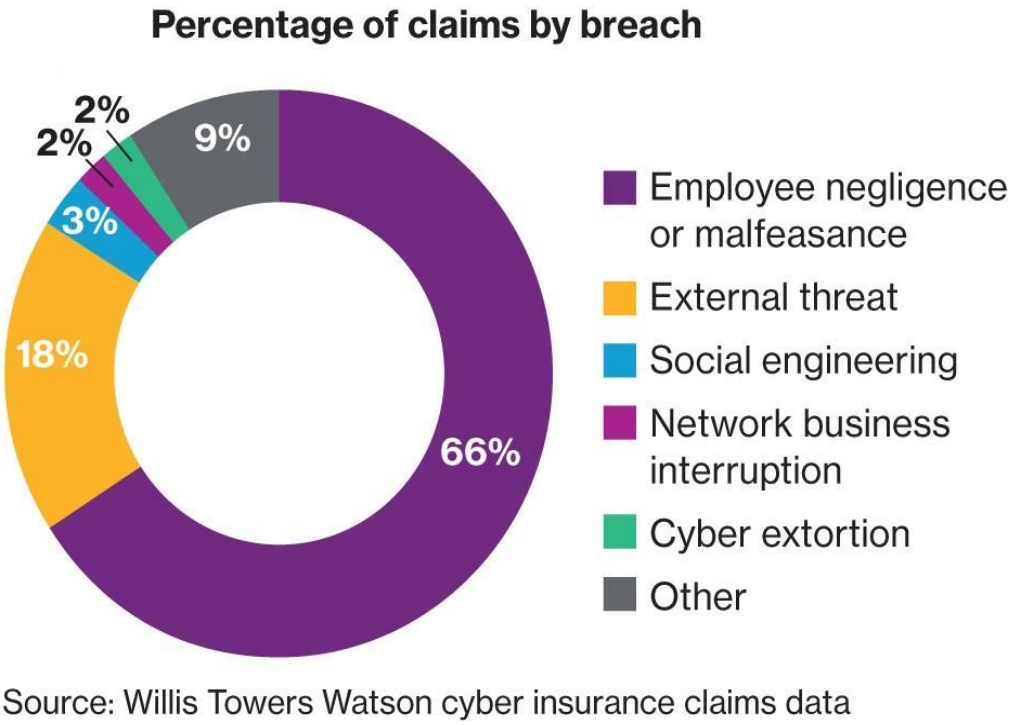


Source: Willis Towers Watson cyber insurance claims data

WiseData

Αύγουστος 2017

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (GENERAL DATA PROTECTION REGULATION – GDPR)

Εισαγωγή.

Ο Γενικός Κανονισμός Προσωπικών Δεδομένων (General Data Protection Regulation – GDPR), αλλάζει την προσέγγιση στον χώρο της Προστασίας των Προσωπικών Δεδομένων, φέρνοντας τα δικαιώματα του φυσικού προσώπου στο επίκεντρο και δίνοντας ευρύτερα δικαιώματα πληροφοριακού αυτοκαθορισμού και ελέγχου των δεδομένων τους στα φυσικά πρόσωπα. Επιβάλλονται πρόσθετες υποχρεώσεις σε Υπεύθυνους Επεξεργασίας (Data Controllers) και Εκτελούντες την Επεξεργασία (Data Processors) ώστε να εξασφαλίζεται, πέρα από τη συναίνεση, η προστασία των προσωπικών δεδομένων στο μέγιστο βαθμό. Επιπλέον εισάγεται και ο θεσμικός ρόλος του Υπεύθυνου Προστασίας Δεδομένων (Data Protection Officer - DPO).

Γιατί ο Κανονισμός είναι Σημαντικός:

Ευρεία εφαρμογή του ορισμού των προσωπικών δεδομένων. Εφόσον υπάρχει ταυτοποίηση φυσικού προσώπου, όλα τα στοιχεία πρέπει να προστατεύονται.

Ευρεία γεωγραφική κάλυψη. Όλα τα φυσικά πρόσωπα που διαμένουν στην Ε.Ε. περιλαμβάνονται. Όλες οι εταιρίες που έχουν δραστηριότητα στην Ε.Ε. επηρεάζονται. Όλες οι επιχειρήσεις (ανεξαρτήτως της εγκατάστασής τους) που επεξεργάζονται δεδομένα ευρωπαίων πολιτών επηρεάζονται.

