ΕΛΛΗΝΙΚΟ ΜΕΣΟΓΕΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Σχολή Επιστημών Διοίκησης και Οικονομίας

Τμήμα Διοίκησης Επιχειρήσεων

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ο ΘΕΣΜΟΣ ΤΟΥ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΣΥΓΧΡΟΝΗ ΕΠΙΧΕΙΡΗΣΗ ΚΑΤΑ ΤΟΝ ΚΑΝΟΝΙΣΜΟ 679/2016 ΚΑΙ ΤΗΝ ΟΔΗΓΙΑ 680/2016

ΣΠΥΡΙΔΑΚΗ ΜΑΡΙΑ ΑΜ: 4528

Επιβλέπουσα Καθηγήτρια : **ΜΠΙΜΠΑ ΕΜΜΑΝΟΥΕΛΑ - ΜΑΡΙΑ**

Ευχαριστίες

Με την ολοκλήρωση της πτυχιακής εργασίας θα ήθελα να ευχαριστήσω την κυρία Μπίμπα Εμμανουέλα Μαρία για την επιστημονική καθοδήγηση , τις γνώσεις και την πολύτιμη βοήθεια που μου παρείχε.

Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου για τη στήριξη τα χρόνια των σπουδών μου.

ΠΕΡΙΛΗΨΗ

Σκοπός της παρούσης πτυχιακής εργασίας είναι να περιγράψει μια σαφή συνοπτική εικόνα του γενικού κανονισμού για τη προστασία των προσωπικών δεδομένων GDPR 2016/679 και να παρουσιάσει μια λεπτομερή ανάλυση της εννοίας της συγκατάθεσης στο κανονισμό σε μια εποχή που τα κοινωνικά δίκτυα είναι στη ζωή μας, τα προσωπικά δεδομένα είναι απαραίτητα για τη χρήση εφαρμογών και υπηρεσιών .
Η οικονομική και κοινωνική ολοκλήρωση της Ευρωπαϊκής Ένωσης, οι ραγδαίες εξελίξεις της τεχνολογίας και η παγκοσμιοποίηση συντέλεσαν στο πέρασμα της ανθρωπότητας σε μία νέα εποχή, την εποχή της πληροφορίας. Στο πλαίσιο αυτό, άρχισε να αναπτύσσεται ο εύλογος προβληματισμός όσον αφορά στην προστασία των δεδομένων και της ιδιωτικότητας των πολιτών. Ως εκ τούτου, κρίνεται απαραίτητο να δημιουργηθούν ασφαλιστικές δικλίδες, οι οποίες να μπορούν να προστατεύουν επαρκώς τα θεμελιώδη δικαιώματα των ανθρώπων, ενώ δε θα δρουν περιοριστικά στην ανάπτυξη της αγοράς και της τεχνολογίας.
Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων που έθεσε εφαρμογή τα τέλη Μάιου 2018 (ευρύτερα γνωστό ω GDPR 2016/679 – General Data Protection Regulation 2016/679 αντικατέστησε τον Ευρωπαϊκό νόμο 95/46/ΕΞ, προστασίας δεδομένων που ισχύει σε ευρωπαϊκό επίπεδο, προσαρμόζοντας τον στην προστασία δεδομένων στις ανάγκες της σύγχρονης εποχής, προσπαθεί να διασφαλίσει ακόμη περισσότερο την ιδιωτικότητα και τα δεδομένα των πολιτών. Λαμβάνοντα υπόψη το νομικό πλαίσιο

Λέξεις κλειδιά : GDPR, Προσωπικά Δεδομένα , Προστασία

ABSTRACT

THE INSITUTION OF THE DATA PROTECTION OFFICER ACCORDING THE EU REG 679/2016 AND 680/2016

The purpose of this thesis is to describe a clear summary of the general regulation on GDPR 2016/679 and to provide a detailed analysis of the concept of consent in regulation at a time when social networks are in our lives, personal data is required for the use of applications and services.
The economic and social integration of the European Union, the rapid advances in technology and globalization have contributed to the passage of humanity into a new age, the information age. In this context, there has been a growing concern about data protection and citizens' privacy. It is therefore necessary to create safeguards that can adequately safeguard fundamental human rights, while not restricting market and technology development.
The General Data Protection Regulation which came into force at the end of May 2018 (better known as GDPR 2016/679 - General Data Protection Regulation 2016/679 replaced European Data Protection Law 95/46 / EC, adapting it to data protection to meet the needs of the modern age, strives to further safeguard the privacy and data of citizens, taking into account the legal framework

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 6

ΚΕΦΑΛΑΙΟ 7

ΕΙΣΑΓΩΓΗ

Ο 21ος αιώνας χαρακτηρίζεται ως εποχή της πληροφορίας και της άνθησης του διαδικτύου .Αυτό έχει ως αποτέλεσμα την ολοένα μεγαλύτερη ανησυχία των χρηστών για τη διαχείριση των προσωπικών δεδομένων .
Η απελευθέρωση ιδιωτικών δεδομένων είναι γεγονός από τη στιγμή που επισκέπτονται ένα ισότοπο ή πραγματοποιούν κάποια συναλλαγή μέσω του διαδικτύου.
Η ιδιωτικότητα είναι μια έννοια που οι ρίζες της πηγάζουν εδώ και 2500 χρόνια όταν για πρώτη φορά ο Έλληνας φιλόσοφος Αριστοτέλης είχε εισάγει την έννοια της αρχαίας Αθήνα στο δοκίμιο του με τίτλο «Πολιτικά»

Το δικαίωμα στην προστασία της ιδιωτικής σφαίρας του ατόμου έναντι αυθαίρετων επεμβάσεων τρίτων, ιδίως του κράτους, κατοχυρώνεται για πρώτη φορά σε διεθνές νομικό κείμενο το 1948 στο άρθρο 12 της Οικουμενικής Διακήρυξης των Ηνωμένων Εθνών για τα Ανθρώπινα Δικαιώματα, σχετικά με το σεβασμό της ιδιωτικής και οικογενειακής ζωής

Το Συμβούλιο της Ευρώπης ιδρύθηκε την επαύριον του Β' Παγκοσμίου Πολέμου από τα ευρωπαϊκά κράτη με σκοπό την προώθηση του κράτους δικαίου, της δημοκρατίας, των ανθρωπίνων δικαιωμάτων και της κοινωνικής ανάπτυξης. Προς τον σκοπό αυτό, υιοθέτησε το 1950 την Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ), η οποία τέθηκε σε ισχύ το 1953.

Στο πλαίσιο αυτό, η ασφάλιση έναντι αυτής της μορφής των κινδύνων, αποτελεί ένα θέμα που προσελκύει το αυξανόμενο ενδιαφέρον της επιστημονικής και επαγγελματικής παγκόσμιας κοινότητας, δεδομένου ότι δείχνει πολλά υποσχόμενη, ως μια αποδοτική εναλλακτική μορφή διαχείρισης των κινδύνων του κυβερνοχώρου.

Προκειμένου να επιτευχθούν οι σκοποί της εργασίας, προχωράμε σε μια εκτενή επισκόπηση της παγκόσμιας βιβλιογραφίας που άπτεται των θεμάτων της προστασίας των προσωπικών δεδομένων, των κινδύνων του κυβερνοχώρου και της στάσης των επιχειρήσεων προς αυτούς, καθώς και της σημασίας της ασφάλισης έναντι αυτής της μορφής των κινδύνων. Η παρούσα διπλωματική εργασία είναι χωρισμένη σε επτά επιμέρους βασικές θεματικές ενότητες. Σε κάθε μια από αυτές παρουσιάζονται, με τρόπο διακριτό, οι πληροφορίες που σχετίζονται με τα επί μέρους ζητήματα που άπτονται του θέματος της εργασίας.

ΚΕΦΑΛΑΙΟ 1

1.1 Η Αρχή της νομιμότητας

Σύμφωνα με το άρθρο 5 του ΓΚΠΔ για να είναι νόμιμη η επεξεργασία προσωπικών δεδομένων απλών και «ειδικών» κατηγοριών θα πρέπει η επεξεργασία να διέπετε από συγκεκριμένες αρχές.

Αυτές είναι :

1) **Η αρχή της νομιμότητας** αντικειμενικότητας και διαφάνειας. Σύμφωνα με τη συγκεκριμένη αυτή αρχή τα δεδομένα θα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Η διαφάνεια απαιτεί την ενημέρωση του υποκειμένου να είναι συνοπτική, εύκολα προσβάσιμη, κατανοητή, με σαφή και απλή διατύπωση.
2) **Η αρχή του περιορισμού του σκοπού**, σύμφωνα με την οποία, τα δεδομένα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με τους σκοπούς αυτούς.
3) **Η αρχή της αναλογικότητας** «ελαχιστοποίηση των δεδομένων » σύμφωνα με την οποία τα δεδομένα θα πρέπει να είναι πρόσφορα συναφή και αναγκαία για τους επιδιωκόμενους σκοπούς επεξεργασίας.
4) **Η αρχή της ακρίβειας των δεδομένων,** σύμφωνα με την οποία τα δεδομένα θα πρέπει να είναι ακριβή, να επικαιροποιούνται και να λαμβάνονται κατάλληλα μέτρα για την άμεση διόρθωση ή διαγραφή ανακριβιών σε σχέση με τους επιδιωκόμενους σκοπούς επεξεργασίας δεδομένων
5) **Η αρχή της «ακεραιότητας και εμπιστευτικότητας»,** σύμφωνα με την οποία τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ασφάλεια και προστασία τους από παράνομη επεξεργασία ,απώλεια, καταστροφή ή φθορά τους.
6) **Η αρχή του καθορισμού της χρονικής επεξεργασίας «περιορισμός της περιόδου αποθήκευση»,** σύμφωνα με την οποία τα δεδομένα πρέπει να τηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για την επίτευξη των σκοπών της επεξεργασίας.
7) **Η αρχή της λογοδοσίας του υπεύθυνου επεξεργασίας,** σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και θα πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση με τον κανονισμό ενώπιον των εποπτικών αρχών και των δικαστηρίων.[1]

1.2 Το δικαίωμα στην προστασία των προσωπικών δεδομένων

Το δικαίωμα στην προστασία της ιδιωτικής σφαίρας του ατόμου έναντι αυθαίρετων επεμβάσεων τρίτων, ιδίως του κράτους, κατοχυρώνεται για πρώτη φορά σε διεθνές νομικό κείμενο το 1948 στο άρθρο 12 της

[1] http://www.dpa.gr/portal/page?_pageid=33,213319&_dad=portal&_schem

Οικουμενικής Διακήρυξης των Ηνωμένων Εθνών για τα Ανθρώπινα Δικαιώματα, σχετικά με το σεβασμό της ιδιωτικής και οικογενειακής ζωής

Το Συμβούλιο της Ευρώπης ιδρύθηκε την επαύριον του Β' Παγκοσμίου Πολέμου από τα ευρωπαϊκά κράτη με σκοπό την προώθηση του κράτους δικαίου, της δημοκρατίας, των ανθρωπίνων δικαιωμάτων και της κοινωνικής ανάπτυξης. Προς τον σκοπό αυτό, υιοθέτησε το 1950 την Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ), η οποία τέθηκε σε ισχύ το 1953.

Η συμμόρφωση προς την ΕΣΔΑ αποτελεί διεθνή υποχρέωση των κρατών. Πλέον, όλα τα κράτη μέλη του ΣτΕ έχουν ενσωματώσει την ΕΣΔΑ στο εθνικό τους δίκαιο και την έχουν θέσει σε ισχύ. Συνεπώς, υποχρεούνται να ενεργούν σύμφωνα με τις διατάξεις της.

Το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) ιδρύθηκε στο Στρασβούργο της Γαλλίας το 1959, με σκοπό να διασφαλίζει την τήρηση -από τα συμβαλλόμενα μέρη- των υποχρεώσεων που υπέχουν από την ΕΣΔΑ. Το ΕΔΔΑ διασφαλίζει την τήρηση των εν λόγω υποχρεώσεων από τα κράτη εξετάζοντας προσφυγές φυσικών προσώπων, ενώσεων προσώπων, ΜΚΟ ή νομικών προσώπων για φερόμενες παραβιάσεις της ΕΣΔΑ. Το 2013, το Συμβούλιο της Ευρώπης αποτελείτο από 47 κράτη μέλη, 28 εκ των οποίων είναι και κράτη μέλη της ΕΕ. Οι προσφεύγοντες στο ΕΔΔΑ δεν είναι απαραίτητο να είναι πολίτες κράτους μέλους του ΣτΕ. Το ΕΔΔΑ εξετάζει επίσης διακρατικές προσφυγές, οι οποίες ασκούνται από ένα ή περισσότερα κράτη μέλη του ΣτΕ κατά άλλου κράτους μέλους.

Το δικαίωμα στην προστασία των προσωπικών δεδομένων αποτελεί μέρος των δικαιωμάτων που κατοχυρώνονται στο άρθρο 8 ΕΣΔΑ, το οποίο εγγυάται το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας και ορίζει τις προϋποθέσεις υπό τις οποίες επιτρέπονται περιορισμοί του εν λόγω δικαιώματος.2

Στο σύνολο της νομολογίας του, το ΕΔΔΑ επιλήφθηκε πολλών υποθέσεων στις οποίες αιγείρε το ζήτημα της προστασίας των προσωπικών δεδομένων. Οι σημαντικότερες εξ αυτών αφορούσαν υποκλοπή επικοινωνιών, ποικίλες μορφές παρακολούθησης και προστασία έναντι της διατήρησης προσωπικών δεδομένων από δημόσιες αρχές. Το ΕΔΔΑ έχει διευκρινίσει ότι το άρθρο 8 ΕΣΔΑ δεν υποχρεώνει απλώς τα κράτη να μην προβαίνουν σε ενέργειες οι οποίες συνιστούν παραβίαση του εν λόγω δικαιώματος, αλλά σε ορισμένες περιστάσεις επιβάλλει σε αυτά και τη θετική υποχρέωση ανάληψης δράσης για τη διασφάλιση του ουσιαστικού σεβασμού της ιδιωτικής και οικογενειακής ζωής.6 Θα ακολουθήσει εκτενέστερη αναφορά σε πολλές από τις υποθέσεις αυτές στα αντίστοιχα κεφάλαια.

1.3 Σύμβαση 108 του Συμβουλίου της Ευρώπης

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.7 Το 1981 άνοιξε προς υπογραφή η Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων (Σύμβαση 108).8 Η Σύμβαση 108 ήταν και

παραμένει η μόνη νομικά δεσμευτική διεθνής πράξη στον τομέα της προστασίας των προσωπικών δεδομένων.

Η Σύμβαση 108 εφαρμόζεται σε κάθε επεξεργασία προσωπικών δεδομένων που διενεργείται τόσο από τον ιδιωτικό όσο και τον δημόσιο τομέα, όπως για παράδειγμα η επεξεργασία που πραγματοποιείται από τις δικαστικές αρχές και τις αρχές επιβολής του νόμου. Η σύμβαση προστατεύει το άτομο από ενδεχόμενες καταχρηστικές ενέργειες κατά τη συλλογή και επεξεργασία προσωπικών δεδομένων και, ταυτόχρονα, επιδιώκει να ρυθμίσει τη διασυνοριακή ροή προσωπικών δεδομένων. Όσον αφορά τη συλλογή και επεξεργασία προσωπικών δεδομένων, οι αρχές που καθιερώνονται αφορούν ιδίως τη θεμιτή και νόμιμη συλλογή και αυτοματοποιημένη επεξεργασία δεδομένων, τα οποία φυλάσσονται για συγκεκριμένους θεμιτούς σκοπούς και δεν χρησιμοποιούνται για σκοπούς ασύμβατους προς αυτούς, ούτε διατηρούνται για χρονικό διάστημα μεγαλύτερο του αναγκαίου. Αφορούν επίσης την ποιότητα των δεδομένων, ιδίως με την πρόβλεψη ότι τα δεδομένα πρέπει να είναι αναγκαία, πρόσφορα και όχι υπερβολικά (αναλογικότητα), καθώς και ακριβή.

Η Σύμβαση, πέραν των εγγυήσεων που παρέχει για τη συλλογή και την επεξεργασία προσωπικών δεδομένων, απαγορεύει, ελλείψει κατάλληλων νομικών εγγυήσεων, την επεξεργασία «ευαίσθητων» δεδομένων, π.χ. δεδομένων που αφορούν τη φυλή, τις πολιτικές πεποιθήσεις, την υγεία, τη θρησκεία, τη σεξουαλική ζωή ή το ποινικό μητρώο του προσώπου.

Η Σύμβαση κατοχυρώνει επίσης το δικαίωμα του προσώπου να γνωρίζει τι είδους στοιχεία φυλάσσονται σχετικά με αυτό και, εάν κρίνεται αναγκαίο, να ζητά τη διόρθωσή τους. Περιορισμοί των δικαιωμάτων που κατοχυρώνονται με τη Σύμβαση μπορούν να τεθούν μόνον όταν διακυβεύεται υπέρτερο συμφέρον, όπως η εθνική ασφάλεια ή η εθνική άμυνα. [2]

Η Σύμβαση προβλέπει μεν την ελεύθερη ροή προσωπικών δεδομένων μεταξύ των συμβαλλόμενων μερών, πλην όμως επιβάλλει ορισμένους περιορισμούς προς κράτη η νομοθεσία των οποίων δεν παρέχει ισοδύναμη προστασία.

Με σκοπό την περαιτέρω ανάπτυξη των γενικών αρχών και κανόνων που θεσπίζονται με τη Σύμβαση 108, η Επιτροπή Υπουργών του ΣΤΕ έχει εκδώσει πλήθος μη δεσμευτικών συστάσεων (βλ. κεφάλαια 7 και 8).

Όλα τα κράτη μέλη της ΕΕ έχουν κυρώσει τη Σύμβαση 108. Το 1999, η Σύμβαση 108 τροποποιήθηκε ώστε να δοθεί η δυνατότητα προσχώρησης και στην ΕΕ. Το 2001 υιοθετήθηκε πρόσθετο πρωτόκολλο στη Σύμβαση 108, το οποίο θεσπίζει διατάξεις σχετικά με τη διασυνοριακή ροή δεδομένων προς μη συμβαλλόμενα μέρη, τις αποκαλούμενες «τρίτες χώρες», και σχετικά με την υποχρεωτική σύσταση εθνικών εποπτικών αρχών προστασίας των δεδομένων

[2] Πλαίσιο και εξέλιξη Ευρωπαϊκού δικαίου για τη προστασία προσωπικών δεδομένων

ΚΕΦΑΛΑΙΟ 2

2.1 Ο ΟΡΙΣΜΟΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Ο 21ος αιώνας χαρακτηρίζεται ως εποχή της πληροφορίας και της άνθησης του διαδικτύου .Αυτό έχει ως αποτέλεσμα την ολοένα μεγαλύτερη ανησυχία των χρηστών για τη διαχείριση των προσωπικών δεδομένων .
Η απελευθέρωση ιδιωτικών δεδομένων είναι γεγονός από τη στιγμή που επισκέπτονται ένα ισότοπο ή πραγματοποιούν κάποια συναλλαγή μέσω του διαδικτύου.
Η ιδιωτικότητα είναι μια έννοια που οι ρίζες της πηγάζουν εδώ και 2500 χρόνια όταν για πρώτη φορά ο Έλληνας φιλόσοφος Αριστοτέλης είχε εισάγει την έννοια της αρχαίας Αθήνα στο δοκίμιο του με τίτλο «Πολιτικά»
Για πρώτη φορά γίνεται ένας ξεκάθαρος διαχωρισμός μεταξύ των δημοσίων θεμάτων του δήμου που απασχολούν όλους τους πολίτες της πόλης και των ιδιωτικών θεμάτων του οίκου που απασχολούν μόνο τα άτομα ενός σπιτιού.
Στη συνέχεια οι Ρωμαίοι ανέπτυξαν ακόμα περισσότερο την ιδέα της ιδιωτικής ζωής σε σχέση με τη δημόσια ζωή κάθε ατόμου.
Στη ρωμαϊκή κοινωνία η έννοια της δημόσιας ζωής είναι συνδεδεμένη με το καλό του κράτους και τη πρόοδο της κοινωνίας ενώ η ιδιωτική ζωή αναφέρεται στα προσωπικά ενδιαφέροντα κάθε ατόμου στην αυτοκρατορία.
Οι έννοιες αυτές είχαν τόσο μεγάλη απήχηση και αποδοχή που συμπεριλήφθηκαν στο Ρωμαϊκό Δίκαιο το 533μ.χ.απο τον αυτοκράτορα Ιουστινιανό.
Επομένως για πρώτη φορά οι όροι «ιδιωτικό» και «δημόσιο »καταγράφονται από τους Ρωμαίους
Στη συνέχεια η έννοια της ιδιωτικότητας παρέμεινε στάσιμη και τίθεται στο περιθώριο μέχρι την εμφάνιση της αναγέννησης όπου το ενδιαφέρον ανανεώνεται. Έτσι η έννοια της ιδιωτικότητας αρχίζει σταδιακά να αναγνωρίζεται ως μια ανθρώπινη αξία. Πλέον γίνεται συστηματική προσπάθεια να κατοχυρωθεί νομικά και να προστατευθεί οπότε περνάμε σε μια νέα εποχή,[3]
Αυτής της νομιμοποίησης της ιδιωτικότητας.
Τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα τακτοποιημένο ή ταχτοποιήσαμε εν ζωή άτομο. Διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν επίσης δεδομένα προσωπικού χαρακτήρα.

Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα, έχουν κρυπτογραφηθεί ή για τα οποία έχουν χρησιμοποιηθεί ψευδώνυμα αλλά τα οποία μπορούν να χρησιμοποιηθούν για την επαναταυτοποίηση ενός ατόμου παραμένουν δεδομένα προσωπικού χαρακτήρα και εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ (Γενικού Κανόνα Προσωπικών Δεδομένων).

Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα με τέτοιον τρόπο ώστε το άτομο να μην είναι ή να μην είναι πια ταυτοποιήσιμο δεν θεωρούνται πλέον δεδομένα προσωπικού χαρακτήρα. Για να είναι πραγματικά ανώνυμα τα δεδομένα, η ανωνυμοποίηση πρέπει να είναι μη αντιστρέψιμη.

Ο ΓΚΠΔ προστατεύει τα δεδομένα προσωπικού χαρακτήρα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία τους. Είναι τεχνολογικά

[3] Κυριαζόγλου Ιωάννης σελ. 10

ουδέτερος και εφαρμόζεται τόσο στην αυτοματοποιημένη όσο και στη χειροκίνητη επεξεργασία, υπό την προϋπόθεση ότι τα δεδομένα οργανώνονται βάσει προκαθορισμένων κριτηρίων (π.χ. αλφαβητική σειρά). Επίσης, δεν έχει σημασία ο τρόπος που αποθηκεύονται τα δεδομένα – σε σύστημα τεχνολογίας πληροφοριών, μέσω βιντεοεπιτήρησης ή σε έντυπη μορφή. Σε όλες τις περιπτώσεις τα δεδομένα προσωπικού χαρακτήρα υπόκεινται στις απαιτήσεις προστασίας που προβλέπει ο ΓΚΠΔ.

Παραδείγματα δεδομένων προσωπικού χαρακτήρα:

- όνομα και επώνυμο·
- διεύθυνση κατοικίας·
- ηλεκτρονική διεύθυνση, π.χ. όνομα.επώνυμο@εταιρεία.com·
- αναγνωριστικός αριθμός κάρτας·
- δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο)*·
- διεύθυνση διαδικτυακού πρωτοκόλλου (IP)·
- αναγνωριστικό cookie*·
- το αναγνωριστικό διαφήμισης του τηλεφώνου σας·
- δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, που θα μπορούσαν να είναι ένα σύμβολο που προσδιορίζει αποκλειστικά ένα άτομο[4]

* Σε ορισμένες περιπτώσεις, υπάρχει ειδική νομοθεσία σχετικά με συγκεκριμένους τομείς που ρυθμίζει, για παράδειγμα, τη χρήση δεδομένων τοποθεσίας ή τη χρήση cookie – οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες [οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002 (ΕΕ L 201 της 31.7.2002, σ. 37) και κανονισμός (ΕΚ) αριθ. 2006/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Οκτωβρίου 2004 (ΕΕ L 364 της 9.12.2004, σ. 1)].

Παραδείγματα δεδομένων που δεν θεωρούνται δεδομένα προσωπικού χαρακτήρα:

- αριθμός μητρώου εταιρείας·
- ηλεκτρονική διεύθυνση του τύπου πληροφορίες@εταιρεία.com·
- ανώνυμα δεδομένα.[5]

2.2 Οι ραγδαίες τεχνολογικές εξελίξεις και οι ανάγκες προσαρμογής.

Με τη λήξη του Β παγκοσμίου πολέμου ιδρύθηκε το συμβούλιο της Ευρώπης με σκοπό την ίδρυση του κράτους δικαίου της δημοκρατίας και της υποστήριξη των ανθρωπίνων δικαιωμάτων .

Έτσι το 1950 υιοθέτησε την ευρωπαϊκή σύμβαση για τα δικαιώματα των ανθρώπων (ΕΣΔΑ) που τέθηκε σε ισχύ το 1953.

[4] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal- data_el
[5] ec.europa.eu

Το δικαίωμα όμως της προστασίας και της ιδιωτηκότητας του ανθρώπου ξεκινάει να κατοχυρώνεται σε διεθνές νομικό πλαίσιο το 1948 στο άρθρο 12 της Οικουμενικής διακήρυξης των Ηνωμένων εθνών για τα ανθρώπινα δικαιώματα

Από τη δεκαετία του 1960 και μετά και με τις συνεχείς επεκτάσεις και πρόοδο των τεχνολογιών πληροφορικής ,λογισμικού, υπολογιστών, smartphone και επικοινωνιών οι επιχειρήσεις και οι κυβερνητικοί οργανισμοί χρησιμοποιούν αυτές τις τεχνολογίες και αποθηκεύουν όλο και περισσότερο αυτές τις προσωπικές πληροφορίες και τα ευαίσθητα δεδομένα τόσο σε ηλεκτρονικές βάσεις δεδομένων όσο και σε διαφορά ψηφιακά μέσα.

Ειδικά αυτές οι βάσεις δεδομένων μπορούν να τις πλησιάσουν άμεσα και μέσω της εκτέλεσης προγραμμάτων αναζήτησης και συγκεκριμένων εντολών να αναζητηθούν γρήγορα να επεξεργασθούν συνοπτικά και να δημιουργηθούν δεδομένα προφίλ και στη συνέχεια μα κοινοποιηθούν σε εταιρείες και οργανισμούς σε όλα τα μήκη και πλάτη της γης.

Τα διάφορα ερωτήματα σχετικά με το τι συνέβαινε με τις πληροφορίες και τι με τη συλλογή προσωπικών στοιχείων από επιχειρήσεις και οργανισμούς ξεκίνησαν με τη διαχείριση συλλογή, επεξεργασία και τη μετάδοση των δεδομένων που πολλές φορές έβλεπαν οι άνθρωποι να διαρρέουν χωρίς την συγκατάθεση τους .

Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων προσωπικού χαρακτήρα (GDPR) 2016/679 υπήρξε προϊόν της ανάγκης για προσαρμογή στις ραγδαίες τεχνολογικές εξελίξεις.

Από τη μία πλευρά, όπως χαρακτηριστικά έχει ειπωθεί, τα προσωπικά δεδομένα αποτελούν το νέο «χρήμα».

Ως εκ τούτου η διακίνηση και η κυκλοφορία τους όχι μόνο θεωρείται απαραίτητη αλλά έχει αποτελέσει και βασικό πυλώνα στην Στρατηγική της Επιτροπής για μία Ψηφιακή Ατζέντα για την Ευρώπη.

Από την άλλη, ακριβώς λόγω των αστείρευτων δυνατοτήτων των νέων τεχνολογιών να διασταυρώνουν και να συλλέγουν προσωπικά δεδομένα, τα φυσικά πρόσωπα (υποκείμενα δεδομένων) βρίσκονται αντιμέτωπα με μία ολοένα και μεγαλύτερη κατάλυση της ιδιωτικότητας τους.Ο GDPR έρχεται να εξισορροπήσει την αδύναμη θέση στην οποία εκ των πραγμάτων βρίσκονται τα υποκείμενα δεδομένων, παρέχοντάς τους πλέον πολύ περισσότερα

δικαιώματα σε σχέση με όσα είχαν υπό το προηγούμενο καθεστώς της Οδηγίας 95/46/ΕΕ και επιβάλλοντας αντίστοιχα σε όσους συλλέγουν και επεξεργάζονται τα δεδομένα αυτά πολύ περισσότερες και πολύ αυστηρότερες υποχρεώσεις προκειμένου η επεξεργασία των δεδομένων να είναι σύννομη.[6]

Ο GDPR είναι ένα πολυσέλιδο, πολύπλοκο και βαθιά τεχνικό νομοθέτημα, του οποίου η ανάγνωση και εφαρμογή ως εκ τούτου απαιτεί την εμπλοκή αφενός σωστά καταρτισμένων σχετικά με το ηλεκτρονικό δίκαιο νομικών και αφετέρου τη στενή συνεργασία τους τόσο με τους επικεφαλής των διαφόρων επιχειρήσεων που επεξεργάζονται δεδομένα όσο και με ειδικούς επιστήμονες της πληροφορικής, οι οποίοι φέρουν το βάρος να θωρακίσουν τεχνικά την επιχείρηση εξασφαλίζοντας το μέγιστο βαθμό προστασίας των δεδομένων που αυτή επεξεργάζεται. Το γεγονός, μάλιστα, ότι οι επιχειρήσεις που χρησιμοποιούν ιστοσελίδες και ηλεκτρονικά

[6] https://www.euro2day.gr/specials/opinions/article/1615180/gdpr-grifos-h- eykairia.html

καταστήματα αυξάνονται με γεωμετρική πρόοδο δημιουργεί επιπρόσθετα ζητήματα σχετικά τόσο με τη σύννομη λειτουργία των ιστοσελίδων όσο και την επεξεργασία δεδομένων online.
Ασφαλώς η πολυπλοκότητα του GDPR, σε συνδυασμό με το υπόλοιπο πλέγμα κανόνων για το ηλεκτρονικό δίκαιο, θα μπορούσε κανείς να σκεφτεί ότι δημιουργεί στις επιχειρήσεις επιπλέον «πονοκεφάλους», καθώς τις εξαναγκάζει να υποβληθούν σε περαιτέρω έξοδα για τη συμμόρφωσή τους, υπό την απειλή δυσβάστακτων προστίμων και κυρώσεων που μπορεί να φτάσουν στην οικονομική τους εξόντωση. Ταυτόχρονα, όμως, η ίδια αυτή πίεση για συμμόρφωση εξασφαλίζει ορθότερες δομές μέσα στην επιχείρηση, συντείνει στην πιο εύρυθμη λειτουργία της και εν τέλει αποτελεί ένα σημαντικότατο εργαλείο στην κούρσα της ανταγωνιστικότητας καθώς η σωστά οργανωμένη έναντι των προσωπικών δεδομένων επιχείρηση είναι βέβαιο ότι τάχιστα θα ξεχωρίσει για την ποιότητά της και θα έχει την ευκαιρία να αυξήσει την πελατεία της καθώς όλο και περισσότερο τα υποκείμενα των δεδομένων θα ενδιαφέρονται για την προστασία της ιδιωτικότητας τους.
Δυστυχώς βέβαια σε αντίθεση με άλλες ευρωπαϊκές χώρες όπου το Κράτος ανέλαβε εγκαίρως να ενημερώσει επιχειρήσεις και φυσικά πρόσωπα εκτενώς σχετικά με τον GDPR, στην Ελλάδα έως τώρα από επίσημους κρατικούς φορείς δεν έχει γίνει το παραμικρό με αποτέλεσμα πολλές επιχειρήσεις τις οποίες θίγει άμεσα ο Κανονισμός από την ημερομηνία θέσης του σε ισχύ την 25η Μαΐου του 2018 είτε να μην γνωρίζουν καθόλου ότι επηρεάζονται είτε να μην γνωρίζουν πώς πρέπει να αντιδράσουν είτε, τέλος, να θεωρούν ότι οι αλλαγές στο επιχειρηματικό τοπίο δεν θα είναι και τόσο σοβαρές.Το παρόν δεν φιλοδοξεί φυσικά να καλύψει, εντός ολίγων γραμμών, ολόκληρο το καθεστώς που εισάγει ο Κανονισμός. Έχει απλώς σκοπό να αναδείξει μερικά από τα βασικά δικαιώματα των φυσικών προσώπων και αντίστοιχα τις υποχρεώσεις των επιχειρήσεων προκειμένου οι τελευταίες να συνειδητοποιήσουν το βάρος που καλούνται να σηκώσουν και να έχουν έτσι το έναυσμα να αναζητήσουν το δυνατό γρηγορότερο τα κενά τους και να τα εξαλείψουν.[7]

[7] https://www.euro2day.gr/specials/opinions/article/1615180/gdpr-grifos-h-eykairia.html

ΚΕΦΑΛΑΙΟ 3

3.1 ΟΙ ΣΥΝΘΗΚΕΣ ΠΟΥ ΟΔΗΓΗΣΑΝ ΣΤΗΝ ΑΝΑΓΚΗ ΓΙΑ ΤΟ ΝΕΟ ΚΑΝΟΝΙΣΜΟ

Η Αναγκαιότητα των προσωπικών δεδομένων ήταν κάτι που είχε απασχόληση την Ευρωπαϊκή Ένωση από το ξεκινήματά της.

Η εξασφάλιση των προσωπικών δεδομένων θεωρήθηκε υποχρέωση τη από το 1995 που ο Ευρωπαίος νομοθέτης εισήγαγε σημαντικές υποχρεώσεις στα κράτη μέλη θέτοντας σε εφαρμογή την οδηγία 95/46 ΕΚ διασφαλίζοντας αφενός τη φυσική προστασία των προσώπων και αφετέρου την εξασφάλιση και την ελεύθερη κυκλοφορία των δεδομένων αυτών ως μέσω επίτευξης οικονομικής και κοινωνικής προόδου.

Ωστόσο, δυο καθοριστικές παράμετροι κατέστησαν αναγκαία τη μεταρρύθμιση του κανονιστικού πλαισίου, όπως αυτή εκφράστηκε με τον νέο Κανονισμό, καθώς τα μετρά πολιτικής που ισχύσαν μέχρι σήμερα εξάντλησαν την οποία αποτελεσματικότητα τους.

Η πρώτη, αφορά στις ραγδαίες τεχνολογικές εξελίξεις που έλαβαν χώρα, αλλάζοντας τον κόσμο όπως τον ξέραμε και καθιστώντας την Οδηγία παρωχημένη.

Η δεύτερη αφορά στην ασυμμετρία εφαρμογής της Οδηγίας από τα κράτη- μέλη, αλλά και τελικά στο έλλειμμα προστασίας της ιδιωτικότητας που φάνηκε στην πράξη.

Παράμετροι που οδήγησαν στην ανάγκη για νέο κανονισμό

Ραγδαίες τεχνολογικές εξελίξεις	- Αύξηση της έκτασης και έντασης της συλλογής, ανταλλαγής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα - - Αύξηση περιπτώσεων παραβίασης της ασφάλειας δεδομένων προσωπικού χαρακτήρα
Ασυμμετρία εφαρμογής της οδηγίας 95/46 ΕΚ από τα κράτη μέλη	• Ανασφάλεια δίκαιου - Αποκλίσεις κατά την εκτέλεση και εφαρμογή • - Στρέβλωση του ανταγωνισμού μεταξύ κρατών- μελών

Την εξέλιξη του διαδικτύου και της τεχνολογίας ήταν λίγοι εκείνοι που θα μπορούσαν να προβλέψουν. Το 1995 όταν θεσπίστηκε η οδηγία 95/46ΕΚ.
Σε λίγα μόλις χρόνια οι ραγδαίες τεχνολογικές εξελίξεις οδήγησαν στην αύξηση της έκτασης και έντασης της συλλογής, ανταλλαγής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα από ιδιωτικές επιχειρήσεις και δημοσιές αρχές με γεωμετρική πρόοδο.
Η Ευρωπαϊκή Επιτροπή προτείνει μια συνολική μεταρρύθμιση των κανόνων της ΕΕ για την προστασία των δεδομένων του 1995 για την ενίσχυση των δικαιωμάτων διαδικτυακής ιδιωτικότητας και την ενίσχυση της ψηφιακής οικονομίας της Ευρώπης.

Ενδεικτικό είναι το γεγονός ότι η Ευρωπαϊκή Επιτροπή επισήμανε την ανάγκη τροποποίησης της Οδηγίας από τον Ιανουάριο του 2012, το Ευρωπαϊκό Κοινοβούλιο υπερψήφισε το σχέδιο Κανονισμού το Μάρτιο του 2014 και η τελική συμφωνία μεταξύ του Κοινοβουλίου, της Επιτροπής και του Συμβουλίου επήλθε το Δεκέμβριο του 2015. Ο Κανονισμός ψηφίστηκε το Μάιο του 2016 και δόθηκε διετής περίοδος προσαρμογής στα κράτη-μέλη έως το Μάιο του 2018.

Το ΕΚ, το Συμβούλιο και η ΕΚ καταλήγουν σε συμφωνία για το GDPR - 15/12/2015

- Η ομάδα εργασίας του άρθρου 29 εκδίδει σχέδιο δράσης για την εφαρμογή του GDPR - 02/02/2016

Το GDPR ενισχύει ένα ευρύ φάσμα υφιστάμενων δικαιωμάτων και θεσπίζει νέα για τα άτομα. Αυτά περιλαμβάνουν τα εξής:

1. Δικαίωμα φορητότητας δεδομένων: Έχετε το δικαίωμα να λαμβάνετε τα προσωπικά σας δεδομένα από έναν οργανισμό σε μια συνήθη μορφή, ώστε να μπορείτε εύκολα να το μοιράζεστε με κάποιον άλλο.
2. Δικαίωμα να μην αποθηκεύεται το προφίλ: Εκτός αν αυτό είναι απαραίτητο από το νόμο ή από μια σύμβαση, οι αποφάσεις που επηρεάζουν εσάς δεν μπορούν να γίνουν μόνο στη βάση της αυτοματοποιημένης επεξεργασίας.

- Ο κανονισμός τίθεται σε ισχύ, 20 ημέρες μετά τη δημοσίευσή του στην Επίσημη Εφημερίδα της ΕΕ - 24/05/2016

Το GDPR ενισχύει ένα ευρύ φάσμα υφιστάμενων δικαιωμάτων και θεσπίζει νέες για τα άτομα, μεταξύ των οποίων:

Το δικαίωμα διαγραφής (δικαίωμα στη λήθη) . Μπορείτε να ζητήσετε από έναν οργανισμό να διαγράψει τα προσωπικά σας δεδομένα, για παράδειγμα όταν τα δεδομένα σας δεν είναι πλέον απαραίτητα για τους σκοπούς για τους οποίους συλλέχθηκαν ή για τους οποίους έχετε αποσυρθεί από τη συγκατάθεσή σας.

- Το ΕΚ προτείνει δύο νέους κανονισμούς για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες καθώς και για τους κανόνες προστασίας δεδομένων που ισχύουν για τα θεσμικά όργανα της ΕΕ - 10/01/2017

Η Ευρωπαϊκή Επιτροπή προτείνει δύο νέους κανονισμούς σχετικά με την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες (ePrivacy) και τους κανόνες προστασίας δεδομένων που ισχύουν για τα θεσμικά όργανα της ΕΕ (επί του παρόντος κανονισμός 45/2001) που ευθυγραμμίζουν τους ισχύοντες κανόνες με το GDPR.

- Οδηγία για την προστασία των δεδομένων για την αστυνομία και τη δικαιοσύνη στην εθνική νομοθεσία που εφαρμόζεται από σήμερα - 06/05/2018[8]

Είναι χαρακτηριστικό ότι έως το 2025 εκτιμάται ότι ο όγκος των δεδομένων θα αυξηθεί από 16,1 ZB σε 163 ZB[9] σύμφωνα με τη μελέτη της εταιρείας επιχειρηματικής πληροφόρησης International Data Corporetion [10]
Η τεχνολογική εξέλιξη δεν άνοιξε μια αναπτυσσόμενη αγορά προσωπικών δεδομένων που απλά έκανε μόνο εύκολη τη συγκέντρωση και την επεξεργασία ,για τη σωστή χρήση τους ,αλλά ταυτόχρονα διευκόλυνε και αυτούς που αποσκοπούσαν στη παραβίαση τους.

3.2 ΚΑΝΟΝΙΣΜΟΣ 679/2016

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 16 Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Μετά από διαβίβαση του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής (1),

Έχοντας υπόψη τη γνώμη της Επιτροπής των Περιφερειών (2),

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία (3),

Εκτιμώντας τα ακόλουθα:
Η προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι θεμελιώδες δικαίωμα. Το άρθρο 8 παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης («Χάρτης») και το άρθρο 16 παράγραφος 1 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης [11]
Ο νέος γενικός κανονισμός ΕΕ2016/679 του ΕΥΡΩΠΑΙΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ και του Συμβουλίου της 27ης Απρίλιου 2016 για τη «προστασία των φυσικών προσωπικών έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για την ελεύθερη κυκλοφορία των δεδομένων αυτών ακουμπάει πάνω στις γενικές αρχές του προηγουμένου πλαισίου προστασίας προσωπικών δεδομένων αλλά παράλληλα προσπαθεί να δημιουργεί
Ένα πιο αυστηρό θεσμικό πλαίσιο επεξεργασίας προσωπικών δεδομένων .Τα νέα χαρακτηριστικά του κανονισμού είναι η ριζική αλλαγή στο τρόπο που οι εταιρείες θα συλλέγουν και θα επεξεργάζονται τα προσωπικά δεδομένα .Επίσης ο νέος κανονισμός επιβάλει την συναίνεση του υποκείμενου των δεδομένων για κάθε χρήση και κάθε σκοπό.

[8] http://www.epixeiro.gr/article/86602

[9] 1ZB = 10^{21} **bytes Όγκος δεδομένων που δημιουργούνται ανά έτος, σε zettabytes**

[10] https://segm.gr/wp-content/uploads/2018/10/meleti_sev_GDPR_final.pdf
[11] http://www.dpa.gr/portal/page?_pageid=33,213319&_dad=portal&_schema

Με τον νέο Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ) 2016/679 που τίθεται σε εφαρμογή στις 25 Μαΐου 2018, καθιερώνεται ενιαίο νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων σε όλα τα κράτη μέλη της ΕΕ.

