Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών &
Μηχανικών Ηλεκτρονικών Υπολογιστών

Πανεπιστήμιο Πειραιά
Τμήμα Βιομηχανικής Διοίκησης &
Τεχνολογίας

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

«ΕΦΑΡΜΟΓΗ ΤΟΥ ΝΕΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (EU 2016/679) ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ»

Ευφροσύνη-Ειρήνη Δημουλά

Επιβλέποντες :

Δρ. Κωνσταντίνος Σιασιάκος
Επιστημονικός Συνεργάτης Ε.Μ.Π

Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π

Αθήνα, Φεβρουάριος 2018

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών &
Μηχανικών Ηλεκτρονικών Υπολογιστών

Πανεπιστήμιο Πειραιά
Τμήμα Βιομηχανικής Διοίκησης &
Τεχνολογίας

«ΕΦΑΡΜΟΓΗ ΤΟΥ ΝΕΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (EU 2016/679) ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ»

Ευφροσύνη-Ειρήνη Δημουλά

Εγκρίθηκε από την τριμελή επιτροπή την 15η Φεβρουαρίου 2018.

.....	.....	.....
Ιωάννης Ψαρράς	Δημήτριος Ασκούνης	Κωνσταντίνος Σιασιάκος
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Επιστημονικός Συνεργάτης Ε.Μ.Π.

.....

Ευφροσύνη-Ειρήνη Δημουλά
Πτυχιούχος Οργάνωσης και Διοίκησης Επιχειρήσεων

Στη μνήμη του Νικολή μου,

που ήταν πάντα δίπλα μου και δεν πρόλαβε να τη δει ολοκληρωμένη,

καθώς και στη μητέρα μου Σόνια,

για την ανιδιοτελή αγάπη και υποστήριξή της όλα αυτά τα χρόνια.

ΕΥΧΑΡΙΣΤΙΕΣ

Με την ολοκλήρωση της μεταπτυχιακής μου εργασίας, θα ήθελα να ευχαριστήσω τους ανθρώπους που με βοήθησαν όλο αυτό τον καιρό, ο καθένας με το δικό του τρόπο.

Πρωτίστως, θα ήθελα να εκφράσω τις θερμές ευχαριστίες και την ευγνωμοσύνη μου, στον επιβλέποντά μου, Δρ. Κωνσταντίνο Σιασιάκο και τον Καθηγητή κ. Δημήτριο Ασκούνη, τόσο για τη εμπιστοσύνη που μου έδειξαν με την ανάθεση της εργασίας αυτής, όσο και για τις κατευθυντήριες γραμμές, τις πολύτιμες συμβουλές και τις εύστοχες υποδείξεις που μου προσέφεραν καθ' όλη τη διάρκεια εκπόνησής της.

Ένα μεγάλο ευχαριστώ θα ήθελα επίσης να εκφράσω στον κύριο Ευαγγελίδη Αντώνη, Διευθυντή Εταιρικής Συμμόρφωσης της ΒΙΑΝΕΞ Α.Ε., για την άμεση ανταπόκρισή του στο αίτημά μου για αξιοποίηση του υλικού της παρουσίασής του στο πρακτικό μέρος της εργασίας μου.

Τέλος, θέλω να ευχαριστήσω θερμά την οικογένεια μου, τους φίλους και τους συναδέλφους μου, για την αμέριστη αγάπη, συμπαράσταση και υπομονή που επέδειξαν όλο αυτό το διάστημα αλλά και κατά τη διάρκεια της διετούς φοίτησής μου στο αναφερόμενο μεταπτυχιακό και κατέστησαν ουσιαστικά συμμέτοχοι στην εκπλήρωση αυτής της μεταπτυχιακής εργασίας.

Ευφροσύνη-Ειρήνη Δημουλά

Φεβρουάριος 2018

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΠΕΡΙΛΗΨΗ

Η ραγδαία και συνεχής τεχνολογική εξέλιξη των τελευταίων ετών, κατέστησε αναγκαία τη θέσπιση ενός νέου ρυθμιστικού πλαισίου για την προστασία των προσωπικών δεδομένων, το οποίο να διευρύνει τις ήδη υπάρχουσες μεθόδους προστασίας και να διασφαλίζει ακόμα περισσότερο τα δικαιώματα των ατόμων.

Σκοπός της παρούσας μεταπτυχιακής εργασίας είναι η περιγραφή των νέων κατευθυντήριων γραμμών και αλλαγών που εισάγει ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ) από τις 25 Μαΐου 2018 τόσο σε ευρωπαϊκό όσο και σε εθνικό επίπεδο, καθώς και οι διαδικασίες που ακολουθούνται σε πρακτικό επίπεδο για τη συμμόρφωση με αυτόν σε μια ελληνική εταιρεία.

Αρχικά, παρουσιάστηκαν τα ισχύοντα νομικά πλαίσια για την προστασία των προσωπικών δεδομένων στην Ευρώπη και στην Ελλάδα, με έμφαση στην Οδηγία 95/46/ΕΚ και στο Νόμο 2472/1997 και διαπιστώθηκε η ανάγκη εκσυγχρονισμού της ισχύουσας νομοθεσίας με την εισαγωγή του νέου ΓΚΠΔ.

Στη συνέχεια, αναλύθηκαν όλες οι νέες αλλαγές και προκλήσεις που εισάγει ο ΓΚΠΔ, για τις επιχειρήσεις στον ιδιωτικό και δημόσιο τομέα, αλλά και τα δικαιώματα που απορρέουν από την εφαρμογή του για τα υποκείμενα των δεδομένων με αναφορά και στην προστασία των ανηλίκων. Περιγράφηκαν ακόμα, οι αρμοδιότητες και ο ρόλος του Υπευθύνου Προστασίας Δεδομένων (DPO) αλλά και τα πρόστιμα και οι κυρώσεις που αντιμετωπίζουν οι επιχειρήσεις από τη μη συμμόρφωσή τους με τον Κανονισμό.

Επιπλέον, προτάθηκαν τα αρχικά βήματα προετοιμασίας που πρέπει να ακολουθήσει μια επιχείρηση για τη μετάβαση στον ΓΚΠΔ και η ενδεικτική μεθοδολογία συμμόρφωσης με αυτόν, με ειδική αναφορά στον κρίσιμο ρόλο του DPO στη διαδικασία αυτή αλλά και στη σημασία ενός εξειδικευμένου και οργανωμένου πλάνου εκπαίδευσης για το προσωπικό. Για την διευκόλυνση στην εφαρμογή της προτεινόμενης μεθοδολογίας, έγινε εκτενής αναφορά σε μερικά ενδεικτικά λογισμικά υποστήριξης κορυφαίων εταιρειών πληροφορικής αλλά και στις υπηρεσίες που παρέχουν εξειδικευμένες εταιρείες συμβουλευτικών υπηρεσιών.

Στο πλαίσιο αυτό, παρουσιάστηκε το στρατηγικό σχέδιο και οι φάσεις υλοποίησης συμμόρφωσης με τον ΓΚΠΔ της ελληνικής φαρμακευτικής εταιρείας ΒΙΑΝΕΞ, με στόχο

τη σύγκριση του θεωρητικού υποβάθρου του νέου Κανονισμού, με την πρακτική του εφαρμογή.

Στο τελευταίο κεφάλαιο παρουσιάζονται τα κύρια συμπεράσματα της μεταπτυχιακής εργασίας, που μπορούν να αξιοποιηθούν για περαιτέρω μελλοντική έρευνα και βελτίωση στην εφαρμογή συμμόρφωσης των επιχειρήσεων και οργανισμών με τον ΓΚΠΔ.

Λέξεις Κλειδιά:

Προσωπικά Δεδομένα, Υποκείμενο των Δεδομένων, Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ), Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Υπεύθυνος Προστασίας Δεδομένων, Υποχρέωση Γνωστοποίησης Παραβιάσεων, Εκτίμηση Αντικτύπου, Μεθοδολογία Συμμόρφωσης, Υλοποίηση Στρατηγικού Πλάνου.

ABSTRACT

The rapid and continuous technological development of recent years have made necessary the establishment of a new regulatory framework for the protection of personal data, which will extend the existing protection methods and further safeguard the rights of individuals.

The purpose of this postgraduate thesis is to describe the new guidelines and changes of the General Data Protection Regulation (GDPR), introduced in May 25, 2018 at both European and national level, as well as to present the procedures followed at a practical level for the compliance with it in a Greek company.

Initially, the first chapter presents the existing legal frameworks for the protection of personal data in Europe and Greece, emphasizing on the Commission Directive 95/46/EC and the national Law 2472/1997 and noticing the need to modernize the existing legislation with the introduction of the new GDPR.

The next chapter analyzes all the new changes and challenges introduced by the GDPR for businesses, both in private and public sector, as well as the rights resulting from its application to data subjects with reference to the protection of children. The responsibilities and role of the Data Protection Officer (DPO), as well as the fines and sanctions faced by enterprises by non-compliance with the GDPR, have also been described.

Moreover, the initial steps to be taken by an enterprise for the transition to the GDPR are suggested, as well as the indicative methodology of compliance, with reference to the crucial role of the DPO in this process and the importance of a specialized and organized training plan for staff. Extensive reference is made to exemplary supportive software from leading IT companies and to the services provided by specialized consultancy companies, with the aim to facilitate the implementation of the suggested methodology.

In this context, the strategic plan and phases of compliance with the GDPR of the Greek pharmaceutical company VIANEX are presented, in order to compare the theoretical background of the new Regulation with its practical application.

In the last chapter, the main conclusions of the postgraduate thesis are presented, which can be utilized for additional future research and improvement of enterprises and organizations' compliance with the GDPR.

Key Words:

Personal Data, Data Subject, General Data Protection Regulation (GDPR), Hellenic Data Protection Authority, Data Protection Officer (DPO), Data Breaches Notification, Data Protection Impact Assessment, Compliance Methodology, Strategic Plan Implementation.

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

Συντομογραφία	Επεξήγηση
C.N.I.L.	Commission National de l' Informatique et de Libertés
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDPB	European Data Protection Board
GDPR	General Data Protection Regulation
IT	Information Technology
NIS	Network and Information Security
PNR	Passenger Name Record
ΑΔΑ	Αριθμός Διαδικτυακής Ανάρτησης
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΓΓΠΣ	Γενική Γραμματεία Πληροφοριακών Συστημάτων
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων
ΔΕΥ	Συμβούλιο Δικαιοσύνης και Εσωτερικών Υποθέσεων
ΕΔΔΑ	Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου
ΕΔΕΤ	Εθνικό Δίκτυο Έρευνας και Τεχνολογίας
ΕΕ	Ευρωπαϊκή Ένωση
ΕΚ	Ευρωπαϊκή Κοινότητα
ΕΟΠΥΥ	Εθνικός Οργανισμός Παροχής Υπηρεσιών Υγείας
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου
ΗΔΙΚΑ	Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης
Ν.	Νόμος
Ν.Π.Δ.Δ.	Νομικό Πρόσωπο Δημοσίου Δικαίου
Ν.Π.Ι.Δ.	Νομικό Πρόσωπο Ιδιωτικού Δικαίου
ΟΗΕ	Οργανισμός Ηνωμένων Εθνών
ΟΟΣΑ	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
παρ.	παράγραφος
ΣΛΕΕ	Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης
ΣΦΕΕ	Σύνδεσμος Φαρμακευτικών Επιχειρήσεων Ελλάδος

1. ΕΙΣΑΓΩΓΗ

1.1 Σκοπός – Αντικείμενο

Οι αλματώδεις τεχνολογικές εξελίξεις των τελευταίων ετών και οι εκπληκτικές δυνατότητες που προσφέρει σήμερα η κοινωνία της πληροφορίας, προσέδωσαν στο ζήτημα της προστασίας από την επεξεργασία προσωπικών δεδομένων μία εντελώς διαφορετική ένταση και έκταση σε σχέση με τις προϋπάρχοντες συνθήκες κατά τις προηγούμενες δεκαετίες.

Οι ηλεκτρονικές τεχνολογίες έχουν πλέον εισχωρήσει σε όλους τους τομείς της κοινωνικής ζωής, προσφέροντας απίστευτες δυνατότητες, όπως ταχύτατη καταγραφή, συλλογή, συσχέτιση και επεξεργασία κάθε είδους πληροφοριών και εξαγωγή συμπερασμάτων ακόμα και από τις φαινομενικά πιο ασήμαντες πληροφορίες. Καθημερινά, τεράστιος αριθμός πληροφοριών διακινείται ανάμεσα σε πολίτες, δημόσιες αρχές και ιδιωτικούς φορείς: δεδομένα τραπεζικών λογαριασμών και πιστωτικών καρτών, δεδομένα επικοινωνίας, ιατρικοί φάκελοι, περιηγήσεις ιστοσελίδων, ερωτήματα μηχανισμών αναζήτησης, αναρτήσεις σε κοινωνικά δίκτυα αποτελούν στοιχεία που συνδεόμενα μεταξύ τους σκιαγραφούν την ταυτότητά τους. Όλα αυτά αποτελούν προσωπικά δεδομένα.

Έτσι, παράλληλα με την αδιαμφισβήτητη συμβολή της νέας τεχνολογίας στην πρόοδο και στην βελτίωση της ζωής των ατόμων πολλαπλασιάζονται και οι κίνδυνοι για το άτομο και την κοινωνία. Ποτέ άλλοτε η συμπεριφορά και οι συνήθειες των ατόμων δεν καταγράφονταν τόσο συστηματικά, η προσπάθεια να επεκταθεί η χρήση της συγκέντρωσης προσωπικών δεδομένων δεν ήταν πιο επιμονή και η εμπορευματοποίηση των προσωπικών πληροφοριών δυνητικών καταναλωτών τόσο εκτεταμένη, αφού η πληροφορίες συλλέγονται, μεταφέρονται και «αξιοποιούνται» μέσα σε ελάχιστο χρόνο και με ελάχιστο κόστος.