Νέα ισχυρά δικαιώματα των φυσικών προσώπων. Δικαίωμα στη λήθη, δικαίωμα στη φορητότητα δεδομένων, δικαίωμα εναντίωσης στην αυτοματοποιημένη επεξεργασία.

Συγκατάθεση. Δηλωμένη και ξεκάθαρη συγκατάθεση των υποκειμένων των δεδομένων σχετικά με την επεξεργασία των προσωπικών τους δεδομένων (ποιος, γιατί, ως πότε).

Data Protection by default & by design. Θέματα προστασίας προσωπικών δεδομένων θα πρέπει να λαμβάνονται υπόψη από τις πρώτες φάσεις σχεδιασμού προϊόντων & υπηρεσιών.

Υποχρέωση Ανακοίνωσης Παραβιάσεων σε συγκεκριμένο χρόνο. Τόσο στις εποπτικές αρχές, όσο και στα φυσικά πρόσωπα σε περίπτωση περιστατικών παραβίασης δεδομένων.

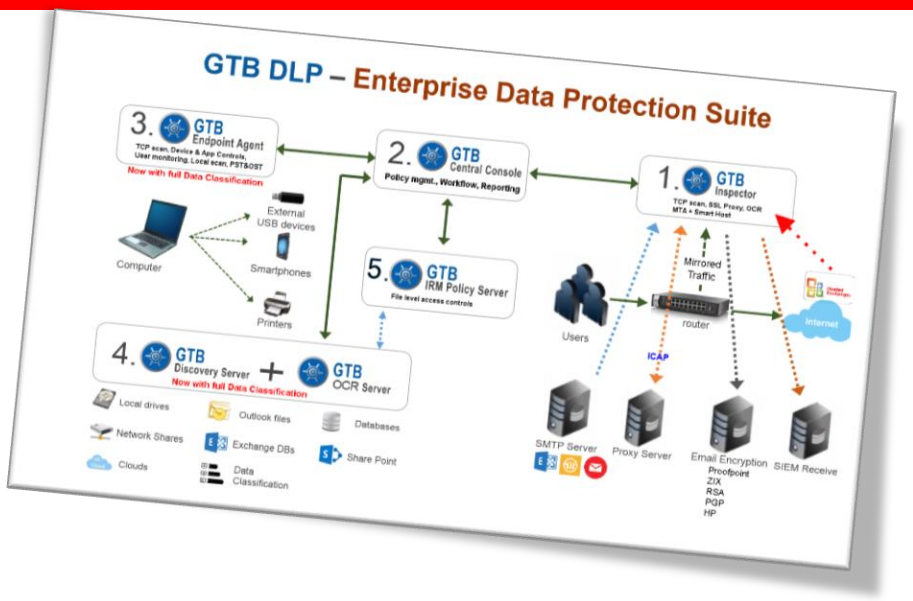
Λογοδοσία. Κάθε επιχείρηση που συλλέγει και επεξεργάζεται δεδομένα οφείλει να είναι σε θέση να αποδείξει ότι τελεί σε συμμόρφωση προς τον GDPR και ότι έχουν ληφθεί όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα που μπορούν να αποτρέψουν την παραβίαση δεδομένων.

Η Αρχή το Ήμισυ του Παντός.

Για την πραγματοποίηση ενός πολυσύνθετου έργου συμμόρφωσης προσωπικών δεδομένων που εμπεριέχει τροποποιήσεις σε οργανωτικά και τεχνικά θέματα, απαιτείται πριν την έναρξη των εργασιών ο σωστός σχεδιασμός του έργου.

Ο σκοπός του πλάνου (project plan) είναι να προσδιορίσει επακριβώς το αντικείμενο του κανονισμού EU GDPR που εφάπτεται στις δραστηριότητες της εταιρείας, τον τρόπο και τη μέθοδο που

θα χρησιμοποιηθεί για να επιτευχθεί η υλοποίησή του. Επιπλέον, προσδιορίζει τα έγγραφα / έντυπα πολιτικών και οδηγιών που πρέπει να δημιουργηθούν, τα χρονικά ορόσημα του έργου, τους ρόλους και τις αρμοδιότητες κατά την διάρκεια του έργου.