Βασικά δικαιώματα των πολιτών

1. Δικαίωμα ενημέρωσης και πρόσβασης στα δεδομένα: Θα έχετε περισσότερη και σαφέστερη ενημέρωση κατά τη συλλογή των δεδομένων για την επεξεργασία τους και το δικαίωμα πρόσβασης σε αυτά.
2. Δικαίωμα διόρθωσης: Έχετε το δικαίωμα να απαιτήσετε από τον υπεύθυνο επεξεργασίας τη διόρθωση ανακριβών δεδομένων καθώς και τη συμπλήρωση ελλιπών δεδομένων που σας αφορούν.
3. Δικαίωμα περιορισμού της επεξεργασίας: Δικαιούστε να εξασφαλίζετε από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας υπό συγκεκριμένες προϋποθέσεις.
4. Δικαίωμα εναντίωσης στην επεξεργασία: Έχετε το δικαίωμα να αντιταχθείτε στην επεξεργασία των δεδομένων σας υπό συγκεκριμένες προϋποθέσεις, ιδίως όταν πρόκειται για κατάρτιση «προφίλ» ή για σκοπούς απευθείας εμπορικής προώθησης.
5. Δικαίωμα στη λήθη: Όταν δεν επιθυμείτε πλέον την επεξεργασία και διατήρηση προσωπικών σας δεδομένων, έχετε το δικαίωμα να ζητήσετε τη διαγραφή τους, υπό την προϋπόθεση ότι τα δεδομένα δεν τηρούνται για κάποιο συγκεκριμένο νόμιμο και δηλωμένο σκοπό.
6. Δικαίωμα στη φορητότητα των δεδομένων: Δικαιούστε να λάβετε ή να ζητήσετε τη μεταφορά των δεδομένων σας, σε μια αναγνώσιμη μορφή, από έναν υπεύθυνο επεξεργασίας σε άλλον υπό συγκεκριμένες προϋποθέσεις, εφόσον το επιθυμείτε.

3.3 Βασικές υποχρεώσεις για τους υπευθύνους επεξεργασίας

Ο νέος Κανονισμός επιβάλλει μια σειρά νέων υποχρεώσεων στους υπεύθυνους επεξεργασίας, οι οποίες απορρέουν από τις βασικές αρχές και ιδίως την ενισχυμένη αρχή της διαφάνειας στον τρόπο συλλογής, επεξεργασίας και τήρησης δεδομένων και τη νέα αρχή της λογοδοσίας, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας

φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωσή του με όλες τις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων:

- Ευθύνη: Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη να αποδεικνύει ότι λαμβάνει όλα τα κατάλληλα οργανωτικά και τεχνικά μέτρα προστασίας των προσωπικών δεδομένων και ότι συμμορφώνεται με τον Κανονισμό.
- Προστασία δεδομένων κατά τον σχεδιασμό («Data protection by design»): Ο Κανονισμός επιβάλλει την εφαρμογή προϊόντων και υπηρεσιών (ηλεκτρονικών και μη) που κατά τον αρχικό σχεδιασμό τους δημιουργούν φιλικές συνθήκες για την προστασία των δεδομένων σας. Για παράδειγμα, στις υπηρεσίες ηλεκτρονικής κοινωνικής δικτύωσης πρέπει να σας δίνεται η δυνατότητα να επιλέγετε ρυθμίσεις που θα προστατεύουν περισσότερο τα προσωπικά σας δεδομένα.
- Προστασία δεδομένων εξ ορισμού («Data protection by default»): Ο Κανονισμός επιβάλλει την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων που να διασφαλίζουν ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για τον σκοπό της επεξεργασίας.
- Ασφάλεια επεξεργασίας: Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία πρέπει να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το ενδεδειγμένο επίπεδο ασφάλειας.
- Γνωστοποίηση παραβιάσεων δεδομένων: Ο υπεύθυνος επεξεργασίας έχει υποχρέωση, μόλις αντιληφθεί παραβίαση, να ενημερώσει τις αρμόδιες εποπτικές Αρχές και εσάς, εφ' όσον η παραβίαση σάς θέτει σε σοβαρό κίνδυνο.
- Εκτίμηση επιπτώσεων και προηγούμενη διαβούλευση: Όταν η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα των ατόμων, ιδίως επειδή είναι συστηματική, μεγάλης κλίμακας, αφορά ειδικές κατηγορίες δεδομένων και βασίζεται στη χρήση νέων τεχνολογιών, ο υπεύθυνος επεξεργασίας πρέπει να διενεργήσει εκτίμηση επιπτώσεων σχετικά με την προστασία των δεδομένων (Data protection impact assessment). Όταν βάσει της διενεργηθείσας εκτίμησης επιπτώσεων και παρά την πρόβλεψη μέτρων προστασίας παραμένει υψηλή επικινδυνότητα της επεξεργασίας, ο υπεύθυνος επεξεργασίας υποχρεούται να προβεί σε προηγούμενη διαβούλευση με την εποπτική Αρχή.
- Υπεύθυνος προστασίας δεδομένων: Προβλέπεται, υπό προϋποθέσεις, ο ορισμός «υπευθύνου προστασίας δεδομένων» ο οποίος έχει εχέγγυα ανεξαρτησίας και παρακολουθεί τη συμμόρφωση με τον νόμο αποτελώντας, συγχρόνως, το σημείο επαφής με την εποπτική Αρχή.
- Κώδικες δεοντολογίας: Ενθαρρύνεται η εκπόνηση κωδίκων δεοντολογίας από τους υπεύθυνους επεξεργασίας, οι οποίοι υποβάλλονται προς έγκριση στην εποπτική Αρχή. Σε περίπτωση διευρωπαϊκής δραστηριότητας ζητείται και η γνώμη του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων.
- Πιστοποίηση: Ενθαρρύνεται η θέσπιση μηχανισμών πιστοποίησης, σφραγίδων και σημάτων προστασίας δεδομένων για την απόδειξη της συμμόρφωσης προς τον Κανονισμό ή για την απόδειξη παροχής κατάλληλων εγγυήσεων κατά την επεξεργασία. Πιστοποίηση: Ενθαρρύνεται η θέσπιση μηχανισμών πιστοποίησης, σφραγίδων και σημάτων προστασίας δεδομένων για την απόδειξη της συμμόρφωσης προς τον Κανονισμό ή για την απόδειξη παροχής κατάλληλων εγγυήσεων κατά την επεξεργασία. Η πιστοποίηση είναι εθελοντική. Σίγουρα αποτελεί ένα βήμα στη προστασία και την ιδιωτικότητα του ανθρώπου μέσω της νομικής προστασίας[12]. Ο κανονισμός έχει στόχο τη προστασία των φυσικών προσώπων ενάντια στην ανεξέλεγκτη κυκλοφορία

[12] http://www.dpa.gr/portal/page?_pageid=33,209418&_dad=portal&_schema

των προσωπικών στοιχείων και δεδομένων .Αυτές αποτελούν τον γενικό κανονισμό προστασίας δεδομένων ο οποίος είναι η επέκταση του Directive 95/46/EC και συνιστά ένα νομοθέτημα άμεσης εφαρμογής των εθνικών νομοθεσιών των κρατών μελών για τη προστασία προσωπικών δεδομένων ,χωρίς να χρειάζεται να εισαχθεί με νομό στην εσωτερική έννομη τάξη. Επιβάλλει δε πολύ αυστηρά πρόστιμα για τη συμμόρφωση με τους κανόνες προστασίας προσωπικών δεδομένων στις επιχειρήσεις που τον παραβιάζουν έως και 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών (τζίρος)του προηγουμένου οικονομικού έτους .

Γι' αυτό όλες οι επιχειρήσεις και οι οργανισμοί θα πρέπει να εξετάσουν το τρόπο που θα συλλέγουν, θα διαχειρίζονται, θα αποθηκεύουν και θα χρησιμοποιούν τα προσωπικά δεδομένα με καλύτερο τρόπο και τι μέτρα (πολιτικές διαδικασίες και πρακτικές) θα εφαρμόζουν ώστε να συμμορφώνονται πιο αποτελεσματικά με το σχετικό πλαίσιο προστασίας δεδομένων και σε κρατικό Ευρωπαϊκό αλλά και διεθνές επίπεδο.[13]

3.4 ΑΠΑΡΑΙΤΗΤΗ Η ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η έννοια «προστασία προσωπικών δεδομένων » περιγράφει τους βασικούς όρους και αιτίες για τη προστασία και το απόρρητο των προσωπικών δεδομένων που συλλέγονται και υποβάλλονται σε επεξεργασία όπου αποθηκεύονται και διαβιβάζονται από επιχειρήσεις και οργανισμούς

Κάθε φορά που αγοράζουμε ένα προϊόν από ένα ηλεκτρονικό κατάστημα χρησιμοποιείται μια υπηρεσία που σε on line σύνδεση κάνουμε εγγραφή και ανοίγουμε λογαριασμό με όλα μας τα προσωπικά στοιχεία.

Το ίδιο συμβαίνει όταν πληρώνουμε λογαριασμούς η όταν συμπληρώνουμε οποιοδήποτε αίτηση σε δημόσιο η ιδιωτικό τομέα, καταγράφουμε όλα τα προσωπικά μας στοιχεία .

Τα στοιχεία αυτά ακόμη και χωρίς την ρητή γνώση ή έγκριση μας οι πληροφορίες με τα προσωπικά μας στοιχεία καταγράφονται από επιχειρήσεις, νοσοκομεία, εταιρίες οργανισμούς δημόσιους και ιδιωτικούς που είναι πιθανό να μην έχουμε ποτέ επικοινωνήσει εν γνώση μας.

Ο μονός τρόπος που οι καταναλωτές, οι πολίτες και οι πελάτες μπορούν να έχουν εμπιστοσύνη τόσο στο κράτος όσο και στις ιδιωτικές επιχειρήσεις είναι η εφαρμογή και η ισχύ της εφαρμογής των μέτρων για τη προστασία προσωπικών δεδομένων που έχουν θέσει μέσω της νομοθεσίας για να βοηθήσει στην ελαχιστοποίηση της παρακολούθησης μας από τις κρατικές αρχές και να ρυθμίζει την εποπτεία των εταιρειών σχετικά με τα δεδομένα [14]

Η προστασία των προσωπικών δεδομένων παρέχει τη διαφύλαξη και τη προστασία του θεμελιώδους δικαιώματος στη ιδιωτική ζωή η οποία κατοχυρώνεται με τις διεθνείς διατάξεις νόμων και κανονισμών όπως ο γενικός κανονισμός για τη

[13] Κυριαζόγλου Ιωάννης σελ. 14
[14] Κυριαζόγλου Ιωάννης σελ. 14

προστασία δεδομένων της Ευρωπαϊκής ένωσης παράτημα 1 αλλά και σε άλλους εθνικούς νόμους πρότυπα κώδικες και συμβάσεις .

Η προστασία δεδομένων ορίζεται ως η νομοθεσία για τη προστασία των προσωπικών σας δεδομένων τα οποία συλλέγονται, διαχειρίζονται επεξεργάζονται και αποθηκεύονται ηλεκτρονικά ή αυτοματοποιημένα μέσα και τεχνολογικές (computerized or automated system,(digital media)ή και με διαδικασίες ενός χειροκίνητου συστήματος αρχειοθέτησης (manual Systems) .Στις σύγχρονες κοινωνίες και στις σύγχρονες οικονομίες του 21^{ου} αιώνα η δυνατότητα να ελεγχθούν οι πληροφορίες και να προστατευθούν από τους διάφορους κινδύνους θα είναι σημαντικό να υπάρχουν νόμοι που να προστατεύουν τα προσωπικά δεδομένα ώστε να προστατεύσουν και να συγκρατήσουν τις δραστηριότητες των επιχειρήσεων ,των οργανισμών ,εταιρειών και κυβερνήσεων.

Όλοι αυτοί οι θεσμοί μας έχουν δείξει κατ' επανάληψη ότι εάν οι κανόνες και οι νόμοι δεν περιορίζουν τις ενέργειες τους, θα προσπαθήσουν ενδεχομένως να συλλέξουν και να διαχειρίζονται προσωπικά δεδομένα , χωρίς να ενημερωνόμαστε γι' όλα αυτά σε αρκετές περιπτώσεις.[15]

3.5 Τα βασικά χαρακτηριστικά και οι κύριες αλλαγές του κανονισμού

Α) Η γενική εφαρμογή αφορά τις επιχειρήσεις του ιδιωτικού τομέα ανεξαρτήτου μεγέθους και χώρο που δραστηριοποιούνται ,αλλά και φορείς του Δημοσίου

Β) Είναι άμεσα εφαρμοστέος με ημερομηνία εφαρμογής 25/5/2018

Γ) Παρουσιάζει κάποια χαρακτηριστικά οδηγίας καθώς αφήνει στη διακριτική ευχέρεια ορισμένων κρατών – μελών ορισμένα σημεία για περαιτέρω διευκρίνηση

Δ) Προβλέπει υψηλά διοικητικά πρόστιμα (έως 20 εκ. ή έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών , ανάλογα με το ποιο είναι το ψηλότερο) ανάλογα με το είδος της παραβίασης των διατάξεων του κανονισμού.

Ε) Αποτέλεσε αντικείμενο έντονο και πολυετών διαπραγματεύσεων μεταξύ των διαφορετικών ομάδων συμφερόντων και τελικά πρόκειται

για ένα «προϊόν » συμβιβασμού που αποδεικνύει η σπουδαιότητα και τις οικονομικές του επεκτάσεις.

ΚΥΡΙΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

- ✓ Γενική εφαρμογή σε όλες τις επιχειρήσεις ανεξαρτήτως μεγέθους και κλάδου δραστηριοποίησης σε ιδιωτικούς και δημοσίους φορείς
- ✓ Αμετάκλητη ημερομηνία έναρξης ε εφαρμογής 25/5/2018
- ✓ Αρκετές διατάξεις στη διακριτική ευχέρεια των κρατών μελών για περεταίρω εξειδίκευση
- ✓ Υψηλά διοικητικά πρόστιμα

[15] Κυριαζόγλου Ιωάννης σελ19

- ✓ Έντονες και πολυετείς διαπραγματεύσεις για το τελικό κείμενο [16]

Ο Κανονισμός επιφέρει σημαντικές αλλαγές στο ρυθμιστικό περιβάλλον για τους υπευθύνους επεξεργασίας δεδομένων, δηλαδή για τις επιχειρήσεις και τους δημοσίους φορείς, κυρίως σε τρία επίπεδα:

α) έχει ως κεντρική λογική την ελαχιστοποίηση της συλλογής, διατήρησης και επεξεργασίας δεδομένων προσωπικού χαρακτήρα,

β) επιδιώκει την ενίσχυση της προστασίας των προσωπικών δεδομένων, αναθεωρώντας τις υποχρεώσεις όλων όσοι επεξεργάζονται δεδομένα, καθώς πλέον, οι επονομαζόμενοι «Υπεύθυνοι Επεξεργασίας» αλλά και οι «Εκτελούντες την Επεξεργασία» για λογαριασμό των «Υπευθύνων» φέρουν το βάρος της απόδειξης της συμμόρφωσης στις διατάξεις του Κανονισμού και

γ) ανανεώνει και ενισχύει τα δικαιώματα των υποκειμένων , των ιδιοκτήτων δηλαδή προσωπικών δεδομένων, γεγονός στο οποίο οφείλουν να προσαρμοστούν οι υπεύθυνοι επεξεργασίας αλλά και οι «Εκτελούντες την Επεξεργασία» για λογαριασμό των «Υπευθύνων» και συνεπώς να μεταβάλλουν ανάλογα τη λειτουργία και τις αποφάσεις τους.

Εν συντομία, ο Κανονισμός αποτελεί ένα κοινό πλαίσιο ρυθμίσεων για τον τρόπο με τον οποίο συλλέγονται, επεξεργάζονται, φυλάσσονται, διακινούνται, αξιοποιούνται, αλλά και καταστρέφονται, δεδομένα προσωπικού χαρακτήρα των πολιτών της ΕΕ, ανεξαρτήτως του τόπου διαμονής τους, τόσο σε ηλεκτρονική όσο και σε φυσική μορφή.

Ταυτίζεται συνεπώς με πολίτικες και διαδικασίες της επιχείρησης (π.χ. για τις συμβάσεις, τη διεξαγωγή διαγωνισμών, την εξυπηρέτηση πελατών), με υποδομές και συστήματα που χρησιμοποιούνται (π.χ. Servers, ηλεκτρονικό ταχυδρομείο, USB sticks, CRM, POS), με πράξεις αυτοδέσμευσης της διοίκησης (π.χ. Κώδικες Δεοντολογίας και συστήματα πιστοποίησης), με το ανθρώπινο δυναμικό (π.χ. διαδικασίες προσλήψεων, συμβάσεις προσωπικού, ομαδικά συμβόλαια ασφάλισης, βιογραφικά σημειώματα και συνεντεύξεις), αλλά κυρίως με την κουλτούρα της επιχείρησης. Δηλαδή αποτελεί έναν εναλλακτικό τρόπο οργάνωσης και λειτουργιάς της επιχείρησης που θέτει στο επίκεντρο τη διαφύλαξη των προσωπικών δεδομένων.
για να ακριβολογούμε, που θέτει στο επίκεντρο την ικανότητα να αποδείξει η επιχείρηση με τεκμήρια ούτι κατά τη λειτουργία της λαμβάνει όλα τα αναγκαία μέτρα για να διαφυλάξει τα προσωπικά δεδομένα. Τα υψηλά πρόστιμα που προβλέπονται σε περίπτωση μη συμμόρφωσης καθιστούν επιτακτική την ανάγκη κατανόησης των νέων απαιτήσεων και επομένως η εξασφάλιση της συμμόρφωσης αποτελεί κρίσιμη διαδικασία για κάθε επιχείρηση. [17]

[16] Από την επίσημη ιστοσελίδα της Επιτροπής https://europa.eu/european-union/eu-law/legal-acts_en

[17] https://segm.gr/wp-content/uploads/2018/10/meleti_sev_GDPR_final.pdf

ΚΕΦΑΛΑΙΟ 4

4.1 DPO Γενικός Κανονισμός για την προστασία Προσωπικών Δεδομένων

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων εισάγει για πρώτη φορά αναλυτικές διατάξεις για τον ρόλο, τις παρεχόμενες εγγυήσεις και τα καθήκοντα του Υπευθύνου Προστασίας Δεδομένων (άρθρα 37-40), ο οποίος βρίσκεται πλέον στο επίκεντρο του νέου νομικού πλαισίου.

Ειδικότερα, ορίζεται ότι υπό συγκεκριμένες προϋποθέσεις, ορισμένοι υπεύθυνοι αλλά και εκτελούντες την επεξεργασία υποχρεούνται πλέον να ορίζουν υπεύθυνο προστασίας δεδομένων.

Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) διευκολύνει τη συμμόρφωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία με τις διατάξεις του ΓΚΠΔ και μεσολαβεί μεταξύ των διαφόρων ενδιαφερομένων (π.χ. εποπτικές αρχές, υποκείμενα των δεδομένων). Ο ρόλος του είναι συμβουλευτικός (όχι αποφασιστικός) και δεν φέρει προσωπική ευθύνη για τη μη συμμόρφωση με τον Κανονισμό.

Υπεύθυνος να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία.

Προβλέπονται συγκεκριμένα καθήκοντα του DPO και αντίστοιχες υποχρεώσεις του εργοδότη του. Παράβαση των σχετικών με τον DPO διατάξεων επιφέρει κυρώσεις (βλ. άρθρα 37-38 και 83 σε συνδυασμό με αιτιολογική σκέψη 97 ΓΚΠΔ).

Τέλος, ορίζεται ρητά ότι τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων πρέπει να δημοσιοποιούνται προκειμένου να διασφαλίζεται η απρόσκοπτη επικοινωνία με τα υποκείμενα των δεδομένων.

Επιπλέον, προβλέπεται υποχρέωση για τον υπεύθυνο και εκτελούντα την επεξεργασία να ανακοινώνουν στην εποπτική αρχή στοιχεία που αφορούν στον ορισμό του υπευθύνου προστασίας δεδομένων.[18]

Ο DPO μπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία (εσωτερικός υπεύθυνος προστασίας δεδομένων) ή να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών (εξωτερικός συνεργάτης). Σε κάθε περίπτωση, μπορεί να συνεπικουρείται από ομάδα, εφόσον απαιτείται. Συνιστάται δε να είναι εγκατεστημένος εντός ΕΕ, ανεξάρτητα από το εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι ή όχι εγκατεστημένοι στην ΕΕ.
Ο DPO διορίζεται ιδίως βάσει της εμπειρίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων του. Το αναγκαίο επίπεδο εμπειρίας θα πρέπει να καθορίζεται ανάλογα με τις πράξεις επεξεργασίας δεδομένων που διενεργούνται και από την προστασία την οποία απαιτούν τα δεδομένα προσωπικού χαρακτήρα που

18 http://www.dpa.gr/portal/page?_pageid=33,211475&_dad=portal&_schema=PORT

υφίστανται επεξεργασία. Παράλληλα, ο DPO πρέπει να έχει γνώση του τομέα δραστηριότητας του οργανισμού ή φορέα στον οποίο απασχολείται αλλά και των τεχνολογιών πληροφορίας και ασφάλειας των δεδομένων.

