστοσελίδων και δημιουργίας ιστοτόπων Weebly επιβεβαίωσε τον Οκτώβριο του 2016, παραβίαση δεδομένων σε περισσότερους από 43,5 εκατομμύρια λογαριασμούς, συμπεριλαμβανομένων των ονομάτων χρηστών, των διευθύνσεων ηλεκτρονικού ταχυδρομείου, των κωδικών πρόσβασης και των διευθύνσεων IP. Η παραβίαση επηρέασε τόσο την ασφάλεια των χρηστών όσο και τους ιστότοπους που σχετίζονται με αυτές. Βέβαια, σύμφωνα με το Weebly, οι πληροφορίες πιστωτικής κάρτας δεν έχουν ληφθεί ή χρησιμοποιηθεί ακατάλληλα μετά την παραβίαση.
- Ο πάροχος υπηρεσιών φροντίδας καρκίνου 21st Century Oncology ανακοίνωσε τον Μάρτιο του 2016 παραβίαση δεδομένων 2,2 εκατομμυρίων ασθενών με έδρα σε όλα τα 50 κράτη και διεθνώς. Σύμφωνα με την εταιρία, οι χάκερς δυείσδυσαν σε μια εταιρική βάση δεδομένων τον Οκτώβριο του 2015, με πρόσβαση σε προσωπικές πληροφορίες των ασθενών, συμπεριλαμβανομένων των ονομάτων, των αριθμών κοινωνικής ασφάλισης, των ιατρών, της διάγνωσης, των δεδομένων θεραπείας και των ασφαλιστικών πληροφοριών.
- Τον Νοέμβριο, το Πολεμικό Ναυτικό ανακοίνωσε ότι τον προηγούμενο μήνα, απέκτησαν πρόσβαση "άγνωστα άτομα« σε πληροφορίες ενός φορητού υπολογιστή που λειτουργούσε από έναν ανάδοχο υπηρεσιών HPE. Οι πληροφορίες περιελάμβαναν ονόματα και αριθμούς κοινωνικής ασφάλισης περισσότερων από 134.000 υπαλλήλων του τρέχοντος και πρώην ναυτικού.

Πηγή: http://www.crn.com/slide-shows/security/300083246/the-10-biggest-data-breaches-of-2016.htm/pgno/0/10

Παγκόσμια Κυβερνοεπίθεση **WannaCry**

- Την Παρασκευή 12 Μαΐου 2017, έλαβε χώρα μία από τις μεγαλύτερες κυβερνοεπιθέσεις αφού τουλάχιστον 200.000 ηλεκτρονικοί υπολογιστές σε τουλάχιστον 150 χώρες μολύνθηκαν από ιό τύπου ransomeware. Η λειτουργία του κακόβουλου αυτού λογισμικού είναι να κλειδώνει τα αρχεία των χρηστών και να τους αναγκάζει να πληρώσουν ένα ποσό σε bitcoin, ίσο με 300 δολάρια (275 ευρώ), προκειμένου να ξεκλειδώσει τα αρχεία. Αναφέρεται μάλιστα, ότι τα θύματα είχαν διορία 3 ημέρες να καταβάλουν τα χρήματα αλλιώς το ποσό θα διπλασιαζόταν.
- Σύμφωνα με το BBC, τα εργαλεία που χρησιμοποιήθηκαν για αυτή την επίθεση έχουν κλαπεί από την Εθνική Υπηρεσία Ασφάλειας (NSA) των ΗΠΑ και συγκεκριμένα ένα κομμάτι από τον κώδικα της NSA γνωστό ως «Eternal Blue» . Οι επιθέσεις είχαν στόχο οργανισμούς σε ολόκληρο σχεδόν τον κόσμο. Όπως αναφέρει η Microsoft, οι εν λόγω χάκερς εκμεταλλεύτηκαν μία ευπάθεια στα Windows και πραγματοποίησαν την επίθεση με τον ιό με την ονομασία WannaCry, που έχει την ικανότητα να διαδίδεται αυτομάτως σε εκτεταμένα δίκτυα. Ειδικότερα, «ξεγέλασαν» χρήστες τους οποίους έκαναν να ανοίξουν μολυσμένα από ιό συνημμένα σε email που έμοιαζαν να περιέχουν τιμολόγια, προσφορές απασχόλησης, προειδοποιήσεις ασφαλείας και άλλους θεμιτούς φακέλους.
- Κορυφαίοι στόχοι της επίθεσης αποτελούν η Ρωσία, η Ουκρανία και η Ταιβάν ενώ οι Ασιατικές Χώρες δεν έχουν αναφέρει μέχρι στιγμής σημαντικές παραβιάσεις. Ωστόσο, η μεγαλύτερη αναστάτωση προκλήθηκε στη Βρετανία και ειδικότερα στην Υπηρεσία Εθνικής Υγείας της. Επιθέσεις ανέφεραν και η εταιρεία διεθνών ταχυμεταφορών FedEx Corp, η γαλλική αυτοκινητοβιομηχανία Renault και πολλά συστήματα της δημόσιας επιχείρησης των γερμανικών σιδηροδρόμων της Deutsche Bahn.