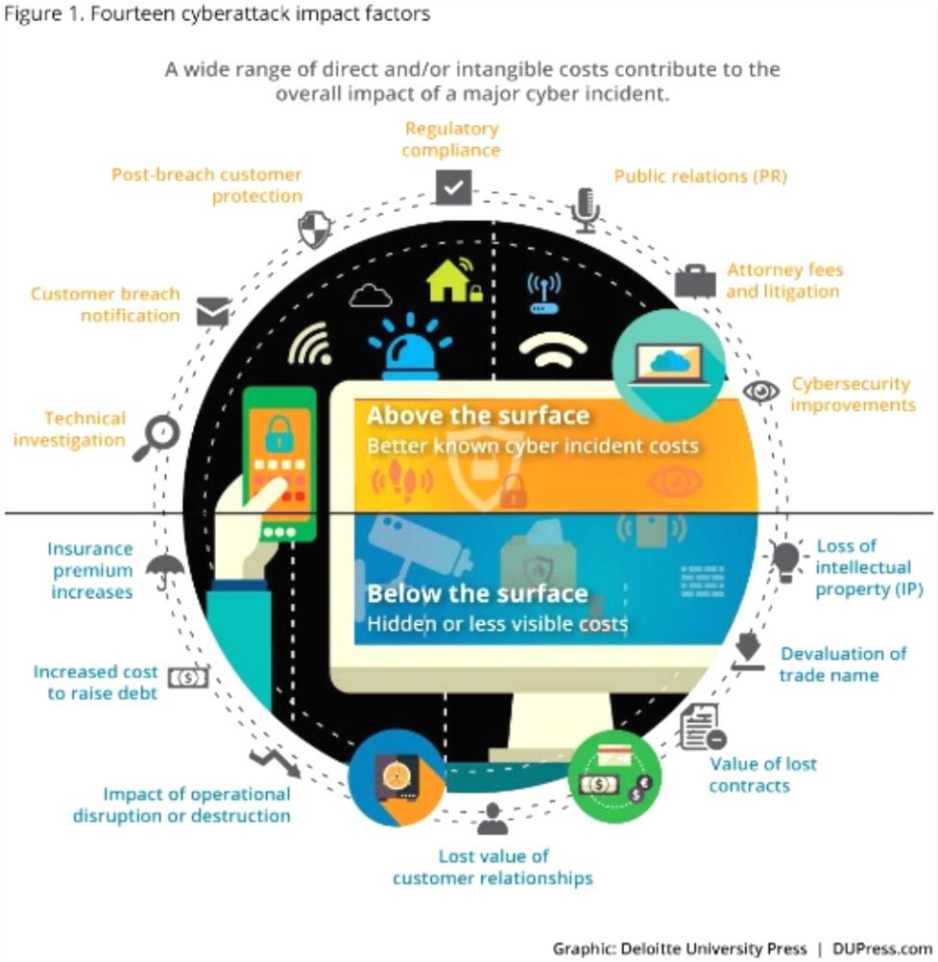


Εταιρική Δέσμευση.

Το πλάνο (project plan) απευθύνεται πρωταρχικά στην διοίκηση της εταιρείας (διοικητικό συμβούλιο) και αποτελεί το εργαλείο για όλη την ομάδα διοίκησης του έργου. Το πλάνο εφαρμόζεται σε όλες τις δραστηριότητες που πραγματοποιούνται στην πορεία του έργου.

Η διοίκηση του έργου και ο τρόπος που θα φέρει η ομάδα εργασίας το τελικό αποτέλεσμα είναι το πρώτο μέλημα της εταιρείας μας. Κατά τον σχεδιασμό (planning) του έργου θα περιγραφεί και θα συμφωνηθεί αμοιβαία το αντικείμενο του έργου. Το αντικείμενο (scope) περιγράφει επακριβώς τα παραδοτέα, τα οποία θα πρέπει να είναι τα κατάλληλα, σύμφωνα με τη φύση και την δραστηριότητα της εταιρείας σας. Θα είναι δε επαρκή και θα καλύπτουν όλο το εύρος των ερμηνειών και τις πτυχές του νέου κανονισμού ΕΕ679/2016. Το αντικείμενο έργου περιλαμβάνει και άλλες παραμέτρους για την επιτυχή ολοκλήρωση της συμμόρφωσης, όπως το δεδομένο περιβάλλον και κουλτούρα της εταιρείας στην πραγματοποίηση έργων ανάλογου μεγέθους. Άλλοι παράμετροι που πρέπει να ακολουθήσει η διοίκηση του έργου είναι η ροή εργασίας των υπαλλήλων κατά την διάρκεια του έργου, ο ιδιαίτερος τρόπος διοίκησης των έργων που η εταιρεία διατηρεί και άλλους περιβαλλοντικούς επιχειρηματικούς παράγοντες.