4.2 Τα καθήκοντα του DPO

Ο DPO προάγει την κουλτούρα της προστασίας προσωπικών δεδομένων εντός του οργανισμού ή φορέα. Τα ελάχιστα καθήκοντα του DPO είναι τα ακόλουθα:

- Να ενημερώνει και να συμβουλεύει τον οργανισμό και τους υπαλλήλους του σχετικά με τις υποχρεώσεις τους που απορρέουν από τον Κανονισμό και άλλες διατάξεις περί προστασίας δεδομένων.
- Να παρακολουθεί την εσωτερική συμμόρφωση με τον Κανονισμό και άλλες διατάξεις περί προστασίας δεδομένων (π.χ. προσδιορισμός και διαχείριση δραστηριοτήτων επεξεργασίας, εκπαίδευση προσωπικού, διενέργεια εσωτερικών ελέγχων).
- Να παρέχει συμβουλές για την εκτίμηση αντίκτυπου και να παρακολουθεί την υλοποίησή της.
- Να είναι το πρώτο σημείο επαφής για τις εποπτικές αρχές και τα υποκείμενα των δεδομένων (εργαζόμενοι, πελάτες κ.λπ.).
- Να συνεργάζεται με την εποπτική αρχή

4.3 Οι υποχρεώσεις του DPO

Ο εργοδότης υποχρεούται να δημοσιεύσει τα στοιχεία επικοινωνίας του DPO και να τα ανακοινώσει στην εποπτική αρχή. Επίσης, οφείλει να διασφαλίζει ότι ο DPO:

- Συμμετέχει σε όλα τα ζητήματα σχετικά με την προστασία προσωπικών δεδομένων (π.χ. παρουσία σε συσκέψεις ανώτερων και μεσαίων στελεχών της διοίκησης και κατά τη λήψη αποφάσεων, καταγραφή λόγων διαφωνίας με τις συμβουλές του, έγκαιρη διαβίβαση πληροφοριών για παροχή γνώμης, άμεση λήψη γνώμης σε περίπτωση περιστατικού παραβίασης).
- Έχει ελεύθερη πρόσβαση σε δεδομένα και πράξεις επεξεργασίας.
- Έχει στη διάθεσή του τους απαραίτητους πόρους για την εκπλήρωση των καθηκόντων του (π.χ. ενεργή στήριξη από τα ανώτερα διοικητικά στελέχη, οικονομικούς πόρους, υποδομές, συνεχής κατάρτιση).
- Εκπληρώνει τα καθήκοντά του με ανεξάρτητο τρόπο (δεν λαμβάνει εντολές για την άσκηση των καθηκόντων του) και δεν απολύεται ούτε υφίσταται κυρώσεις επειδή επιτέλεσε τα καθήκοντά του.
- Λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του εργοδότη.
- Όταν ασκεί πρόσθετα καθήκοντα, αυτά να μην συνεπάγονται σύγκρουση συμφερόντων (π.χ. δεν μπορεί να κατέχει θέση από την οποία μπορεί να καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας, όπως θέσεις ανώτερης διοίκησης, νομικού συμβούλου).

- Δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του.[19]

4.4 Το Σχέδιο Νομού για την μεταφορά του Κανονισμού στην εθνική νομοθεσία

Δημοσιεύθηκε στην Εφημερίδα της Κυβερνήσεως ο Νόμος 4624/2019 "Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις".

Ο νόμος αφορά:

α) στην αντικατάσταση του νομοθετικού πλαισίου που ρυθμίζει τη συγκρότηση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,

β) τη λήψη μέτρων εφαρμογής του Κανονισμού 2016/679 (ΓΚΠΔ/GDPR)
γ) την ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων.

Ο νόμος περιλαμβάνει πολλές ενδιαφέρουσες διατάξεις, μεταξύ των οποίων:

Συγκατάθεση ανηλίκου
1. Όταν εφαρμόζεται το άρθρο 6 παράγραφος 1 στοιχείο α) του ΓΚΠΔ, η επεξεργασία δεδομένων προσωπικού χαρακτήρα ανηλίκου, κατά την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών απευθείας σε αυτόν, είναι σύννομη, εφόσον ο ανήλικος έχει συμπληρώσει το 15ο έτος της ηλικίας του και παρέχει τη συγκατάθεσή του.

2. Εάν ο ανήλικος είναι κάτω των 15 ετών η επεξεργασία της παραγράφου 1 είναι σύννομη μόνο μετά την παροχή συγκατάθεσης του νομίμου αντιπροσώπου του.

Επεξεργασία γενετικών δεδομένων
Κατ' εφαρμογή της παραγράφου 4 του άρθρου 9 του ΓΚΠΔ απαγορεύεται η επεξεργασία γενετικών δεδομένων για σκοπούς ασφάλισης υγείας και ζωής.
Επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των σχέσεων απασχόλησης

1. Δεδομένα προσωπικού χαρακτήρα των εργαζομένων μπορούν να υποβάλλονται σε επεξεργασία για σκοπούς της σύμβασης εργασίας, εφόσον είναι απολύτως απαραίτητο για την απόφαση σύναψης σύμβασης εργασίας ή μετά τη σύναψη της σύμβασης εργασίας για την εκτέλεσή της.

2. Στην περίπτωση που η επεξεργασία δεδομένων προσωπικού χαρακτήρα εργαζομένου έχει κατ' εξαίρεση ως νομική βάση τη συγκατάθεσή του, για την κρίση ότι αυτή ήταν αποτέλεσμα ελεύθερης επιλογής, πρέπει να λαμβάνονται υπόψη κυρίως: α) η υφιστάμενη στη σύμβαση εργασίας εξάρτηση του εργαζομένου και β) οι

19 http://www.dpa.gr/portal/page?_pageid=33,211515&_dad=portal&_schema=PORT

περιστάσεις κάτω από τις οποίες χορηγήθηκε η συγκατάθεση. Η συγκατάθεση παρέχεται είτε σε έγγραφη είτε σε ηλεκτρονική μορφή και πρέπει να διακρίνεται σαφώς από τη σύμβαση εργασίας. Ο εργοδότης πρέπει να ενημερώνει τον εργαζόμενο είτε σε έγγραφη είτε σε ηλεκτρονική μορφή σχετικά με τον σκοπό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και το δικαίωμά του να ανακαλέσει τη συγκατάθεση σύμφωνα με το άρθρο 7 παράγραφος 3 του ΓΚΠΔ.
3. Κατά παρέκκλιση από το άρθρο 9 παράγραφος 1 του ΓΚΠΔ η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα με την έννοια του άρθρου 9 παράγραφος 1 του ΓΚΠΔ για τους σκοπούς της σύμβασης εργασίας επιτρέπεται, εάν είναι απαραίτητη για την άσκηση των δικαιωμάτων ή την εκπλήρωση νόμιμων υποχρεώσεων που απορρέουν από το εργατικό δίκαιο, το δίκαιο της κοινωνικής ασφάλισης και της κοινωνικής προστασίας και δεν υπάρχει κανένας λόγος να θεωρηθεί ότι το έννομο συμφέρον του υποκειμένου των δεδομένων σε σχέση με την επεξεργασία υπερτερεί. Η παράγραφος 2 ισχύει επίσης για τη συγκατάθεση στην επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα. Η συγκατάθεση πρέπει να αναφέρεται ρητά στα δεδομένα αυτά. Το άρθρο 22 παράγραφος 3 εδάφιο β΄ εφαρμόζεται ανάλογα.
4. Επιτρέπεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων των ειδικών κατηγοριών δεδομένων Προσωπικού Χαρακτήρα των εργαζομένων για τους σκοπούς της σύμβασης εργασίας βάσει συλλογικών συμβάσεων εργασίας. Τα διαπραγματευόμενα μέρη συμμορφώνονται με το άρθρο 88 παράγραφος 2 του ΓΚΠΔ.
5. Ο υπεύθυνος επεξεργασίας λαμβάνει τα ενδεδειγμένα μέτρα για να εξασφαλίσει ότι τηρούνται ιδίως οι αρχές για την επεξεργασία δεδομένων προσωπικού χαρακτήρα που ορίζονται στο άρθρο 5 του ΓΚΠΔ.

6. Οι παράγραφοι 1 έως 5 εφαρμόζονται επίσης, όταν δεδομένα προσωπικού χαρακτήρα, συμπεριλαμβανομένων των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα των εργαζομένων, υπόκεινται σε επεξεργασία, χωρίς αυτά να αποθηκεύονται ή να προορίζονται να αποθηκευτούν σε ένα σύστημα αρχειοθέτησης.

7. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω κλειστού κυκλώματος οπτικής καταγραφής εντός των χώρων εργασίας, είτε είναι δημοσίως προσβάσιμοι είτε μη, επιτρέπεται μόνο εάν είναι απαραίτητη για την προστασία προσώπων και αγαθών. Τα δεδομένα που συλλέγονται μέσω κλειστού κυκλώματος οπτικής καταγραφής δεν επιτρέπεται να χρησιμοποιηθούν ως κριτήριο για την αξιολόγηση της αποδοτικότητας των εργαζομένων. Οι εργαζόμενοι ενημερώνονται εγγράφως, είτε σε γραπτή είτε σε ηλεκτρονική μορφή για την εγκατάσταση και λειτουργία κλειστού κυκλώματος οπτικής καταγραφής εντός των χώρων εργασίας.

8. Για τους σκοπούς του παρόντος νόμου ως εργαζόμενοι νοούνται οι απασχολούμενοι με οποιαδήποτε σχέση εργασίας ή σύμβαση έργου ή παροχής υπηρεσιών στο δημόσιο και στον ιδιωτικό φορέα, ανεξαρτήτως του κύρους της σύμβασης, οι υποψήφιοι για εργασία και οι πρώην απασχολούμενοι.

Επεξεργασία και ελευθερία έκφρασης και πληροφόρησης

1. Στον βαθμό που είναι αναγκαίο να συμβιβαστεί το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα με το δικαίωμα στην ελευθερία της έκφρασης και πληροφόρησης, συμπεριλαμβανομένης της επεξεργασίας για δημοσιογραφικούς σκοπούς και για σκοπούς ακαδημαϊκής, καλλιτεχνικής ή λογοτεχνικής έκφρασης, η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται όταν:

α) το υποκείμενο των δεδομένων έχει παράσχει τη ρητή συγκατάθεσή του,

β) αφορά δεδομένα προσωπικού χαρακτήρα που έχουν προδήλως δημοσιοποιηθεί από το ίδιο το υποκείμενο,

γ) υπερέχει το δικαίωμα στην ελευθερία της έκφρασης και το δικαίωμα της πληροφόρησης έναντι του δικαιώματος προστασίας των δεδομένων προσωπικού χαρακτήρα του υποκειμένου, ιδίως για θέματα γενικότερου ενδιαφέροντος ή όταν αφορά δεδομένα προσωπικού χαρακτήρα δημοσίων προσώπων και

δ) όταν περιορίζεται στο αναγκαίο μέτρο για την εξασφάλιση της ελευθερίας της έκφρασης και του δικαιώματος ενημέρωσης, ιδίως όταν αφορά ειδικών κατηγοριών δεδομένα Προσωπικού Χαρακτήρα, καθώς και ποινικές διώξεις, καταδίκες και τα σχετικά με αυτές μέτρα ασφαλείας, λαμβάνοντας υπόψη το δικαίωμα του υποκειμένου στην ιδιωτική και οικογενειακή του ζωή.

4.5 Ο ρόλος των εποπτικών Αρχών

ο ρόλος των εποπτικών Αρχών στη συμμόρφωση των επιχειρήσεων με το οποιοδήποτε θεσμικό πλαίσιο είναι κομβικός, καθώς:

- ✓ διασφαλίζει την εκπλήρωση του σκοπού του νομοθέτη
- ✓ εγγυάται την ίση μεταχείριση ρυθμιζόμενων και ρυθμιστών (αποφυγή φαινομένων νόθευσης του ανταγωνισμού μεταξύ των συμμορφούμενων και όσων συνειδητά συμμορφώνονται πλημμελώς),
- ✓ μεριμνά για την ελαχιστοποίηση του διοικητικού βάρους συμμόρφωσης και
- ✓ φροντίζει για την αναλογικότητα των διορθωτικών μέτρων και προστίμων.

Ο ρόλος των εποπτικών Αρχών εν γενεί είναι αλώστε πολλαπλός, μεταξύ άλλων ενημερωτικός, ρυθμιστικός και ελεγκτικός / κυρωτικός. Ο Κανονισμός θέτει μια διαφορετική προσέγγιση από ότι μέχρι σήμερα, σε ότι αφορά το ρολό των εποπτικών Αρχών, καθώς πλέον το βάρος απόδειξης λήψης μέτρων για την προστασία των προσωπικών δεδομένων «μετακινείται» στους Υπευθύνους Επεξεργασίας, με τις εποπτικές Αρχές να αναλαμβάνουν δράση σε «δεύτερο χρόνο» και να δίνεται έμφαση στα θέματα εξασφάλισης της συνεκτικής εφαρμογής των διατάξεων (αντί για τον έλεγχο της συμμόρφωσης). Με άλλα λόγια, από ένα πλαίσιο «προληπτικής δίνει έμφαση στη νόμιμη και ασφαλή επεξεργασία των προσωπικών δεδομένων από τους ιδίους τους οργανισμούς (επιχειρήσεις και φορείς του δημοσίου). Η εξέλιξη αυτή αποτελεί τομή στη λειτουργιά των ρυθμιστικών Αρχών, η οποία κατά τη γνώμη μας θα πυροδοτήσει αλυσιδωτές αντιδράσεις και σε αλλά πεδία πολιτικής.

Ιδίως για τη χωρά μας, οπού ο ρόλος των εποπτικών ή και ρυθμιστικών αρχών δεν είναι πάντα ξεκάθαρος (κυρίως λόγω θεμάτων συναρμοδιότητας με κεντρική διοίκηση), η αποσαφήνιση των αρμοδιοτήτων και του πεδίου δραστηριοποίησης της ΑΠ ΠΧ, του Υπουργείου Δικαιοσύνης και άλλων εμπλεκομένων δημοσίων φορέων, είναι περισσότερο από καίριος για την εφαρμογή του Κανονισμού. [20]

[20] https://segm.gr/wp-content/uploads/2018/10/meleti_sev_GDP

ΚΕΦΑΛΑΙΟ 5

5.1 Βαθμός ετοιμότητας των επιχειρήσεων στο εξωτερικό και την Ελλάδα

Η αυξανόμενη χρήση των τεχνολογιών της πληροφορίας και των επικοινωνιών(Information and Communications Technologies) μαζί με το διαδίκτυο (Internet) επιβάλλουν ένα σύνολο νόμων και κανονισμών που σχετίζεται με την προστασία των δεδομένων , την ασφάλεια των δεδομένων και την προστασία της ιδιωτικής ζωής των ατόμων.

Όλα αυτά παραμένουν ότι πιο σημαντικό για όλες τις **επιχειρήσεις** και **οργανισμούς** σε όλο τον κόσμο και οι οποίες υποχρεούνται να συμμορφώνονται με τους σχετικούς νόμους και κανόνες.

Για αυτό όλες οι **επιχειρήσεις** και οι **οργανισμοί** θα πρέπει να εξετάσουν τώρα πως συλλέγουν ,διαχειρίζονται, αποθηκεύουν, και χρησιμοποιούν τα προσωπικά δεδομένα με το καλύτερο τρόπο και τι μέτρα (πολίτικες, διαδικασίες, πρακτικές κ.λπ.) εφαρμόζουν για να συμμορφώνονται πιο αποτελεσματικά με το σχετικό νομοθετικό πλαίσιο προστασίας δεδομένων και σε τοπικό (κρατικό) επίπεδο και σε διεθνές(Ευρωπαϊκό κλπ.) επίπεδο.[21]

ο βαθμός ετοιμότητας των επιχειρήσεων σχετικά με τη συμμόρφωση τους στις διατάξεις του Κανονισμού, βάσει ερευνών που έχουν πραγματοποιηθεί, τόσο στο εξωτερικό όσο και στην Ελλάδα. Σκοπός του Κεφαλαίου είναι να αποτυπωθούν ποσοτικά στοιχειά για το βαθμό συμμόρφωσης των επιχειρήσεων, προκειμένου να καταγραφεί η υφισταμένη κατάσταση στην Ελλάδα και να είναι δυνατή η παρακολούθηση της πορείας συμμόρφωσης διαχρονικά (και επομένως να καταγραφεί η οποία βελτίωση η υστέρηση) , αλλά και να υπάρχει ένα μετρό σύγκρισης (benchmarking) για την εγχώρια αγορά σε σχέση με τις υπόλοιπες χώρες της ΕΕ.

Σημειώνεται ούτι οι έρευνες που πραγματοποιηθήκαν έφεραν στην επιφάνεια και αλλά χρήσιμα στοιχειά σχετικά με την πορεία συμμόρφωσης στον Κανονισμό, για τα οποία αξίζει να ληφθεί μερίμνα, καθώς αποτύπωσαν την άποψη των επιχειρήσεων σε ένα θέμα που αναδείχτηκε «βίαια» στην ατζέντα των προτεραιοτήτων τους.

Τέλος, αξίζει να σημειώσουμε ότι παρόλο που στην Ελλάδα ο βαθμός ετοιμότητας των επιχειρήσεων, όπως καταγράφεται στις σχετικές έρευνες, «υπολείπεται» των αντίστοιχων του εξωτερικού, οι επιχειρήσεις ούλων των κρατών-μελών αντιμετωπίζουν προκλήσεις στην προσπάθεια τους να προσαρμοστούν στο νέο θεσμικό πλαίσιο για τα προσωπικά δεδομένα. [22]

Εκτιμήσεις για τη συμμόρφωση των επιχειρήσεων στο εξωτερικό

Ο βαθμός ετοιμότητας των επιχειρήσεων στο εξωτερικό κρίθηκε σκόπιμο να παρουσιαστεί μέσα από δυο πρόσφατες και ιδιαιτέρα αντιπροσωπευτικές και

[21] Κυριαζόγλου Ιωάννης
[22] https://segm.gr/wp-content/uploads/2018/10/meleti_sev_GDPR

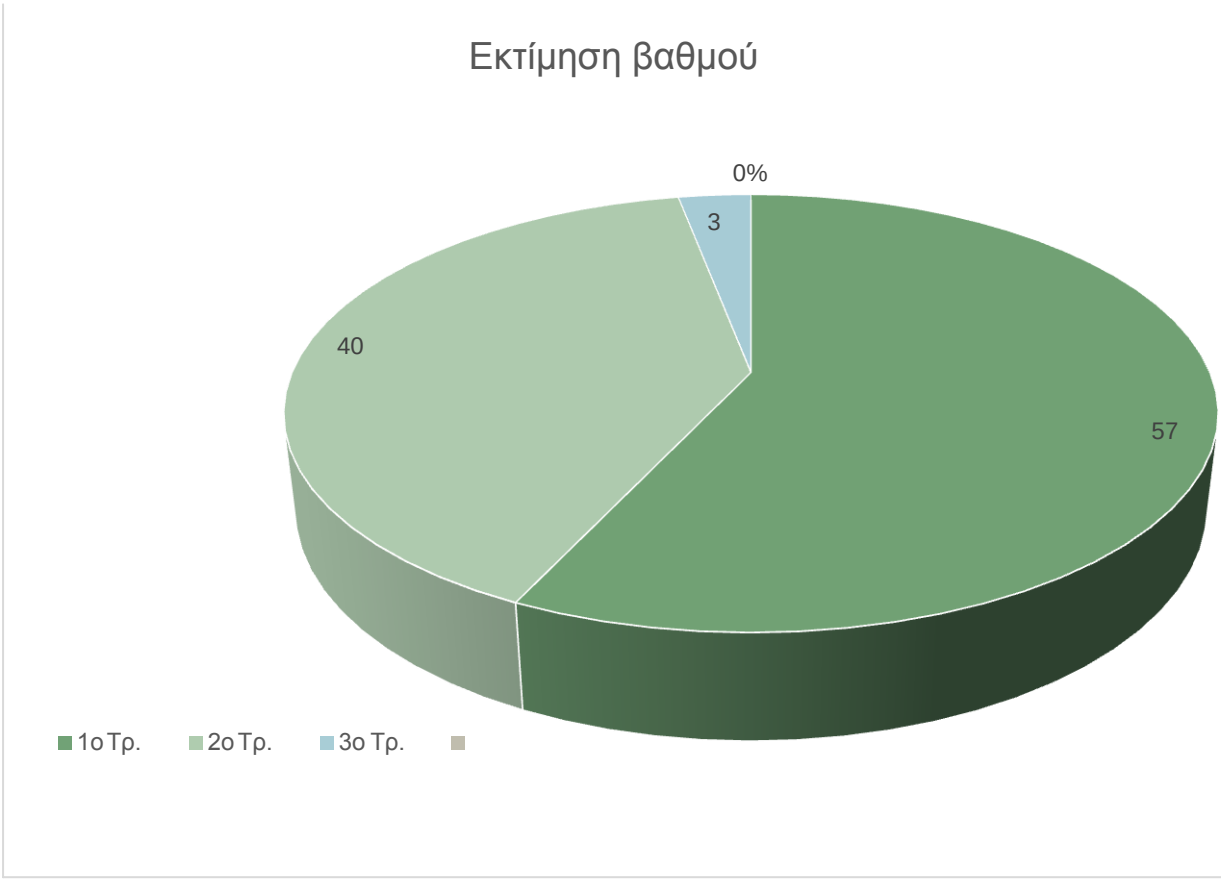
αξιόπιστες έρευνες, οι οποίες αναδεικνύουν σαν γενικό συμπέρασμα ότι οι επιχειρήσεις δεν θα καταφέρουν να συμμορφωθούν έγκαιρα και πλήρως στις διατάξεις του Κανονισμού.

Η έρευνα των International Association of Privacy Professionals (IAPP) και EY

Στη διεθνή έρευνα των International Association of Privacy Professionals (IAPP) και EY, η οποία πραγματοποιείσθε το 2017, σχετικά με την πορεία συμμόρφωσης των επιχειρήσεων

στον Κανονισμό, προκύπτει ότι (Δ18):

- ➢ Περισσότερες από 1 στις 2 επιχειρήσεις θεωρούν ότι έως το Μάιο του 2018 θα έχουν καταφέρει να πετύχει μερική μόνο συμμόρφωση στο νέο Κανονισμό (57%).
- ➢ Ωστόσο, το ποσοστό εκείνων που εκτιμούν ότι θα «απέχουν» σημαντικά από τη συμμόρφωση είναι περιορισμένο (μόλις 3%).