EU

- Η εταιρεία δανεισμού Payday Wonga έχει πέσει θύμα μιας μεγάλης παραβίασης δεδομένων που θα μπορούσε να χτυπήσει μέχρι και 245.000 πελάτες της, συμπεριλαμβανομένων αριθμών τραπεζικών λογαριασμών και κωδικών ταξινόμησης. Η Wonga πιστεύει ότι τα πλήρη ονόματα, οι διευθύνσεις ηλεκτρονικού ταχυδρομείου, οι διευθύνσεις κατοικίας, οι αριθμοί τηλεφώνου και τα τελευταία τέσσερα ψηφία των αριθμών χρεωστικών καρτών έχουν επίσης χαθεί. Βέβαια, υποστηρίζει ότι οι κωδικοί πρόσβασης είναι ασφαλείς. Ωστόσο, συνιστά στους πελάτες να τους αλλάξουν ανεξάρτητα και τους συμβουλεύει να ενημερώνουν τις τράπεζές τους και να ζητούν να τεθούν σε επαφή οι λογαριασμοί τους για ασυνήθιστη δραστηριότητα.
- Μία σημαντική παραβίαση της βάσης δεδομένων αναβάθμισης των πελατών του Three, που αποκαλύφθηκε τον Νοέμβριο του 2016, συνέβη όταν έγινε πρόσβαση στη βάση δεδομένων της Three με χρήση της σύνδεσης ενός υπαλλήλου. Η εταιρία δήλωσε ότι παραβιάστηκαν προσωπικά δεδομένα (ονόματα, αριθμοί τηλεφώνου, διευθύνσεις και ημερομηνίες γέννησης) 210.200 πελατών όχι όμως οικονομικές τους πληροφορίες.
- Η εταιρία Sports Direct διαπίστωσε ότι τα συστήματά της είχαν διαταραχθεί τον Σεπτέμβριο του 2016, αλλά μόλις τον Δεκέμβριο ανακάλυψε την παραβίαση δεδομένων - συμπεριλαμβανομένων των ονομάτων, των διευθύνσεων ηλεκτρονικού ταχυδρομείου και των αριθμών τηλεφώνου. Ο επιτιθέμενος κατάφερε να αποκτήσει πρόσβαση μέσω ενός συστήματος διαχείρισης περιεχομένου που δεν λειτουργεί με ανοικτή πηγή (DNN Platform). Η εταιρία ενημέρωσε το Γραφείο του Επιτρόπου Πληροφόρησης αλλά απέφυγε να μοιραστεί λεπτομέρειες σχετικά με την παραβίαση με το προσωπικό - επειδή δεν υπήρχαν αποδείξεις ότι τα δεδομένα είχαν αντιγραφεί.
- Στα τέλη του 2016, η τράπεζα Tesco Bank, πάγωσε τις online συναλλαγές της αφού κλάπηκαν χρήματα από τους λογαριασμούς 20.000 πελατών. Η τράπεζα επιβεβαίωσε μόνο ότι υποβλήθηκε σε εγκληματική δραστηριότητα χωρίς να περιγράφει την επίθεση. Επίσης, δήλωσε ότι θα καλύψει οποιοδήποτε οικονομικό κόστος της παραβίασης.
- Η εταιρία λογιστικής και λογισμικού HR, Sage, έπεσε θύμα εσωτερικής επίθεσης με τα στοιχεία προσωπικού των 280 πελατών του Ηνωμένου Βασιλείου που αντιπροσωπεύουν μεγάλο αριθμό μεμονωμένων χρηστών να διατρέχουν κίνδυνο.

Πηγή: http://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

ΕΛΛΑΔΑ !!!

Πρόστιμο στη **ΓΓΠΣ** για διαρροή φορολογικών δεδομένων

- **Διαρροή προσωπικών δεδομένων** του συνόλου των Ελλήνων φορολογουμένων προς εταιρείες εμπορίας προσωπικών δεδομένων συνέβαινε **επί τουλάχιστον δώδεκα χρόνια**, λόγω ανεπάρκειας των μέτρων ασφαλείας της Γενικής Γραμματείας Πληροφοριακών Συστημάτων του υπουργείου Οικονομικών.
- Η **Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα** επέβαλε **πρόστιμο €150.000** στο υπουργείο Οικονομικών, ζητώντας παράλληλα την ισχυροποίηση των μέτρων ασφαλείας για την προστασία των φορολογουμένων. Στην Αρχή προσέφυγε εκ νέου η Γενική Γραμματεία Πληροφοριακών Συστημάτων, ζητώντας μείωση του προστίμου και πίστωση χρόνου για τη συμμόρφωση με την απόφαση, ωστόσο η προσφυγή απορρίφθηκε (απόφαση 117/2014).
- Σύμφωνα με τα όσα περιλαμβάνονται στην απόφαση της Αρχής, πλήθος απόρρητων προσωπικών δεδομένων που αφορούν το σύνολο των φορολογουμένων στην Ελλάδα, όπως είναι τα Ε1, Ε9, στοιχεία για το ΕΤΑΚ, τα τέλη κυκλοφορίας κτλ., διέρρευσαν σε εταιρείες εμπορίας δεδομένων προσωπικού χαρακτήρα. Οπως επισημαίνεται μάλιστα στην απόφαση, η διαρροή, η οποία αποδίδεται στα ελλιπή μέτρα ασφαλείας της Γ.Γ., είναι «πρωτοφανούς έκτασης, αφού αφορά στο σύνολο των φορολογουμένων στην Ελλάδα, για ιδιαίτερα μακρύ χρονικό διάστημα». **Η όλη υπόθεση αποκαλύφθηκε κατά τη διάρκεια ελέγχων της Αρχής σε εταιρείες εμπορίας προσωπικών δεδομένων, που έγιναν το 2012.** Στο πλαίσιο των ερευνών διαπιστώθηκε ότι οι εταιρείες είχαν στη διάθεσή τους αναλυτικά στοιχεία δηλώσεων φορολογίας εισοδήματος, έντυπα Ε1 και Ε9, στοιχεία για το ΕΤΑΚ και την έκτακτη εισφορά, για το ύψος των τελών κυκλοφορίας αλλά και για το ποιοι φορολογούμενοι έκαναν περαίωση το 2010.
- Ιδιαίτερα ενδιαφέρον είναι το γεγονός ότι, όπως χαρακτηριστικά αναφέρεται στην απόφαση της Αρχής, η Γενική Γραμματεία δεν αμφισβητεί τα πραγματικά δεδομένα της διαρροής προσωπικών δεδομένων φορολογουμένων αλλά και τις παραβάσεις που της αποδίδονται.

Πηγή: http://www.kathimerini.gr/788568/article/oikonomia/ellhnikh-oikonomia/prostimo-sth-ggps--gia-diarroh-forologikwn-dedomenwn

Διοικητικός έλεγχος σε μεγάλη εταιρεία Επιχειρηματικών Πληροφοριών – Επιβολή κυρώσεων

- Η Αρχή, κατόπιν σχετικού διοικητικού ελέγχου που διενήργησε στην εταιρεία , διαπίστωσε σωρεία παραβάσεων του ν. 2472/1997 και, ως εκ τούτου, επέβαλε σε αυτήν κυρώσεις **(πρόστιμα συνολικού ύψους €150.000 για παράνομη συλλογή και περαιτέρω επεξεργασία δεδομένων** από τα αρχεία της ΤΕΙΡΕΣΙΑΣ για ίδιο λογαριασμό και καθ' υπέρβαση της σύμβασης με Τράπεζα, για παράνομη συλλογή και χρήση δεδομένων που προέρχονταν από τα τηρούμενα στη ΓΓΠΣ αρχεία μητρώου φορολογουμένων, για μη λήψη των απαραίτητων μέτρων που εξασφαλίζουν την τήρηση των δεδομένων αποκλειστικά εντός του εκ του νόμου προβλεπόμενου χρονικού διαστήματος και για μη προσήκουσα ενημέρωση των υποκειμένων των δεδομένων), της απεύθυνε δε ανάλογες συστάσεις.

Πηγή: www.dpa.gr

Επιβολή κυρώσεων στην **ΤΕΙΡΕΣΙΑΣ ΑΕ**

- Η Αρχή επέβαλε **πρόστιμο €30.000** στην εταιρεία ΤΕΙΡΕΣΙΑΣ για παράλειψη λήψης μέτρων κατά τη διάθεση δεδομένων των αρχείων της σε εταιρεία Επιχειρηματικών Πληροφοριών μέσω παροχής πρόσβασης σε αυτά, καθώς και προειδοποίηση να διαφοροποιήσει εντός τριμήνου τα δικαιώματα πρόσβασης των χρηστών στα αρχεία της. Δείτε την απόφαση 64/2015.