Κατά συνέπεια, η συλλογή και επεξεργασία των προσωπικών δεδομένων των εν δυνάμει καταναλωτών ανάγεται πλέον σε εγγενές και συστατικό στοιχείο του οικονομικού προγραμματισμού των επιχειρήσεων, ενώ τόσο η συλλογή όσο και η επεξεργασία αυτή γίνεται κατά κανόνα με απόλυτη μυστικότητα, εν αγνοία των ατόμων

και χωρίς ασφαλώς τη συμμετοχή των υποκειμένων των εμπορευματοποιούμενων πληροφοριών στα κέρδη των επιχειρήσεων.

Με τον νέο Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ ή GDPR) που τίθεται σε εφαρμογή στις 25 Μαΐου 2018, η Ευρωπαϊκή Ένωση επιδιώκει την υιοθέτηση ενός νέου πλαισίου στην προστασία των προσωπικών δεδομένων των φυσικών προσώπων, με σκοπό την επικαιροποίηση και τον εκσυγχρονισμό των υφιστάμενων κανόνων της προστασίας των δεδομένων και την αντιμετώπιση της αδιάκοπης συλλογής και επεξεργασίας αυτών.

Μέσα από την παρούσα εργασία θα γίνει προσπάθεια να αναλυθεί όλο το προϋπάρχον και υφιστάμενο πλαίσιο του νέου Κανονισμού και των κανόνων που εισάγει, καθώς και τα βήματα προετοιμασίας που πρέπει να ακολουθήσουν οι επιχειρήσεις για να συμμορφωθούν με τα νέα δεδομένα. Τέλος, θα προταθούν λύσεις για την ευκολότερη μετάβαση και εφαρμογή του νέου Κανονισμού.

1.2 Δομή – Διάρθρωση των κεφαλαίων της εργασίας

Για την καλύτερη κατανόηση του θέματος της εργασίας παρατίθεται η διάρθρωση των κεφαλαίων της.

Στο κεφάλαιο 1 περιγράφεται το αντικείμενο της εργασίας και τίθενται οι στόχοι και τα θέματα τα οποία η παρούσα εργασία καλείται να μελετήσει και να παρουσιάσει.

Στο κεφάλαιο 2 γίνεται μια ιστορική αναδρομή στην πορεία και την εξέλιξη των προσωπικών δεδομένων στη διάρκεια των ετών, με εκτενείς αναφορές στο ευρωπαϊκό και ελληνικό νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων, ενώ αναλύονται οι έννοιες και οι ορισμοί που εμπεριέχονται στον Ν. 2472/1997 του ελληνικού συστήματος.

Στο κεφάλαιο 3 παρουσιάζεται αναλυτικά ο νέος Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων και περιγράφονται οι αλλαγές, οι κυρώσεις και τα δικαιώματα που επιφέρει τόσο στις ευρωπαϊκές και ελληνικές επιχειρήσεις, όσο και στα φυσικά πρόσωπα.

Στο κεφάλαιο 4 αναπτύσσονται σε θεωρητικό επίπεδο τα βήματα προετοιμασίας και οι μεθοδολογίες που μπορούν να ακολουθήσουν οι επιχειρήσεις προκειμένου να εντάξουν τον ΓΚΠΔ στην οργάνωση και τη λειτουργία τους.

Στο κεφάλαιο 5 περιγράφονται τα υφιστάμενα πληροφοριακά συστήματα και λογισμικά υποστήριξης που διευκολύνουν τη μετάβαση των επιχειρήσεων στη συμμόρφωση με τους κανόνες του ΓΚΠΔ. Δίνεται έμφαση στα λογισμικά διαφόρων εταιρειών όπως της Oracle, της SAP, της Microsoft, καθώς και των υπηρεσιών υποστήριξης που παρέχουν εταιρείες όπως η Priority.

Στο κεφάλαιο 6 επιδιώκεται με βάση τα προηγούμενα, η περιγραφή της υλοποίησης στην πράξη της μεθοδολογίας και προετοιμασίας συμμόρφωσης με το νέο Κανονισμό από μια ελληνική επιχείρηση.

Τέλος, στο κεφάλαιο 7 παρουσιάζονται τα τελικά συμπεράσματα που προκύπτουν από την ανάλυση και το σχεδιασμό του θέματος και εξετάζεται το κατά πόσο τα θέματα τα οποία τέθηκαν ως στόχοι έχουν απαντηθεί.

1.3 Στόχοι της εργασίας

Οι στόχοι – θέματα που τίθενται υπό διερεύνηση και εξέταση κατά τη διάρκεια αυτής της εργασίας συνοψίζονται ως εξής:

- Ιστορία προσωπικών δεδομένων και επιτακτική ανάγκη προστασίας αυτών.
- Παρουσίαση του νομικού πλαισίου για την προστασία των δεδομένων σε ευρωπαϊκό και εθνικό επίπεδο.
- Δεδομένα, αλλαγές και νέες ρυθμίσεις που εισάγει ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, στον ιδιωτικό και δημόσιο τομέα.
- Δικαιώματα που αποκτούν τα φυσικά πρόσωπα με το νέο Κανονισμό.
- Περιορισμοί και κυρώσεις που αντιμετωπίζουν οι επιχειρήσεις.
- Γενικό πλάνο και βήματα προετοιμασίας για την ένταξη και τη συμμόρφωση με το νέο Κανονισμό.
- Ο ρόλος του Υπευθύνου Προστασίας Δεδομένων και οι προκλήσεις που αντιμετωπίζει.

- Χρήση και εφαρμογή λογισμικών υποστήριξης και παροχή υπηρεσιών, που διευκολύνουν τη συμμόρφωση των επιχειρήσεων με τον ΓΚΠΔ.
- Συνδυασμός των παραπάνω για την εφαρμογή και υλοποίηση της μεθοδολογίας συμμόρφωσης με τον ΓΚΠΔ σε μια ελληνική επιχείρηση ή κλάδο.

2. Η ΧΡΟΝΙΚΗ ΕΞΕΛΙΞΗ ΘΕΜΑΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

2.1 Εισαγωγή

Το ζήτημα προστασίας των ατόμων από τους κινδύνους που δημιουργούνται από τη συλλογή, επεξεργασία και εν γένει αξιοποίηση των «προσωπικών δεδομένων», πληροφοριών δηλαδή που προσδίδουν «μια ιδιότητα» στο πρόσωπό τους, ανάγεται σε εποχή προγενέστερη της ηλεκτρονικής τεχνολογίας, της τηλεπληροφορικής και του Ίντερνετ, όμως είναι η αλματώδης ανάπτυξη των μέσων αυτών κατά τις τελευταίες δεκαετίες που κατέστησε την προστασίας τους απολύτως επιτακτική.

Έτσι, ήδη από τη δεκαετία του 1970 παρατηρείται μια διαρκώς αυξανόμενη και εντεινόμενη επιρροή μεταξύ αφενός των εξελισσόμενων τεχνολογιών της πληροφορίας και επικοινωνίας και αφετέρου της κοινωνικής και οικονομικής οργάνωσης τους κράτους. Κύρια αιτία ανάπτυξης των τεχνολογιών αυτών, που στην πράξη σήμαινε ελεύθερη ροή πληροφοριών για τους πολίτες μεταξύ των κυβερνητικών οργανισμών, υπήρξε η ανταπόκριση προς τις αυξημένες ανάγκες σε πληροφόρηση των κοινωνικών κρατών της εποχής εκείνης για την επιτέλεση τους παρεμβατικού τους ρόλου. Ορθολογική οργάνωση, περισσότερο αξιόπιστος σχεδιασμός για την πρόβλεψη των κοινωνικών και οικονομικών αλλαγών, εντυπωσιακή μείωση του κόστους διακυβέρνησης αλλά και βελτιωμένη παροχή υπηρεσιών προς τους πολίτες, υπήρξαν τα αδιαμφισβήτητα επιχειρήματα της δημόσιας διοίκησης υπέρ του «εκμοντερνισμού» και του «εξορθολογισμού» αυτού.

Ωστόσο, δεν άργησε να γίνει αντιληπτό ότι η ουσιαστικά απεριόριστη συγκέντρωση πληροφοριών με προσωπικό περιεχόμενο των πολιτών σε συνδυασμό με την τεχνικά πλέον εφικτή δυνατότητα αυτοματοποιημένης, πολύμορφης επεξεργασίας και διασύνδεσης των (κρατικών, αρχικά) αρχείων, οδηγούσε πολύ συχνά σε μια καταχρηστική εκμετάλλευση των πληροφοριών αυτών, με πολλαπλούς και εναλλασσόμενους σκοπούς, όπως π.χ. στην παρακολούθηση και τον πλήρη έλεγχο των πολιτών, χωρίς μάλιστα τη γνώση και πολύ περισσότερο τη συγκατάθεσή τους προς αυτό.

Επίσης, σύντομα έγινε αντιληπτό ότι η κατοχή και περαιτέρω η κατάλληλη επεξεργασία των πληροφοριών προσωπικού χαρακτήρα των ατόμων ήταν σε θέση

όχι μόνο να εξυπηρετεί με τον καλύτερο τρόπο τις επιχειρηματικές ανάγκες, αλλά να επιφέρει και τεράστια οικονομικά οφέλη στους κατόχους τους, ιδιαίτερα στον τομέα της διαφήμισης και στις λοιπές μεθόδους προώθησης των προϊόντων και υπηρεσιών. Στα πλαίσια αυτά άρχισε να αναπτύσσεται μια «βιομηχανία προσωπικών πληροφοριών», απειλώντας έτσι θεμελιώδη δικαιώματά των πολιτών, ιδίως εκείνα της ιδιωτικής ζωής και του απορρήτου τους.

Οι παραδοσιακές θεσμικές εγγυήσεις και δικαιϊκές ρυθμίσεις της εποχής εκείνης δεν φαίνονταν επαρκείς για την προστασία των ατόμων μέσα στα πλαίσια της εξελικτικά διαμορφούμενης κοινωνίας της πληροφορίας και επομένως απαιτούνταν ειδικές προστατευτικές ρυθμίσεις που να παρέχουν μια πιο αποτελεσματική προστασία στα υποκείμενα των προσωπικών αυτών δεδομένων. Έτσι, αρχίζουν να κάνουν την εμφάνισή τους κατά τις δεκαετίες του 1970 (νομοθεσίες «πρώτης γενιάς») και 1980 (νομοθεσίες «δεύτερης γενιάς») σημαντικά εθνικά νομοθετήματα με, προφανώς διόλου τυχαία, τους νομοθέτες των τεχνολογικά ανεπτυγμένων κρατών να αντιδρούν πρώτους.

Στο παρόν κεφάλαιο θα παρουσιαστεί η εξέλιξη της έννοιας των προσωπικών δεδομένων σε βάθος χρόνου, καθώς και τα γεγονότα που συντέλεσαν στη δημιουργία νομοθετικών πλαισίων για την προστασία των προσωπικών δεδομένων, τόσο στην Ευρώπη όσο και στην Ελλάδα. Επιπλέον, θα παρουσιαστούν οι κανονισμοί του Ν. 2472/1997 που ίσχυε μέχρι προσφάτως σε εθνικό επίπεδο, ενώ θα αποσαφηνιστούν οι όροι και οι προϋποθέσεις για την επεξεργασία και την καταστροφή των προσωπικών δεδομένων, τα δικαιώματα που αποκτούν τα «υποκείμενα των δεδομένων» και οι αρμοδιότητες των υπευθύνων εποπτικών αρχών για τη διασφάλιση της προστασίας του απορρήτου.

2.2 Ιστορική Αναδρομή στα προσωπικά δεδομένα

Η προστασία του ατόμου από την αυτόματη επεξεργασία των προσωπικών του πληροφοριών αντιμετωπίσθηκε για πρώτη φορά από τον περίφημο νόμο του ομόσπονδου κρατιδίου της Έσσης στη Γερμανία το 1970. Ακολούθησαν ο Σουηδικός νόμος του 1973, ο Ομοσπονδιακός νόμος της Γερμανίας το 1977 και οι νόμοι της Αυστρίας, Γαλλίας, Δανίας, Νορβηγίας (1978) και του Λουξεμβούργου (1979).

Στις ΗΠΑ, αντιστοίχως, θεσπίστηκαν ο Privacy Act το 1974 και ο μεταγενέστερος Computer Matching and Privacy Act το 1981. Ωστόσο, τα νομοθετήματα αυτά περιορίζουν την προστασία των προσωπικών δεδομένων στο δημόσιο τομέα, ενώ στον ιδιωτικό τομέα δεν υφίσταται κάποια ενιαία νομοθεσία σε ομοσπονδιακό τουλάχιστον επίπεδο. Στον Καναδά αντίστοιχα, σχετικός είναι ο νόμος για τα ανθρώπινα δικαιώματα (άρθρα 49-62).

Βασικός στόχος των νομοθεσιών αυτών, υπήρξε η προστασία της «πληροφοριακής ιδιωτικότητας» και του «πληροφοριακού αυτοκαθορισμού» των ατόμων, το δικαίωμά τους δηλαδή να αποφασίζουν τα ίδια για τη συλλογή, διάδοση και τη γνωστοποίηση σε τρίτους των σχετικών με αυτά πληροφοριών.

Στα πλαίσια αυτά, οι σχετικές εθνικές νομοθεσίες περιόριζαν τη δυνατότητα επεξεργασίας των προσωπικών πληροφοριών των ατόμων σε σκοπούς σαφώς προκαθορισμένους, οι οποίοι όχι μόνο θα έπρεπε να είναι γνωστοί στο υποκείμενο των προσωπικών δεδομένων αλλά θα έπρεπε, επιπλέον, να έχουν γίνει και ρητά αποδεκτοί από αυτό.