Τα αποτελέσματα αποδεικνύουν ποσό σημαντικά οφέλη μπορούν να προκύψουν για τις επιχειρήσεις στην εποχή του ψηφιακού μετασχηματισμού, χάρη στη λήψη μέτρων για την επίτευξη της συμμόρφωσης στον Κανονισμό. Οφέλη όπως: απόκτηση δεδομένων που συμβάλλουν στην καλύτερη γνώση των πελατών της επιχείρησης και των χαρακτηριστικών τους (customer intelligence), καλύτερη διαχείριση κίνδυνου

(risk management), ενίσχυση του “machine learning”, ακόμα και εντοπισμό περιστατικών απατής

Τέλος, η εν λόγω έρευνα ανέδειξε τα σημεία της προετοιμασίας συμμόρφωσης με τον Κανονισμό που δυσκολεύουν περισσότερο τις επιχειρήσεις. Όπως προκύπτει:
➢ Ιδιαιτέρα υψηλό είναι το ποσοστό των επιχειρήσεων που εκφράζει αβεβαιότητα για

το αν επαρκούν οι ενέργειες συμμόρφωσης που αναλαμβάνει (59%). Το γεγονός αυτό αποτυπώνει τόσο τη γενική δυσκολία κατά την προσπάθεια συμμόρφωσης στον Κανονισμό, όσο και το πλήθος των προκλήσεων που προκύπτουν ειδικά από τις διατάξεις που αφήνουν «γκρίζες ζώνες» για την ερμηνεία τους, προκαλώντας προφανώς ανησυχία και αβεβαιότητα στις επιχειρήσεις.

➢Η φορητότητα δεδομένων και το δικαίωμα στη λήθη αποτελούν τις υποχρεώσεις που οι επιχειρήσεις αξιολογούν ως πιο δύσκολες.

➢Από τις εσωτερικές λειτουργιές των επιχειρήσεων, ο περιορισμός της πρόσβασης σε προσωπικά δεδομένα μονό στα άτομα που προβλέπεται η / και είναι αναγκαίο αποτελεί πρόκληση για μια στις δυο επιχειρήσεις. Αυτό δεικνύει ούτι δεν πρέπει να υποτιμάται καμιά εσωτερική πολιτική και διαδικασία, κατά την προσπάθεια συμμόρφωσης στον Κανονισμό, καθώς ακόμα και φαινομενικά απλές λειτουργιές (εν προκειμένω, πρόσβαση στα προσωπικά δεδομένα μονό από όσους χρειάζεται), τελικά στην πράξη δεν υλοποιούνται τόσο εύκολα.

5.2 Εκτιμήσεις για τη συμμόρφωση των επιχειρήσεων στην Ελλάδα

Ο βαθμός ετοιμότητας των επιχειρήσεων στην Ελλάδα απασχόλησε έντονα καθ’ όλη την περίοδο πριν την ημερομηνία έναρξης εφαρμογής του Κανονισμού2018, κάτι που αναμένεται να συνεχιστεί και στο μέλλον, όταν για παράδειγμα θα επιχειρηθεί να καταγραφεί εκ νέου ο βαθμός συμμόρφωσης (ενδεικτικά ένα χρόνο μετρά).

Στα στοιχεία που παρουσιάζουμε παρακάτω, από δυο πρόσφατες έρευνες που δημοσιοποιηθήκαν, αποτυπώνεται με σχετική αντιπροσωπευτικότητα κατά την άποψη της συντακτικής ομάδας, ο βαθμός ετοιμότητας των επιχειρήσεων και αναδεικνύεται ούτι υπάρχει αρκετός δρόμος ακόμα, προκειμένου οι επιχειρήσεις να καταφέρουν να συμμορφωθούν στις διατάξεις του Κανονισμού. Τα βασικά συμπεράσματα των ερευνών παρουσιάζονται στις επόμενες ενότητες.

5.3 Η ΕΡΕΥΝΑ ΤΗΣ ICAP

- ➢ 1 στις 4 επιχειρήσεις δηλώνει ούτι δεν γνωρίζει τον νέο Κανονισμό. Το ποσοστό αυτό

  αυξάνεται σε 35% για τις επιχειρήσεις με λιγότερο από 100 εργαζομένους.

- ➢ Μερίδιο 22% δηλώνει ούτι, ακόμα (Δεκέμβριος 2017), δεν γνωρίζει τον ορισμό των προσωπικών δεδομένων. Το ποσοστό αυτό αυξάνεται σε 32% για τις επιχειρήσεις

  που δραστηριοποιούνται στον κλάδο του Τουρισμού. Εκτιμάται ούτι ακόμα και μεταξύ των επιχειρήσεων που δηλώνουν ότι γνωρίζουν τον ορισμό, ενδέχεται να περιλαμβάνονται αρκετές που νομίζουν ότι κατέχουν σχετική γνώση, ενώ στην πραγματικότητα δεν έχουν.

- ➢ Σχεδόν 1 στις 3 επιχειρήσεις δηλώνει ότι δεν επεξεργάζεται προσωπικά δεδομένα, εκτός από εκείνα των εργαζομένων της (π.χ. πελατών και προμηθευτών). Αξιοσημείωτο είναι - και αυτήν την περίπτωση - το υψηλότερο ποσοστό των τουριστικών επιχειρήσεων (40%).
- ➢ Σχεδόν 1 στις 4 επιχειρήσεις δηλώνει ούτι δεν συμμορφώνεται στον Κανονισμό. Σε συνδυασμό με ποσοστό 58% των επιχειρήσεων που δηλώνει ούτι συμμορφώνεται
- μερικώς, διαπιστώνεται ότι απαιτείται άμεση δράση και εντατικοποίηση ενεργειών από την πλειονότητα των επιχειρήσεων. Ειδικά στις επιχειρήσεις με λιγότερους από 100 εργαζομένους, το σωρευτικό ποσοστό μερική η μη συμμόρφωσης ανέρχεται σε 87%.
- ➢Μερίδιο 31% αξιολογεί ως μέτριο η ανεπαρκές το επίπεδο ασφάλειας των συστημάτων του (και κατ' επέκταση των συστημάτων για την προστασία των προσωπικών δεδομένων). Ειδικά στις τουριστικές επιχειρήσεις το ποσοστό αυξάνεται σε 40%.
- ➢Όσον αφορά στην ανάληψη καθηκόντων από τον Υπεύθυνο Προστασίας Δεδομένων, προκύπτει ούτι σχεδόν 1 στις 2 επιχειρήσεις είτε δεν έχει κατανοήσει εάν υποχρεούται να προχωρήσει σε ορισμό ΥΔ είτε αγνοεί γενικώς τις σχετικές διατάξεις του Κανονισμού. Το ποσοστό αυτό αυξάνεται όσο μικρότερο είναι το μέγεθος των επιχειρήσεων, βάσει αριθμού εργαζομένων. Επομένως, παραμένει αναγκαία η αποσαφήνιση και περαιτέρω ενημέρωση των επιχειρήσεων σχετικά με τον ΥΔ. [23]

5.4 Οδηγός συμμόρφωσης για τις επιχειρήσεις

Κύριος στόχος της παρούσας Μελέτης είναι η ανάπτυξη ενός εύχρηστου «οδηγού συμμόρφωσης» με τον Κανονισμό για τις επιχειρήσεις. Φιλοδοξία της συντακτικής ομάδας αποτελεί το παρόν κείμενο να τις βοηθήσει με πρακτικό τρόπο να κατανοήσουν τα οφέλη που μπορούν να προκύψουν από τη διαδικασία συμμόρφωσης, τις απαιτήσεις συμμόρφωσης και τον τρόπο επίτευξης αυτής. Ιδίως για τις μικρές και μεσαίες επιχειρήσεις, με το κόστος συμμόρφωσης να είναι ενδεχομένως δυσανάλογα μεγάλο, η ύπαρξη ενός απλού εισαγωγικού οδηγού αναμένεται να έχει μεγαλύτερη ωφέλεια, ουχί μονό για την πρώτη περίοδο συμμόρφωσης και τις ελάχιστες αναγκαίες ενέργειες στις οποίες οι επιχειρήσεις αναμένεται ήδη να έχουν προβεί, όσο κυριότερα στον τρόπο με τον οποίο θα προσεγγίζουν το θέμα στο εξής, ενσωματώνοντας τις αρχές και υποχρεώσεις του Κανονισμού στην κουλτούρα και κατ' επέκταση στη λειτουργιά της επιχείρησης τους. Αξίζει επίσης να σημειωθεί ούτι παρόλο που η Μελέτη εστιάζεται αποκλειστικά στις ιδιωτικές επιχειρήσεις, δεν θα πρέπει να παραβλέπει κάνεις τις σημαντικές απαιτήσεις συμμόρφωσης που προκύπτουν για τους φορείς του δημόσιου και αρά τη δυνητική ωφέλεια που ο ίδιος αυτός οδηγός μπορεί να έχει και για τους οργανισμούς του δημοσίου τομέα. Με τις απαιτούμενες προσαρμογές, τα βήματα που προβλέπει μπορούν να φανούν χρήσιμα και για τις υπηρεσίες και φορείς του δημοσίου, οι

[23] https://www.icap.gr/Default.aspx?id=10594&nt=146&lang=1

οποίες υπολείπονται στις περισσότερες των περιπτώσεων έναντι των ιδιωτικών επιχειρήσεων ως προς τις δράσεις συμμόρφωσης.

Για ένα μάλλον μεγάλο αριθμό επιχειρήσεων ο νέος Κανονισμός αποτελεί στην πράξη άλλη μια υποχρέωση που «πρέπει να εκπληρώσουν», αναθέτοντας σε κάποιο εξωτερικό σύμβουλο τη σύνταξη κάποιας έκθεσης (την οποία θα διατηρούν «ξεχασμένη» σε κάποιο συρτάρι), αγοράζοντας κάποια προσθετά πληροφοριακά συστήματα (τα οποία ούτε καν θα αναβαθμίζουν) και αναθέτοντας την ιδιότητα του ΥΠΔ σε ένα στέλεχος που διαθέτει ήδη μερικές ακόμη (π.χ. Υπεύθυνος Κανονιστικής Συμμόρφωσης, Νομικός Σύμβουλος κ.λπ.). Δηλαδή, ως μια υποχρέωση στατική, σημειακή και πάντως ουχί ως οργανικό κομμάτι της λειτουργιάς η της κουλτούρας τους. Αυτή η προσέγγιση πρέπει να αλλάξει πριν καν εδραιωθεί και ο οδηγός που ακολουθία, όπως και το σύνολο της παρούσας μελέτης μπορεί να συμβάλει στην ανάδειξη της πραγματικής συμβολής του Κανονισμού στον εκσυγχρονισμό των ελληνικών επιχειρήσεων. Για ένα μικρότερο αριθμό επιχειρήσεων (που ευελπιστούμε να μεγαλώσει) ο νέος Κανονισμός αποτελεί μια ευκαιρία να αποκτήσουν ανταγωνιστικό πλεονέκτημα και να ενισχύσουν την αξία τους, επενδύοντας στην ασφάλεια των δεδομένων, πελατών, προμηθευτών και προσωπικού και αυτό επιδιώκουμε να προβάλουμε. [24]**Σκοπός δεν πρέπει να είναι η εφαρμογή του Κανονισμού «μόνο στα χαρτιά». Πραγματική στόχευση αυτής της «υποχρεωτικής άσκησης» στην οποία θα υποβληθούν όλοι οι οργανισμοί είναι η ουσιαστική αλλαγή της κουλτούρας των επιχειρήσεων, με επίκεντρο τη διαφύλαξη των προσωπικών δεδομένων**. Σε αυτό το πλαίσιο, στις επόμενες ενότητες του παρόντος Κεφαλαίου παρουσιάζουμε **τον τρόπο με τον οποίο μπορεί να υπάρξει μια ουσιαστική αλλά και έξυπνη συμμόρφωση**, που δεν θα επιβαρύνει με σημαντικό χρηματικό και διοικητικό κόστος την καθημερινή λειτουργιά των επιχειρήσεων. Ειδικότερα, αναφερόμαστε σε εκείνες τις ενέργειες στις οποίες πρέπει να προβούν οι επιχειρήσεις, προκειμένου να συμμορφωθούν στις απαιτήσεις του Κανονισμού, δηλαδή να είναι σε θέση να αποδείξουν ότι έχουν λάβει ούλα τα απαραίτητα μέτρα για την προστασίας των προσωπικών δεδομένων υποστηρίζουμε ότι μέσα από αυτή τη διαδικασία προκύπτουν πολλαπλά οφέλη.

Είναι σημαντικό να διευκρινιστεί ότι η λίστα των ενεργειών δεν είναι εξαντλητική, ούτε μοναδική (δεν υφίσταται δηλαδή μια λύση για όλους). Όμως, κάθε επιχείρηση, με βάση τις δίκες τις ανάγκες, τα χαρακτηριστικά (φύση και όγκος δεδομένων), το μέγεθος, το αντικείμενο των εργασιών και τη στρατηγική της, μπορεί να προσαρμοστεί σε αυτόν τον «οδηγό» και να επιτύχει το σκοπό της

Σημειώνεται ότι για τον ΣΕΒ, **τρεις είναι οι βασικές προϋποθέσεις** με οριζόντια ισχύ, **προτού μια επιχείρηση εκκινήσει την προσπάθεια της να ακολουθήσει τα βήματα για την ορθή εφαρμογή του Κανονισμού**, δίχως τις οποίες δεν μπορεί να επιτευχτεί η συμμόρφωση.

Πρώτον, απαιτείται η ευαισθητοποίηση και δέσμευση της ανώτατης διοίκησης, να κατανοήσει δηλαδή την αναγκαιότητα συμμόρφωσης και έμπρακτα να αποφασίσει να δράσει προς αυτήν την κατεύθυνση.

Δεύτερον, απαιτείται εξασφάλιση του σχετικού προϋπολογισμού, ο οποίος είναι απαραίτητος για την υλοποίηση του πλάνου συμμόρφωσης.

[24] https://segm.gr/wp-content/uploads/2018/10/meleti_sev_GDPR

Τρίτον, είναι σημαντικό να ενημερωθεί το σύνολο του προσωπικού για το νέο νομικό πλαίσιο και τις επερχόμενες αλλαγές, διαφορετικά θα προκύψουν προβλήματα στην υλοποίηση.

Οι Βασικές προϋποθέσεις για τη συμμόρφωση με τις προβλέψεις του κανονισμού
Δέσμευση της ανώτατης διοίκησης
Εξασφάλιση του σχετικού προϋπολογισμού
Ενημέρωση του συνόλου του προσωπικού για το νέο νομικό πλαίσιο και τις επερχόμενες αλλαγές

Τα προτεινόμενα βήματα για την ορθή εφαρμογή του Κανονισμού

1ο Βήμα Σύσταση Ομάδα εργασίας

Αφορά στη **σύσταση Ομάδα Εργασίας, η οποία θα απαρτίζεται από εκπροσώπους των Διευθύνσεων που εμπλέκονται περισσότερο με την προστασία των προσωπικών δεδομένων.** Ενδεικτικά, αναφέρονται οι Διευθύνσεις Πληροφορικής, Νομικής και Ανθρωπίνου Δυναμικού, οι οποίες σχετίζονται εξ ορισμού λόγω του αντικειμένου τους. Στις επιχειρήσεις που τα προσωπικά δεδομένα αποτελούν βασικό αντικείμενο της δραστηριότητας (π.χ. εταιρείες τηλεπικοινωνιών, ασφαλιστικές, τράπεζες), τότε είναι προφανές ούτι πρέπει να συμμετέχει και, τουλάχιστον ένας, εκπρόσωπος από κάθε επιχειρησιακή Διεύθυνση (ως “business owner”). Με αυτόν τον τρόπο, εξασφαλίζεται η αρμονική συμμετοχή όλων των εμπλεκομένων και η παροχή της απαιτούμενης βοήθειας και υποστήριξης του ΥΔ. Σε κάθε περίπτωση, η Ομάδα Εργασίας πρέπει να έχει μικρό και ευέλικτο μέγεθος, αλλά και δυνατότητα λήψης αποφάσεων.

2ο Βήμα Ορισμός Υπευθύνου προστασίας Δεδομένων

Πρόκειται για υποχρεωτικό βήμα για ούσες επιχειρήσεις προβαίνουν σε μεγάλης κλίμακας επεξεργασία προσωπικών δεδομένων, προαιρετικό για τις υπόλοιπες. Ο ΥΠΔ συμβουλεύει την επιχείρηση για τις υποχρεώσεις που απορρέουν από τον Κανονισμό και παρακολουθεί τις ενέργειες συμμόρφωσης με αυτόν. Συμμετέχει ενεργά σε ούλα τα ζητήματα που σχετίζονται με τον Κανονισμό και αποτελεί το πρόσωπο επικοινωνίας τόσο με τα υποκείμενα των δεδομένων όσο και με την εποπτική Αρχή. Ο ΥΠΔ πρέπει να είναι άτομο κατάλληλα καταρτισμένο και προσεκτικά επιλεγμένο ώστε να είναι σε θέση να διεκπεραιώσει τις υποχρεώσεις του, δίχως σύγκρουση συμφερόντων. Στους οργανισμούς που κριθεί απαραίτητο (π.χ. λόγω μεγάλου όγκου προσωπικών δεδομένων) ο ΥΠΔ μπορεί να έχει υπό την ευθύνη του ολόκληρη ομάδα στελεχών.

3ο Βήμα Χαρτογράφηση Ροής των δεδομένων (data mapping)

Η χαρτογράφηση της πορείας των δεδομένων προσωπικού χαρακτήρα που τηρούνται και επεξεργάζονται εντός επιχείρησης (δηλαδή των δεδομένων προσωπικού, πελατών, προμηθευτών και τρίτων προσώπων) **αποτελεί μια διαδικασία μέσω της οποίας απαντώνται τα εξής ερωτήματα: τι είδους δεδομένα, για ποιο σκοπό, ποσό συχνά, πως αποκτώνται, που υπάρχουν, ποιος έχει πρόσβαση και τα επεξεργάζεται, για ποσό χρόνο διακηρύττονται.** Για την ολοκλήρωση της διαδικασίας χαρτογράφησης, προτείνεται η χρήση ερωτηματολογίων και η πραγματοποίηση συνεντεύξεων ανά Διεύθυνση, προκειμένου να γίνει πλήρης καταγραφή / αποτύπωση της υφισταμένης κατάστασης της επιχείρησης. Μέσα από αυτή τη διαδικασία, δημιουργείται, επί της ουσίας, το επονομαζόμενο «Αρχείο Δραστηριοτήτων Επεξεργασίας» (άρθρο 30 του Κανονισμού), το οποίο στη συνέχεια πρέπει να είναι συνεχώς επικαιροποιημένο, ώστε, σε ενδεχόμενο έλεγχο, να αποτελεί στοιχειό απόδειξης της συμμόρφωσης της κάθε επιχείρησης. Πρόκειται για ένα πολύ σημαντικό στάδιο της διαδικασίας συμμόρφωσης, το οποίο στην ουσία «ξεκλειδώνει» τα επόμενα βήματα.

4οΒήμα Εντοπισμός και ανάλυση κίνδυνων και ελλείψεων

Αξιοποιώντας την πλήρη γνώση της ροής των προσωπικών δεδομένων), η **επιχείρηση οφείλει να καταγράψει τους πιθανούς κίνδυνους και τις ελλείψεις που - ενδεχομένως - εντοπίστηκαν** (να πραγματοποιήσει δηλαδή την επονομαζόμενη “gap analysis”). Έτσι **καταρτίζεται ένας πίνακας ο οποίος περιέχει τις δραστηριότητες που εντοπιστήκαν με ελλείψεις, την προτεραιότητα τους με βάση τον κίνδυνο που ενέχουν και τις προτεινόμενες ενέργειες για την αντιμετώπιση τους.** Παραδείγματα σχετικών «κενών» είναι: πολύ μεγάλη περίοδος διατήρησης των δεδομένων άνευ λογού, διατήρηση των ιδίων δεδομένων σε περισσότερα του ενός σημεία και ανεμπόδιστη πρόσβαση σε δεδομένα από ούλα τα στελέχη ενώ δεν χρειάζεται.

5ο Βήμα Εκπόνηση Εκτίμησης Αντίκτυπου σχετικά με την προστασία δεδομένων

Πρόκειται για **υποχρεωτικό βήμα για ούσες επιχειρήσεις προβαίνουν σε επεξεργασία που ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθέριές των φυσικών προσώπων, προαιρετικό για τις υπόλοιπες**. Η εκπόνηση της ΕΑ εξ ορισμού προηγείται της επεξεργασίας των δεδομένων και **περιλαμβάνει ανάλυση για τις πιθανότητες επέλευσης κίνδυνων και τις συνέπειες στα προσωπικά δεδομένα.** Καταλήγει σε κατηγοριοποίηση των δραστηριοτήτων επεξεργασίας σε υψηλού, μεσαίου και χαμηλού κίνδυνου και σε επανεξέταση των απαιτούμενων διαδικασιών σε κάθε περίπτωση. Σημειώνεται ούτι οι πολίτικες και διαδικασίες της επιχείρησης πρέπει, οπού αυτό είναι δυνατόν, να λαμβάνουν υπόψη την αρχή της προστασίας των δεδομένων ήδη από το σχεδιασμό (privacy by default). Δηλαδή, όποτε αυτό είναι δυνατόν, ο Υπεύθυνος Επεξεργασίας να εφαρμόζει κατά τη στιγμή του καθορισμού των μεσών επεξεργασίας αλλά και της ιδίας της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μετρά, σχεδιασμένα για την εφαρμογή των αρχών προστασίας των δεδομένων.