Πηγή: www.dpa.gr

- **Πρόστιμο** στην Τειρεσίας **για διαρροή δεδομένων**
  - **«Καμπάνα» €75.000 «έπεσε» στην εταιρεία ΤΕΙΡΕΣΙΑΣ ΑΕ, επειδή χωρίς να έχει εξασφαλίσει σχετική άδεια, από τις αρχές του 2014 άρχισε να παρέχει σε επιχειρηματίες πληροφορίες που αφορούν την πιστοληπτική ικανότητα και φερεγγυότητα διαφόρων συναλλασσόμενων πολιτών.**
  - Η Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΠΔ) επιβάλλοντας το πρόστιμο, έκρινε ότι η ΤΕΙΡΕΣΙΑΣ ΑΕ διεύρυνε παράνομα τον σκοπό της επεξεργασίας των αρχείων που διαθέτει (και αφορούν αποκλειστικά την εξυπηρέτηση των τραπεζών), ενώ παράλληλα γνωστοποίησε τις ενέργειές της στην Αρχή με χρονική καθυστέρηση (τουλάχιστον 6 μηνών) χωρίς να έχει ενημερώσει τους ενδιαφερόμενους πολίτες για τη νεότερη χρήση των προσωπικών τους δεδομένων.
  - **Με άλλη απόφαση, η Αρχή επέβαλε πρόστιμο €30.000 σε τράπεζα, γιατί επί 3,5 χρόνια μετά την εξόφληση, καταναλωτής εξακολουθούσε να είναι καταχωρημένος ως «οφειλέτης - εγγυητής» δανείου και στο σύστημα ΤΕΙΡΕΣΙΑΣ.**

Πηγή: http://www.ethnos.gr/article.asp?catid=22768&subid=2&pubid=64122869

Μεγάλος Τηλεπικοινωνιακός Πάροχος: Ζητά να ακυρωθεί πρόστιμο για διαρροή προσωπικών δεδομένων

- **Προσωπικά δεδομένα παλαιών και νέων πελατών του βρέθηκαν σε εταιρία εμπορίας δεδομένων**
- **Την ακύρωση προστίμου €60.000 που του επιβλήθηκε από την Αρχή Προστασίας Προσωπικών Δεδομένων για τη διαρροή απόρρητων στοιχείων χιλιάδων πελατών του διεκδικεί με προσφυγή του στο Συμβούλιο της Επικρατείας ο Τηλεπικοινωνιακός Πάροχος.**
- Μετά από έρευνα της υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος της ΕΛ.ΑΣ βρέθηκαν σε εταιρεία εμπορίας προσωπικών δεδομένων προσωπικά δεδομένα παλαιών και νέων πελατών-συνδρομητών του Τηλεπικοινωνιακού Παρόχου της διετίας 2008-2010.
- **Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα επέβαλε στον Τ.Π πρόστιμο €60.000 επειδή αποδείχθηκαν στην πράξη ανεπαρκή τα μέτρα ασφαλείας για την προστασία των δεδομένων προσωπικού χαρακτήρα των πελατών του Τ.Π.**
- Στη συνέχεια ο Τ.Π προσέφυγε στο Συμβούλιο της Επικρατείας και ζητάει να ακυρωθεί ως παράνομη η απόφαση της Αρχής που επέβαλε το επίμαχο πρόστιμο.
- Στην αίτηση που κατέθεσε ο Τ.Π στο Συμβούλιο της Επικρατείας υποστηρίζει ότι δεν ήταν νόμιμη η συγκρότηση των μελών της Αρχής που εξέδωσαν την απόφαση με την οποία του επιβλήθηκε το πρόστιμο των €60.000 με αποτέλεσμα να είναι άκυρη.
- Ακόμη, υποστηρίζει ο Τ.Π ότι η απόφαση με την οποία του επιβλήθηκε το πρόστιμο παραβιάζει τις αρχές της αναλογικότητας και της επιείκειας, αλλά είναι και μη νόμιμη όπως είναι και εσφαλμένη.

Πηγή: http://www.tovima.gr/finance/article/?aid=690179

Οδηγός Έντυπη & Ηλεκτρονική Πληροφόρηση

- **Επιβολή προστίμου €10.000 σε υπεύθυνο επεξεργασίας που τηρεί υπηρεσία επαγγελματικού καταλόγου για παράνομη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα** και για μη ικανοποίηση των δικαιωμάτων ενημέρωσης, πρόσβασης και αντίρρησης.

Πηγή: www.dpa.gr

Επιβολή κυρώσεων σε Τράπεζα

- Η Αρχή **επέβαλε δύο πρόστιμα στην Τράπεζα συνολικού ύψους €130.000** για παράνομη διάθεση/ χορήγηση δεδομένων από τα αρχεία της ΤΕΙΡΕΣΙΑΣ στην εταιρεία Επιχειρηματικών Πληροφοριών και για παράλειψη γνωστοποίησης στην Αρχή βασικών στοιχείων της επεξεργασίας, όπως του τόπου και των εγκαταστάσεων επεξεργασίας της εταιρείας Επιχειρηματικών Πληροφοριών.

Πηγή: www.dpa.gr

Πρόστιμο €10.000 από την Αρχή Προστασίας Προσωπικών Δεδομένων

Παραβίαση προσωπικών δεδομένων σε εταιρεία παραγωγής φωνογραφημάτων, φορέων ήχου και εικόνας.

