Κυριε Πρόεδρε,

Κυριοι και Κυρίες

Καταρχήν να ευχαριστήσω για την πρόσκληση που απευθύνατε στο Δικηγορικό Σύλλογο Λάρισας υποστήριξης της σημερινής ημερίδας ευαισθητοποίησης και να μεταφέρω τους χαιρετισμούς της Προέδρου κας Νικολέτας Μπασδέκη και να σας διαβεβαιώσω ότι ο Δικηγορικός Σύλλογος Λάρισας θα είναι πάντα στο πλευρό σας για ότι ζήτημα ανακύψει σχετικά με την εφαρμογή του κανονισμού συμβάλλοντας με την τεχνογνωσία των μελών του στα προσωπικά δεδομένα.

Η εισήγηση μου έχει τρία μέρη: **Στο πρώτο μέρος θα εκταθώ σε σύντομη ενημέρωση για την νομική και κανονιστική συμμόρφωση του ΤΕΕ. Στο δεύτερο μέρος θα αναφερθώ στην εφαρμογή του κανονισμού στον κόσμο των μηχανικών, πώς σχετίζεται με την επαγγελματική τους δραστηριότητα, πώς επηρεάζονται και τι ενέργειες πρέπει να κάνουν. Στο τρίτο μέρος θα αναφερθώ στο υποκείμενο των δεδομένων δηλαδή ολους εμας ως ταυτοποιημένα ή ταυτοποιήσιμα φυσικά πρόσωπα και ειδικά στα δικαιώματα μας στο νέο κανονιστικό πλαίσιο**

Με την εμφάνιση της πληροφορικής τη δεκαετία του 1960, άρχισε να διαφαίνεται η εντεινόμενη ανάγκη θέσπισης λεπτομερέστερων κανόνων για την προάσπιση των δικαιωμάτων του ατόμου μέσω της προστασίας των προσωπικών δεδομένων του. Έως τα μέσα της δεκαετίας του 1970, η Επιτροπή Υπουργών του Συμβουλίου της Ευρώπης εξέδωσε ποικίλα ψηφίσματα σχετικά με την προστασία των προσωπικών δεδομένων, διά παραπομπής στο άρθρο 8 ΕΣΔΑ. Το 1981 άνοιξε προς υπογραφή η Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων (Σύμβαση 108). Η Σύμβαση 108 ήταν η μόνη νομικά δεσμευτική διεθνής πράξη στον τομέα της προστασίας των προσωπικών δεδομένων. Τον Ιανουάριο του 2012 η Ευρωπαϊκή

Ένωση προτείνει μεταρρύθμισητων κανόνων προστασίας των δεδομένων. Μάρτιος 2014: Το Ευρωπαϊκό Κοινοβούλιο εγκρίνει την πρόταση για τον νέο Κανονισμό (πρώτη ανάγνωση). Τον Απρίλιο 2016 το Ευρωπαϊκό Κοινοβούλιο ψηφίζει τον Κανονισμό 679/2016 – Γενικός Κανονισμός για την Προστασία Προσωπικών Δεδομένων (General Data Protection Regulation). Τον Μάιος 2016 ο Κανονισμός τίθεται σε ισχύ, με μεταβατική περίοδο δύο (2) ετών. Και φτάσαμε στην 25η Μαΐου 2018 οπου ο Κανονισμός εφαρμόζεται, ως νομοθέτημα άμεσης εφαρμογής σε όλες τις χώρες – μέλη της ΕυρωπαϊκήςΈνωσης

Σε αναζήτηση λέξεων στο Κανονισμό Προστασίας Δεδομένων Προσωπικού Χαρακτήρα η λέξη πρόστιμο εμφανίζεται 36 φορές και εκεί που σταματάει το μάτι του αναγνώστη είναι στο σημείο που περιγράφονται διοικητικά πρόστιμα έως 20 000 000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο. **Βεβαια στη φαρέτρα της εποπτικής αρχής δεν είναι μονο χρηματικά ποσά αλλά η προειδοποίηση, η σύσταση, η επίπληξη, οι οδηγίες, τα μέτρα σύμφωνα πάντα με την αρχή της αναλογικότητας**