Άλλωστε, συνειδητοποιώντας το πρόβλημα αυτό και οι Διεθνείς Οργανισμοί είχαν από νωρίς αναλάβει σημαντικές πρωτοβουλίες, είτε υπό τη μορφή μη δεσμευτικών, κατευθυντήριων οδηγιών και συστάσεων, όπως εκείνες του ΟΟΣΑ, είτε υπό τη μορφή διεθνών συμβάσεων, όπως η εξαιρετικά σημαντική Σύμβαση 108 της 28.1.1981 του Συμβουλίου της Ευρώπης «για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα». Η εν λόγω Σύμβαση του Συμβουλίου της Ευρώπης, η οποία, στη συνέχεια, κωδικοποίησε τις αρχές εκείνες που αποτελούσαν το «σκληρό πυρήνα» της προστασίας των δεδομένων προσωπικού χαρακτήρα των ατόμων (όπως π.χ. την ποιότητα της επεξεργασίας, τα ευαίσθητα δεδομένα, κ.λπ.), έδωσε το έναυσμα για τη δημιουργία μιας νέας, «δεύτερης γενιάς» νομοθετημάτων. Έτσι, αρκετές χώρες προέβησαν στη ψήφιση ειδικών νομοθεσιών ενώ άλλες προχώρησαν σε τροποποίηση της υπάρχουσας νομοθεσίας τους, αναθεωρώντας τις αντιλήψεις των νομοθετημάτων της «πρώτης γενιάς». Άλλωστε και η κατά πολύ μεταγενέστερη κοινοτική Οδηγία 95/46/ΕΚ «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», αν και πολύ πιο εξειδικευμένη και λεπτομερειακή, βασίσθηκε, ουσιαστικά, στη

Σύμβαση αυτή του Συμβουλίου της Ευρώπης. Η ψήφιση της Οδηγίας 95/46/ΕΚ σηματοδότησε την «τρίτη γενιά» νομοθετημάτων.

Το 1990, ο Ο.Η.Ε. εξέδωσε κατευθυντήριες οδηγίες σε σχέση με την προστασία των ηλεκτρονικών βάσεων δεδομένων, περιλαμβάνοντας για πρώτη φορά και διατάξεις για την εποπτεία και για τα συστήματα κυρώσεων από τις παραβάσεις, γεγονός που αποδεικνύει την μετέπειτα συνειδητοποίηση της ανάγκης ορθής εφαρμογής των κανόνων προστασίας προσωπικών δεδομένων.

Επιπλέον, είναι σημαντικό να υπογραμμισθεί ότι και η προστασία του απαραβίαστου της ιδιωτικής και οικογενειακής ζωής των ατόμων και του απορρήτου των επικοινωνιών έχει βαθιές ρίζες αλλά και διεθνή διάσταση καθώς το δικαίωμα αυτό κατοχυρώνονταν ήδη από την «Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου» του 1948. Έτσι, το άρθρο 12 αυτής διεκήρυσσε ότι: «Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία, ή την αλληλογραφία του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους».

Όμως, το σημαντικότερο υπερεθνικό νομοθετικό κείμενο για την προστασία της ιδιωτικότητας με αντίκτυπο στον ευρωπαϊκό χώρο αποτελεί το άρθρο 8 της «Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου» (ΕΣΔΑ) του 1950 το οποίο κατοχυρώνει το δικαίωμα της ιδιωτικής ζωής παντός προσώπου και ορίζει ότι: 1. «Κάθε πρόσωπο έχει δικαίωμα για σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας τους και της αλληλογραφίας του» και, εν συνεχεία 2. «Δεν επιτρέπεται να υπάρξει επέμβαση δημόσιας αρχής στην άσκηση του δικαιώματος αυτού, εκτός εάν η επέμβαση αυτή προβλέπεται από το νόμο και αποτελεί μέτρο το οποίο, σε μια δημοκρατική κοινωνία, είναι αναγκαίο για την εθνική ασφάλεια, τη δημόσια ασφάλεια, την οικονομική ευημερία της χώρας, την προάσπιση της τάξης και την πρόληψη ποινικών παραβάσεων, την προστασία της υγείας ή της ηθικής ή την προστασία των δικαιωμάτων και των ελευθεριών των άλλων». Το άρθρο 8 της ΕΣΔΑ αποτελεί το βασικό άξονα γύρω από τον οποίο περιστρέφεται η Ενωσιακή νομοθεσία. Επίσης, το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) έχει συμβάλλει αποφασιστικά με τη νομολογία στην αναγνώριση της προστασίας των προσωπικών δεδομένων και στην ερμηνευτική προσέγγιση της έννοιας της ιδιωτικότητας.

Πρόκειται ουσιαστικά για το δικαίωμα κάθε ανθρώπου να μην καθίσταται πληροφοριακό αντικείμενο και να (συν)προσδιορίζει ο ίδιος ποιες πληροφορίες που τον αφορούν θα καταστούν γνωστές στο περιβάλλον.

2.3 Το Ευρωπαϊκό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων

Η προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Νομοθεσία αναφέρθηκε για πρώτη φορά στο άρθρο 6 της Συνθήκης για την Ευρωπαϊκή Ένωση, στο άρθρο 8 της Ευρωπαϊκής Σύμβασης των δικαιωμάτων του ανθρώπου και στο άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.

Συγκεκριμένα, στο Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ, που μετά την θέση σε ισχύ της Συνθήκης της Λισαβόνας το Δεκέμβριο του 2009 έχει το ίδιο κύρος με τη Συνθήκη της ΕΕ και τη ΣΛΕΕ, κατοχυρώνεται ρητά το δικαίωμα στην προστασία τόσο της ιδιωτικής και οικογενειακή ζωής, ήτοι: «Κάθε πρόσωπο έχει δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και των επικοινωνιών του» (άρθρο 7), όσο και των προσωπικών του δεδομένων, ήτοι:

1. «Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν» και

2. «Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση την συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει την διόρθωσή τους». (άρθρο 8).

Η πρώτη ωστόσο ολοκληρωμένη αναφορά για την προστασία των δεδομένων προσωπικού χαρακτήρα, έγινε με την Οδηγία 95/46/ΕΚ, «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών».

Με τις ρυθμίσεις της γενικής Οδηγίας 95/46/ΕΚ επιδιώκεται, αφενός η εξασφάλιση της προστασίας θεμελιωδών δικαιωμάτων των φυσικών προσώπων, με κυριότερο εκείνο της προστασίας της ιδιωτικής ζωής αυτών από την επεξεργασία δεδομένων

προσωπικού χαρακτήρα, αφετέρου δε η διασφάλιση της απρόσκοπτης διασυνοριακής ροής προσωπικών δεδομένων μεταξύ των κρατών μελών σε τομείς της οικονομικής, διοικητικής και κοινωνικής δραστηριότητας. Έτσι, η Οδηγία αποσκοπεί στην εναρμόνιση των εθνικών νομοθεσιών στο ζήτημα της προστασίας των δεδομένων προσωπικού χαρακτήρα ούτως ώστε να εξαλειφθούν τα εμπόδια στην κυκλοφορία των δεδομένων αυτών, ενώ παράλληλα επιδιώκει να εξασφαλιστεί η ελεύθερη ροή των δεδομένων. Περαιτέρω, στόχος της επιδιωκόμενης εναρμόνισης είναι η κατοχύρωση ενός υψηλού επιπέδου προστασίας των προσωπικών δεδομένων των ατόμων στην κοινότητα. Η Οδηγία 95/46/ΕΚ είναι τεχνολογικά ουδέτερη και ως εκ τούτου δύναται να εφαρμοστεί στο διαρκώς μεταβαλλόμενο τεχνολογικά περιβάλλον.

Αξίζει να τονιστεί ότι η Οδηγία 95/46/ΕΚ βρίσκει εφαρμογή, καταρχήν, όταν η επεξεργασία προσωπικών δεδομένων εκτελείται στα πλαίσια των δραστηριοτήτων υπευθύνου εγκατεστημένου στο έδαφος του κράτους μέλους (άρθρο 4 παρ. 1 περ. α'). Συνεπώς, δεν εμπίπτει στο πεδίο εφαρμογής του νόμου η επεξεργασία προσωπικών δεδομένων από παρόχους υπηρεσιών π.χ. κοινωνικής δικτύωσης που δεν έχουν εγκατάσταση στην επικράτεια κράτους μέλους της ΕΕ.

Ως «***προσωπικά δεδομένα***» ορίζονται από το άρθρο 2 της Οδηγίας «όλες οι πληροφορίες που αφορούν κάποιο πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί το πρόσωπο στο οποίο αναφέρονται τα δεδομένα». Επίσης, ως πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί λογίζεται «το πρόσωπο εκείνο που μπορεί να προσδιοριστεί άμεσα ή έμμεσα, ιδίως βάση αριθμού ταυτότητας ή βάση συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόσταση του από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη».

Η «***επεξεργασία***» ορίζεται ευρύτατα από την Οδηγία ως: «κάθε εργασία που πραγματοποιείται με ή χωρίς τη βοήθεια αυτοματοποιημένων διαδικασιών και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώρηση, η οργάνωση, η αποθήκευση, η προσαρμογή ή η τροποποίηση, η ανάκτηση ή η αναζήτηση πληροφοριών, η χρήση, η ανακοίνωση με διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η εναρμόνιση, ο συνδυασμός καθώς και το κλείδωμα, η διαγραφή ή η καταστροφή» (άρθρο 2 β').

Η Οδηγία εισάγει περαιτέρω ορισμένες πολύ σημαντικές αρχές που θα πρέπει να τηρούνται κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως ιδίως:

Α) Την *αρχή του σκοπού*, σύμφωνα με την οποία τα δεδομένα πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο, για καθορισμένους σκοπούς και να υφίσταται επεξεργασία μόνο όταν αυτή δεν αντίκειται στους σκοπούς αυτούς (άρθρο 6),

Β) την *αρχή της νομιμότητας* κατά την οποία θα πρέπει να τηρείται τουλάχιστον μία από τις διαζευκτικά αναγραφόμενες στο άρθρο 7 προϋποθέσεις, όπως π.χ. ότι το πρόσωπο στο οποίο αφορά η πληροφορία θα πρέπει να έχει δώσει τη ρητή συγκατάθεσή του για την επεξεργασία. Η συγκατάθεση μάλιστα αυτή θα πρέπει να είναι ελεύθερη, ρητή και να δίνεται από το υποκείμενο τον δεδομένων εν πλήρη επιγνώσει (άρθρο 2 η').

Γ) Επίσης, η Οδηγία υιοθετεί την *αρχή της διαφάνειας και πληροφόρησης των υποκειμένων των δεδομένων* (άρθρα 10 και 12). Ως προς τα παρεχόμενα προς τα άτομα δικαιώματα, η Οδηγία αναγνωρίζει το δικαίωμα πρόσβασης, διόρθωσης και αντίταξης, που σημαίνει ότι τα πρόσωπα στα οποία αναφέρονται τα δεδομένα έχουν το δικαίωμα να αποκτούν αντίγραφα των υπό επεξεργασία δεδομένων που τα αφορούν, καθώς και το δικαίωμα να ζητούν διόρθωση των ανακριβών δεδομένων. Παρέχεται επίσης το δικαίωμα, στο πρόσωπο στο οποίο αναφέρονται τα δεδομένα να αντιταχθεί στην επεξεργασία αυτών, εκτός αν στην εθνική νομοθεσία ορίζεται διαφορετικά.

Πέραν τούτων, η Οδηγία περιέχει διατάξεις για τη διαβίβαση προσωπικών δεδομένων σε τρίτες χώρες. Ως βασική αρχή τίθεται ότι τα κράτη-μέλη δεν θα πρέπει να επιτρέπουν την διαβίβαση παρά μόνο στις περιπτώσεις όπου εξασφαλίζεται ένα ικανοποιητικό επίπεδο προστασίας των δεδομένων (άρθρο 25).

Η έκδοση της δεύτερης χρονικά, ειδικής, Οδηγίας, 97/66/ΕΚ για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και της προστασίας της ιδιωτικής ζωής ειδικά στον τηλεπικοινωνιακό χώρο, είχε κριθεί απαραίτητη από τον κοινοτικό νομοθέτη καθώς η σταδιακή κατάργηση των κρατικών μονοπωλίων και η απελευθέρωση των τηλεπικοινωνιών, που είχε δρομολογηθεί από το 1990 και είχε συμπληρωθεί με το ρυθμιστικό πλαίσιο για «τις ηλεκτρονικές επικοινωνίες», είχε προκαλέσει αυξημένες απαιτήσεις προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής των χρηστών τους. Η ενσωμάτωσή της στο ελληνικό δίκαιο είχε γίνει με το Ν. 2774/1999.

Το 2002, η Ευρωπαϊκή Ένωση με την Οδηγία 2002/58/ΕΚ αντικατέστησε την Οδηγία 97/66/ΕΚ, για να συμπεριλάβει και την επεξεργασία των δεδομένων προσωπικού χαρακτήρα με γνώμονα την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Η αντικατάσταση αυτή είχε κριθεί αναγκαία από τον κοινοτικό νομοθέτη ενόψει των ραγδαίων τεχνολογικών εξελίξεων στον τομέα των τηλεπικοινωνιών και ιδίως εκείνων που είχαν επέλθει στον τομέα του Διαδικτύου. Έτσι, η Οδηγία 2002/58/ΕΚ περιέχει πιο εξειδικευμένες, αλλά και «τεχνολογικά ουδέτερες» ρυθμίσεις, και εφαρμόζεται στην επεξεργασία των προσωπικών δεδομένων στο χώρο των τηλεπικοινωνιών ανεξάρτητα από το μέσο που χρησιμοποιείται, καταλαμβάνοντας σαφώς και τις υπηρεσίες Διαδικτύου. Ακόμα, η διάταξη του άρθρου 15 παρ. 1 της Οδηγίας παρείχε στα κράτη-μέλη την διακριτική ευχέρεια να λαμβάνουν νομοθετικά μέτρα που να επιτρέπουν την φύλαξη δεδομένων για ορισμένο χρονικό διάστημα για λόγους, όπως η διαφύλαξη της εθνικής ασφάλειας, της εθνικής άμυνας και η πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών αδικημάτων ή της άνευ αδείας χρήσης του συστήματος ηλεκτρονικών επικοινωνιών.