Πηγή: www.dpa.gr

Πρόστιμο 75.000€ σε Τράπεζα για παράνομη συλλογή προσωπικών δεδομένων

- **Καμπάνα 75.000 ευρώ επέβαλε η Αρχή Προστασίας Προσωπικών Δεδομένων στην Τράπεζα διότι αγόρασε, τήρησε σε αρχείο και επεξεργάστηκε, για δικούς της οικονομικούς σκοπούς, λίστες με προσωπικά δεδομένα χιλιάδων πολιτών που είχαν συγκεντρωθεί παράνομα.**
- Προκειμένου να προωθήσει προϊόντα και υπηρεσίες σε δυνητικούς υποψήφιους πελάτες της που κατά προτίμηση είχαν υψηλό εισόδημα (πάνω από 60.000 ευρώ), η Τράπεζα αγόραζε από το 2007 μέχρι και το 2011 από εταιρεία συλλογής και διαχείρισης πληροφοριών αλλά και από διαφημιστική εταιρεία λίστες με προσωπικά στοιχεία χιλιάδων πολιτών, όπως ονοματεπώνυμα, αριθμούς φορολογικού μητρώου, κωδικούς ΔΟΥ, αριθμούς δελτίων Α.Τ., εισόδημα, εισόδημα συζύγου, συνολικό εισόδημα, ταχυδρομικές διευθύνσεις, τηλέφωνα και επαγγέλματα. Είναι ενδεικτικό ότι η μεγαλύτερη λίστα περιείχε 52.864 καταχωρίσεις.
- Μάλιστα η αγορά έγινε με βάση συγκεκριμένα κριτήρια ως προς τα πρόσωπα που θα περιλαμβάνονται σε αυτές, όπως κριτήρια εισοδήματος, ύπαρξης στεγαστικού δανείου, κατοχής συγκεκριμένων μοντέλων αυτοκινήτων κ.λπ., για τα οποία όμως οι σχετικές πληροφορίες δεν μπορούν να προκύψουν από δημόσια πρόσβαση σε πηγές.
- **Πελάτες με συγκεκριμένο προφίλ**
  - Η Τράπεζα ενδιαφερόταν για άτομα συγκεκριμένου προφίλ, τα οποία θα ήταν υποψήφιοι πελάτες της για την προωθητική καμπάνια τραπεζικών υπηρεσιών της.
  - Οι ίδιοι οι υπάλληλοι της Τράπεζας επισήμαιναν σε ηλεκτρονικά μηνύματα προς την εταιρεία στην οποία θα έδιναν τα στοιχεία ότι οι πληροφορίες που ζητούσαν θα έπρεπε να αναζητηθούν από το εκκαθαριστικό της Εφορίας.
  - Η παράνομη συλλογή των στοιχείων διαπιστώθηκε ύστερα από επιτόπιο διοικητικό έλεγχο που διενεργήθηκε τον Νοέμβριο του 2012.
  - **Η Αρχή επέβαλε το πρόστιμο αφού συνυπολόγισε τη βαρύτητα της παράβασης, το πλήθος των προσώπων των οποίων τα δεδομένα υπέστησαν επεξεργασία, καθώς και το ότι ο σκοπός της Τράπεζας ήταν να αποκομίσει κέρδος.**

Πηγές: Πηγή:http://www.enet.gr/?i=news.el.article&id=392951

Read more: http://www.cyberinsurancegreece.com/peristatika-paraviasis/

Εύρημα Στατιστικής Έρευνας

- Μόνο ~7% των περιστατικών είναι κακόβουλες παραβιάσεις
- ~ 93% των περιστατικών προέρχονται από ελλιπή οργανωτικά και τεχνικά μέτρα των επιχειρήσεων –οργανισμών

Ο Νέος Ευρωπαϊκός Κανονισμός GDPR λαμβάνει υπόψη αυτή την κατάσταση

Ας ξεκινήσουμε με την Εναρμόνιση των επιχειρήσεων με τον GDPR!!

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ GDPR 2016/679

Ιωαννίδης Τάσος

Ποιον αφορά;

- Ο Γενικός Κανονισμός Προστασίας Δεδομένων (EU GDPR) **αφορά κάθε εταιρία** και οργανισμό, εφόσον διατηρεί ή επεξεργάζεται προσωπικά δεδομένα Ευρωπαίων πολιτών. Ανεξαρτήτως μεγέθους, κλάδου ή δραστηριότητας, αφορά εξίσου όλους τους οργανισμούς, από τις πιο μικρές εταιρίες έως τους πιο μεγάλους ομίλους, δημοσίου και ιδιωτικού δικαίου. Αφορά τόσο τους υπευθύνους επεξεργασίας, όσο και τους εκτελούντες την επεξεργασία δεδομένων (data controllers και data processors - εξηγείται στη συνέχεια).

Πότε τίθεται σε ισχύ;

- Ο Κανονισμός **είναι σε ισχύ** και δεν απαιτείται επιπλέον έγκριση από κυβερνήσεις κρατών. 'Εχει ήδη εγκριθεί από το Ευρωκοινοβούλιο τον Απρίλιο του 2016. Δόθηκε απλώς μια 2-ετής περίοδος προσαρμογής μέχρι τις 25 Μαΐου 2018, οπότε θα τεθούν σε πλήρη ισχύ και τα υψηλά πρόστιμα. Ο Γενικός Κανονισμός Προστασίας Δεδομένων δεν είναι ένας εντελώς καινούργιος νόμος. Αποτελεί μια ισχυρότερη και εκσυγχρονισμένη εκδοχή της Οδηγίας του 1995 (Data Protection Directive 95/46/EC), με τη διαφορά ότι τώρα ο Κανονισμός έχει **καθολική ισχύ στα κράτη μέλη**, ορίζει **αυστηρότερες απαιτήσεις** και προβλέπει **υψηλά πρόστιμα** για τους παραβάτες.

Ποια είναι τα πρόστιμα;

- Τα πρόστιμα που ορίζει ο Γενικός Κανονισμός είναι υψηλά: **4%** του ετήσιου παγκόσμιου κύκλου εργασιών του οργανισμού ή **€20 εκατομμύρια** – **όποιο είναι υψηλότερο**. Αυτό είναι το ανώτατο ύψος προστίμου που δύναται να επιβληθεί σε σοβαρές παραβιάσεις του Κανονισμού, όπως π.χ. απουσία συγκατάθεσης. Υπάρχουν και περιπτώσεις όπου προβλέπεται πρόστιμο 2% του ετήσιου παγκόσμου τζίρου, για παράδειγμα: μή τήρηση οργανωμένων αρχείων, μή γνωστοποίηση για παραβίαση ασφαλείας, έλλειψη DPO στις περιπτώσεις που επιβάλλεται, παράλειψη Εκτίμησης Αντικτύπου, κλπ.

Ποιες είναι οι κυριότερες απαιτήσεις;(1)

1. **Περιορισμός του σκοπού**: κάθε οργανισμός οφείλει να προσδιορίζει ρητά και να είναι σε θέση να τεκμηριώσει τους νόμιμους σκοπούς, για τους οποίους συλλέγει και επεξεργάζεται προσωπικά δεδομένα. Οφείλει επίσης να μην διενεργεί περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς (Άρθρο 5).
2. **Ελαχιστοποίηση των δεδομένων**: τα δεδομένα που συλλέγονται οφείλουν να είναι κατάλληλα, συναφή και απολύτως αναγκαία για τους συγκεκριμένους σκοπούς που ορίστηκαν (Άρθρο 5).
3. **Χρονική διάρκεια**: κάθε οργανισμός οφείλει να τηρεί δεδομένα μόνο για όσο χρονικό διάστημα αυτό απαιτείται, σύμφωνα με το νόμιμο σκοπό (Άρθρο 5).