6ο Βήμα Αναθεώρηση πολίτικων και διαδικασιών

Με βάση τα συμπεράσματα των βημάτων 4 και 5, η επιχείρηση προβαίνει σε αναθεώρηση των πολίτικων και των διαδικασιών τήρησης και επεξεργασίας δεδομένων προσωπικού χαρακτήρα Τέτοια παραδείγματα αποτελούν ενδεικτικά τα εξής: οριστική διαγραφή και καταστροφή δεδομένων με το πέρας Χ ετών, διαμόρφωση κοινού γλωσσάριου ώστε να υπάρχει σωστή και κοινή κατανόηση από ούλο το προσωπικό, θέσπιση πολιτικής «καθαρού γραφείου», απαγόρευση εξόδου από την επιχείρηση USB sticks και laptops, απαγόρευση αντιγραφής αρχείων από το σκληρό δίσκο σε USB sticks και εξωτερικούς δίσκους, ανάπτυξη πολιτικής διαβαθμισμένης πρόσβασης, ανάπτυξη πολιτικής για τις διαδρομές των φυσικών αρχείων εντός της επιχείρησης, θέσπιση ορισμένου χρόνου διατήρησης CVs κλπ

7ο Βήμα Αξιοποίηση των εργαλείων πληροφορικής

Κάθε επιχείρηση ανάλογα με τη φύση των εργασιών της, τα μεγέθη και τις δυνατότητες της, οφείλει να αξιοποιήσει κάποια από τα εργαλεία πληροφορικής που ενισχύουν την ασφάλεια των συστημάτων. Ενδεικτικά παραδείγματα αποτελούν εργαλεία που με αυτοματοποιημένο τρόπο χαρτογραφούν τα δεδομένα εργαλεία που αξιολογούν την αποτελεσματικότητα των πολίτικων και διαδικασιών που έχουν αναπτυχθέν και εργαλεία που βοηθούν στην αποτροπή ή τον εντοπισμό των αποπειρών παραβίασης δεδομένων. Επιπλέον, η κρυπτογράφηση και η ψευδωνυμοποίηση αποτελούν δυο εκ των απλούστερων τεχνικών μέτρων προστασίας

8ο Βήμα Ανάπτυξη διαδικασιών γνωστοποίησης εποπτικής Αρχής και ανακοίνωσης υποκείμενου

Πρόκειται για δυο υποχρεωτικές διαδικασίες για κάθε επιχείρηση. Η πρώτη αφορά στη διαδικασία γνωστοποίησης της παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική Αρχή, εντός μόλις 72 ωρών από τη στιγμή που η επιχείρηση αποκτά γνώση του γεγονότος Το σύντομο χρονικό διάστημα που προβλέπεται είναι προφανές ότι αυξάνει το βαθμό δυσκολίας. Η δεύτερη αφορά στη διαδικασία άμεσης ανακοίνωσης της παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, όταν υπάρχει ενδεχόμενο να τεθούν σε υψηλό κίνδυνο τα δικαιώματα και οι ελευθέριές του Ο επικοινωνιακός χειρισμός σε αυτήν την περίπτωση είναι κρίσιμης σημασίας και μπορεί να κάνει τη διαφορά όσον αφορά στη φήμη της επιχείρησης.

9ο Βήμα Δοκιμαστικοί ελέγχου συστημάτων και διαδικασιών

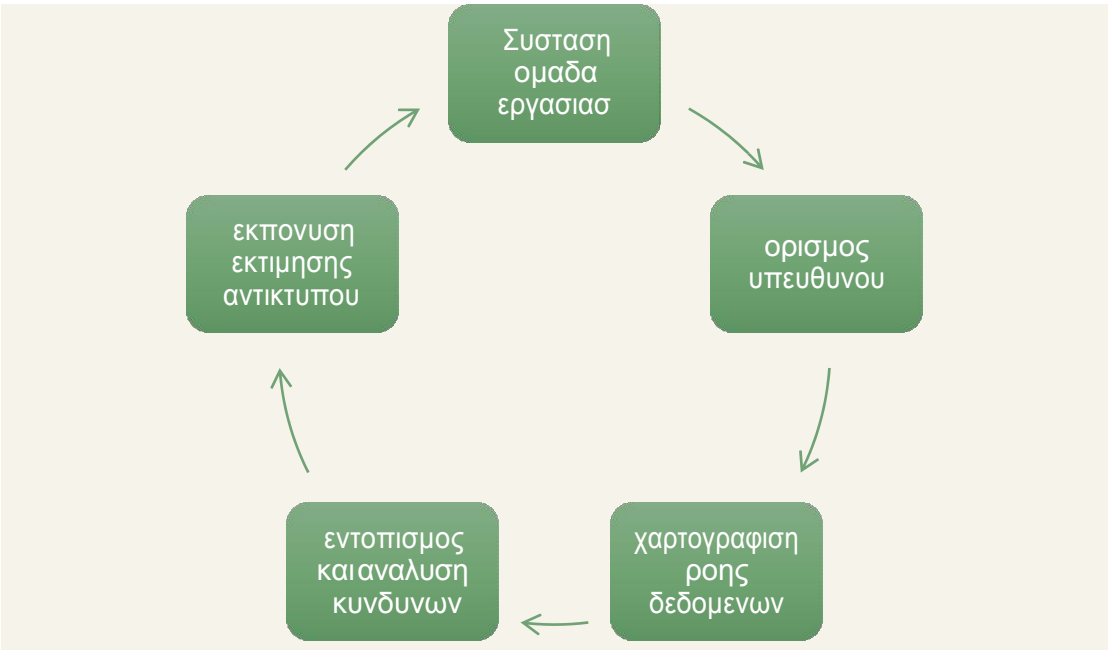
Πρόκειται για το τελευταίο χρονικό στάδιο. Αναφέρεται σε δοκιμαστικούς ελέγχους επι των συστημάτων και διαδικασιών που έχει αναπτύξει η επιχείρηση στα προηγούμενα βήματα, ώστε να αποδειχθεί ότι μετρά την 25ή Μάιου οι ενεργείς συμμόρφωσης δούλεψαν αποτελεσματικά .

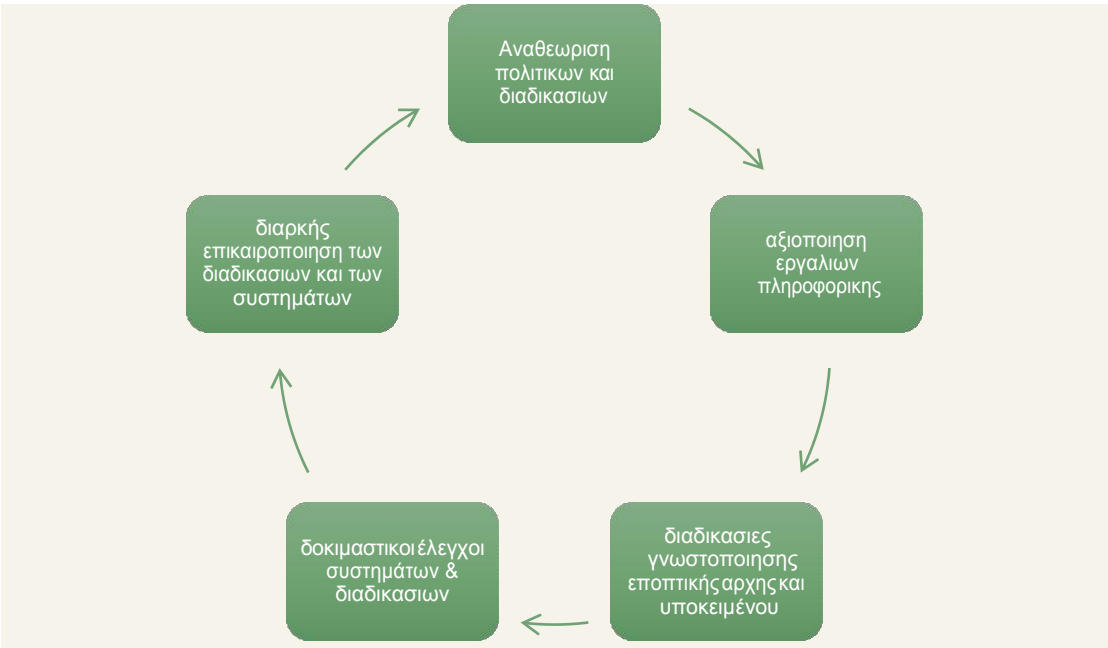
10ο Βήμα Διαρκής παρακολούθηση και επικαιροποίηση των διαδικασιών και των συστημάτων

Η συμμόρφωση στον Κανονισμό είναι μια δυναμική «άσκηση» και στο πλαίσιο αυτό οι επιχειρήσεις οφείλουν συνεχώς να επικαιροποιούν τις διαδικασίες τους (ή έστω να εξετάζουν την αναγκαιότητα επικαιροποίησής τους) και να αναβαθμίζουν τα συστήματα τους. Επιβάλλεται συνεχής επαγρύπνηση και διαρκής παρακολούθηση, καθώς οι κίνδυνοι παραβίασης των δεδομένων είναι πιθανοί ανά πασά στιγμή. Με

αλλά λογία, όπως στο βήμα 9 συστήνονται δοκιμαστικοί ελέγχου των συστημάτων και διαδικασιών πριν την έναρξη εφαρμογής του Κανονισμού, όμοια προτείνονται αντίστοιχες δοκιμές και μετρά την έναρξη εφαρμογής του.

Ο ΔΡΟΜΟΣ ΓΙΑ ΤΗΝ «ΕΞΥΠΝΗ» ΣΥΜΜΟΡΦΩΣΗ





Η Δομή της ομάδας εργασίας για τη συμμόρφωση για το Κανονισμό

ΚΕΦΑΛΑΙΟ 6

6.1 Ορισμός Προστασίας Δεδομένων σε Εταιρίες

Ένα ζήτημα που απασχολεί αρκετά τους Υπευθύνους Επεξεργασίας είναι ποιο είναι το κατάλληλο πρόσωπο να οριστεί ως ΥΠΔ, εφόσον αυτό προβλέπεται από τον Κανονισμό (ή εφόσον ο ίδιος ο οργανισμός το έχει επιλέξει).

Αφετηρία της απόφασης αυτής αποτελούν τα πραγματικά προσόντα του, γι' αυτό και είναι προφανές ούτι ο ΥΠΔ πρέπει να έχει μια βαθιά γνώση του Κανονισμού και κατανόηση των προβλέψεων του. Ως εκ τούτου, επαγγελματίες με νομικό υπόβαθρο ή/και τεχνογνωσία στις πρακτικές προστασίας δεδομένων έχουν σαφές «προβάδισμα», δίχως ωστόσο αυτό να είναι περιοριστικό ή να υποδεικνύει περιοριστικά αντικείμενα σπουδών / επαγγελματικούς τίτλους που είναι περισσότερο ενδεδειγμένοι. Ο Κανονισμός

δημιουργεί πλέον από μονός του ένα νέο διεπιστημονικό αντικείμενο και ένα νέο τύπο στελέχους /επαγγελματία.

Όσον αφορά στα ζητήματα σύγκρουσης συμφερόντων, απαιτείται ιδιαίτερη προσοχή από τους Υπευθύνους Επεξεργασίας. Είναι προφανές ότι ο ΥΠΔ δεν μπορεί ταυτόχρονα να κατέχει και θέση από την οποία μπορεί να καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας. Για παράδειγμα, ο Διευθυντής Πληροφορικής είναι το άτομο της ανώτατης διοίκησης που αποφασίζει για τα συστήματα και τους μηχανισμούς ασφάλειας για την επεξεργασία δεδομένων στον οργανισμό, επομένως δεν μπορεί να είναι και το άτομο που παρακολουθεί και τη συμμόρφωση με τις προβλέψεις του Κανονισμού. Ομοίως ισχύει και για το Νομικό Σύμβουλο του οργανισμού.

Ταυτόχρονα, οι Υπεύθυνοι Επεξεργασίας πρέπει να αντιληφθούν ότι στην ουσία ο ΥΠΔ είναι ένας Project manager και ως εκ τούτου, η θέση του έχει υψηλές απαιτήσεις για συγκεκριμένα προσόντα και χαρακτηριστικά, όπως υπευθυνότητα και εμπιστευτικότητα, τήρηση χρονοδιαγραμμάτων, τήρηση πολίτικων και διαδικασιών, επικοινωνιακές δεξιότητες, δεξιότητες συντονισμού ομάδας και συνεργασίας κ.α. Παράλληλα, ο ΥΠΔ πρέπει να έχει αντίληψη του τομέα δραστηριότητας του οργανισμού στον οποίο απασχολείται.

Σε σχέση με την Ομάδα Εργασίας και τον ΥΠΔ, υπογραμμίζεται ούτι επί της ουσίας ο ΥΠΔ έχει το συντονιστικό ρολό. Όπως προαναφέρθηκε, είναι σημαντικό στην Ομάδα Εργασίας να συμμετέχει υπεύθυνος εκπρόσωπος από τις Διευθύνσεις Πληροφορικής, Νομικής και Ανθρωπίνου Δυναμικού, οι οποίες εμπλέκονται εξ ορισμού λόγω του αντικειμένου τους, Επιπλέον, συστήνεται να συμμετέχει ένας εκπρόσωπος από κάθε επιχειρησιακή Διεύθυνση, ώστε να εξασφαλίζεται ούτι η διαδικασία συμμόρφωσης με τον Κανονισμό ευθυγραμμίζεται με τη λειτουργιά του οργανισμού, ούτι παρέχεται η απαιτούμενη ανατροφοδότηση / επικοινωνία από και προς τις επιχειρησιακές Διευθύνσεις κ.λπ.

Τέλος, ειδικά σε μεγάλους οργανισμούς, βάσει όγκου προσωπικών δεδομένων, είναι προφανές ότι ο ΥΠΔ χρειάζεται να υποστηριχτεί από στελέχη, υπό την επίβλεψη του, για την εξυπηρέτηση των υποκείμενων (ως front desk). Μπορεί κάνεις εύκολα να φανταστεί για μια ασφαλιστική επιχείρηση ή μια επιχείρηση κινητής τηλεφωνίας τον όγκο των αιτημάτων προς τον ΥΔ, η διαχείριση των οποίων πρέπει να γίνει σε

σαφώς ορισμένα χρονοδιαγράμματα από τον Κανονισμό, αλλά κυρίως με τρόπο που θα προστατεύουν τα συμφέρονται και περισσότερο τη φήμη του οργανισμού.[25]

6.2 Πρακτικά παραδείγματα συμμόρφωσης στον Κανονισμό

Στην παρούσα ενότητα παρουσιάζονται πρακτικά παραδείγματα για την επίτευξη συμμόρφωσης με τον Κανονισμό, μέσα από την εμπειρία δυο εταιρειών με αυξημένες υποχρεώσεις συμμόρφωσης με τον Κανονισμό και ειδικότερα μια επιχείρηση του ασφαλιστικού κλάδου και μια του οργανωμένου λιανεμπορίου.

Περίπτωση Α': Επιχείρηση από τον ασφαλιστικό κλάδο

Η πορεία συμμόρφωσης με τις διατάξεις του Κανονισμού για τη συγκεκριμένη επιχείρηση ξεκίνησε ήδη από το Σεπτέμβριο του 2016, μέσα σε ένα περιβάλλον «φόβου» για το μέγεθος των αλλαγών που θα απαιτούνταν κυρίως γιατί ο ασφαλιστικός κλάδος, όπως και η τηλεφωνία, οι τράπεζες και ορισμένοι άλλοι κλάδοι κατέχουν μεγάλο όγκο προσωπικών δεδομένων εξ ορισμού.

Η εταιρεία μέσα από τη διαδικασία εκπόνησης Εκτίμησης Αντίκτυπου είχε τη δυνατότητα να χαρτογραφήσει την υφισταμένη κατάσταση της σχετικά με την προστασία δεδομένων, να εντοπίσει ποια κενά υπήρχαν στα συστήματα της και κατ' επέκταση να προσδιορίσει τα μετρά που έπρεπε να υιοθετήσει προκειμένου να επιτύχει το στόχο της συμμόρφωσης.

Ειδικότερα, ακολουθηθήκαν τα εξής βήματα για την επίτευξη της συμμόρφωσης με τον Κανονισμό:

1. Συστάθηκε Ομάδα Εργασίας, με τον ΥΠΔ αλλά και τη συμμετοχή στελεχών ούλων των Διευθύνσεων της εταιρείας που σχετίζονται άμεσα με τον Κανονισμό (π.χ. Νομική Διεύθυνση, Διεύθυνση Πληροφορικής, Διεύθυνση Διαχείρισης Κίνδυνου, Διεύθυνση Κανονιστικής Συμμόρφωσης κ.λπ.).
2. Ορίστηκαν εκείνα τα Τμήματα της εταιρείας που εμπλέκονται με προσωπικά δεδομένα (π.χ. Marketing, Operations και Εξυπηρέτηση Πελατών), με στόχο τη χαρτογράφηση αυτών. Σε αυτό το σημείο η εμπειρία της εταιρείας ανέδειξε ότι απαιτείται ιδιαίτερη προσοχή, καθώς πολλές φορές υπάρχουν προσωπικά δεδομένα σε Τμήματα που δεν είναι αναμενόμενο ή άμεσα προφανές. Δυο ενδεικτικά παραδείγματα αποτυπώνουν εύληπτα το γεγονός αυτό: α) με αφορμή πραγματοποίηση διαγωνισμού για συμβόλαιο υγειάς από το Τμήμα Δημοσιών Σχέσεων, τελικά εντοπίστηκε ούτι το Τμήμα συγκέντρωνε ιατρικά στοιχειά των πελατών/νικητών οι οποίοι επικοινωνούσαν μαζί τους για το συμβόλαιο τους και β) προκλήθηκε προβληματισμός σχετικά με εάν το Τμήμα Ανθρωπίνου Δυναμικού μιας εταιρείας πρέπει να έχει πρόσβαση στο ομαδικό συμβόλαιο υγειάς των εργαζομένων, καθώς αυτό συνεπάγεται ότι έχει πρόσβαση σε ευαίσθητα προσωπικά δεδομένα, τα οποία ενδεχομένως χρησιμοποιηθούν για την αξιολόγηση στελεχών δίχως αντικειμενικότητα (π.χ. προαγωγή, με βάση το ιατρικό ιστορικό). Επίσης, κρίσιμο σημείο στη διαδικασία της χαρτογράφησης αποτελεί ο εντοπισμός επαναλήψεων των προσωπικών δεδομένων (να διατηρούνται ακριβώς τα ιδία δεδομένα σε περισσότερα του ενός σημεία στην εταιρεία - duplications).

[25] https://segm.gr/wp-content/uploads/2018/10/meleti_sev_GDPR

3. Η Ομάδα Έργου προχώρησε σε ανάλυση και κατανόηση των απαιτήσεων του Κανονισμού.
4. Πραγματοποιήθηκε σχετική παρουσίαση / ενημέρωση προς την ανώτατη Διοίκηση της εταιρείας, ώστε να εξασφαλιστεί η δέσμευση και η διάθεση των απαιτούμενων πόρων για την υλοποίηση του έργου συμμόρφωσης
5. Εκπονήθηκε Εκτίμηση Αντίκτυπου σχετικά με την προστασία δεδομένων, με την ενεργή εμπλοκή όλων των Τμημάτων της εταιρείας. Μέσω αυτής της διαδικασίας, αναδείχθηκαν τα κενά ασφάλειας (gaps), τα οποία έπρεπε να αντιμετωπιστούν. Επιπλέον, η εταιρεία αξιοποίησε τη διαδικασία εκπόνησης της Εκτίμησης Αντίκτυπου με τρόπο ώστε ταυτόχρονα να διαγνώσει την ψηφιακή της ετοιμότητα (digital benchmark) και σε δεύτερο χρόνο να αναλάβει δράση για την αναβάθμιση της ως προς το στοιχειό αυτό.
6. Για κάθε κενό ασφάλειας σχεδιάστηκε συγκεκριμένη λύση η οποία στη συνέχεια εναρμονίστηκε με τις πολίτικες και διαδικασίες των Τμημάτων της εταιρείας.
7. Υλοποιηθήκαν δοκιμαστικοί ελέγχου των συστημάτων και διαδικασιών, με διαφορετικά σενάρια, ώστε να εξασφαλιστεί η όσο το δυνατόν μεγαλύτερη προστασία
8. Ορίστηκαν Βασικοί Δείκτες Απόδοσης (Key Performance Indicators - KPIs), προκειμένου η εταιρεία να μπορεί να αξιολογήσει την πορεία συμμόρφωσης της στον Κανονισμό.
9. Οργανωθήκαν εκπαιδευτικές δράσεις για το σύνολο του προσωπικού (π.χ. βίντεο, κουίζ σε ηλεκτρονική πλατφόρμα, παρουσιάσεις), προκειμένου αφενός να ενημερωθούν τα στελέχη και αφετέρου να ενισχυθεί η ευαισθητοποίηση τους σχετικά με την προστασία των προσωπικών δεδομένων. Σημειώνεται ούτι η εκπαίδευση του προσωπικού συμβάλλει καταλυτικά στο να αποφευχθούν φαινόμενα απώλειας ή κλοπής δεδομένων. Τέλος, είναι σημαντικό κάθε εταιρεία να πραγματοποιεί εκπαιδευτικές δράσεις σε συνεχή βάση, δεν αποτελεί δηλαδή “on-off” διαδικασία.[26]

6.3 Ο δρόμος για την επίτευξη της συμμόρφωσης επιχείρησης από τον ασφαλιστικό κλάδο

[26] https://segm.gr/wp-content/uploads/2018/10/meleti_sev_GDP

Ορισμένες χαρακτηριστικές ενέργειες στις οποίες προέβη η εταιρεία ήταν οι εξής:

- Δόθηκε ιδιαίτερη έμφαση στις φόρμες που συμπληρώνουν οι πελάτες τα στοιχειά τους, ώστε να εξεταστούν εκ νέου υπό το πρίσμα του σκοπού της επεξεργασίας: δηλαδή εάν είναι απαραίτητο κάθε πεδίο (πράγματι αξιοποιείται από τις Λειτουργικές Διευθύνσεις της εταιρείας;) και αν είναι σύννομο.

- Ορίστηκαν συγκεκριμένα και δομημένα χρονικό διαστήματα για τη διατήρησητων προσωπικών δεδομένων (retention periods). Στο πλαίσιο αυτό, διαγραφήκαν ή καταστραφήκαν πολλά δεδομένα, σε ηλεκτρονική ή έντυπη μορφή, που πλέον δεν υπήρχε λόγος να αποθηκεύονται. Μάλιστα, επισημαίνεται ότι η εν λόγω διαδικασία στην πράξη αποδεικνύεται χρονοβόρα και δύσκολη, ενώ συνήθως υποτιμάται.