Η ενσωμάτωση της Οδηγίας 2002/58/ΕΚ στο εθνικό μας δίκαιο πραγματοποιήθηκε με το Ν. 3471/2006.

Στη συνέχεια, η Οδηγία 2002/58/ΕΚ τροποποιήθηκε από την Οδηγία 2006/24/ΕΚ, βασικός στόχος της οποίας, ήταν η εναρμόνιση των υποχρεώσεων των διαθέσιμων στο κοινό παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών όσον αφορά τη διατήρηση ορισμένων δεδομένων που παράγονται ή υφίστανται επεξεργασία από αυτούς, ώστε να διασφαλιστεί ότι τα δεδομένα καθίστανται διαθέσιμα για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων (άρθρο 1 παρ. 1). Η ενσωμάτωση της Οδηγίας 2006/24/ΕΚ στο εθνικό μας δίκαιο είχε γίνει με το Ν. 3917/2011.

Ωστόσο, η Οδηγία 2006/24/ΕΚ υπέστη δριμεία κριτική και αποδοκιμάστηκε έντονα από ευρωπαϊκές Αρχές Προστασίας Προσωπικών Δεδομένων, από μη κυβερνητικές οργανώσεις, καθώς και από πολλά κράτη μέλη της ΕΕ. Στον απόηχο των αντιδράσεων αυτών και μετά από μακρές διαπραγματεύσεις και συζητήσεις η ΕΕ υιοθέτησε την Οδηγία 2009/136/ΕΚ, με την οποία τροποποιεί πέντε οδηγίες που συσχετίζονται με την ρύθμιση ηλεκτρονικών επικοινωνιών, μεταξύ των οποίων και την Οδηγία 2002/58/ΕΚ. Όσον αφορά τα ζητήματα της προστασίας της ιδιωτική ζωής και των

ηλεκτρονικών δεδομένων, οι νέες ρυθμίσεις κινούνται προς την σωστή κατεύθυνση καθώς περιέχουν βελτιώσεις που αφορούν τις παραβιάσεις της ασφάλειας της επεξεργασίας των δεδομένων, την πρακτική των cookies, το spamming καθώς και κατάλληλους μηχανισμούς για την ορθότερη επιβολή των κανόνων.

Η ενσωμάτωση της Οδηγίας αυτής στο ελληνικό δίκαιο επήλθε με το Ν. 4070/2012 «ρυθμίσεις ηλεκτρονικών επικοινωνιών, μεταφορών, δημοσίων έργων και άλλες διατάξεις», επιφέροντας εκ νέου σημαντικές αλλαγές, μεταξύ άλλων, στο πεδίο της προστασίας των προσωπικών δεδομένων στον ειδικότερο τομέα των ηλεκτρονικών επικοινωνιών.

Πλέον, είναι αδιαμφισβήτητο ότι η Οδηγία 95/46/ΕΚ έχει πλέον ξεπεραστεί και χρήζει εκσυγχρονισμού ιδίως διότι οι ραγδαίες τεχνολογικές εξελίξεις έχουν αλλάξει πλήρως τον τρόπο παροχής των υπηρεσιών της κοινωνίας της πληροφορίας. Επίσης, δεν έτυχε ποτέ ενιαίας εφαρμογής σε όλα τα κράτη-μέλη, αφού πρόκειται για μία Οδηγία «ελάχιστης εναρμόνισης», προκαλώντας έτσι, σύμφωνα με την Επιτροπή, αβεβαιότητα και εμπόδια στη ροή της πληροφορίας εντός της ΕΕ. Στο πλαίσιο αυτών των δεδομένων η Ευρωπαϊκή Επιτροπή έδωσε, στη δημοσιότητα την από 25/1/2012 «Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου αναφορικά με την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων και την ελεύθερη διακίνηση αυτών (Γενικός Κανονισμός Προστασίας Δεδομένων)».

Στην πρόταση αυτή Κανονισμού καταγράφεται η πρόθεση του Ενωσιακού νομοθέτη να υπάρξει πλήρης εναρμόνιση της προστασίας προσωπικών δεδομένων στην ΕΕ, αποσκοπεί δε στην παροχή αυξημένου επιπέδου προστασίας, ενώ γίνονται βήματα προς την κατεύθυνση μιας πιο συνεπούς αντιμετώπισης των ζητημάτων προστασίας προσωπικών δεδομένων ειδικά στις υπηρεσίες κοινωνικής δικτύωσης. Το πλέον καινοτόμο όμως σημείο της είναι ότι προβαίνει στην αναγνώριση ενός «*δικαιώματος στη λήθη»,* το οποίο δεν περιλαμβάνει μόνο το δικαίωμα του ατόμου να ζητήσει την διαγραφή των προσωπικών του δεδομένων και τη μη περαιτέρω διάδοσή τους, αλλά επιπλέον το δικαίωμα να ζητήσει από τρίτους την διαγραφή των παραπομπών σε δεδομένα (άρθρο 17 της Πρότασης).

Πιο πρόσφατα, η Ευρωπαϊκή Ένωση εξέδωσε τον Κανονισμό 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και

την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

Επιπλέον, εξέδωσε δύο ακόμα Οδηγίες, την Οδηγία 2016/680 και την Οδηγία 2016/681. Η πρώτη σχετίζεται με 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 και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου, ενώ η δεύτερη αφορά τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων.

2.4 Το Ελληνικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων

Στην Ελλάδα, η προστασία των προσωπικών δεδομένων έχει πλέον Συνταγματική κατοχύρωση, καθόσον ο αναθεωρητικός νομοθέτης του 2001, προσέθεσε νέα διάταξη (άρθρο 9^{A}) η οποία συμπληρώνει την διάταξη του άρθρου 9 παρ. 1 εδάφιο Β' για «το απαραβίαστο της ιδιωτικής και οικογενειακή ζωής του ατόμου». Σύμφωνα με το άρθρο 9^{A}: «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει».

Ο κορμός της προστασίας των προσωπικών δεδομένων στην χώρα μας είναι ο Ν. 2472/1997 «για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής». Οι Αποφάσεις και Γνωμοδοτήσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα αλλά και η πλούσια ελληνική νομολογία συμπληρώνουν το ρυθμιστικό πλαίσιο του δικαίου προστασίας των δεδομένων προσωπικού χαρακτήρα στη χώρα μας.

Ειδικά για τις ηλεκτρονικές υπηρεσίες έχει θεσμοθετηθεί ο Ν. 3471/2006 ώστε να συμπεριλάβει και την «προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών». Ο Ν. 3471/2006

τροποποιήθηκε αρχικά από το Ν.3917/2011 για τη «διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις», ο οποίος συνιστά ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2006/24/ΕΚ. Στη συνέχεια τροποποιήθηκε εκ νέου από τους Ν. 3994/2011 και 4024/2011, προκειμένου να ενσωματώσει την Οδηγία 2009/136/ΕΚ στο ελληνικό δίκαιο.

Αξιοσημείωτο είναι ότι ο Έλληνας νομοθέτης εκμεταλλευόμενος τις υπό της ελάχιστης εναρμόνισης Οδηγίας 95/46/ΕΚ παρεχόμενες δυνατότητες και διακριτικές ευχέρειες, ενίσχυσε σε σημαντικό βαθμό την προστασία των πολιτών. Επομένως, ο Ν. 2472/1997 δε συνιστά πιστή μεταφορά της Οδηγίας στο εθνικό νομικό μας πλαίσιο, καθώς ο Έλληνας νομοθέτης απέκλινε σε ορισμένες διατάξεις από κοινοτικές ρυθμίσεις, αξιοποιώντας το περιθώριο που του παρείχε η Οδηγία. Το νομοθέτημα αυτό λοιπόν, παρά τις όποιες επιμέρους ατέλειες του, μπορεί αβίαστα να χαρακτηριστεί ως προοδευτικό και ικανό να προσφέρει επαρκή προστασία της ιδιωτικότητας και του «πληροφοριακού αυτοπροσδιορισμού» στα άτομα.

2.4.1 Ο Ν. 2472/1997 στο ελληνικό σύστημα

Ο βασικός άξονας γύρω από τον οποίο διαμορφώνεται ο Ν. 2472/1997 είναι ότι η συλλογή και η επεξεργασία προσωπικών δεδομένων είναι καταρχήν παράνομη και επομένως απαγορεύεται. Καθίσταται δε νόμιμη μόνον εφόσον πληρούνται οι προϋποθέσεις που θέτει ο νόμος. Τα νομικά πρόσωπα δεν εμπίπτουν στο ρυθμιστικό πεδίο του νόμου, διότι όπως διευκρινίζεται στην εισηγητική έκθεσή του, κρίθηκε ότι η ρύθμιση της επεξεργασίας των δεδομένων που τα αφορούν πρέπει να γίνεται με βάση εντελώς διαφορετικές αρχές και κριτήρια.

Ο Ν. 2472/97 εδράζεται στους εξής πυλώνες:

1) Σε ένα σύστημα ουσιαστικών ρυθμίσεων που θέτουν, αφενός τις προϋποθέσεις νομιμότητας της επεξεργασίας, προσδιορίζοντας δεσμευτικά το σημείο ισορροπίας μεταξύ των αντιτιθέμενων δικαιωμάτων και συμφερόντων, και

αφετέρου τις βασικές αρχές του νόμου με έμφαση στην αρχή του σκοπού και της αναλογικότητας (άρθρα 4-10).

2) Στην απονομή δικαιωμάτων στα πρόσωπα ώστε να είναι σε θέση να προστατέψουν τα δικαιώματα και συμφέροντά τους (άρθρα 11-14).
3) Στην εισαγωγή και οργάνωση ανεξάρτητου θεσμικού ελέγχου της προστασίας προσωπικών δεδομένων ώστε να εξασφαλίσει την εφαρμογή της νομοθεσίας. Έτσι, ο Ν. 2472/97 ίδρυσε την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που έχει την κεντρική και αποφασιστική θέση στο σύστημα προστασίας των προσωπικών δεδομένων των ατόμων. Η Ανεξάρτητη αυτή Διοικητική Αρχή έχει συνταγματική κατοχύρωση και αποτελεί το θεματοφύλακα του όλου συστήματος προστασίας και επεξεργασίας των προσωπικών δεδομένων που εισάγει ο Νόμος (άρθρα 15-20).
4) Στους κανόνες που προβλέπουν διοικητικές, ποινικές και αστικές κυρώσεις σε περίπτωση παράβασης του νόμου (άρθρα 21-23).

2.4.2 Οι γενικές αρχές επεξεργασίας των προσωπικών δεδομένων

Στο άρθρο 4 του Ν. 2472/97 ανευρίσκονται οι αρχές που πρέπει να διέπουν την ποιότητα των δεδομένων και οι οποίες πρέπει να ακολουθούνται κατά τον έλεγχο της νομιμότητας της επεξεργασίας. Είναι απόλυτα δεσμευτικές και αποτελούν κανόνες αναγκαστικού δικαίου από τους οποίους δεν μπορεί να παρεκκλίνει η ιδιωτική βούληση.

Ειδικότερα ως προϋπόθεση νόμιμης επεξεργασίας των προσωπικών δεδομένων ορίζεται από το άρθρο 4 του νόμου ότι αυτά θα πρέπει:

1) Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών. Πρόκειται για την «αρχή του σκοπού και της θεμιτής και νόμιμης επεξεργασίας».
2) Να είναι συναφή, πρόσφορα και όχι περισσότερα απ' όσα κάθε φορά απαιτείται ενόψει των σκοπών του επεξεργασίας. Πρόκειται για την «αρχή της αναλογικότητας» ή αλλιώς, «της αντιστοιχίας σκοπού και δεδομένων».
3) Να είναι ακριβή. Πρόκειται για την «αρχή της ακρίβειας των δεδομένων». Τα δεδομένα δηλαδή πρέπει να ανταποκρίνονται στην πραγματικότητα και εφόσον

χρειάζεται, να υπόκεινται σε επικαιροποίηση έτσι ώστε να εξακολουθούν να ανταποκρίνονται στην τρέχουσα πραγματικότητα.

4) Να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής Προστασίας Προσωπικών Δεδομένων για την πραγματοποίηση του σκοπού της συλλογής τους και της επεξεργασία τους. Πρόκειται για την «αρχή της χρονικά πεπερασμένης διατήρησης των δεδομένων».

2.4.3 Προϋποθέσεις νομιμότητας επεξεργασίας των απλών δεδομένων

Ως θεμελιώδης κανόνας επεξεργασίας προσωπικών δεδομένων εισάγεται από το νόμο το επιτρεπτό της επεξεργασίας τους, μόνο όταν το υποκείμενο αυτών έχει δώσει τη συγκατάθεση του.

Η συγκατάθεση του υποκειμένου των δεδομένων θα πρέπει να είναι ελεύθερη, ρητή και ειδική και να παρέχεται από το άτομο εν πλήρη επιγνώσει και αφού προηγουμένως έχει ενημερωθεί πλήρως. Ελεύθερη είναι η συγκατάθεση, η οποία δεν αποτελεί προϊόν ελαττωματικής βουλήσεως (πλάνη, απάτη, απειλή) ούτε προϊόν ανάγκης ή σχέσης εξάρτησης του υποκειμένου από τον υπεύθυνο επεξεργασίας.