Τα διοικητικά πρόστιμα ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης, επιβάλλονται και πρεπει να είναι αναλογικά, αποτρεπτικά και αποτελεσματικά. Κατά τη λήψη απόφασης σχετικά με την επιβολή διοικητικού προστίμου, καθώς και σχετικά με το ύψος του διοικητικού προστίμου για κάθε μεμονωμένη περίπτωση, λαμβάνονται δεόντως υπόψη : α) 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, β) ο δόλος ή η αμέλεια που προκάλεσε την παράβαση, γ) οποιεσδήποτε ενέργειες στις οποίες προέβη ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία για να μετριάσει τη ζημία που υπέστησαν τα υποκείμενα των δεδομένων, δ) ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα που εφαρμόζουν δυνάμει των άρθρων 25 και 32, ε) τυχόν σχετικές προηγούμενες παραβάσεις του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, στ) ο βαθμός συνεργασίας με

την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των πιθανών δυσμενών επιπτώσεών της, ζ) οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει η παράβαση, η) 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, θ) σε περίπτωση που διατάχθηκε προηγουμένως η λήψη των μέτρων που αναφέρονται στο άρθρο 58 παράγραφος 2 κατά του εμπλεκόμενου υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σχετικά με το ίδιο αντικείμενο, η συμμόρφωση με τα εν λόγω μέτρα, ι) η τήρηση εγκεκριμένων κωδίκων δεοντολογίας σύμφωνα με το άρθρο 40 ή εγκεκριμένων μηχανισμών πιστοποίησης σύμφωνα με το άρθρο 42 και ια) 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

Πρώτα όμως θα πρέπει να ορίσουμε τα προσωπικά δεδομένα που είναι κάθε πληροφορία που αφορά ταυτοποιήμενο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων») ‘ το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί άμεσα ή έμμεσα ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν τη σωματική, φυσιολογική, γεννετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου

ΠΡΩΤΟ ΜΕΡΟΣ : Νομική και κανονιστική συμμόρφωση ΤΕΕ

Η συμμόρφωση περιλαμβάνει τα εξής στάδια : την μελέτη, την υλοποίηση και την επιβλεψη, υποστήριξη και εκπαίδευση του ΥΠΔ

1. Μελέτη
   1.1 Έγγραφο Συνεργασίας και Υποστήριξης από τη Διοίκηση
   1.2 Ανάλυση, Καταγραφή υπάρχουσας κατάστασης και Έλεγχος Αποκλίσεων

1.3 Αρχείο Καταγραφής Ενεργειών Συμμόρφωσης, Σχέδιο Δράσης (Action Plan).

2. Υλοποίηση
   2.1 Μητρώα Δεδομένων, Επεξεργασίας & Πρόσβασης
   2.2 Μητρώα συναίνεσης
   2.3 Κώδικας Δεοντολογίας και Πολιτική Ασφαλείας Δεδομένων
   2.4 Ανάλυση Ασφάλειας Πληροφοριακών Συστημάτων
   2.5 Ανάλυση Συμβάσεων και Δεδομένων Μακράς Αποθήκευσης
   2.6 Διεξαγωγή Μελέτης Εκτίμησης Ρίσκου, Αντικτύπου & Αποφυγής – Μητρώα Κινδύνων.
3. Επίβλεψη, Υποστήριξη, Εκπαίδευση – ΥΠΔ(DPO)
   3.1 Παρακολούθηση Συμμόρφωσης & Συντήρηση Μητρώων.
   3.2 Εκπαιδευτικές, Ενημερωτικές και Συμβουλευτικές Υπηρεσίες.
   3.3 Συνεργασία με Εποπτική Αρχή
   3.4 Περιοδικές Δοκιμές Προστασίας & Συμμόρφωσης (Penetration Testing)