- Αναθεωρηθήκαν ούλα τα συμβόλαια (εκτός ούλων ούσα έληγαν στον επόμενο χρόνο), ώστε οι οροί να είναι συμβατοί με τον Κανονισμό.

- Επιλέχθηκε εξωτερικός συνεργάτης για την παροχή των εργαλείων και λύσεων πληροφορικής που συμβάλλουν αποτελεσματικά στη διαδικασία συμμόρφωσης (π.χ. χαρτογράφηση προσωπικών δεδομένων, κρυπτογράφηση κ.λπ.).

- Εντάχθηκε στη Διεύθυνση Εσωτερικού Ελέγχου ξεχωριστή λειτουργιά για τον έλεγχο του Κανονισμού.

- Αναθεωρήθηκε η πολιτική σχετικά με τη χρήση usb sticks, σκληρών δίσκων και laptops, με τρόπο ώστε να εξασφαλιστεί ότι τίποτα δεν μπαίνει ή βγαίνει από το δίκτυο της εταιρείας.

- Δόθηκε ιδιαίτερη προσοχή στα ζητήματα ασφάλειας των κινητών τηλέφωνων των ασφαλιστών, καθώς αποτελούν βασικό εργαλείο της δουλείας τους εκτός εταιρείας.

- Δημιουργήθηκε κοινό γλωσσάρι των προσωπικών δεδομένων, ώστε να υπάρχει κοινή κατανόηση των εννοιών και των διαδικασιών από όλους τους εργαζομένους στην εταιρεία.

- Υιοθετήθηκε πολιτική εκκαθάρισης των επιφανειών εργασίας (clean desk assessment) και οργάνωσης των αποθηκευτικών χώρων. Πρόκειται για μια διαδικασία η οποία μπορεί να διαρκέσει περισσότερο από το αναμενόμενο στην αρχική της υλοποίηση. Επίσης, αναδεικνύει τις μεγάλες ανάγκες σε αποθηκευτικό χώρο, ιδίως για τα έγχαρτα αρχεία, γεγονός που συνεπάγεται κόστος για την εταιρεία σε υποδομές και εξοπλισμό. Σημειώνεται οτι η δράση συνδέεται και με την πολιτική για τη διατήρηση των δεδομένων (retention periods).

- Υιοθετηθήκαν πολίτικες καταγραφής του ιστορικού των δεδομένων (data lineage) και τήρησης αρχείου επεξεργασίας προσωπικών δεδομένων (personal data processing registry), με ιδιαίτερη επισήμανση των προσωπικών και ευαίσθητων δεδομένων, καθώς και των δεδομένων με αξία για την εταιρεία.

- Δημιουργήθηκε διαδικασία ελέγχου κίνησης δεδομένων (data traffic control) ώστε για οποιοδήποτε εξερχόμενο να ακολουθείται συγκεκριμένη διαδικασία.

- Εντοπίστηκαν τα περιττά (waste) αλλά και τα αδόμητα δεδομένα

(unstructured). Η εμπειρία της εταιρείας ανέδειξε οτι ο όγκος τους ήταν μεγαλύτερος από τον εκτιμώμενο. Σημειώνεται οτι απαιτείται διαρκής παρακολούθηση και εκκαθάριση των εν λόγω δεδομένων, δεν αποτελεί δηλαδή “on-off” διαδικασία.

Περίπτωση Β’: Επιχείρηση από το οργανωμένο λιανεμπόριο (μέλος πολυεθνικού ομίλου)

Για τον πολυεθνικό όμιλο στον οποίο ανήκει η εταιρεία του παραδείγματος μας, η διαδικασία συμμόρφωσης στις νέες διατάξεις αντιμετωπίστηκαν εξ αρχής ως «ευκαιρία» και ουχί ως «πρόκληση». Το γεγονός ότι στον Όμιλο προϋπήρχε του Κανονισμού η κουλτούρα σεβασμού των προσωπικών δεδομένων, αποτέλεσε σημαντική βοηθητική παράμετρο, καθώς υπήρχε όχι μόνο η σχετική εμπειρία αλλά κυριότερα η ευαισθητοποίηση της διοίκησης και των στελεχών.

Ο Όμιλος προέβη σε συγκεκριμένες ενέργειες προκειμένου να εναρμονίσει τις πολίτικες και τις διαδικασίες του στις προβλέψεις του Κανονισμού, υπό το πρίσμα ούτι επεξεργάζεται προσωπικά δεδομένα τεσσάρων κατηγοριών: α) προμηθευτών, β) πελατών, γ) υπάλληλων και δ) τρίτων προσώπων. Ειδικότερα, η διαδικασία επίτευξης της συμμόρφωσης ξεκίνησε το Φεβρουάριο του 2017 (περισσότερο από ένα χρόνο πριν την έναρξη εφαρμογής του Κανονισμού) και πραγματοποιηθήκαν σταδιακά τα ακόλουθα βήματα:

1. Συστάθηκε Ομάδα Εργασίας, σε κάθε επιχείρηση του Ομίλου, για την παρακολούθηση της προόδου του έργου συμμόρφωσης (αποτελούμενη από στελέχη κυρίως της Νομικής Διεύθυνσης και της Διεύθυνσης Πληροφοριακών Συστημάτων). Από τους πρώτους στόχους κάθε Ομάδας ήταν η εξασφάλιση της δέσμευσης των ιεραρχικά ανωτέρων στελεχών για τη διάθεση των απαιτούμενων πόρων για τους σκοπούς του έργου (π.χ. προϋπολογισμός, τεχνικοί και ανθρώπινοι πόροι). Προς την κατεύθυνση αυτή, οργανωθήκαν ενημερώσεις προς τους Γενικούς Διευθυντές.
2. Πραγματοποιηθήκαν στοχευόμενες ενημερώσεις προς το σύνολο των Τμημάτων που διαχειρίζονται προσωπικά δεδομένα. Σημειώνεται ότι «κλειδί» σε αυτό το στάδιο είναι η εκάστοτε Ομάδα Εργασίας να αναγνωρίσει επιτυχώς ποιοι διαχειρίζονται προσωπικά δεδομένα εντός της επιχείρησης (σημ.: δεν είναι πάντοτε προφανές και εύκολα αναγνωρίσιμο).
3. Δημιουργηθήκαν ερωτηματολόγια προς τα ως άνω Τμήματα για την καταγραφή των προσωπικών δεδομένων (π.χ. τι είδους δεδομένα, για ποιο σκοπό, για πόσο κ.λπ.) και την κατηγοριοποίηση αυτών με βάση το επίπεδο κίνδυνου (π.χ. χαμηλού, μεσαίου, υψηλού).
4. Με αφετηρία τα ερωτηματολόγια, συντάχθηκαν περισσότερο αναλυτικά αρχεία για κάθε επεξεργασία, τα επονομαζόμενα “record keepings”, με στόχο τον αναλυτικό προσδιορισμό των τηρουμένων διαδικασιών και των αρμοδίων προσώπων σχετικά με τα προσωπικά δεδομένα. Ενδεικτικά, ποιος είναι ο υπεύθυνος επεξεργασίας και ποιος ο εκτελών την επεξεργασία, που διαβιβάζονται τα δεδομένα, ποια συστήματα εμπλέκονται σε αυτή τη διαδικασία, ποια είναι η περίοδος διατήρησης των δεδομένων (retention period) κ.ά.
5. Αξιοποιώντας τα δυο προηγούμενα στάδια, καταγραφήκαν τα κενά (gaps) στα οποία έπρεπε να δοθεί μεγαλύτερη προσοχή. Στον Όμιλο το κυριότερο

κενό αφορούσε την περίοδο διατήρησης των δεδομένων (retention period), καθώς δεν γινόταν διαγραφή δεδομένων.

6. Ενημερωθήκαν τα αρμόδια στελέχη σχετικά με τα εντοπισμένα κενά και οργανωθήκαν οι επόμενες ενέργειες ώστε να αντιμετωπιστούν.
7. Εκπονήθηκε Εκτίμηση Αντίκτυπου σχετικά με την προστασία δεδομένων.

Με βάση τα στάδια (6) και (7), λήφθηκαν συγκεκριμένες αποφάσεις και αναπτυχθήκαν σχετικές πολίτικες, με στόχο την εξασφάλιση της προστασίας των προσωπικών δεδομένων. Ενδεικτικά, αναφέρονται:

- ➢ Αλλαγή του τρόπου ενημέρωσης των υποκείμενων όσον αφορά στα σχήματα πιστότητας (loyalty schemes).
- ➢ Ορισμό συγκεκριμένου χρόνου διατήρησης των βιογραφικών σημειωμάτων για ην αναζήτηση νέων στελεχών.
- ➢ Αλλαγές των ορών των συμβάσεων με προμηθευτές.
- ➢ Αξιολόγηση του επιπέδου συμμόρφωσης με τον νέο Κανονισμό των συνεργατών που έχουν, άμεση ή έμμεση, πρόσβαση στις βάσεις και στα δεδομένα, καθώς έχουν και οι ίδιοι ευθύνη.
  ➢Ανάθεση διακριτών ρολών και ανάλογης διαβάθμισης της δυνατότητας πρόσβασης στα προσωπικά δεδομένα, ανάλογα με το ρολό / θέση κάθε στελέχους.

- ➢ Αλλαγές στις διαδικασίες για τα φυσικά αρχεία με προσωπικά δεδομένα (π.χ. φύλλα παράπονων στα καταστήματα) και τις διαδρομές που ακολουθούν εντός της επιχείρησης.

- ➢ Ανάληψη δράσεων εκπαίδευσης και ενημέρωσης του συνόλου του προσωπικού, ώστε να γίνει αντιληπτός από όλους ο λόγος για τον οποίο καλούνται να ακολουθήσουν μια συγκεκριμένη – νέα – διαδικασία και ποια είναι αυτή. Οι δράσεις εκπαίδευσης προτείνεται να οργανωθούν σε στάδια, π.χ. πρώτα στους πλέον άμεσα εμπλεκομένους και σε δεύτερο χρόνο στο σύνολο του προσωπικού. Τα κυριότερα οφέλη που αποκομίζει ο Όμιλος μέσα από τη διαδικασία συμμόρφωσης στον Κανονισμό συνοψίζονται στα εξής:

✓Δημιουργία αισθήματος ασφαλούς περιβάλλοντος στον πελάτη, το οποίο συνεπάγεται την εμπιστοσύνη του πελάτη και κατ' επέκταση εξασφαλίζει την πιστότητα του.

- ✓ Ανάδειξη ευκαιριών για οργανωτικές αλλαγές στην επιχείρηση.
- ✓ Κίνητρο για έλεγχο και αναβάθμιση των συστημάτων και των διαδικασιών, σε τακτική βάση. [27]

[27] https://segm.gr/wp-content/uploads/2018/10/meleti_sev_GDPR

ΚΕΦΑΛΑΙΟ 7

7.1 Κέρδη από τη συμμόρφωση με τον Κανονισμό

- ✓ Δημιουργία ασφαλούς περιβάλλοντος
- ✓ Εμπιστοσύνη πελατών
- ✓ Υψηλό επίπεδο υπάλληλων
- ✓ Οργανωτικές αλλαγές με θέσπιση πολίτικων & διαδικασιών
- ✓ Έλεγχος και αναβάθμιση συστημάτων και διαδικασιών σε τακτική βάση
- ✓ Έλεγχος των συνεργατών που έχουν πρόσβαση άμεση ή έμμεση στις βάσεις και στα δεδομένα

Χρήσιμες συμβουλές για τις μικρές και μεσαίες επιχειρήσεις για την συμμόρφωση στον Κανονισμό
1. Προσαρμογή των βημάτων συμμόρφωσης στην κατάλληλη κλίμακα Κάθε επιχείρηση οφείλει να προσαρμόσει τα βήματα και τις έξυπνες αρχές συμμόρφωσης, με βάση τις δίκες της ανάγκες, τα χαρακτηριστικά (φύση και όγκος δεδομένων), το μέγεθος, το αντικείμενο των εργασιών και τη στρατηγική της.
2. Μικρό μέγεθος επιχείρησης δεν σημαίνει και μικρή επεξεργασία Ιδιαίτερη προσοχή απαιτείται, στην περίπτωση που οι επιχειρήσεις είναι μικρού μεγέθους (βάσει κύκλου εργασιών ή /και προσωπικού), ωστόσο προβαίνουν σε εκτενή επεξεργασία προσωπικών δεδομένων, κυρίως λόγω της δραστηριότητας τους (π.χ. μια εταιρεία παροχής υπηρεσιών φύλαξης, ή μια εταιρεία παροχής υπηρεσιών “cloud”). Με αλλά λογία, η έμφαση που πρέπει να δοθεί από τον κάθε επιχειρηματία που εξετάζει κατά ποσό επηρεάζεται από τις απαιτήσεις του Κανονισμού είναι στον όγκο και στο βαθμό επεξεργασίας των προσωπικών δεδομένων που κατέχει και ουχί στο μέγεθος του.
3. Αποφυγή υπερβολών σε πολίτικες και διαδικασίες Σκοπός είναι η επίτευξη της συμμόρφωσης δίχως να επιβαρυνθούν

περισσότερο με περιττά βάρη και πολύπλοκες ή ανεφάρμοστες διαδικασίες οι μικρομεσαίες επιχειρήσεις, οι οποίες διαθέτουν περιορισμένους πόρους. Κάθε επιχείρηση πρέπει να υιοθετήσει εκείνα τα μετρά προστασίας προσωπικών δεδομένων που τις ταιριάζουν και που σκοπεύει έμπρακτα να εφαρμόσει (όχι δηλαδή απλά για τους τύπους), κάποια εκ των οποίων δε είναι ανέξοδα (π.χ. οριστική διαγραφή δεδομένων που δεν χρησιμοποιούνται κ.λπ.).

7.2 Συμβουλές για τις μικρές και μεσαίες επιχειρήσεις για την συμμόρφωση στον Κανονισμό

Για τις μικρές και μεσαίες επιχειρήσεις το κόστος συμμόρφωσης είναι, ενδεχομένως, δυσανάλογα μεγάλο. Ειδικά για τις επιχειρήσεις αυτές, παραθέτουμε παρακάτω ορισμένες χρήσιμες συμβουλές στην προσπάθεια τους να προσαρμοστούν στον Κανονισμό, ώστε να διευκολυνθούν στην «αγωνιά» τους να συμμορφωθούν και να αποφύγουν τα υψηλό πρόστιμα, τα οποία σε περίπτωση επιβολής θα ήταν για αυτές παράγοντας επιβίωσης.

7.3 Τα οφέλη του Κανονισμού στην επιχειρηματική στρατηγική

Ο Κανονισμός παρουσιάζει σημαντικές ευκαιρίες, που αν αξιοποιηθούν, μπορούν να συμβάλουν στην ουσιαστική βελτίωση του τρόπου λειτουργιάς του επιχειρηματικού μοντέλου, με αποτέλεσμα όχι απλά την τυπική συμμόρφωση, αλλά την επίτευξη θετικού πρόσημου μέσα από την εν λόγω διαδικασία. Αυτό μπορεί να επιτευχτεί εάν οι επιχειρήσεις, αντί για ένα ακόμα «στείρο» νομικό κείμενο υποχρεώσεων, εκλάβουν τον Κανονισμό ως υποχρεωτική «άσκηση» χάρη στην οποία θα αλλάξουν την επιχειρηματική κουλτούρα προς οφέλους τους, δίχως να επιβαρυνθούν με σημαντικό χρηματικό και διοικητικό κόστος.

Η πρώτη αρχή αφορά στο «νοικοκύρεμα» των (προσωπικών) δεδομένων. Μέχρι σήμερα οι επιχειρήσεις, κατά συνήθης πρακτική, επιδίδονται σε ένα «κυνήγι όγκου» δεδομένων, γεγονός που συνεπάγεται σημαντικό κόστος συγκέντρωσης, καταχώρισης, ψηφιοποιήσεις, φύλαξης, επεξεργασίας, ανάλυσης κ.λπ. Ο Κανονισμός «αναγκάζει» τις επιχειρήσεις να επανεξετάσουν τα δεδομένα τους, αλλά και τις δομές, τις εσωτερικές λειτουργιές και τις διαδικασίες τους σε σχέση με αυτά. Δηλαδή τις καλεί να επανεξετάσουν ποια δεδομένα διατηρούν, πως τα συλλέγουν, για ποιο σκοπό, για πόση διάρκεια, ποιος έχει πρόσβαση σε αυτά και πως φυλάσσονται

Μέσα από αυτή τη διαδικασία είναι βέβαιο ότι θα προκύψουν χρήσιμα συμπεράσματα σχετικά με το αν τα δεδομένα αξιοποιούνται επαρκώς από την επιχείρηση, ή μήπως πολύτιμες πληροφορίες μένουν ανεκμετάλλευτες χάνοντας επιχειρηματικές ευκαιρίες (π.χ. πληροφορίες σχετικές με το προφίλ των πελατών). Παράλληλα, θα αναδειχθούν οι κίνδυνοι που αφορούν τις συνθήκες ασφάλειας των δεδομένων (π.χ. το σύνολο του προσωπικού έχει πρόσβαση σε ευαίσθητα δεδομένα δίχως αυτό να είναι απαραίτητο για την εργασία του, ή πάλαια προσωπικά δεδομένα φυλάσσονται ακόμα, δίχως πραγματικό πλέον λόγο και μάλιστα σε χώρους με ανεμπόδιστη πρόσβαση). Ως εκ τούτου, θα αναδειχθούν τα αναγκαία μετρά προφύλαξης που πρέπει να υιοθετηθούν και τα οποία προστατεύουν τις επιχειρήσεις από νομικούς και οικονομικούς κίνδυνους, όπως η επιβολή προστίμων από την

εποπτική Αρχή. Τέλος, είναι προφανές οτι όσο μικρότερος είναι ο όγκος των δεδομένων που διατηρούνται, τόσο μειώνεται το κόστος όπως αυτό εκφράζεται σε εργατοώρες, υλικοτεχνικό εξοπλισμό και έπιπλα, χώρο γραφείων, σε χρόνο και χώρο για backup κ.λπ. Επομένως, τα οφέλη της ελαχιστοποίησης των προσωπικών δεδομένων είναι πολλαπλά.

Η δεύτερη αρχή αφορά στη μετατροπή της υποχρέωσης συμμόρφωσης σε ανταγωνιστικό πλεονέκτημα. Όταν ακόμη οι αναζητήσεις μας στο διαδίκτυο αποκαλύπτουν τις προσωπικές ή επαγγελματικές προτιμήσεις μας και το κινητό μας «εκπέμπει» τα προσωπικά μας δεδομένα, είναι εύλογο ούτι ο τρόπος προστασίας τους γρήγορα θα αποτελέσει κριτήριο για τις επιλογές που θα κάνουν οι πελάτες, οι προμηθευτές και οι ίδιοι οι εργαζόμενοι. Είναι δε χαρακτηριστικό ούτι έχει ήδη ξεκινήσει διεθνώς μια πολύ ζωντανή και ενδιαφέρουσα συζήτηση γύρω από την προστασία των προσωπικών δεδομένων και την ανάγκη αυτορρύθμισης των επιχειρήσεων, ώστε να αποφευχθούν δυστροπία σενάρια μιας επερχόμενης «ψηφιακής δικτατορίας».

Υπό αυτήν την έννοια, η προστασία των προσωπικών δεδομένων σχετίζεται άμεσα με την εμπιστοσύνη πελατών, προμηθευτών και εργαζομένων και κατ' επέκταση με τη φήμη της επιχείρησης. Αυτό που είναι σημαντικό για κάθε **επιχείρηση** είναι να μπορεί να αποδείξει (σε όλες τις προαναφερθείσες κατηγορίες ενδιαφερομένων) ότι προστατεύει τα προσωπικά τους δεδομένα από τις τέσσερις βασικές περιπτώσεις παραβίασης τους: α) την εισβολή, δηλαδή το να εισέρχεται μια επιχείρηση στον προσωπικό χώρο κάποιου υποκείμενου, να επικοινωνεί μαζί του και να του υποδεικνύει τι να κάνει, β) τη συγκέντρωση δεδομένων σε βαθμό που να εισπράττει το υποκείμενο ούτι παρακολουθείται σε μεγαλύτερη έκταση από αυτή που θα έπρεπε, γ) την επεξεργασία δεδομένων με τρόπο που να εισπράττει το υποκείμενο ότι μια επιχείρηση κατέχει πολλά προσωπικά του δεδομένα και προβαίνει σε επεξεργασία αυτών και δ) την αποκάλυψη των δεδομένων του από την επιχείρηση με τρόπο που το υποκείμενο δεν είναι σύμφωνο

Συνεπώς, η **επιχείρηση** που θα κάνει το σεβασμό της προσωπικότητας και της ιδιωτικότητας στοιχειό της κουλτούρας της και θα το εντάξει στην επιχειρηματική της στρατηγική θα αποκτήσει σαφές ανταγωνιστικό πλεονέκτημα έναντι των υπολοίπων.

Τέλος, **η τρίτη αρχή** αφορά στην επένδυση σε λύσεις που προσφέρει η τεχνολογία και, μέσω αυτής της διαδικασίας, στην είσοδο στην εποχή της ψηφιακής οικονομίας. Είναι γεγονός ούτι η ενσωμάτωση των ψηφιακών τεχνολογιών στην επιχειρηματική λειτουργιά αποτελεί πλέον μονόδρομο για την επιβίωση και ανάπτυξη των **επιχειρήσεων**. Υπό αυτήν την έννοια, ο Κανονισμός μπορεί να αποτελέσει πύλη εισόδου στη ψηφιακή κοσμογονία (ενδεικτικά, business analytics, big data), καθώς οι τεχνολογίες πληροφορικής και επικοινωνιών παρέχουν ουχί μονό εργαλεία συμμόρφωσης χαμηλού κόστους (π.χ. cloud computing, firewalls, κρυπτογράφηση, ψευδωνυμοποίηση κ.α.), αλλά και λύσεις που τελικά θα αναβαθμίσουν το ίδιο το επιχειρηματικό μοντέλο.