Η ενημέρωση αυτή περιλαμβάνει πληροφόρηση τουλάχιστον για το σκοπό της επεξεργασίας, τα δεδομένα στα οποία αφορά η επεξεργασία, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα καθώς και τα στοιχεία του υπεύθυνου επεξεργασίας. Η ενημέρωση αυτή θα πρέπει να είναι εύκολα κατανοητή από το κοινό στο οποίο απευθύνεται, αληθινή, σωστή και πλήρης, να περιέχει δηλαδή τόσο τις θετικές όσο και τις αρνητικές συνέπειες που συνεπάγεται η επεξεργασία των δεδομένων του χρήστη ή συνδρομητή.

Το υποχρεωτικό της συγκατάθεσης του υποκειμένου των δεδομένων προκειμένου να καταστεί η επεξεργασία αυτών νόμιμη αποτελεί τη ραχοκοκαλιά του ελληνικού δικαίου προστασίας προσωπικών δεδομένων και έχει ιδιαίτερα μεγάλη σημασία καθώς διασφαλίζει το δικαίωμα του πληροφοριακού αυτοκαθορισμού του ατόμου.

Κατ’ εξαίρεση η επεξεργασία των προσωπικών δεδομένων χωρίς την συγκατάθεση του υποκειμένου επιτρέπεται σύμφωνα με το Ν. 2472/97, όταν είναι αναγκαία για:

Α) Την εκτέλεση της σύμβασης στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος,

Β) Την εκπλήρωση υποχρέωσης του υπεύθυνου επεξεργασίας η οποία επιβάλλεται από το νόμο,

Γ) Την διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων, εφόσον αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει την συγκατάθεσή του,

Δ) Την εκτέλεση έργου δημοσίου συμφέροντος, ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια αρχή και

Ε) Την ικανοποίηση εννόμου συμφέροντος του υπεύθυνου επεξεργασίας, υπό τον όρο ότι αυτό υπερέχει προφανώς των δικαιωμάτων και συμφερόντων του υποκειμένου των δεδομένων και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτού.

Πέρα από τις προαναφερθείσες ουσιαστικές προϋποθέσεις για τη νομιμότητα της επεξεργασίας ο νόμος προβλέπει την υποχρέωση του υπευθύνου επεξεργασίας να γνωστοποιεί στην Αρχή Προστασίας Προσωπικών Δεδομένων τη σύσταση και λειτουργία αρχείου επεξεργασίας προσωπικών δεδομένων. Η εν λόγω δήλωση έχει ωστόσο απλά δηλωτικό χαρακτήρα.

2.4.4 Η επεξεργασία των ευαίσθητων προσωπικών δεδομένων

Όσον αφορά την επεξεργασία των «ευαίσθητων δεδομένων» τίθενται ακόμα αυστηρότερες προϋποθέσεις.

Ειδικότερα, για τα ευαίσθητα δεδομένα θεσπίζεται ως γενικός κανόνας η απαγόρευση της συλλογής και επεξεργασίας τους. Ωστόσο, κατά την παρ. 2 επιτρέπεται κατ' εξαίρεση η συλλογή και επεξεργασία ευαίσθητων δεδομένων εάν πληρούνται οι ουσιαστικές προϋποθέσεις που ορίζονται δεσμευτικά από το νόμο και, μόνο κατόπιν αδείας της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Πιο συγκεκριμένα η συλλογή και επεξεργασία ευαίσθητων δεδομένων επιτρέπεται μόνο κατ' εξαίρεση και όταν συντρέχουν οι περισσότερες από τις ακόλουθες προϋποθέσεις:

1) Να έχει συγκατατεθεί έγγραφο στο υποκείμενο, εκτός εάν η συγκατάθεση έχει αποσπαστεί με τρόπο που αντίκειται στο νόμο ή στα χρηστά ήθη
2) Η επεξεργασία είναι αναγκαία για την διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή προβλεπόμενου από το νόμο συμφέροντος τρίτου, εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεση του.
3) Η επεξεργασία αφορά δεδομένα που δημοσιοποιεί το ίδιο το υποκείμενο ή είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση του δικαιώματος του ενώπιον δικαστηρίου ή πειθαρχικού οργάνου.
4) Η επεξεργασία αφορά θέματα υγείας και εκτελείται από πρόσωπο που υπόκειται σε καθήκον εχεμύθειας, υπό τον όρο ότι είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή τη διαχείριση υπηρεσιών υγείας.
5) Η επεξεργασία εκτελείται από δημόσια αρχή και είναι αναγκαία είτε για λόγους εθνικής ασφάλειας είτε για την εξυπηρέτηση των αναγκών εγκληματολογικής ή σωφρονιστικής πολιτικής και αφορά την διακρίβωση εγκλημάτων, ποινικές καταδίκες ή μέτρα ασφαλείας, είτε για λόγους προστασίας της δημόσιας υγείας, είτε για την άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών.

Περαιτέρω, ο Έλληνας νομοθέτης κάνοντας χρήση της δυνατότητας που παρέχει η παρ. 4 άρθρο 8 της Οδηγίας 95/46/ΕΚ στα κράτη μέλη, προσέθεσε στον σχετικό κατάλογο της παρ. 2 άρθρο 8 της Οδηγίας δύο ακόμα εξαιρέσεις επιτρέποντας την επεξεργασία προσωπικών δεδομένων και όταν:

6) Η επεξεργασία πραγματοποιείται για ερευνητικούς και επιστημονικούς αποκλειστικά σκοπούς, υπό τον όρο ότι τηρείται η ανωνυμία και λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται.
7) Η επεξεργασία αφορά δεδομένα δημοσίων προσώπων, εφόσον αυτά συνδέονται με την άσκηση δημοσίου λειτουργήματος ή την διαχείριση συμφερόντων τρίτων, και πραγματοποιείται αποκλειστικά για την άσκηση του δημοσιογραφικού επαγγέλματος.

2.4.5 Η ασφαλής καταστροφή των προσωπικών δεδομένων

Σύμφωνα με το άρθρο 3 της Οδηγίας 1/2005 της Αρχής Προστασίας Προσωπικών Δεδομένων, τα προσωπικά δεδομένα πρέπει να καταστρέφονται με ευθύνη του υπευθύνου επεξεργασίας αμέσως μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας. Η καταστροφή πρέπει να πραγματοποιείται με ασφαλή τρόπο, ώστε να αποκλειστεί η περαιτέρω μη νόμιμη και αθέμιτη επεξεργασία τους, όπως είναι η κάθε μορφή διάθεσης σε τρίτους.

Ως ασφαλής τρόπος καταστροφής των δεδομένων θεωρείται «κάθε σύνολο διαδικασιών και μέτρων που μετά από την ολοκλήρωση της εφαρμογής τους δεν είναι δυνατό να αναγνωρισθούν τα υποκείμενα των δεδομένων και δεν είναι δυνατή η ανάκτηση των δεδομένων με τεχνικά ή άλλα μέσα».

Ο υπεύθυνος επεξεργασίας υποχρεούται να εφαρμόζει συγκεκριμένη διαδικασία και κατάλληλους μηχανισμούς ελέγχου για την ασφαλή καταστροφή των προσωπικών δεδομένων, τους οποίους οφείλει να διατυπώνει γραπτώς και να υποβάλλει υπογεγραμμένα στην Αρχή Προστασίας Προσωπικών Δεδομένων

Σε περίπτωση ανάθεσης της διαδικασίας σε τρίτο άτομο (εκτελών την επεξεργασία), ο υπεύθυνος επεξεργασίας υποχρεούται στην υπογραφή σύμβασης με αυτόν, όπου θα αναφέρονται αναλυτικά όλες οι ενέργειες που οφείλει να εφαρμόσει ο εκτελών την επεξεργασία. Σε περίπτωση καταστροφής απόρρητων δεδομένων από τρίτο άτομο, ο υπεύθυνος επεξεργασίας, οφείλει να έχει τη συνολική επίβλεψη της διαδικασίας της καταστροφής.

Όσον αφορά τη διαδικασία καταστροφής των δεδομένων, αυτή εξαρτάται από την μορφή στην οποία βρίσκονται.

Συγκεκριμένα, για καταστροφή δεδομένων σε έντυπη μορφή, απαιτείται αρχικά η εναπόθεσή τους από τους υπαλλήλους του υπευθύνου επεξεργασίας σε ειδικούς υποδοχείς, όπου στη συνέχεια συλλέγονται και τοποθετούνται σε κεντρικό σημείο. Ακολούθως, τεμαχίζονται με ειδικά μηχανήματα σε λωρίδες εντός των εγκαταστάσεων του υπευθύνου επεξεργασίας ή παραδίδονται εκτός των εγκαταστάσεων στον εκτελούντα την επεξεργασία για να ολοκληρώσει την καταστροφή με τεμαχισμό, πολτοποίηση ή ανακύκλωση αυτών. Τέλος, συντάσσεται το πρωτόκολλο

καταστροφής, στο οποίο πρέπει να περιλαμβάνονται τουλάχιστον τα παρακάτω στοιχεία:

- Ημερομηνία καταστροφής των δεδομένων.
- Περιγραφή των δεδομένων που καταστράφηκαν.
- Μέθοδος καταστροφής.
- Ονοματεπώνυμο αρμόδιου υπαλλήλου του υπεύθυνου επεξεργασίας που είναι υπεύθυνος για την καταστροφή.
- Εκτελών την καταστροφή (στη περίπτωση που η καταστροφή ανατίθεται σε εκτελούντα την επεξεργασία).

Για περίπτωση δεδομένων που βρίσκονται σε ηλεκτρονική ή άλλη μορφή, ο ενδεικνυόμενος τρόπος για την ασφαλή καταστροφή τους είναι η αλλοίωση των δεδομένων μέσω της αντικατάστασης τους με τυχαίους χαρακτήρες (overwrite). Η αλλοίωση μπορεί να γίνει με τη χρήση ειδικών προγραμμάτων (file erasers, file shredders, file pulveritizers) ή με μορφοποίηση του υλικού υποστρώματος (format), σε περίπτωση καθημερινής καταστροφής δεδομένων ή με φυσική καταστροφή του ίδιου του υλικού υποστρώματος (π.χ. με θρυμματισμό, κονιορτοποίηση, αποτέφρωση), σε περίπτωση προγραμματισμένης καταστροφής. Η καταστροφή των δεδομένων περιλαμβάνει και την καταστροφή όλων των αντιγράφων ασφαλείας (back up) που τηρεί ο υπεύθυνος επεξεργασίας. Σε κάθε περίπτωση, η διαδικασία πρέπει να συνοδεύεται με την ολοκλήρωσή της από πρωτόκολλο καταστροφής,

2.4.6 Τα δικαιώματα του υποκειμένου των δεδομένων

Ο Ν. 2472/97 αναγνωρίζει συγκεκριμένα δικαιώματα στα υποκείμενα των δεδομένων, εξοπλίζοντας έτσι τα θιγόμενα από την κατάχρηση προσωπικών τους δεδομένων πρόσωπα με συγκεκριμένα «μέσα άμυνας» και παρέχοντάς τους εν τέλει το δικαίωμα να συναποφασίσουν ποιες πληροφορίες που τα αφορούν μπορούν να αποτελέσουν αντικείμενο επεξεργασίας.

Τα δικαιώματα που προασπίζει ο νόμος είναι:

1) Το δικαίωμα ενημέρωσης (άρθρο 11), όπου καθιερώνεται το δικαίωμα προηγούμενης ενημέρωσης του προσώπου από τον ίδιο τον υπεύθυνο επεξεργασίας για τα βασικά στοιχεία της επεξεργασίας,
2) Το δικαίωμα πρόσβασης στα αρχεία (άρθρο 12), δεδομένου ότι παρέχει τη δυνατότητα στους ενδιαφερόμενους να διαπιστώσουν αν έχουν καταχωρηθεί δεδομένα που τους αφορούν.
3) Το δικαίωμα αντίρρησης (άρθρο 13), που συνίσταται στο δικαίωμα του υποκειμένου να προβάλλει οποτεδήποτε αντιρρήσεις για την επεξεργασία των δεδομένων που το αφορούν ή να ζητάει υπό την ιδιότητά του ως καταναλωτή να μην περιλαμβάνονται τα δεδομένα που το αφορούν σε αρχεία με σκοπό την διαφήμιση ή/και την προώθηση πωλήσεως αγαθών ή υπηρεσιών εξ αποστάσεως.
4) Τέλος, το δικαίωμα προσωρινής διοικητικής και δικαστικής προστασίας (άρθρο 14), που αφορά για το δικαίωμα του υποκειμένου των δεδομένων να ζητάει από το εκάστοτε αρμόδιο δικαστήριο την άμεση αναστολή ή τη μη εφαρμογή μιας απόφασης που θίγει το άτομο, εφόσον η απόφαση έχει ληφθεί αποκλειστικά με αυτοματοποιημένη επεξεργασία στοιχείων, δηλαδή χωρίς την ανθρώπινη κρίση και αξιολόγηση.

.

2.4.7 Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Σύμφωνα με το άρθρο 9^{A} Σ «η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί όπως νόμος ορίζει». Ουσιαστικά το Σύνταγμα επιβεβαίωσε το ρυθμιστικό σχήμα που είχε ήδη εισαγάγει ο Ν. 2472/97. Η Αρχή Προστασίας Προσωπικών Δεδομένων είναι μία από τις πέντε ανεξάρτητες αρχές που κατοχυρώθηκε με τη συνταγματική αναθεώρηση του 2001. Δεν μπορεί να καταργηθεί ή να τροποποιηθεί, όσον αφορά στο συνταγματικά προσδιορισμένο θεσμικό της περιεχόμενο με νόμο, παρά μόνο με νεότερη συνταγματική αναθεώρηση.