Ο νομικός θα επεξεργαστεί το έγγραφο συνεργασίας και υποστήριξης από τη διοίκηση, τις συμβάσεις εμπιστευτικότητας, την έγγραφη συγκατάθεση του υποκειμένου, τον κώδικα δεοντολογίας και την πολιτική ασφάλειας δεδομένων

Ο φορέας πρέπει να διασφαλίσει την εμπιστευτικότητα με αντίστοιχες συμβάσεις ώστε τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα να έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή να τελούν υπό τη δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας,

Ο φορέας πρέπει να εφοδιαστεί με έγγραφη συγκατάθεση του υποκειμένου : Η συγκατάθεση θα πρέπει να παρέχεται με σαφή θετική ενέργεια η οποία να συνιστά ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει ένδειξη της συμφωνίας του υποκειμένου των δεδομένων υπέρ της επεξεργασίας των δεδομένων που το αφορούν, για παράδειγμα με γραπτή δήλωση, μεταξύ άλλων

με ηλεκτρονικά μέσα, ή με προφορική δήλωση. Αυτό θα μπορούσε να περιλαμβάνει τη συμπλήρωση ενός τετραγωνιδίου κατά την επίσκεψη σε διαδικτυακή ιστοσελίδα, την επιλογή των επιθυμητών τεχνικών ρυθμίσεων για υπηρεσίες της κοινωνίας των πληροφοριών ή μια δήλωση ή συμπεριφορά που δηλώνει σαφώς, στο συγκεκριμένο πλαίσιο, ότι το υποκείμενο των δεδομένων αποδέχεται την πρόταση επεξεργασίας των οικείων δεδομένων προσωπικού χαρακτήρα. Επομένως, η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια δεν θα πρέπει να εκλαμβάνονται ως συγκατάθεση. Η συγκατάθεση θα πρέπει να καλύπτει το σύνολο των δραστηριοτήτων επεξεργασίας που διενεργείται για τον ίδιο σκοπό ή για τους ίδιους σκοπούς. Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, θα πρέπει να δίνεται συγκατάθεση για όλους αυτούς τους σκοπούς. Εάν η συγκατάθεση του υποκειμένου των δεδομένων πρόκειται να δοθεί κατόπιν αιτήματος με ηλεκτρονικά μέσα, το αίτημα πρέπει να είναι σαφές, περιεκτικό και να μην διαταράσσει αδικαιολόγητα τη χρήση της υπηρεσίας για την οποία παρέχεται.

Ο φορέας θα πρέπει να εκπονήσει Κώδικα Δεοντολογίας που αποτελεί το 25% της συμμόρφωσης του φορέα και των μελών του και αποτελεί λόγο μειωσης των τυχον προστιμων : Η εκπόνηση κωδίκων δεοντολογίας που έχουν ως στόχο να συμβάλουν στην ορθή εφαρμογή του παρόντος κανονισμού, λαμβάνοντας υπόψη τα ειδικά χαρακτηριστικά των διάφορων τομέων επεξεργασίας και τις ειδικές ανάγκες των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων. 2. Ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μπορούν να εκπονούν κώδικες δεοντολογίας ή να τροποποιούν ή να επεκτείνουν υφιστάμενους κώδικες δεοντολογίας, προκειμένου να προσδιορίσουν την εφαρμογή του παρόντος κανονισμού, όπως όσον αφορά: α) τη θεμιτή και με διαφάνεια επεξεργασία, β) τα έννομα συμφέροντα που επιδιώκουν οι υπεύθυνοι επεξεργασίας σε συγκεκριμένα πλαίσια, γ) τη συλλογή δεδομένων προσωπικού χαρακτήρα, δ) την ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα, ε) την ενημέρωση του κοινού και των υποκειμένων των δεδομένων, στ) την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων, ζ) την ενημέρωση και την προστασία των παιδιών και τον τρόπο απόκτησης της συγκατάθεσης του ασκούντος τη γονική μέριμνα του παιδιού, η) τα μέτρα και τις διαδικασίες που