Figure 1. Fourteen cyberattack impact factors



Επικοινωνία & εμπλεκόμενοι φορείς.

Το αντικείμενο της επικοινωνίας και η διαχείριση της είναι μεγάλης σημασίας για την επιτυχή και απρόσκοπτη ολοκλήρωση του έργου αφού ενθαρρύνει και ενισχύει την συνεργασία μεταξύ των υπαλλήλων.

Απογραφής Δεδομένων και Δραστηριοτήτων Επεξεργασίας.

Η WiseData ακολουθεί μέθοδο με οδηγίες, συστάσεις και επίβλεψη για να δημιουργηθεί αρχείο όλων των ‘’δραστηριοτήτων επεξεργασίας’’ της εταιρείας σας ως ορίζεται από τον νόμο, που αφορούν τα προσωπικά δεδομένα. Η διαδικασία χωρίζεται σε αρκετά στάδια και υλοποιείται κυρίως με συνεντεύξεις και συναντήσεις με τις οργανωτικές μονάδες και με τους υπευθύνους του IT.

Πριν ακολουθήσει οποιαδήποτε άλλη ενέργεια συμμόρφωσης θα πρέπει να υπάρξει μία ολοκληρωμένη χαρτογράφηση των εφαρμογών και των

συστημάτων αποθήκευσης προσωπικών δεδομένων. Οι πολιτικές ασφάλειας πληροφοριών όπως το ISMS και πιστοποιήσεις ISO 27000 θα υποβοηθήσουν σημαντικά την καταγραφή προσωπικών δεδομένων. Αν ο Οργανισμός δεν έχει εφαρμόσει παρόμοιες πολιτικές, τότε η διερεύνηση και απεικόνιση των δεδομένων θα είναι σημαντική προσπάθεια και χρονοβόρα. Η ολοκλήρωση του δεύτερου βήματος είναι η απεικόνιση της ροής της πληροφορίας (Data Flow) μεταξύ συστημάτων εντός και εκτός ορίων του οργανισμού και η διαχείριση της πληροφορίας από τους χρήστες.
Σε συνάρτηση με τις ανωτέρω απεικονίσεις και περιγραφές προκύπτουν σημαντικά συμπεράσματα για τα προσωπικά δεδομένα και πώς αυτά τα διαχειρίζεται ο Οργανισμός σας. Τα συμπεράσματα αυτά θα τροφοδοτήσουν άλλα στάδια στη διαδικασία συμμόρφωσης.

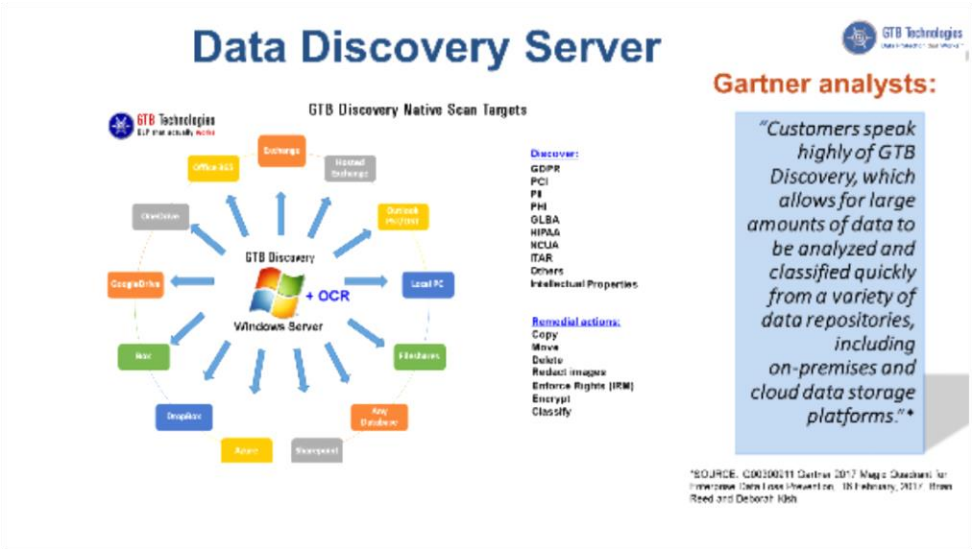
Η Wisedata, με μεγάλη εμπειρία στο χώρο ασφάλειας δεδομένων, θα χρησιμοποιήσει αρχικά ερωτηματολόγια για μία εκτίμηση της κατάστασης με τους τελικούς χρήστες ώστε, σε συνεργασία με το IT, να αποκτήσει σφαιρική εικόνα, πριν ενεργοποιήσει εξειδικευμένες τεχνικές μεθόδους. Η διερεύνηση βασίζεται σε εξειδικευμένα εργαλεία (Data Discovery) που θα εντοπίσουν προσωπικά δεδομένα που ενδεχομένως παραμένουν άγνωστα (δομημένα ή σε αδόμητη μορφή) ακόμα και σήμερα. Η επεξεργασία δεν θα αφήσει περιθώρια λάθους ή παραλήψεων στα μετέπειτα βήματα για την προστασία των προσωπικών δεδομένων.