Με αλλά λογία, όπως αναφέρθηκε στην αρχή της παρούσας έκθεσης, οι τεχνολογικές εξελίξεις ήταν αυτές που σε μεγάλο βαθμό προκάλεσαν την ανάγκη μετάβασης από την Οδηγία στον Κανονισμό για την προστασία των προσωπικών δεδομένων, αλλά ταυτόχρονα είναι εκείνες που προσφέρουν και τις λύσεις συμμόρφωσης σε αυτόν. Μέσω αυτής της διαδικασίας, οι επιχειρήσεις καλούνται να εξοικειωθούν, προβληματιστούν, ερευνήσουν, ανασχεδιάσουν τις δομές και τις λειτουργιές τους με βάση τα εργαλεία που προσφέρει η τεχνολογία συνολικά, όχι μονό για τις ανάγκες

συμμόρφωσης στο νέο κανονιστικό πλαίσιο. Εξάλλου, η ενσωμάτωση των ψηφιακών τεχνολογιών στην επιχειρηματική στρατηγική αποτελεί πλέον προαπαιτούμενος για την επιβίωση και ανάπτυξη των επιχειρήσεων [28]

Οι αρχές για έξυπνη συμμόρφωση με το κανονισμό και τα οφέλη της επιχείρησης	
Νοικοκύρεμα των (προσωπικών) δεδομένων	• ✓ Ανάδειξη δεδομένων που - ενδεχομένως -συνδέονται με επιχειρηματικές ευκαιρίες • ✓ Ανάδειξη κίνδυνων που αφορούν τις συνθήκες ασφάλειας των δεδομένων και κατ' επέκταση ενέργειες για αποτελεσματική προστασία • ✓ Μείωση όγκου δεδομένων που διατηρούνται και κατ' μείωση κόστους (σε εργατοώρες, υλικοτεχνικό εξοπλισμό και έπιπλα, χώρο γραφείων, χρόνο και χώρο για backup κ.ά.)
Μετατροπή της υποχρέωσης συμμόρφωσης σε ανταγωνιστικό πλεονέκτημα	✓ Εμπιστοσύνη πελατών, προμηθευτών και εργαζομένων ✓ Προστασία φήμης της επιχείρησης
Επένδυση σε λύσεις που προσφέρει η τεχνολογία	✓ Ενσωμάτωση των ψηφιακών τεχνολογιών στην επιχειρηματική λειτουργιά

7.4 Τα σημεία πρέπει να προσέξουν οι επιχειρήσεις κατά την εφαρμογή του Κανονισμού

Ο Κανονισμός θέτει νέες κανονιστικές απαιτήσεις προς τις επιχειρήσεις, οι οποίες έρχονται να προστεθούν στις ήδη υφιστάμενες για την προστασία των προσωπικών δεδομένων (αλλά και φυσικά σε όλες τις υπόλοιπες απαιτήσεις που προκύπτουν από το λοιπό θεσμικό πλαίσιο κάθε κλάδου). Έχει πολύ μεγαλύτερο πεδίο εφαρμογής από ο, τι η Οδηγία, αφορά πολύ περισσότερες **επιχειρήσεις**, «καταργεί» τα σύνορα δραστηριοποίησης, προβλέπει πολύ μεγαλύτερες ποινές, στρέφει όλο το βάρος της απόδειξης συμμόρφωσης στις επιχειρήσεις δίνοντας «δευτερεύοντα» ρολό στις εποπτικές Αρχές και στην κατεύθυνση αυτή θέτει πολύ συγκεκριμένες απαιτήσεις που εξασφαλίζουν τη συμμόρφωση.

Ποια σημεία πρέπει να προσέξουν οι επιχειρήσεις κατά την εφαρμογή του κανονισμού

[28] https://segm.gr/wp-content/uploads/2018/10/meleti_sev_GDPR

✓ Διαχείριση του κόστους που επιβαρύνει την καθημερινή λειτουργιά για την επίτευξη συμμόρφωσης
✓ Επιλογή των κατάλληλων στελεχών ή / και εξωτερικών συνεργατών (κύριο κριτήριο επιλογής: αξιοπιστία και αποτελεσματικότητα)
✓ Λανθασμένη εντύπωση ούτι δεν εμπίπτουν στον Κανονισμό και ως εκ τούτου ούτι δεν χρειάζεται να προβούν σε καμιά δράση συμμόρφωσης.
✓ Λανθασμένη εντύπωση ούτι δεν απειλούνται από περιστατικά παραβίασης των συστημάτων τους και ούτι είναι ασφαλείς
✓ Σημεία υψηλής τεχνικότητας: ο Φορτικότητα των δεδομένων ο Δικαίωμα στη λήθη ο Εξασφάλιση συγκατάθεσης υποκείμενου ο Συμβάσεις με τρίτα μέρη - Σχέσεις με Εκτελούντες την Επεξεργασία

7.5 Γενικές προκλήσεις και παγίδες

Αναλυτικότερα, με τον Κανονισμό προκύπτουν κόστη που επιβαρύνουν την καθημερινή λειτουργιά των επιχειρήσεων και ο τρόπος που θα επιδιώξουν να τα διαχειριστούν αποτελεί σημαντική πρόκληση:

- Συγκρότηση και μισθοδοσία της Ομάδας Εργασίας ή /και του ΥΠΔ που θα αναλάβει τις ενέργειες συμμόρφωσης στον Κανονισμό.
- Εκπόνηση της εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων, είτε αξιοποιηθούν ίδιες δυνάμεις της επιχείρησης, είτε υπάρξει συνεργασία με εξωτερικό σύμβουλο.
- Ανασχεδιασμό των συστημάτων σχετικά με τον τρόπο εξασφάλισης της συγκατάθεσης των υποκείμενων.
- Ανασχεδιασμό όλων των πληροφοριακών συστημάτων για την ενίσχυση της προστασίας από επιθέσεις παραβίασης ασφάλειας.

Διαμόρφωση των νέων πολίτικων και διαδικασιών για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

Διάδοση και κατανόηση εντός της επιχείρησης των νέων υποχρεώσεων, πολίτικων και διαδικασιών που προκύπτουν.

Τα κόστη αυτά είναι αναμενόμενο ότι προκαλούν - το λιγότερο - προβληματισμό όσον αφορά στον τρόπο που μπορεί να κερδηθεί το στοίχημα της συμμόρφωσης

με τον Κανονισμό, ειδικά τη στιγμή που η ελληνική επιχειρηματικότητα, και κυρίως οι μικρομεσαίες επιχειρήσεις, αντιμετωπίζει δύσκολες οικονομικές συνθήκες, πάρα τα - διστακτικά - σημάδια ανάκαμψης. Επιπροσθέτως, αποτελεί πρόκληση για τις επιχειρήσεις η επιλογή των κατάλληλων στελεχών ή / και συνεργατών που θα τους βοηθήσουν στην ικανοποίηση των απαιτήσεων του Κανονισμού, καθώς ήδη «ανοίγεται» μια νέα αγορά παροχής συμβουλευτικών και εκπαιδευτικών υπηρεσιών, αλλά και στελεχών ΥΠΔ, η οποία προφανώς δεν μπορεί να είναι ούλη υψηλού επιπέδου. Απαιτείται επομένως, ιδιαίτερη προσοχή στον τρόπο και τα κριτήρια επιλογής, αλλά και προσεκτική αξιολόγηση των προσφερόμενων υπηρεσιών κάθε συνεργάτη.

Η αξιοπιστία και η αποτελεσματικότητα πρέπει να αποτελούν τη βάση επιλογής, με τις επιχειρήσεις να εστιάζουν σε επιλογές που ταιριάζουν στα δικά τους χαρακτηριστικά, ανάγκες, πληροφοριακά συστήματα κ.λπ. Κατά τη γνώμη μας, οι επιχειρήσεις μπορούν να θέσουν σε δεύτερο επίπεδο το καθαρά οικονομικό κόστος, καθώς αυτό που είναι σημαντικό είναι ότι μέσα από τη διαδικασία συμμόρφωσης στον Κανονισμό φιλοδοξείτε να προκύψουν οφέλη που θα αναμορφώσουν συνολικά το επιχειρηματικό μοντέλο και την επιχειρηματική κουλτούρα. Σημαντική «παγίδα» για τις **επιχειρήσεις** αποτελεί επίσης, το γεγονός λανθασμένα να έχουν την πεποίθηση ότι δεν εμπίπτουν στον Κανονισμό και ως εκ τούτου να θεωρούν ότι δεν χρειάζεται να προβούν σε καμιά δράση συμμόρφωσης.

Η αντίληψη αυτή είναι ιδιαιτέρα επικίνδυνη καθώς μπορεί να φέρει τις **επιχειρήσεις** αντιμέτωπες με υψηλό πρόστιμα και ισχυρό πλήγμα στη φήμη τους και για το λόγο αυτό καλούμε για την ιδιαίτερη προσοχή τους. Ενδεικτικά, οι **επιχειρήσεις** μπορεί να μην έχουν αντιληφθεί ότι κατέχουν και επεξεργάζονται προσωπικά δεδομένα, ή να μην κατανοούν πως αυτά ορίζονται, ή να νομίζουν ούτι μονό οι μεγάλες επιχειρήσεις πρέπει να λάβουν μετρά Κ.Ο.Κ.

Τέλος, η πεποίθηση ορισμένων επιχειρήσεων ότι δεν απειλούνται από περιστατικά παραβίασης των συστημάτων τους πρόκειται περί πλάνης. Παραφράζοντας τον πρώην Διευθυντή του FBI, Robert S. Mueller III, οι οργανισμοί διακρίνονται σε τρεις κατηγορίες: α) σε εκείνους που έχουν ήδη πέσει θύμα παραβίασης των δεδομένων τους και το έχουν αντιληφθέν, β) σε εκείνους που έχουν ήδη πέσει θύμα παραβίασης των δεδομένων τους και δεν το αντιληφθέν ακόμα και γ) σε εκείνους που δεν έχουν ακόμα πέσει θύμα παραβίασης των δεδομένων τους, αλλά θα πέσουν στο προσεχές μέλλον. Πρέπει επομένως να γίνει απολυτά κατανοητό ούτι κανένας οργανισμός (επιχείρηση ή δημόσιος φορέας) δεν έχει συστήματα 100% ασφαλή έναντι περιστατικών παραβίασης δεδομένων, για αυτό αλώστε χρειάζεται επαγρύπνηση και διαρκής παρακολούθηση. [29]

7.6 Οι εξελίξεις και τα επόμενα βήματα

Ένα χρόνο μετά την έναρξη εφαρμογής του Κανονισμού για την προστασία των προσωπικών δεδομένων, τα ερωτήματα που παραμένουν «ανοιχτή», τόσο σε επίπεδο ΕΕ, όσο και σε εθνικό επίπεδο, είναι πολλά. Ενδεικτικά, αναφέρουμε παρακάτω τα κυριότερα σημεία προβληματισμού για την επομένη ημέρα του Κανονισμού, όπως τα έχουμε καταγράψει από την επικοινωνία με τις επιχειρήσεις, από επαφές με εμπειρογνώμονες, ειδικούς και στελέχη των αρχών και των συναρμοδίων υπουργείων, καθώς και από την παρακολούθηση της ευρωπαϊκής επικαιρότητας (αρθρογραφία, νομολογία, ευρωπαϊκός δημόσιος διάλογος κ.α.).

[29] https://segm.gr/wp-content/uploads/2018/10/meleti_sev_GDPR

Οι προκλήσεις της επόμενης ημέρας την έναρξης εφαρμογής του Κανονισμού
1. Ψήφιση εθνικής νομοθεσίας που είναι σε εκκρεμότητα
2. Αυξημένες ευθύνες για την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
3. Βαθμός ανταπόκρισης Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, με δεδομένη την υποστελέχωση της
4. Τρόπος λειτουργιάς Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων
5. Βαθμός ανταπόκρισης επιχειρήσεων στις υποχρεώσεις
6. Βαθμός ανταπόκρισης υποκείμενων
7. Βαθμός ανταπόκρισης φορέων δημοσίου τομέα

7.7 Βαθμός ανταπόκρισης επιχειρήσεων

Οι έρευνες που πραγματοποιηθήκαν κατά το διάστημα πριν Μαΐου 2018 στην Ελλάδα έδειξαν ούτι ο βαθμός ετοιμότητας των επιχειρήσεων σχετικά με τη συμμόρφωση τους στις διατάξεις του Κανονισμού είναι μάλλον «μέτριος». Η επομένη ημέρα της έναρξης εφαρμογής του Κανονισμού έφερε μεγάλη αναστάτωση στις **επιχειρήσεις**, η οποία αποτυπώθηκε μέσω της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου προς τα υποκείμενα των δεδομένων, τα οποία τηρούσαν, ζητώντας τη συγκατάθεση τους για την διατήρηση των δεδομένων και την επεξεργασία αυτών. Ακόμα όμως και οι **επιχειρήσεις** που δεν είχαν ολοκληρώσει τα βήματα συμμόρφωσης συνεχίζουν να λαμβάνουν τα κατάλληλα μετρά ώστε να το πράξουν τουλάχιστον έως την ημερομηνία δημοσίευσης του εθνικού Νομού.

Προκύπτουν όμως ακόμα ερωτήματα όπως: θα αναδεχθεί η συμμόρφωση στον Κανονισμό ως μια πραγματικά δυναμική άσκηση στην πράξη, μέσω της οποίας βελτιώνεται το ιώδιο το επιχειρηματικό μοντέλο; Ποια θα είναι η αντίδραση στην επιβολή των πρώτων προστίμων; Ποια θα είναι η αντίδραση στα πρώτα αιτήματα διαγράφης ή φορτικότητας δεδομένων; [30]

Όπως έχει αναφερθεί, οι τεχνολογικές εξελίξεις ήταν μια από τις παραμέτρους που ανέδειξαν την αναγκαιότητα θέσπισης του Κανονισμού. Οι τεχνολογικές εξελίξεις είναι αυτές που θέτουν επίσης, προκλήσεις - ως προς την εφαρμογή - στον ιώδιο τον Κανονισμό από την αρχή της ισχύος του. Πιο χαρακτηριστικό είναι το παράδειγμα της «σύγκρουσης» μεταξύ των διατάξεων του Κανονισμού για τη λήψη συγκατάθεσης

[30] https://segm.gr/wp-content/uploads/2018/10/meleti_sev_GDPp

(συγκέντρωση προσωπικών δεδομένων με ξεκάθαρο τον σκοπό επεξεργασίας) από τη μια πλευρά και των δυνατοτήτων που προσφέρει η μηχανική μάθηση (machine learning) και η επεξεργασία μεγάλων δεδομένων (big data) από την άλλη, οπού συχνά δεν είναι δυνατόν ο σκοπός (ή οι σκοποί) επεξεργασίας να είναι προσδιορισμένος από την αρχή (συχνά, δεν μπορούμε καν να τον φανταστούμε με τη σημερινή

γνώση).

Επομένως, εύλογα προκύπτουν ερωτήματα σχετικά με το πως μπορεί να βρεθεί η ισορροπία στην πράξη, με τρόπο που να βοηθάει τόσο την τεχνολογική εξέλιξη και τα οφέλη που προκύπτουν, όσο και την προστασία των δικαιωμάτων των υποκείμενων.

ΕΠΙΛΟΓΟΣ

Η ανάγκη ενιαίας ρύθμισης της αγοράς των προσωπικών δεδομένων, οδήγησαν στην αυστηρότητα του νομικού πλαισίου πανευρωπαϊκά και στη θέσπιση του νέου Γενικού Κανονισμού GDPR. Με έναρξη εφαρμογής την 25η Μαΐου 2018, ο νέος Κανονισμός, αν και με ένα αρκετά αυστηρό και γραφειοκρατικό πλαίσιο, ήρθε να θωρακίσει την ιδιωτικότητα και να μεταθέσει την ευθύνη της προστασίας στην ιδία την επιχείρηση, προβλέποντας κυρώσεις ύψους έως και 4% του παγκοσμίου τζίρου για όσους αποτύχουν να συμμορφωθούν με τις απαιτήσεις του. Συνεπώς η συμμόρφωση με τις απαιτήσεις του Ευρωπαϊκού Κανονισμού παρουσιάζει ένα δίλημμα για τον επιχειρηματικό κόσμο: θα την αντιμετωπίσουμε ως άλλη μια κανονιστική υποχρέωση - δηλαδή σαν βάρος - ή σαν μια ευκαιρία ουσιαστικής και εκ βαθών αλλαγής του **επιχειρηματικού** μοντέλου και εισαγωγής των ελληνικών επιχειρήσεων στον κόσμο της ψηφιακής οικονομίας;

Παρότι η συμμόρφωση φαίνεται να συνεπάγεται υψηλά κόστη και βαριές διαδικασίες, οι ειδικοί του χώρου επιμένουν: Εκείνος που θα μετατρέψει την κουλτούρα σεβασμού και προστασίας των προσωπικών δεδομένων σε πυρήνα της καθημερινής του λειτουργιάς, θα αποκτήσει αυτόματα ένα «ανταγωνιστικό πλεονέκτημα». Γιατί θα είναι εκείνος που θα είναι διαρκώς σε θέση να αποδείξει στον **καταναλωτή**, τον **πελάτη**, τον **εργαζόμενο**, όχι μονό ότι έχει λάβει τα απαραίτητα μετρά προστασίας των

προσωπικών δεδομένων τους, αλλά και ότι είναι διαρκώς σε θέση να τα διατηρεί προστατευμένα.

Στην παρούσα Μελέτη επικεντρωθήκαμε σε δυο κυρίως ζητήματα**: α) στην παρουσίαση των βασικών σημείων του Κανονισμού με τρόπο απλό και κατανοητό και**

β) στην καθοδήγηση των επιχειρήσεων σχετικά με τον τρόπο επίτευξης της «έξυπνης» συμμόρφωσης, δηλαδή της αξιοποίησης των ευκαιριών που παρουσιάζονται από τον Κανονισμό.

Συνοψίζοντας, θα θέλαμε να σημειώσουμε ούτι τα κυρία σημεία του Κανονισμού που διαφαίνεται να δυσκολεύουν τις επιχειρήσεις στην πορεία

συμμόρφωσης, στη δεδομένη χρονική στιγμή (δηλαδή τους πρώτους μήνες συμμόρφωσης) είναι: α) οι υποχρεώσεις γύρω από τον ΥΔΠ (κυρίως ποιο είναι το σωστό πρόσωπο και πως θα ασκήσει τα καθήκοντα του στην πράξη), β) τα ζητήματα σχετικά με την εκπόνηση Εκτίμησης Αντίκτυπου, γ) η ετοιμότητα για τη διαχείριση των περιπτώσεων παραβίασης των δεδομένων, δ) ο χειρισμός του δικαιώματος στη λήθη, ε) ο τρόπος εξασφάλισης της συγκατάθεσης, ζ) ο χειρισμός των αιτημάτων περί φορητότητας δεδομένων και η) οι οροί των συμβάσεων με τρίτα μέρη. Είναι κατανοητό ότι όσο οι επιχειρήσεις, αλλά και τα υποκείμενα προσωπικών δεδομένων, εξοικειώνονται με τις υποχρεώσεις και τις απαιτήσεις του Κανονισμού, τόσο τα πεδία που σήμερα φαίνονται να προβληματίζουν θα εξαλείφονται ή θα αντικαθίστανται από αλλά.

Όσον αφορά στη διαδικασία συμμόρφωσης, παρουσιάσαμε πως, με την τεχνολογία πολύτιμο συμπαραστάτη, και ακολουθώντας τα 10 + 1 βήματα για έξυπνη συμμόρφωση προτείνει, είναι εφικτή η υιοθέτηση λύσεων προσαρμοσμένων στις ανάγκες και τις ιδιαιτερότητες κάθε οργανισμού. Το «νοικοκύρεμα» των προσωπικών δεδομένων, η μετατροπή της υποχρέωσης συμμόρφωσης σε ανταγωνιστικό

πλεονέκτημα και η επένδυση σε λύσεις που προσφέρει η τεχνολογία και, μέσω αυτής της διαδικασίας, η είσοδος στην εποχή της ψηφιακής οικονομίας, αποτελούν τις βασικές αρχές που θα πρέπει να διέπουν κάθε οργανισμό.

Εν κατακλείδι, είναι σημαντικό οι επιχειρήσεις να κατανοήσουν ούτι η διαδικασία συμμόρφωσης με τον Κανονισμό αφενός επιφέρει οφέλη στη λειτουργιά τους, σε επίπεδο φήμης και αναδιοργάνωσης και αφετέρου ούτι πρόκειται για ένα ταξίδι που δεν τέλειωσε με την παρέλευση της, ούτε με την ολοκλήρωση των ενεργειών συμμόρφωσης. Αντιθέτως, είναι ένα συνεχές ταξίδι συμμόρφωσης που μπορεί να αναδεχθεί σε ταξίδι **επιχειρηματικής** επιτυχίας[31].

ΒΙΒΛΙΟΓΡΑΦΙΑ

http://www.dpa.gr/portal/page?_pageid=33,213319&_dad=portal&_schem

https://segm.gr/wp-content/uploads/2018/10/meleti_sev_GDPρ

https://www.icap.gr/Default.aspx?id=10594&nt=146&lang=1

https://www.euro2day.gr/specials/opinions/article/1615180/gdpr-grifos-h-eykairia.html

https://www.lawspot.gr/nomika-nea/gdpr-dimosieythike-o-nomos-4624-2019-gia-tin-prostasia-prosopikon-dedomenon

Από την επίσημη ιστοσελίδα της Επιτροπής
https://europa.eu/european-union/eu-law/legal-acts_en

https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el

Κυριαζόγλου Ιωάννης (2019) Προστασία Προσωπικών Δεδομένων (GDPR Protection)