αναφέρονται στα άρθρα 24 και 25 και τα μέτρα για τη διασφάλιση της ασφάλειας της επεξεργασίας που αναφέρεται στο άρθρο 32, θ) τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα στις εποπτικές αρχές και την ανακοίνωση των εν λόγω παραβιάσεων δεδομένων προσωπικού χαρακτήρα στα υποκείμενα των δεδομένων, ι) τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς, ή ια) εξωδικαστικές διαδικασίες και άλλες διαδικασίες επίλυσης διαφορών για την επίλυση διαφορών μεταξύ υπευθύνων επεξεργασίας και υποκειμένων των δεδομένων όσον αφορά την επεξεργασία, με την επιφύλαξη των δικαιωμάτων των υποκειμένων των δεδομένων δυνάμει των άρθρων 77 και 79

ΔΕΥΤΕΡΟ ΜΕΡΟΣ : Η εφαρμογή του κανονισμού στον κόσμο των μηχανικών, πώς σχετίζεται με την επαγγελματική τους δραστηριότητα, πώς επηρεάζονται και τι ενέργειες πρέπει να κάνουν.

Ως επαγγελματίες έρχονται στα χέρια σας διάφορα έγγραφα φωτοαντίγραφα ταυτοτήτων, Ε9, συμβόλαια, κλπ για τα οποία δεν έχουμε κάποια π.χ. γραπτή συγκατάθεση για την επεξεργασία τους, πολλά από αυτά τα διατηρούμε εμείς στο αρχείο μας είτε ως αντίγραφα είτε σκαναρισμένα στον υπολογιστη μας. Οποιοδήποτε προσωπικό δεδομένο τρίτου είναι στο γραφείο σας ανήκει στην κυριότητα του πελάτης σας και οφείλετε να διασφαλίζετε την προστασία του δεδομένου έναντι τρίτων που θα θελήσουν να παραβιάσουν και να αφαιρέσουν αυτό το δεδομένο.

Το πλαίσιο συμμόρφωσης που προβλέπει ο Κανονισμός είναι αρκετά αόριστο, αλλά ιδιαίτερα αυστηρό στην περίπτωση που τα δεδομένα είναι ευαίσθητα, και οι ενδεικτικές οδηγίες συμμόρφωσης :

1.Θα πρέπει όλοι οι επαγγελματίες να συλλέγουν από τις 25 Μάιου **γραπτά και σε ηλεκτρονική μορφή** τη **συγκατάθεση** του παρόχου των δεδομένων.

2.Θα πρέπει να διαθέτουν **επικαιροποιημένα Ηλεκτρονικά Μητρώα Δεδομένων** και να **καταγράφουν** όλα τα προσωπικά δεδομένα που κατακρατούν.

3.Θα πρέπει να διαθέτουν **επικαιροπιημένα ηλεκτρονικά Μητρώα Δραστηριοτήτων Επεξεργασίας** που να περιέχουν την προέλευση και όλες τις επεξεργασίες των δεδομένων.

4.Θα πρέπει να διαθέτουν και να τηρούν ένα κοινό επαγγελματικό Κώδικα Δεοντολογίας

5.Θα πρέπει όλοι να διαθέτουν κατάλληλους μηχανισμούς **φύλαξης Ευαίσθητων δεδομένων μακράς αποθήκευσης**.

6.Θεμιτή είναι τέλος η όποια **εκπαίδευση** και η **διεξαγωγή Εκτίμησης Αντικτύπου.**

Είναι, πολύ σημαντικό θεωρείται οι ιδιώτες να έχουν εκκινήσει τις παραπάνω διαδικασίες συμμόρφωσης στο περιεχόμενο του Κανονισμού, μέχρι την έναρξη εφαρμογής του την 25η Μαΐου 2018, ώστε τουλάχιστον να έχουν δημιουργήσει ένα πλαίσιο μέσα στο οποίο θα συνεχίσουν αυτή την προσπάθεια.