Πιο συγκεκριμένα, η Αρχή Προστασίας Προσωπικών Δεδομένων (στο εξής: η Αρχή), αποτελεί κεντρικό όργανο εφαρμογής των ρυθμίσεων του Ν. 2472/97, η οποία συνιστάται ως Ανεξάρτητη Διοικητική Αρχή (ΑΔΑ), με δικό της προϋπολογισμό και δική της γραμματεία. Στην Αρχή, η οποία ιδρύθηκε κατά το πρότυπο της αντίστοιχης

γαλλικής Commission National de l' Informatique et de Libertés (C.N.I.L), ο νόμος παρέχει ευρύτατες αρμοδιότητες τόσο προληπτικές όσο και κατασταλτικές. Από το άρθρο 15 του Νόμου διακηρύσσεται η προσωπική και λειτουργική ανεξαρτησία των μελών της Αρχής και κατοχυρώνεται η μη υπαγωγή της λειτουργίας της σε οποιονδήποτε ιεραρχικό, κυβερνητικό ή διοικητικό έλεγχο. Για λόγους συνταγματικής τάξης προβλέπεται μεν η υπαγωγή της Αρχής στον Υπουργό Δικαιοσύνης, υπαγωγής που θα πρέπει ωστόσο να νοείται αποκλειστικά ως κατασταλτικός έλεγχος νομιμότητας. Ακόμα, όπως άλλωστε και οι λοιπές ΑΔΑ, υπόκειται σε κοινοβουλευτικό έλεγχο, έργο που αποτελεί αντικείμενο της Επιτροπής Θεσμών και Διαφάνειας της Βουλής σύμφωνα με τον Κανονισμό της Βουλής. Πέραν αυτού, οι Αποφάσεις της Αρχής, υπόκεινται στο νομικό έλεγχο των Διοικητικών Δικαστηρίων.

Η Αρχή, είναι ουσιαστικά το θεμέλιο του συστήματος επάνω στο οποίο οικοδομείται ο μηχανισμός τήρησης και εφαρμογής του Ν. 2472/97. Κατά συνέπεια, η διασφάλιση της ανεξαρτησίας της Αρχής, ανάγεται σε πρωταρχικής σημασίας ζήτημα. Κατά την άσκηση των καθηκόντων τους, τα μέλη της Αρχής υπακούουν στη συνείδησή τους και το Νόμο και δεν υπόκεινται σε οδηγίες ή εντολές ιεραρχικά ανωτέρων, ενώ διέπονται από προσωπική και λειτουργική ανεξαρτησία. Στο πλαίσιο της εξασφάλισης της ανεξαρτησίας των μελών της Αρχής, το άρθρο 17 του νόμου ορίζει κωλύματα και ασυμβίβαστα και καθιερώνει σύστημα αυτοελέγχου, χωρίς βεβαίως συμμετοχή στην λήψη σχετικών αποφάσεων του μέλους της Αρχής, στο πρόσωπο του οποίου ενδέχεται να συντρέχει το ασυμβίβαστο.

Σύμφωνα με την παρ. 1 άρθρο 16, η Αρχή είναι επταμελής και συγκροτείται από ένα ανώτατο δικαστικό λειτουργό, ως Πρόεδρο, και έξι μέλη.

Οι αρμοδιότητες της Αρχής διακρίνονται σε:

1) **Εποπτικές και ελεγκτικές αρμοδιότητες,** δηλαδή εκδίδει οδηγίες, καλεί και επικουρεί τα επαγγελματικά σωματεία στην κατάρτιση κωδικών δεοντολογίας και απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους επεξεργασίας και δίδει κατά την κρίση της δημοσιότητα σε αυτές.

2) **Αποφασιστικές και κυρωτικές αρμοδιότητες,** όπου αποφασίζει ή όχι για τη χορήγηση αδειών επεξεργασίας για την συλλογή και επεξεργασία ευαίσθητων προσωπικών δεδομένων, για τη διασύνδεση αρχείων όταν αφορούν ευαίσθητα

δεδομένα και για τη διαβίβαση δεδομένων προς χώρα που δεν ανήκει στην Ευρωπαϊκή Ένωση.

3) **Νομοθετικές και γνωμοδοτικές αρμοδιότητες,** όπου εκδίδει κανονιστικές πράξεις για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων, στα οποία αναφέρεται ο Νόμος. Γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα και εξετάζει αιτήσεις υπευθύνων επεξεργασίας με τις οποίες ζητείται ο έλεγχος και η νομιμότητα της επεξεργασίας.

Τέλος, ο νόμος της παρέχει τη δυνατότητα επιβολής διοικητικών (άρθρο 21), ποινικών (άρθρο 22) και αστικών (άρθρο 23) κυρώσεων.

Ειδικότερα, όσον αφορά τις διοικητικές κυρώσεις, αυτές επιβάλλονται από την Αρχή στους υπευθύνους επεξεργασίας ή στους τυχόν εκπροσώπους τους και ξεκινούν, στις πιο απλές περιπτώσεις από μία απλή προειδοποίηση με αποκλειστική προθεσμία για άρση της παράβασης, εκτείνονται σε πρόστιμα και δύνανται να φτάσουν έως την οριστική ανάκληση της άδειας και την καταστροφή του αρχείου ή τη διακοπή της επεξεργασίας των σχετικών δεδομένων.

Ποινικές κυρώσεις επιβάλλονται ιδίως στην περίπτωση μη γνωστοποιήσης αρχείου, λειτουργίας αρχείου με ευαίσθητα δεδομένα χωρίς άδεια κ.λπ., καθώς και στην περίπτωση μη συμμόρφωσης προς τις αποφάσεις της Αρχής. Οι ποινικές κυρώσεις κυμαίνονται από φυλάκιση ενός μέχρι 10 έτη και χρηματική ποινή.

Το πλέγμα των προβλεπόμενων από το νόμο κυρώσεων ολοκληρώνεται με τις αστικές κυρώσεις, την αστική δηλαδή ευθύνη των υπαιτίων για κάθε ζημία περιουσιακής ή μη περιουσιακής φύσεως.

Σύμφωνα με την Αρχή Προστασίας Προσωπικών Δεδομένων (2017):

Ως **«προσωπικό δεδομένο»** ορίζεται «κάθε πληροφορία που αναφέρεται σε και περιγράφει ένα άτομο, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κ.λπ.), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα,

δραστηριότητες, συνήθειες. Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα ονομάζεται **υποκείμενο των δεδομένων**.

Ως **«ευαίσθητα»** χαρακτηρίζονται «τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Τα ευαίσθητα δεδομένα προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά προσωπικά δεδομένα». Στις παραπάνω κατηγορίες, συμπεριλαμβάνονται επίσης και από άλλα νομοθετήματα:

- Τα μητρώα και Αρχεία της Εθνικής Αρχής Ιατρικώς Υποβοηθούμενης Αναπαραγωγής,
- Τα δεδομένα των ληπτών και δωρητών ανθρωπίνων ιστών και οργάνων που περιέχονται στο Εθνικό Μητρώο με τους λήπτες και Αρχεία Δωρητών,
- Οι δηλώσεις του αιτούντος άσυλο και τα λοιπά στοιχεία της αιτήσεώς του και
- Τα γενετικά δεδομένα

Ως **«επεξεργασία»** ορίζεται «κάθε εργασία ή σειρά εργασιών που πραγματοποιούνται από το Δημόσιο ή από Ν.Π.Δ.Δ. ή Ν.Π.Ι.Δ. ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς την βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζεται σε δεδομένα προσωπικού χαρακτήρα όπως η συλλογή, η καταχώρηση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή».

Προκειμένου για την νόμιμη επεξεργασία ευαίσθητων δεδομένων απαιτείται γραπτή συγκατάθεση του υποκειμένου τους μόνο εφόσον ισχύει μία τουλάχιστον από τις εξαιρέσεις που ορίζει ο Νόμος 2472/1997 στο άρθρο 7 ενώ για την νόμιμη επεξεργασία των απλών προσωπικών δεδομένων αρκεί, σε πρώτη φάση, η προφορική συγκατάθεση, όταν συντρέχουν οι προϋποθέσεις που ορίζει ο Νόμος 2472/1997 στο άρθρο 5.

Επίσης, ο κατ' εξοχήν πρωταγωνιστής του δικαίου προσωπικών δεδομένων είναι ο «**υπεύθυνος επεξεργασίας**», που είναι οποιοσδήποτε καθορίζει το σκοπό και τον

τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός. Τα κομβικά σημεία εν προκειμένω είναι ο υπεύθυνος επεξεργασίας να καθορίζει αφενός την επιλογή του σκοπού και αφετέρου τον τρόπο της επεξεργασίας.

Ο υπεύθυνος επεξεργασίας ενδέχεται να είναι ταυτόχρονα και «εκτελών» την επεξεργασία. Ο «**εκτελών την επεξεργασία»**, εφόσον βεβαίως δεν ταυτίζεται με τον υπεύθυνο επεξεργασίας, ορίζεται από το νόμο ως «οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπεύθυνου επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός».

Κάθε υπεύθυνος επεξεργασίας οφείλει να γνωστοποιεί στην Αρχή την επεξεργασία προσωπικών δεδομένων που πραγματοποιεί, εκτός αν εμπίπτει σε μία από τις περιπτώσεις του άρθρου 7Α του Ν. 2472/1997. Η Αρχή καταχωρεί τη γνωστοποίηση σε ειδικό μητρώο.

Όταν η επεξεργασία αφορά ευαίσθητα δεδομένα, ο υπεύθυνος επεξεργασίας μπορεί να την πραγματοποιήσει μόνο μετά από άδεια της Αρχής, η οποία χορηγείται με ειδικούς όρους και προϋποθέσεις. Άδεια επίσης μπορεί να απαιτείται για τη διαβίβαση δεδομένων σε χώρα εκτός Ε.Ε., καθώς και για τη διασύνδεση αρχείων.

Περαιτέρω, εξειδικευμένη αναφορά γίνεται από τον Έλληνα νομοθέτη στην διασύνδεση, η οποία αποτελεί μια μορφή επεξεργασίας που συνίσταται στην δυνατότητα συσχέτισης των δεδομένων ενός αρχείου με δεδομένα αρχείου ή αρχείων που τηρούνται από άλλον ή άλλους υπεύθυνους επεξεργασίας, ή που τηρούνται από τον ίδιο υπεύθυνο για άλλο σκοπό. Ο νόμος καθιερώνει καταρχήν σύστημα γνωστοποίησης κάθε διασύνδεσης στην Αρχή Προστασίας Προσωπικών Δεδομένων και, παράλληλα, σύστημα προηγούμενης άδειας της Αρχής (άδεια διασύνδεσης) εάν ένα τουλάχιστον από τα αρχεία ή τις επεξεργασίες που πρόκειται να διασυνδεθούν περιέχει ευαίσθητα δεδομένα.

2.5 Σύνοψη

Στο κεφάλαιο αυτό, πραγματοποιήθηκε μια ιστορική αναδρομή στην εξέλιξη των προσωπικών δεδομένων στη διάρκεια των ετών, όπου φάνηκε η επιτακτική ανάγκη των Νομοθετών να θεσπίσουν νόμους και κανονιστικά πλαίσια για την όσο το δυνατόν μεγαλύτερη διασφάλιση των προσωπικών δεδομένων των ατόμων.

Αναλύθηκαν ακόμα, τα νομοθετικά πλαίσια σχετικά με την προστασία των δεδομένων τόσο σε ευρωπαϊκό όσο και σε εθνικό επίπεδο, με ιδιαίτερη έμφαση στο περιεχόμενο του Ν. 2472/1997, στις αρχές νομιμότητας και επεξεργασίας των δεδομένων και στα δικαιώματα των ατόμων για κατοχύρωση της προστασίας των προσωπικών τους δεδομένων. Τέλος, παρουσιάστηκε ο ρόλος και οι αρμοδιότητες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στη διασφάλιση των δικαιωμάτων των υποκειμένων, όπως επίσης και οι διαδικασίες τόσο του υπευθύνου όσο και του εκτελούντος την επεξεργασία για τη γνωστοποίηση των ενεργειών τους στην Αρχή.

Με την ολοκλήρωση αυτού του κεφαλαίου, γίνονται αντιληπτοί οι λόγοι για τους οποίους καθίσταται αναγκαία η επικαιροποίηση και ο εκσυγχρονισμός των υφιστάμενων κανόνων της προστασίας των δεδομένων, με την υιοθέτηση ενός νέου ρυθμιστικού πλαισίου στην προστασία των προσωπικών δεδομένων φυσικών προσώπων, το οποίο παρουσιάζεται στο ακόλουθο κεφάλαιο.

3. Ο ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

3.1 Εισαγωγή

Το νομοθετικό πλαίσιο που ρυθμίζει την προστασία των προσωπικών δεδομένων θα αποτελέσει σύντομα παρελθόν εξαιτίας της εκ βάθρων αλλαγής του. Η ραγδαία τεχνολογική εξέλιξη, η παγκοσμιοποίηση, η πρόσβαση στο διαδίκτυο με την χρήση ασύρματων μέσων, τα κοινωνικά δίκτυα, οι υπηρεσίες υπολογιστικών νεφών και εν γένει η χρήση του διαδικτύου στο πλαίσιο τόσο προσωπικών, όσο και επαγγελματικών δραστηριοτήτων και συμπεριφορών που οδηγούν στην δημιουργία «δεξαμενών» προσωπικών δεδομένων, η παγκοσμιοποίηση καθώς και η διαβίβαση και ανταλλαγή δεδομένων μεταξύ διαφορετικών κρατών, κατέστησαν την Οδηγία 95/46/ΕΚ ξεπερασμένη.