Υποκείμενα των δεδομένων και Δικαιώματα.

Ο κανονισμός δίνει ιδιαίτερη έμφαση στα δικαιώματα των φυσικών προσώπων και δημιουργεί την υποχρέωση στον Οργανισμό να διαχειρίζεται τα προσωπικά δεδομένα με νομιμότητα, αντικειμενικότητα και διαφάνεια (άρθρο 5).
Αυτό επιφέρει μια σειρά από υποχρεώσεις και ευθύνες στον Οργανισμό σας, καθώς και την αποσαφήνιση της νομικής βάσης συλλογής και επεξεργασίας των δεδομένων.

> Ο Κανονισμός ενσωματώνεται στη λειτουργία της επιχείρησης.

Η αντιμετώπιση των απαιτήσεων του Κανονισμού απαιτεί συστηματική καταγραφή της κατάστασης και περιγραφής της νέας προσέγγισης βάσει των νέων απαιτήσεων. Η νομιμότητα συλλογής και τήρησης των δεδομένων βάσει της οποίας ο Οργανισμός σας επεξεργάζεται τα δεδομένα αναθεωρείται και με την βοήθεια έγκριτων νομικών συμβούλων στο αντικείμενο, παρουσιάζονται δε και εκτιμώνται στη Διοίκηση της εταιρείας.



Στην διαδικασία καθορίζονται και οι υποχρεώσεις της εταιρίας σας στην αντιμετώπιση γνωστοποίησης παραβίασης προσωπικών δεδομένων στην εποπτική αρχή και στο υποκείμενο των δεδομένων.

Διασυνοριακές Μεταφορές Προσωπικών Δεδομένων.

Η διαδικασία αντιμετωπίζεται με πλήρη αποτύπωση της σημερινής κατάστασης, ελέγχοντας την ροή των δεδομένων που αφορούν προσωπικά δεδομένα, είτε σποραδικά και μη συστημικά είτε όταν αυτό συμβαίνει στην κανονική ροή εργασιών της εταιρείας. Οι ρόλοι του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία αποσαφηνίζονται και ορίζονται πλήρως. Διεξάγεται πλήρης ανάλυση όλων των σεναρίων μεταφοράς ΠΔ και των παραληπτών. Το έγκριτο νομικό επιτελείο της Wisedata θα υποδείξει περαιτέρω τις συμβάσεις επεξεργασίας τα μέτρα ασφάλειας και νομιμότητας της μεταφοράς σε χώρες που δεν κρίνονται ή δεν δεσμεύονται για την ασφάλεια των ΠΔ. Οι Υποδείξεις της Αρχής λαμβάνονται υπόψη εφόσον είναι σκόπιμο.

Προσδιορισμός, Ανάλυση Παρούσας και Επιθυμητής Θέσης (GAP Analysis). Εκτίμηση Αντικτύπου.

Η εκτίμηση αντικτύπου και η ανάλυση μεταξύ τωρινής και μελλοντικής κατάστασης (GAP analysis) θα υποδείξει στην εταιρεία το ρίσκο, τα οργανωτικά και τα τεχνικά μέτρα που πρέπει να λάβει για τη συμμόρφωση.
Σημαντικός παράγοντας στη συμμόρφωση είναι τα βιώσιμα οργανωτικά και τεχνικά μέτρα, που θα ενσωματωθούν στην λειτουργία της εταιρείας για την συνεχή τήρηση του κανονισμού. Η χρήση της μεθοδολογίας δίνει τη δυνατότητα στην εταιρεία σας να λάβει τεκμηριωμένες αποφάσεις σχετικά με τις δραστηριότητες και τις επενδύσεις στον τομέα της ασφάλειας και να υποστηρίξει τη διαχείριση κινδύνου.