Ποιες είναι οι κυριότερες απαιτήσεις;(2)

4. **Ρητή συγκατάθεση**: απαιτείται η ρητή, σαφής και συγκεκριμένη συγκατάθεση του ατόμου για την συλλογή κι επεξεργασία των προσωπικών του δεδομένων. Για προσωπικά δεδομένα ανηλίκων κάτω των 16 ετών, απαιτείται σαφής συγκατάθεση γονέα ή κηδεμόνα. Ο οργανισμός οφείλει να τηρεί αρχείο και να επιτρέπει στο άτομο να διαφοροποιήσει τη συγκατάθεση που έδωσε για μια συγκεκριμένη χρήση, όσες φορές αλλάξει γνώμη (Άρθρα 6,7,8).
5. **Σαφής Πολιτική Απορρήτου**: οι οργανισμοί απαιτούνται να δηλώνουν με διαφάνεια, σαφή γλώσσα και κατανοητό τρόπο την πολιτική απορρήτου που εφαρμόζουν. Δηλαδή, να δηλώνουν αναλυτικά ποια δεδομένα συλλέγουν, για ποιο νόμιμο σκοπό, πώς τα διαχειρίζονται, για πόσο χρονικό διάστημα τα διατηρούν, με ποιες μεθόδους ασφαλείας τα προστατεύουν κλπ. (Άρθρο 12).

Ποιες είναι οι κυριότερες απαιτήσεις;(3)

6. **Πλήθος Ατομικά δικαιώματα**: όλα τα άτομα έχουν δικαίωμα να επεμβαίνουν στα δεδομένα τους προκειμένου να τα διορθώσουν (**Δικαίωμα Διόρθωσης**), να ζητήσουν την παραλαβή των δεδομένων τους σε δομημένο, συμβατό και διαλειτουργικό μορφότυπο, προκειμένου να τα διαβιβάσουν σε άλλον υπεύθυνο επεξεργασίας (**Δικαίωμα στη Φορητότητα**), ακόμη και τη διαγραφή των προσωπικών τους δεδομένων (**Δικαίωμα στη Λήθη**) υπό προϋποθέσεις (Άρθρα 13 ως 23).
7. **Ευθύνη και Λογοδοσία**: οι οργανισμοί είναι διαρκώς υπόλογοι στα άτομα και στις Αρχές. Οφείλουν, όχι απλώς να εφαρμόζουν το νέο Κανονισμό, αλλά και να είναι κάθε στιγμή σε θέση να αποδείξουν ότι συμμορφώνονται με όλες τις απαιτήσεις του (Άρθρο 24).

Ποιες είναι οι κυριότερες απαιτήσεις;(4)

8. **Προστασία ήδη από τον αρχικό σχεδιασμό και εξ' ορισμού**: ο οργανισμός οφείλει να εφαρμόζει αποτελεσματικά, τα κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, η ελαχιστοποίηση των δεδομένων και η ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία τους, κατά τρόπο ώστε να προστατεύονται τα δικαιώματα του ατόμου *(Άρθρο 25).*

- **Για παράδειγμα:** στις υπηρεσίες του οργανισμού, πρέπει να υπάρχουν ενσωματωμένες ρυθμίσεις ασφαλείας δεδομένων, κατανοητές και φιλικές προς το χρήστη, είτε πρόκεται για Υπάλληλο ή Πελάτη, είτε για εξωτερικό Συνεργάτη ή Προμηθευτή. Επίσης, πρέπει να είναι εξ' ορισμού (by default) ενεργοποιημένες οι ρυθμίσεις στην ύψιστη προστασία απορρήτου και πάντα σύμφωνα με τις αρχές της ελαχιστοποίησης και του περιορισμού του σκοπού. **Για παράδειγμα:** στις "φόρμες επικοινωνίας" που υπάρχουν συνήθως στον ιστότοπο ενός οργανισμού, να συλλέγονται αυστηρά και μόνο τα δεδομένα που είναι απαραίτητα για τον νόμιμο σκοπό της επικοινωνίας και όχι περισσότερα.

Ποιες είναι οι κυριότερες απαιτήσεις;(5)

9. **Ασφάλεια Επεξεργασίας**: ο οργανισμός που τηρεί και διαχειρίζεται προσωπικά δεδομένα οφείλει να εφαρμόζει τα απαραίτητα συστήματα, πολιτικές και διαδικασίες που εξασφαλίζουν τα απαιτούμενα επίπεδα προστασίας των δεδομένων αυτών, συμπεριλαμβανομένης της προστασίας από την παράνομη πρόσβαση κι επεξεργασία, τόσο από το προσωπικό του οργανισμού, όσο και από τρίτους, την κατά λάθος απώλεια, καταστροφή ή αλλοίωσή τους. Οφείλει επίσης να διασφαλίζει ότι τα δεδομένα που τηρεί είναι ορθά και επίκαιρα (Άρθρο 32).

Ποιες είναι οι κυριότερες απαιτήσεις;(6)

10. **Γνωστοποίηση παραβίασης εντός 72 ωρών**: Σε περίπτωση παραβίασης ασφαλείας που αφορά προσωπικά δεδομένα, οι οργανισμοί οφείλουν να ενημερώνουν εντός 72 ωρών – από τη στιγμή που αποκτούν γνώση του γεγονότος – τις αρμόδιες Αρχές καθώς και τα άτομα των οποίων τα προσωπικά δεδομένα έχουν τεθεί σε κίνδυνο. Οφείλουν επίσης να τηρούν αρχείο με όλα τα περιστατικά παραβίασης ασφαλείας προσωπικών δεδομένων (Άρθρα 33, 34).
11. **Εκτίμηση αντικτύπου**: οι οργανισμοί οφείλουν να διεξάγουν μελέτες εκτίμησης αντικτύπου, με σκοπό την εκτίμηση και καταγραφή των επιπτώσεων της επεξεργασίας προσωπικών δεδομένων, τον εντοπισμό των κινδύνων ασφάλειας και τον σχεδιασμό της αντιμετώπισης αυτών (Άρθρα 35, 36).

Ποιες είναι οι κυριότερες απαιτήσεις;(7)

12. **Υπεύθυνος Προστασίας Δεδομένων** (Data Protection Officer, εν συντομία DPO): οι οργανισμοί οφείλουν υπό προϋποθέσεις να ορίσουν έναν Υπεύθυνο Προστασίας Δεδομένων. Ο ρόλος του είναι να παρακολουθεί τη διαρκή και επαρκή συμμόρφωση του οργανισμού με τον νόμο, ενώ παράλληλα αποτελεί τον σύνδεσμο του οργανισμού με την αρμόδια εποπτική Αρχή. Η υποχρέωση για διορισμό DPO εξαρτάται από διάφορους παράγοντες, κυρίως όμως από το ύψος του κινδύνου που «απειλεί» τα προσωπικά δεδομένα.

- **Για παράδειγμα**, μια πολύ μικρή εταιρία, έστω 3 ατόμων, που επεξεργάζεται ευαίσθητα προσωπικά δεδομένα, όπως ιατρικούς φακέλους ασθενών, οφείλει να ορίσει DPO, εξαιτίας του μεγέθους του κινδύνου που διατρέχουν τα άτομα, αν π.χ. διαρρεύσουν ή αλλοιωθούν τα δεδομένα που τηρεί. Δεν είναι απαραίτητο να γίνει πρόσληψη. Δύναται να ορισθεί εξωτερικός Συνεργάτης (Άρθρα 37, 38, 39).