Έτσι, η ΕΕ ψήφισε πρόσφατα ένα νέο ρυθμιστικό πλαίσιο, τον «Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) ή αλλιώς «General Data Protection Regulation» (GDPR), ο οποίος για τους πολίτες αποτελεί ένα εγχειρίδιο διαχείρισης των προσωπικών τους δεδομένων και για τις επιχειρήσεις ένα απλοποιημένο και ενιαίο πλαίσιο λειτουργίας.

Ο νέος Κανονισμός 2016/679/ΕΕ για την προστασία των προσωπικών δεδομένων (GDPR) που θα τεθεί σε εφαρμογή από τις 25 Μαΐου 2018 επιχειρεί να δημιουργήσει ένα αυστηρότερο θεσμικό πλαίσιο προστασίας τους, κατ' αρχήν εντός της Ευρωπαϊκής Ένωσης. Οι καινοτομίες του αποτελούν πρόκληση για όλες τις επιχειρήσεις και το Δημόσιο που καλούνται να τροποποιήσουν τις δομές τους και να λάβουν τα αναγκαία μέτρα για τη συμμόρφωση με τις αυστηρές επιταγές του, με τη συνδρομή εξειδικευμένων νομικών και επιστημόνων πληροφορικής.

Τα 99 άρθρα του νέου Κανονισμού για τα οποία απαιτήθηκαν τουλάχιστον τέσσερα χρόνια διαπραγματεύσεων αποσκοπούν στη διασφάλιση του θεμελιώδους δικαιώματος της προστασίας των προσωπικών δεδομένων με τη δημιουργία ενός ενιαίου και ισχυρού συστήματος προστασίας τους.

Πρακτικά λοιπόν, βρισκόμαστε ήδη στο χρονικό σημείο όπου θα λέγαμε ότι έχει αρχίσει η αντίστροφη μέτρηση για μια νέα εποχή, με αυξημένες μεν ‘’γραφειοκρατικές’’ και άλλες υποχρεώσεις και απαιτούμενη τυπολογία από πλευράς επιχειρήσεων, η οποία όμως μακροπρόθεσμα στοχεύει να διασφαλίσει το δικαίωμα αυτοδιάθεσης των προσωπικών δεδομένων του υποκειμένου στην αδιάλειπτη διαρροή και διαχείριση της προσωπικής πληροφορίας.

Η προάσπιση επομένως της προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας των ατόμων, είναι βασικό ζητούμενο και πρόκληση του νέου Κανονισμού που φιλοδοξεί να αντιμετωπίσει στη σύγχρονη πραγματικότητα των εφαρμογών, των έξυπνων συσκευών, των αισθητήρων και κάθε λογής τεχνολογία που επικοινωνεί με το διαδίκτυο και με απομακρυσμένους υπολογιστές.

Σε παρόν κεφάλαιο λοιπόν, αναλύονται όλες οι προκλήσεις και τα νέα δεδομένα που φέρνει ο συγκεκριμένος Κανονισμός, με τους πολίτες και τις επιχειρήσεις να έχουν τον κυρίαρχο ρόλο στην αποδοχή των αλλαγών αυτών.

3.2 Περιεχόμενο και ορισμοί του νέου Κανονισμού

Είκοσι χρόνια μετά τη θέση σε ισχύ του Ν. 2472/1997 για την προστασία των προσωπικών δεδομένων, ένας νέος Κανονισμός έρχεται να επαναπροσδιορίσει άμεσα, χωρίς άλλη ειδική νομοθεσία τις υποχρεώσεις όσων επεξεργάζονται προσωπικά δεδομένα στην Ε.Ε.

Στις 25.1.2012, η Ευρωπαϊκή Επιτροπή πρότεινε τη μεταρρύθμιση των κανόνων προστασίας προσωπικών δεδομένων στην ΕΕ. Μετά από πολυετείς συζητήσεις και διαβουλεύσεις, το Συμβούλιο ενέκρινε τη θέση του σε πρώτη ανάγνωση στις 8.4.2016 και στις 14.4.2016, ο Κανονισμός και η Οδηγία (ΕΕ) 2016/680 εγκρίθηκαν από το Ευρωπαϊκό Κοινοβούλιο. Στις 27.4.2016 ψηφίστηκε ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) που αποτελεί το κύριο νομοθέτημα της νέας δέσμης κανόνων. Στις 4.5.2016 ο Κανονισμός και η Οδηγία δημοσιεύονται στην Επίσημη Εφημερίδα της ΕΕ, στις 5.5.2016 η Οδηγία τίθεται σε ισχύ και στις 24.5.2016 τίθεται σε ισχύ ο Κανονισμός. Στο εξής, τα κράτη-μέλη πρέπει να έχουν ενσωματώσει την

Οδηγία στο εθνικό τους δίκαιο μέχρι τις 6.5.2018, καθώς από τις 25.5.2018 ο Κανονισμός τίθεται σε εφαρμογή τόσο στις επιχειρήσεις, όσο και στα φυσικά πρόσωπα σε όλη την Ευρώπη.

Συνεπώς και στην Ελλάδα, από τις 25.5.2018 όλες οι επιχειρήσεις, οι οργανισμοί και οι κυβερνητικές υπηρεσίες που συλλέγουν, διατηρούν, επεξεργάζονται, αποθηκεύουν και χρησιμοποιούν προσωπικά δεδομένα (εργαζομένων, πελατών, προμηθευτών ή τρίτων) έχουν την υποχρέωση να εφαρμόζουν τις νέες διατάξεις του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων. Η προσαρμογή των επιχειρήσεων αφορά νέα δικαιώματα που πρέπει να ικανοποιούν και νέες διαδικασίες που πρέπει να τηρούν, ενώ η μη συμμόρφωση προς τον Κανονισμό θα επιφέρει μεγάλα πρόστιμα σε όσους δεν λαμβάνουν τα απαραίτητα μέτρα.

Κάθε πληροφορία που αφορά φυσικό πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί άμεσα ή έμμεσα ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας όπως όνομα σε αριθμό ταυτότητας, σε δεδομένα θέσης , σε επιγραμματικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που παραπέμπουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου ή υποκείμενου δεδομένων, ελέγχεται από τον ισχύοντα Κανονισμό. Επίσης δεδομένα που αποκαλύπτουν την φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν την σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό καλύπτονται από τον νέο Κανονισμό ως προς την χρήση ή επεξεργασία τους.

Ουσιαστικά, ο ΓΚΠΔ διευρύνει τον ορισμό του προσωπικού δεδομένου ώστε να περιλαμβάνει πληροφορίες όπως διευθύνσεις διαδικτυακού πρωτοκόλλου (IP), διευθύνσεις καρτών δικτύου (MAC), δεδομένα τοποθεσίας, τα IMEI (μοναδικοί σειριακοί αριθμοί παρτίδας) για τις συσκευές κινητών, αλλά και ευαίσθητα δεδομένα όπως γενετικά ή βιομετρικά δεδομένα, που θα μπορούσαν να ταυτοποιήσουν μοναδικά το άτομο.

Ο ορισμός του όρου «προσωπικά δεδομένα» στο πλαίσιο του Κανονισμού, είναι αρκετά ενδεικτικός για το ύφος της νέας νομοθεσίας, σύμφωνα με την οποία τα προσωπικά δεδομένα θεωρούνται ως ένα πολύτιμο περιουσιακό στοιχείο και οι κανόνες που τα αφορούν πρόκειται να γίνουν αυστηρότεροι. Δεν είναι τυχαίο ότι αυτό συμβαδίζει με τεχνολογικές τάσεις, όπως το cloud computing, τα social media, τα κινητά και τις ηλεκτρονικές συσκευές με ενσωματωμένους αισθητήρες συλλογής δεδομένων (Internet of Things), όπου η συλλογή δεδομένων και η επαρκής ανάλυσή τους γίνονται στρατηγικοί φορείς διαφοροποίησης για τους οργανισμούς. Υπό αυτή την έννοια, ο Ευρωπαίος νομοθέτης έχει αρχίσει να συμβαδίζει με την πραγματικότητα.

Κατά κύριο λόγο, ο ΓΚΠΔ είναι ένα νέο σύνολο κανόνων, σχεδιασμένο να παρέχει στα άτομα μεγαλύτερο έλεγχο των προσωπικών τους δεδομένων. Στοχεύει στο να απλοποιήσει το ρυθμιστικό περιβάλλον των επιχειρήσεων, ώστε τόσο οι πολίτες όσο και οι επιχειρήσεις να μπορούν να επωφεληθούν πλήρως από την ψηφιακή οικονομία.

Οι μεταρρυθμίσεις έχουν σχεδιαστεί έτσι ώστε να αντικατοπτρίζουν την παρούσα κατάσταση των χωρών και της Κοινότητας και φέρνουν νόμους και υποχρεώσεις για όλη την Ευρώπη ώστε να προφτάσουν τη ραγδαία εξέλιξη της τεχνολογίας και ιδιαίτερα του Διαδικτύου.

Επιπλέον, ο ΓΚΠΔ αποτελεί Κανονισμό με άμεση ισχύ και ως εκ τούτου δεν αναμένεται νομοθετική πράξη των χωρών μελών της Ευρωπαϊκής Ένωσης, η οποία ως διαδικασία γνωστοποιεί στο ευρύ κοινό τις ιδιαίτερες αλλά και βασικές αρχές της εκάστοτε νομοθεσίας. Το έργο συνεπώς πρώτιστα της ενημέρωσης και της εφαρμογής αφήνεται στην αρμόδια εθνική αρχή, στους επαγγελματίες του τομέα αλλά και στις ίδιες επιχειρήσεις που επιβαλλόμενα θα χρειαστεί να εναρμονιστούν με το νέο πλαίσιο αλλά και να το εφαρμόσουν χωρίς παρεκκλίσεις. Ο σκοπός του επηρεάζει μεγαλύτερο αριθμό οντοτήτων οι οποίες θα πρέπει να εναρμονιστούν εντός και εκτός της Ευρωπαϊκής Ένωσης, εφαρμόζει νέες αρχές και κωδικοποιεί την διαδικασία επεξεργασίας, ενώ επίσης εισάγει λειτουργούς ή υπεύθυνους συμμόρφωσης στην φύλαξη αλλά και επεξεργασία δεδομένων.

Κάθε πληροφορία που εμπίπτει στον ορισμό των προσωπικών δεδομένων του εν λόγω φυσικού προσώπου ή υποκείμενου δεδομένων ελέγχεται από τον ισχύοντα Κανονισμό και καλύπτεται από αυτόν προς την χρήση ή επεξεργασία της.

Από τα πιο πάνω στοιχεία είναι φανερό ότι σχεδόν όλες οι επιχειρήσεις ή επαγγελματικές δραστηριότητες που συνδέονται ή συνεργάζονται ή δραστηριοποιούνται με φυσικά πρόσωπα επηρεάζονται, άμεσα ή έμμεσα, από την νέα νομοθετική τάξη πραγμάτων.

Ο νέος Κανονισμός, ο οποίος όπως προκύπτει συνιστά ένα σύνολο αρχών και διαδικασιών για την αποτελεσματική προστασία των προσωπικών δεδομένων, εισάγει νέες αρχές στην επεξεργασία των δεδομένων. Οι νέες λοιπόν αρχές επιβάλλουν σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων ώστε οι διαδικασίες επεξεργασίας να καλύπτονται από νομιμότητα, αντικειμενικότητα και διαφάνεια. Τα δεδομένα πλέον διέπονται από την αρχή του περιορισμού του σκοπού, που σημαίνει πως τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να συλλέγονται για καθορισμένους ρητούς και νόμιμους σκοπούς και δεν θα υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς.

Ο νέος Κανονισμός ελαχιστοποιεί τα δεδομένα ώστε να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία, επιβάλλει την ακρίβεια και την επικαιροποίηση τους όταν αυτό κρίνεται αναγκαίο με τρόπο που να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων τα οποία είναι ή καθίστανται ανακριβή σε σχέση με τους σκοπούς της επεξεργασίας. Τα δεδομένα διατηρούνται στην μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων δεδομένων αλλά και αποθηκεύονται μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας με τρόπο που να περιορίζεται η περίοδος αποθήκευσης.

Τέλος, τα δεδομένα υποβάλλονται σε επεξεργασία κατά τρόπο που να εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων και μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέσων, αρχές που επιβάλλουν την ακεραιότητα, εμπιστευτικότητα και διαφάνεια.

Η επεξεργασία καθίσταται επιτρεπτή και νόμιμη όταν επίσης υπάρχει συγκατάθεση του υποκειμένου των δεδομένων. Ο νέος Κανονισμός διαφοροποιείται και σ' αυτό το σημείο από το προηγούμενο νομικό καθεστώς, έτσι ώστε η συγκατάθεση του υποκειμένου να γίνεται με τρόπο σαφή, διακριτό από άλλα θέματα και απλά διατυπωμένο. Περαιτέρω το ίδιο υποκείμενο θα πρέπει να έχει ανά πάσα στιγμή το δικαίωμα της ανάκλησης της συγκατάθεσης.

Έτσι λοιπόν, ο ΓΚΠΔ, επιβάλλει τη συμμόρφωση με τους κανονισμούς του τόσο των επιχειρήσεων όσο και των ατόμων που επεξεργάζονται στοιχεία. Υπό τους όρους του ΓΚΠΔ, όχι μόνο οι οργανισμοί θα πρέπει να εξασφαλίσουν ότι τα προσωπικά δεδομένα έχουν αποκτηθεί νόμιμα και υπό αυστηρές προϋποθέσεις, αλλά και αυτοί που συλλέγουν και διαχειρίζονται δεδομένα, θα είναι υποχρεωμένοι να τα προστατεύουν από κατάχρηση και εκμετάλλευση, καθώς επίσης και να σέβονται τα δικαιώματα των υποκειμένων των δεδομένων. Σε διαφορετική περίπτωση, θα τους επιβάλλονται πρόστιμα και κυρώσεις.