ΤΡΙΤΟ ΜΕΡΟΣ

Στο τρίτο μέρος θα αναφερθώ στο υποκείμενο των δεδομένων δηλαδή ολους εμας ως ταυτοποιημένα ή ταυτοποιήσιμα φυσικά πρόσωπα και ειδικά στα δικαιώματα μας στο νέο κανονιστικό πλαίσιο

1/ Δικαίωμα ενημέρωσης και πρόσβασης στα δεδομένα (Άρθρο 15) : Εχετε περισσότερη και σαφέστερη ενημέρωση κατά τη συλλογή των δεδομένων για την επεξεργασία τους και το δικαίωμα προσβασης σε αυτά

2/Δικαίωμα διόρθωσης, (Άρθρο 16) : Εχετε το δικαίωμα να απαιτήσετε από τον υπεύθυνο επεξεργασίας την διόρθωση ανακριβών δεδομένων καθώς και τη συμπλήρωση ελλιπών δεδομένων που σας αφορούν

3/ Δικαίωμα στη λήθη (διαγραφής), (Άρθρο 17) : Όταν δεν επιθυμείτε πλεον την επεξεργασία και διατήρηση προσωπικών σας δεδομένων έχετε το δικαίωμα να ζητήσετε τη διαγραφή τους υπο την προυπόθεση ότι τα δεδομένα δεν διατηρούνται για κάποιο νομιμο ή και δηλωμένο σκοπό

4/ Δικαίωμα περιορισμού της επεξεργασίας, (Άρθρο 18) : Δικαιούστε να εξασφαλίζετε από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας υπο συγκεκριμένες προυποθέσεις

Για όλα τα παραπάνω υπάρχει υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή διαγραφή ή περιορισμό επεξεργασίας, (Άρθρο 19)

5/Δικαίωμα φορητότητας σε δομημένο, συμβατό και μηχαναγνώσιμο μορφότυπο, (Άρθρο 20). Δικαιούστε να λάβετε ή να ζητήσετε την μεταφορά των δεδομένων σας σε μηχαναγνώσιμη μορφή από ένα υπεύθυνο επεξεργασίας υπο συγκεκριμένες προυποθέσεις εφόσον το επιθυμείτε

6/Δικαίωμα εναντίωσης στην επεξεργασία, (Άρθρο 21) : Εχετε το δικαίωμα να αντιταχθείτε στην επεξεργασία των δεδομένων σας υπο συγκεκριμένες προυποθέσεις ιδίως όταν πρόκειται για κατάρτιση «προφιλ» ή για σκοπους απευθείας εμπορικής προώθησης

Σχετικά με την αυτοματοποιημένη ατομική λήψη αποφάσεων συμπεριλαμβανομένης της κατάρτισης **προφίλ** (την οποία θα έχετε ήδη εντοπίσει, όπως περιγράφεται παραπάνω, υπό το σημείο 2: "Καταγραφή προσωπικών δεδομένων"), έχετε θεσπίσει **διαδικασίες** για την ικανοποίηση του **δικαιώματος εναντίωσης** των υποκειμένων σε λήψη αυτοματοποιημένων αποφάσεων και προφιλοποίησης,

Οι ραγδαίες τεχνολογικές εξελίξεις και η παγκοσμιοποίηση δημιούργησαν νέες προκλήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα. Τα νεα καθήκοντα του Υπεύθυνου Προστασίας Δεδομένων ανοίγουν νέο πεδίο δραστηριότητας και για τους μηχανικούς πληροφορικής και για τους νομικούς.. Πλαι στα εύλογα μέτρα και τις πρακτικές που θα υιοθετήσουν οι φορείς αλλά και οι επαγγελματίες με τη συνεργασία του μηχανικού πληροφορικής ενας νομικός θα συνεργάζεται μαζί του καθώς πέρα από την εκπόνηση των νομικών

κειμένων που αναφέρθηκαν στην αρχή της εισήγησης θα σταθμίζει τα δικαίωματα, την προστασία τους