Ποιες είναι οι κυριότερες απαιτήσεις;(8)

13. **Εκπαίδευση προσωπικού**: οι οργανισμοί οφείλουν να εκπαιδεύσουν το προσωπικό τους στο πως να εφαρμόζει καθημερινά την πολιτική προστασίας προσωπικών δεδομένων.

Προκλήσεις για την εφαρμογή του GDPR

- Διεύρυνση του ορισμού των προσωπικών δεδομένων
- Νέα δικαιώματα για τα υποκείμενα των δεδομένων
- Διεύρυνση των αρμοδιοτήτων των Υπευθύνων και των Εκτελούντων την επεξεργασία
- Υποχρέωση γνωστοποιήσεων της Αρχής και των Υποκειμένων Δεδομένων για παραβιάσεις των δεδομένων
- Διεύρυνση των δικαιωμάτων των Αρχών Προσωπικών Δεδομένων
- Επιβολή υψηλών προστίμων για μη Συμμόρφωση
- Ορισμός DPO
- Μελέτες εκτίμησης Αντικτύπου Ιδιωτικότητας (DPIA)
- Διαβίβαση Δεδομένων

www.motive.com.gr

Πλάνο εναρμόνισης των επιχειρήσεων-οργανισμών με τον GDPR

02/11/2017

Ιωαννίδης Τάσος, Motive Συμβουλευτική

12 Περιοχές προς διερεύνηση

- Επίγνωση
  Awareness
- Δεδομένα που κατέχετε
  Data you hold
- Επικοινωνία
  Communication
- Ανθρώπινα δικαιώματα
  Individual rights
- Subject access requests
  Αίτημα του υποκειμένου για πρόσβαση
- Legal Basis for processing
  Νομικό πλαίσιο για επεξεργασία
- Consent
  Συγκατάθεση
- Children
  Παιδιά
- Data Breach
  Παραβίαση προστασίας Δεδομένων
- Protection by design
  Προστασία By Design & Default
- Data Protection Officer
  Υπεύθυνος Προστασίας Δεδομένων
- International
  Διεθνής δραστηριότητα

Awareness-Επίγνωση

- Ο GDPR όπως και άλλα frameworks εφαρμόζεται οργανωτικά μόνο εκ των άνω (Διοίκηση) προς τα κάτω (Προσωπικό). Ξεκινήστε από το ΔΣ και τα στελέχη
- Χρειάζεστε την υποστήριξή τους (time, money, resources)
- Τα ανώτερα διοικητικά στελέχη πρέπει να είναι ενήμεροι για τις επιπτώσεις του GDPR και τι σημαίνει για αυτούς
- Τα ανώτερα διοικητικά στελέχη πρέπει να είναι σύμφωνα ως εμπλεκόμενα άτομα, αφού τελικά αυτά έχουν την ευθύνη
- Τότε ο υπόλοιπος οργανισμός πρέπει να ενημερωθεί

Data που κατέχετε

- Θα ακούσετε πολλές πληροφορίες για τη χρήση της τεχνολογίας ώστε να βρείτε τα προσωπικά δεδομένα που κατέχετε, και αυτό είναι σημαντικό αφού πρέπει να δεσμευτείτε για έναν έλεγχο data (data audit)
  - Περιλαμβάνει τα ψηφιακά data και το hardcopy
  - Επίσης περιλαμβάνει ψευδο-ανωνυμοποιημένα δεδομένα ανάλογα τη χρήση
- Ποιες είναι οι διαδικασίες της επιχείρησης που υποστηρίζουν το τρόπο με το οποίο αποκτήσατε τα δεδομένα;
- Πως τα επεξεργάζεστε;

Data που κατέχετε (2)

- Με ποιους τα μοιράζεστε και τι κάνουν αυτοί, με αυτά;
  - Μπορείτε να αναθέσετε σε εξωτερικό συνεργάτη την αρμοδιότητα αλλά όχι την ευθύνη (δηλαδή υποχρέωση)
  - Αν είστε ο controller είστε ακόμα υπεύθυνος!

Επικοινωνία

Ποιες πληροφορίες πρέπει να συλλέξετε;	Πληροφορίες αποκτούμενες απευθείας από το υποκείμενο των δεδομένων	Πληροφορίες μη αποκτούμενες απευθείας από το υποκείμενο των δεδομένων
Ταυτότητα και πληροφορίες επικοινωνίας του ελεγκτή ή εκπροσώπου	✓	✓
Σκοπός της επεξεργασίας και το νομικό υπόβαθρό της	✓	✓
Τα νομικά ενδιαφέροντα του ελεγκτή/τρίτων	✓	✓
Κατηγορίες των προσωπικών δεδομένων		✓
Κάθε παραλήπτη ή κατηγορίες παραληπτών των προσωπικών δεδομένων	✓	✓
Λεπτομέρειες για τη μεταφορά τους σε Τρίτη χώρα και μέτρα προστασίας	✓	✓

Επικοινωνία (2)

Ποιες πληροφορίες πρέπει να συλλέξετε;	Πληροφορίες αποκτούμενες απευθείας από το υποκείμενο των δεδομένων	Πληροφορίες μη αποκτούμενες απευθείας από το υποκείμενο των δεδομένων
Περίοδος διατήρησης ή κριτήρια που καθορίζουν την περίοδο διατήρησης	✓	✓
Η ύπαρξη των δικαιωμάτων των υποκειμένων των πληροφοριών	✓	✓
Το δικαίωμα της αναίρεσης της συγκατάθεσης οποιαδήποτε στιγμή	✓	✓
Το δικαίωμα να υποβληθεί παράπονο σε μια διαχειριστική αρχή	✓	✓
Η πηγή των προσωπικών δεδομένων και αν αποκτήθηκαν από δημοσίως προσβάσιμες πηγές		✓

Επικοινωνία (3)

Ποιες πληροφορίες πρέπει να συλλέξετε;	**Πληροφορίες αποκτούμενες απευθείας από το υποκείμενο των δεδομένων**	**Πληροφορίες μη αποκτούμενες απευθείας από το υποκείμενο των δεδομένων**
Εάν η προμήθεια των προσωπικών δεδομένων είναι μέρος θεσμικής ή συμβατικής απαίτησης		
Η ύπαρξη αυτόματης συγκατάθεσης		
Πότε πρέπει να παρέχονται οι πληροφορίες;	Όλη την ώρα	Μέσα σε ένα μήνα ή την ώρα της επικοινωνίας