Εργαλεία Υποστήριξης του Κανονισμού.

Ο Κανονισμός υποχρεώνει τις εταιρείες, μέσα από τις απαιτήσεις συμμόρφωσης, να ενσωματώσουν την ασφάλεια ΠΔ στο DNA τους, στην καθημερινή λειτουργία και τις δραστηριότητές τους. Η ευθύνη μετατοπίζεται στην εταιρεία και ο μόνος τρόπος είναι η ένταξη, εκτός των Οργανωτικών μέτρων, της υλοποίησης ηλεκτρονικών μέτρων ασφάλειας, αποφεύγοντας λανθασμένες ενέργειες χρηστών ή αμέλεια. Τα ηλεκτρονικά μέτρα, όπως το Data Discovery, είναι χρήσιμα εργαλεία όχι μόνο στον εντοπισμό ΠΔ στη διαδικασία χαρτογράφησης αλλά και στην υλοποίηση υποχρεώσεων των δικαιωμάτων των υποκειμένων.

Η προστασία ΠΔ από σκόπιμη ή από αμέλεια αποστολή δεδομένων (e-mail, USB) είναι επίσης παράμετρος ρίσκου και έκθεσης κινδύνου. Η εταιρεία οφείλει να λάβει μέτρα προστασίας DLP.

Η εμπειρία της Wisedata στο χώρο της ασφάλειας ΠΔ και σε συνεργασία με Οίκους απόλυτα εξειδικευμένους στο αντικείμενο, θα αξιολογήσει και θα υποδείξει την κατάλληλη τεχνολογία σε συνάρτηση του μεγέθους της εταιρείας, της πολυπλοκότητας και της αναλογικότητας του κόστους / οφέλους που προκύπτει.

Κρυπτογράφηση (Encryption).

Η οδηγία ορίζει πως η τεχνική της κρυπτογραφίας και τα σημεία που εφαρμόζεται με κλειδιά κλπ. προσφέρουν προστασία, εμπιστευτικότητα και ακεραιότητα των δεδομένων.

Anonymization, Pseudonymization

Η οδηγία ορίζει πώς να χρησιμοποιηθούν οι τεχνικές αυτές με σκοπό την προστασία προσωπικών δεδομένων στην επεξεργασία τους.

Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων.

Η εταιρεία σας, για την συνεχή υποστήριξη του κανονισμού, οφείλει να εναρμονισθεί με πολιτική ασφάλειας πληροφοριών (ISMS) ανάλογη των πληροφοριακών συστημάτων που διαθέτει, ανάλογα και με το μέγεθος και το ρίσκο της επεξεργασίας των ΠΔ. Κάθε προσπάθεια της εταιρείας στην μελλοντική πιστοποίηση μέσω προτύπου ISO αντιμετωπίζεται από την Αρχή ευνοϊκά.

Πλάνο Αποκατάστασης Καταστροφών.

Πολιτική που κατευθύνει, εφόσον έχει έννοια, την ανάκτηση χαμένης πληροφορίας που έχει προκύψει από διάφορες αιτίες και είχαν ως αποτέλεσμα την διακοπή λειτουργίας των πληροφοριακών και επικοινωνιακών μέσων.

Υλοποίηση και Συνεχής Τεχνική Υποστήριξη.

Με την ολοκλήρωση των εργασιών συμμόρφωσης η εταιρεία σας έχει την δυνατότητα να λάβει τεχνική υποστήριξη σε καθημερινή βάση σε θέματα ασφάλειας ΠΔ, γνωστοποίησης παραβίασης ή συμβουλευτικές υπηρεσίες Υπευθύνου Προστασίας Προσωπικών δεδομένων μέσω σύμβασης συνεργασίας. Επιπλέον, κάθε τεχνική λύση προστασίας ΠΔ υποστηρίζεται 24/7 και παρέχονται και υπηρεσίες on site (κατόπιν συμφωνίας).

WiseData

It's all about data!

Βασ. Γεωργίου 3, Χαλάνδρι
15232, Αθήνα
Τηλ.: 211 800 9070