Τα δικαιώματα των Υποκειμένων

1. Το δικαίωμα να ενημερώνεται (όπως αναφέρθηκε και σε προηγούμενη διαφάνεια)
2. Πρόσβαση στα δεδομένα (θα εξηγηθεί σε επόμενη διαφάνεια)
3. Διόρθωση των δεδομένων
4. Διαγραφή των δεδομένων
5. Περιορισμό ή άρνηση της επεξεργασίας
6. Φορητότητα των δεδομένων
7. Ένσταση
8. Δικαιώματα σχετικά με την αυτοματοποιημένη απόφαση και σκιαγράφηση προφίλ

Αίτηση υποκειμένου για πρόσβαση Subject access requests (SAR's)

- Στις περισσότερες περιπτώσεις δεν θα μπορείτε να χρεώσετε για SAR's
  - Μπορείτε να χρεώσετε ένα λογικό πρόστιμο (για να καλύψετε διοικητικά κόστη) όταν μια αίτηση είναι αβάσιμη ή πλεονάζουσα (ειδικά εάν είναι επαναλαμβανόμενη)
- Θα έχετε μόνο ένα μήνα για να ανταποκριθείτε και όχι 40 μέρες
  - Μπορείτε να επεκτείνετε αυτή τη περίοδο για άλλους 2 μήνες όταν οι αιτήσεις είναι περίπλοκες και πολλές
  - Αλλά πρέπει να ενημερώσετε το υποκείμενο μέσα σε ένα μήνα από την αίτηση
- Μπορείτε να αρνηθείτε ένα αίτημα αλλά πρέπει να εξηγήσετε τους λόγους και το υποκείμενο έχει το δικαίωμα να παραπονεθεί

Αίτηση υποκειμένου για πρόσβαση Subject access requests (SAR's) (2)

- Πρέπει να αναγνωρίζετε το υποκείμενο που κάνει την αίτηση χρησιμοποιώντας λογικά μέσα
- Αν η αίτηση είναι ηλεκτρονική θα πρέπει να απαντήσετε σε μια κοινή φόρμα
- Η καλύτερη τακτική λέει ότι θα πρέπει να παρέχετε ασφαλή, άμεση, self service πρόσβαση στα δεδομένα ενός υποκειμένου

Νομικό πλαίσιο για την επεξεργασία

- 6(1)(a)- το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,
- 6(1)(b)- η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,
- 6(1)(c)- η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,
- 6(1)(d)- η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

Νομικό πλαίσιο για επεξεργασία (2)

- 6(1)(e)- η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,
- 6(1)(f)- η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Συγκατάθεση

- Η συγκατάθεση κάτω από το GDPR απαιτεί μια μορφή ξεκάθαρης καταφατικής ενέργειας. Η σιωπή, τα ήδη συμπληρωμένα κουτάκια ή η αδράνεια δεν συνιστούν συγκατάθεση
- Η συγκατάθεση πρέπει να είναι επαληθεύσιμη. Αυτό σημαίνει ότι πρέπει να κρατείται κάποιου είδους καταχώρηση του πως και πότε δόθηκε η συγκατάθεση και τα άτομα έχουν το δικαίωμα να αναιρέσουν την συγκατάθεση οποιαδήποτε στιγμή
- Όταν ήδη βασίζεστε στη συγκατάθεση που αναζητούνταν υπό τον DPA ή τον Γενικό Κανονισμό για την προστασία των προσωπικών δεδομένων (95/46/ΕΚ), δεν θα απαιτείται να παίρνετε καινούρια συγκατάθεση από τα άτομα αν οι προδιαγραφές αυτής της συγκατάθεσης συμφωνούν με τις νέες απαιτήσεις

Παιδιά

- Όπου προσφέρονται υπηρεσίες απευθείας σε παιδιά, πρέπει να εξασφαλίζετε ότι οι όροι απορρήτου είναι γραμμένοι με ξεκάθαρο, απλό τρόπο που ένα παιδί θα καταλάβει
- Αν προσφέρετε “social media υπηρεσία” (ζητάτε αμοιβή, άμεσο μάρκετινγκ ή μπορεί να δημιουργηθεί online προφίλ) απευθείας σε παιδιά, θα πρέπει να πάρετε συγκατάθεση από έναν γονέα ή κηδεμόνα για να επεξεργαστείτε τα δεδομένα του παιδιού
- Παιδιά θεωρούνται 16 ετών και κάτω (η UK έχει υποδείξει αυτό να μετατραπεί σε 14 για να συμβαδίζει με την USA νομοθεσία)

Παραβίαση-διαρροή Δεδομένων

- Παραβίαση δεδομένων σημαίνει μια παραβίαση της ασφάλειας, οδηγώντας στην καταστροφή, απώλεια, αλλαγή, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε προσωπικά δεδομένα. Αυτό σημαίνει ότι μια παραβίαση είναι περισσότερο από μια απλή απώλεια δεδομένων
- Για παράδειγμα, θα πρέπει να ειδοποιήσετε τη σχετική υπεύθυνη αρχή για την απώλεια των δεδομένων του πελάτη όπου η παραβίαση αφήνει το άτομο εκτεθειμένο στην κλοπή της ταυτότητάς του. Από την άλλη, η απώλεια ή ακατάλληλη αλλαγή μιας τηλεφωνικής λίστας προσωπικού, για παράδειγμα, δεν θα ενέπιπτε στη ίδια περίπτωση.

Παραβίαση-διαρροή Δεδομένων (2)

- Επίσης, πρέπει να ειδοποιήσετε το άτομο όπου μια παραβίαση είναι πιθανό να οδηγήσει σε υψηλό ρίσκο των δικαιωμάτων και ελευθεριών του ατόμου. Πρέπει να ειδοποιήσετε τους ενδιαφερόμενους αμέσως
- Μια υποχρεωτική δήλωση παραβίασης πρέπει να δηλωθεί στη σχετική αρμόδια αρχή, μέσα σε 72 ώρες από τη στιγμή που ο οργανισμός αποκτήσει επίγνωση της παραβίασης, και μπορείτε να προσφέρετε πληροφορίες μόλις γίνουν διαθέσιμες
- Αν η παραβίαση είναι αρκετά σοβαρή για να δικαιολογήσει γνωστοποίηση στο κοινό, ο κάθε υπεύθυνος οργανισμός πρέπει να το κάνει, χωρίς αδικαιολόγητη καθυστέρηση

Προστασία By Design & Default

- Έχετε μια υποχρέωση να εφαρμόσετε τεχνικά και οργανωτικά μέτρα για να δείξετε ότι λάβατε υπόψη και ενσωματώσατε προστασία δεδομένων κατά τον σχεδιασμό (προϊόντος-υπηρεσίας)
- DPIA (Data Protection Impact Assessment) θα πρέπει να χρησιμοποιηθούν κατά το ελάχιστο για:
  - Χρήση νέων τεχνολογιών
  - Επεξεργασία που είναι πιθανόν να οδηγήσει σε υψηλό ρίσκο των δικαιωμάτων και ελευθεριών των ατόμων

Προστασία By Design & Default (2)

- DPIA θα πρέπει να χρησιμοποιήσετε σε όλες τις περιπτώσεις για να διαβεβαιώσετε εάν επηρεάζονται πληροφορίες απορρήτου
- Να ενσωματώσετε review και risk assessment διαδικασίες σε project management solutions . Ειδικά, αφού ο GDPR προωθεί τη διακυβέρνηση και υπευθυνότητα στις επιχειρήσεις

Υπεύθυνος προστασίας δεδομένων (DPO)

- Πρέπει να ορίσετε έναν υπεύθυνο προστασίας δεδομένων (DPO) εάν είστε δημόσια αρχή, εκτελείτε μεγάλης κλίμακας συστημική παρακολούθηση ή έχετε επεξεργασία ειδικών κατηγοριών δεδομένων ή σχετικά με εγκληματικές καταδίκες/αδικήματα
- ΣΗΜΕΙΩΣΗ: Ανεξαρτήτως εάν ο GDPR σας υποχρεώνει να διορίσετε έναν DPO, πρέπει να εξασφαλίσετε ότι ο οργανισμός σας έχει επαρκές προσωπικό και δεξιότητες για να εκπληρώσει τις υποχρεώσεις του υπό τον GDPR

Υπεύθυνος προστασίας δεδομένων (DPO) (2)

Αρμοδιότητες του DPO:

- Να ενημερώνει και να συμβουλεύει τους οργανισμούς και τους υπαλλήλους τους για τις υποχρεώσεις τους για συμμόρφωση
- Να επιτηρεί τη συμμόρφωση με τον GDPR συμπεριλαμβανομένου τη διαχείριση εσωτερικών διαδικασιών για τη προστασία των δεδομένων, να συμβουλεύει στις DPIA, να εκπαιδεύει προσωπικό και να εκτελεί εσωτερικούς ελέγχους
- Να είναι το σημείο επικοινωνίας της επιχείρησης-οργανισμού με τις αρμόδιες αρχές και των υποκειμένων των οποίων τα δεδομένα τίθενται σε επεξεργασία

Υπεύθυνος προστασίας δεδομένων (DPO) (3)

Υποχρεώσεις εργοδότη:

- Ο DPO αναφέρεται στο ανώτατο διοικητικό επίπεδο του οργανισμού σας-δηλαδή επίπεδο ΔΣ ή Γενικής Διεύθυνσης
- Ο DPO λειτουργεί αυτόνομα και δεν απολύεται ή τιμωρείται για την εκτέλεση των εργασιών του
- Επαρκείς πηγές δίνονται για να επιτραπεί στους DPOs να ικανοποιήσουν τις GDPR υποχρεώσεις τους

Διεθνής δραστηριότητα

- Αν λειτουργείτε διεθνώς τότε σε ποια αρμόδια αρχή εμπίπτετε;
- Η υπεύθυνη αρμόδια αρχή ορίζεται σύμφωνα με το μέρος που ο οργανισμός σας έχει τη κεντρική του διοίκηση ή το μέρος που λαμβάνονται αποφάσεις για επεξεργασία δεδομένων
- Αν είστε αβέβαιοι για το ποια αρμόδια αρχή είναι υπεύθυνη για τον οργανισμό σας, ορίστε το μέρος που ο οργανισμός παίρνει τις πιο σημαντικές αποφάσεις σχετικά με την επεξεργασία δεδομένων

Λίστα ενεργειών

Business συμβουλές:

- GAP Analysis για τις αποκλίσεις από τον GDPR
- Compliance Action Plan για τον σχεδιασμό λήψης απαραίτητων μέτρων
- Data Protection Impact Assessment ώστε να αξιολογηθούν οι επιπτώσεις από τους σημαντικότερους κινδύνους σχετικών με την προστασία δεδομένων
- Εφαρμόστε ένα διαχειριστικό πλαίσιο και συμμορφωθείτε με το ISO27001 ή άλλο κατάλληλο Privacy Seal (best practice)
- Πιστοποιηθείτε με το ISO27001 ή άλλο κατάλληλο Privacy Seal με το οποίο αποδεικνύεται η συμμόρφωσή σας με το πλαίσιο
- Χαρτογραφήστε επιχειρησιακές διαδικασίες σχετικές με την προστασία των δεδομένων (να γνωρίζετε ποια είναι, που βρίσκονται, για ποιο σκοπό και πως επεξεργάζονται τα δεδομένα)

Λίστα ενεργειών (2)

- Δημιουργήστε αρχείο δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων
- Επικοινωνήστε ξεκάθαρα με τα άτομα και δημιουργήστε αξία για να συλλέξετε τα δεδομένα τους
- Αναπτύξτε και χρησιμοποιείστε αποδεκτούς κώδικες δεοντολογίας
- Τροποποιήστε το οργανόγραμμα της επιχείρησης κατάλληλα ώστε να παρέχετε εταιρική διακυβέρνηση για την DPIA
- Έλεγχος και παρακολούθηση τρίτων που εμπλέκονται στις διαδικασίες επεξεργασίας
- Λάβετε επαρκείς και εξειδικευμένες νομικές συμβουλές
- Να οριστεί και να εκπαιδευτεί κατάλληλα ο DPO της εταιρείας

Λίστα ενεργειών (3)

IT συμβουλές:

- Προσαρμόστε το ISMS (Information Security Management System) κατά ISO27001 ή άλλο κατάλληλο Privacy Seal με τις απαιτήσεις του GDPR για την προστασία δεδομένων
- Προϋπολογισμός, υποστήριξη και πηγές από τη διοίκηση της επιχείρησης απαιτούνται για να εξασφαλιστεί ότι δεν θα εκτεθείτε σε κίνδυνο
- Δημιουργήστε ένα βασικό επίπεδο ασφάλειας πληροφοριών (asset information, configuration management, patching, anti-virus, encryption e.t.c)

Λίστα ενεργειών (4)

- Αναζητείστε δεδομένα, διαγράψτε ότι δεν είναι απαραίτητο, κάντε μη αναγνωρίσιμο ότι μπορείτε και περιορίστε την πρόσβαση στα υπόλοιπα δεδομένα
- Βεβαιωθείτε ότι η IT ευθυγραμμίζεται με την Business στρατηγική
- Σχεδιάστε και υλοποιήστε 3rd party technical audits and data controls
- Αναπτύξτε όπου απαιτείται από τον GDPR διαδικασίες αντιμετώπισης data breaches

start now!

Ας ξεκινήσουμε!!!!!

Ερωτήσεις;;

ΕΥΧΑΡΙΣΤΩ ΠΟΛΥ
ΓΙΑ ΤΗΝ ΠΡΟΣΟΧΗ ΣΑΣ!

Ιωαννίδης Αναστάσιος

MSc in Quality Management

Γενικός διευθυντής

ioannidis@motive.com.gr

6972 50 34 13

ioannidis.tasos