Επιπλέον, ο ΓΚΠΔ εφαρμόζεται και αφορά οποιαδήποτε επιχείρηση ή οργανισμό λειτουργεί εντός της Ευρωπαϊκής Ένωσης, καθώς επίσης και οποιαδήποτε εκτός, της οποίας τα αγαθά και οι υπηρεσίες προσφέρονται σε πελάτες ή άλλες επιχειρήσεις εντός της ΕΕ. Αυτό σημαίνει ότι σχεδόν κάθε μεγάλη εταιρία παγκοσμίως θα πρέπει να αρχίσει να δουλεύει στη στρατηγική που θα ακολουθήσει για την εφαρμογή του Κανονισμού, ώστε να είναι έτοιμη όταν ο ΓΚΠΔ τεθεί σε ισχύ.

Ο Κανονισμός επιτάσσει την αυστηρή τήρηση αρχείων δραστηριοτήτων επεξεργασίας και την ύπαρξη ξεκάθαρης συναίνεσης του υποκειμένου των δεδομένων για κάθε επεξεργασία. Το γεγονός αυτό δημιουργεί την ανάγκη άμεσου εκσυγχρονισμού των συστημάτων που εφαρμόζονται για την επεξεργασία των προσωπικών δεδομένων, καθώς σε περίπτωση που γίνει έλεγχος από την εποπτική αρχή και δεν τηρούνται οι αυστηρές προϋποθέσεις συγκατάθεσης και επεξεργασίας επίκεινται ιδιαιτέρως αυστηρά πρόστιμα. Επιπλέον, η αυστηρή τήρηση των εν λόγω προϋποθέσεων είναι επιτακτικής σημασίας, γιατί ο Κανονισμός προβλέπει την υποχρέωση γνωστοποίησης από την πλευρά των επιχειρήσεων της παραβίασης των δεδομένων προσωπικού χαρακτήρα που συνέβη προς την εποπτική αρχή εντός 72 ωρών (breach notification). Έτσι, ο χρόνος ανταπόκρισης των υπευθύνων επεξεργασίας των δεδομένων για την

παροχή των απαιτούμενων διευκρινίσεων εντός της σύντομης αυτής προθεσμίας, καθίσταται πιεστικός, αφού θα πρέπει να έχουν στην διάθεσή τους ανά πάσα στιγμή τις απαιτούμενες πληροφορίες για τις επεξεργασίες που εκτελούν.

Το εχέγγυο της αυξημένης προστασίας των προσωπικών δεδομένων αναλαμβάνει να εξασφαλίσει ένας νέος θεσμός που εισάγεται, αυτός του Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer), ο οποίος θα πρέπει να ορίζεται σε αρκετές περιπτώσεις τόσο από τις επιχειρήσεις, όσο και από το Δημόσιο και ο οποίος θα κληθεί να αναλάβει το ρόλο του θεματοφύλακα των προσωπικών δεδομένων, καθώς με τις ειδικές επιστημονικές του γνώσεις στο αντικείμενο θα μπορεί να προλαμβάνει περιπτώσεις παραβίασης προσωπικών δεδομένων διασφαλίζοντας την ομαλή τήρηση των προϋποθέσεων του Κανονισμού.

Ακόμα, ο νέος Κανονισμός δίνει ιδιαίτερη βαρύτητα στα δικαιώματα των υποκειμένων επεξεργασίας, όπως η κατοχύρωση του δικαιώματος διαγραφής γνωστό και ως «δικαίωμα στη λήθη», το οποίο θεσπίζει τις προϋποθέσεις για την πλήρη διαγραφή ορισμένων προσωπικών δεδομένων που διατηρούν οι υπεύθυνοι επεξεργασίας και αποτελεί μια ουσιαστική εξέλιξή στην προστασία τους.

Σύμφωνα με το άρθρο 4 του νέου Κανονισμού, υπάρχουν δύο τύποι «χειριστών» δεδομένων:

1) Ο «υπεύθυνος επεξεργασίας», δηλαδή «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους»,
2) Ο «εκτελών την επεξεργασία», δηλαδή «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας».

Ουσιαστικά ο νέος Κανονισμός επιβαρύνει με μεγαλύτερη νομικά ευθύνη σε περίπτωση παραβίασης, τον «εκτελών την επεξεργασία», αφού οφείλει να διατηρεί και

να επεξεργάζεται τα αρχεία των προσωπικών δεδομένων, παρέχοντας ένα μεγαλύτερο επίπεδο νομικής προστασίας από παραβιάσεις στον οργανισμό ή την επιχείρηση. Αυτές οι υποχρεώσεις είναι μια καινούρια παράμετρος που εισάγεται με τον ΓΚΠΔ.

Οι «υπεύθυνοι επεξεργασίας» θα είναι επίσης επιφορτισμένοι με την αρμοδιότητα να διασφαλίζουν ότι όλες οι συναλλαγές και επικοινωνίες με τους «εκτελούντες την επεξεργασία», είναι πλήρως εναρμονισμένες με την εφαρμογή του ΓΚΠΔ.

Τέλος, με το νέο Κανονισμό, κάθε Αρχή Ελέγχου, αποκτά και διευρυμένες εξουσίες. Ειδικότερα, κάθε Αρχή διαθέτει την εξουσία να απευθύνει προειδοποιήσεις, επιπλήξεις, να εκδίδει εντολές αλλά και να επιβάλλει πολύ σοβαρά διοικητικά πρόστιμα που μπορεί να ανέλθουν έως και 20.000.000€ ευρώ ή στο 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, όποιο από τα δύο είναι μεγαλύτερο.

Συνεπώς, τα φυσικά πρόσωπα αλλά και πολύ περισσότερο οι επιχειρήσεις, θα πρέπει επιμελώς να προβούν σε όλες τις δέουσες ενέργειες για να ενημερωθούν, να προσαρμοστούν και να συμμορφωθούν με την νέα τάξη δεδομένων.

3.3 Αλλαγές που επιφέρει ο νέος Κανονισμός για τους πολίτες

Λόγω του μεγάλου αριθμού παραβιάσεων και εκμετάλλευσης δεδομένων που έχουν συμβεί στη διάρκεια των ετών, η ατυχής πραγματικότητα για πολλούς είναι ότι ορισμένα από τα στοιχεία τους, είτε πρόκειται για διεύθυνση ηλεκτρονικού ταχυδρομείου, κωδικό πρόσβασης, αριθμό κοινωνικής ασφάλισης ή για εμπιστευτικά αρχεία υγείας, έχουν εκτεθεί στο διαδίκτυο.

Μια από τις σημαντικότερες αλλαγές που θα φέρει ο ΓΚΠΔ είναι η παροχή στους καταναλωτές του δικαιώματος να γνωρίζουν πότε έχουν αλλοιωθεί τα δεδομένα τους. Οι οργανισμοί θα πρέπει να ενημερώσουν το συντομότερο δυνατόν τους αρμόδιους εθνικούς φορείς, προκειμένου να διασφαλίσουν ότι οι πολίτες μπορούν να λάβουν τα κατάλληλα μέτρα για να αποτρέψουν την κατάχρηση των δεδομένων τους.

Εξασφαλίζεται, επίσης ευκολότερη πρόσβαση στα δεδομένα των καταναλωτών ως προς τον τρόπο που αναλύονται και επεξεργάζονται, με τους οργανισμούς να ισχυρίζονται ότι πρέπει να αναλύσουν λεπτομερώς τον τρόπο με τον οποίο χρησιμοποιούν τις πληροφορίες των πελατών με τρόπο σαφή και κατανοητό.

Ορισμένες επιχειρήσεις έχουν ήδη λάβει πρωτοβουλίες για να εξασφαλίσουν ότι αυτό συμβαίνει, ακόμη και αν είναι τόσο βασικό όσο η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου πελατών με πληροφορίες σχετικά με τον τρόπο χρήσης των δεδομένων τους. Πολλοί οργανισμοί, όπως αυτοί στους κλάδους λιανικής και μάρκετινγκ, έρχονται σε επαφή με πελάτες για να ρωτήσουν αν θέλουν να είναι μέρος της βάσης δεδομένων τους. Υπό αυτές τις συνθήκες, ο πελάτης θα πρέπει να έχει έναν εύκολο τρόπο να αποχωρήσει από τα στοιχεία του που βρίσκονται σε μια λίστα αλληλογραφίας.

Ο νέος Κανονισμός, φέρνει μεταξύ άλλων ένα σύνολο αλλαγών, μεταρρυθμίσεων και νέων ενισχυμένων δικαιωμάτων για τους πολίτες των κρατών-μελών της Ευρωπαϊκής Ένωσης.

Συγκεκριμένα, τα υποκείμενα των δεδομένων αποκτούν μεγαλύτερο έλεγχο επί των προσωπικών τους δεδομένων, αφού έχουν πλέον:

1) Δικαίωμα πρόσβασης στα δεδομένα, αφού απαιτείται σαφής συγκατάθεση του ενδιαφερομένου για την επεξεργασία των δεδομένων του αλλά και δυνατότητα να αιτηθεί πληρέστερης και εμπεριστατωμένης ενημέρωσης σχετικά με τον τρόπο αξιοποίησης αυτών.
2) Δικαίωμα εναντίωσης στην επεξεργασία, εφόσον δεν επιθυμούν την επεξεργασία των δεδομένων που τα αφορούν, μεταξύ άλλων στη χρησιμοποίηση τους για την «κατάρτιση προφίλ».
3) Δικαίωμα στη λήθη, δηλαδή το δικαίωμα να ζητήσουν τη διόρθωση ή τη διαγραφή των δεδομένων τους υπό προϋποθέσεις, όταν δεν επιθυμούν πλέον την επεξεργασία και τη διατήρηση προσωπικών τους δεδομένων.
4) Δικαίωμα στη φορητότητα των δεδομένων, να αιτηθούν δηλαδή τη μεταφορά των δεδομένων τους από πάροχο σε πάροχο ή αλλιώς από έναν υπεύθυνο επεξεργασίας σε άλλον.
5) Υποχρέωση ενημέρωσης σε περίπτωση παραβιάσεων: Οι υπεύθυνοι επεξεργασίας, έχουν υποχρέωση, εκτός του να παρέχουν «διαφανείς» και εύκολα προσβάσιμες πληροφορίες στα υποκείμενα των δεδομένων, να

ενημερώσουν τις αρμόδιες Αρχές, μόλις αντιληφθούν παραβίαση, αλλά και τα ίδια τα φυσικά πρόσωπα, των οποίων παραβιάστηκαν τα δεδομένα, εφ' όσον η παραβίαση τα θέτει σε σοβαρό κίνδυνο.

6) Προστασία δεδομένων κατά το σχεδιασμό («Data protection by design»): Επιβάλλεται η δημιουργία προϊόντων και υπηρεσιών (ηλεκτρονικών και μη) που κατά τον αρχικό σχεδιασμό δημιουργούν φιλικές συνθήκες για την προστασία των δεδομένων τους.
7) Προστασία δεδομένων εξ' ορισμού («Data protection by default»): Επιβάλλεται η εφαρμογή κατάλληλων μέτρων που θα διασφαλίζουν ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για το σκοπό της επεξεργασίας.
8) Ειδική πρόβλεψη για την προστασία δεδομένων των παιδιών: Για τη χρήση υπηρεσιών της κοινωνίας των πληροφοριών από ανηλίκους, παρέχεται η δυνατότητα στην εθνική νομοθεσία να μειώσει το όριο ηλικίας για τη συγκατάθεση του ανηλίκου στο 16ο έτος αλλά όχι μικρότερο του 13ου έτους. Για παιδιά μικρότερης ηλικίας προβλέπονται αυστηρότερες διαδικασίες συγκατάθεσης από το πρόσωπο που έχει τη γονική μέριμνα.

Οι επιχειρήσεις θα πρέπει να λάβουν υπόψη αυτά δικαιώματα των υποκειμένων των δεδομένων μόλις τεθεί σε ισχύ ο Κανονισμός.

Ωστόσο, και τα ίδια τα υποκείμενα των δεδομένων δεν θα πρέπει να ξεχνάνε ότι η ιδιωτική τους ζωή είναι πολύτιμη. Οι ίδιοι οι πολίτες έχουν τον πρώτο λόγο στο να επιλέγουν ποιες πληροφορίες δίνουν στους άλλους και ποιες διατηρούν μόνο για τον εαυτό τους, είναι υπεύθυνοι να διατηρούν τον έλεγχο των προσωπικών τους δεδομένων και της ιδιωτικής τους ζωής. Συνεπώς, πρέπει πάντα να σκέφτονται πριν δημοσιεύσουν κάτι στο διαδίκτυο ή πριν δώσουν πληροφορίες προσωπικών τους δεδομένων σε τρίτους.

3.4 Αλλαγές που επιφέρει ο νέος Κανονισμός για τις επιχειρήσεις

Ο νέος Κανονισμός επιβάλλει στους Υπευθύνους Επεξεργασίας περισσότερη διαφάνεια στον τρόπο συλλογής, επεξεργασίας και τήρησης των δεδομένων (Υποχρέωση Διαφάνειας). Οι Υπεύθυνοι Επεξεργασίας:

- Φέρουν την ευθύνη να αποδεικνύουν ότι λαμβάνουν όλα τα κατάλληλα οργανωτικά και τεχνικά μέτρα προστασίας των προσωπικών δεδομένων και ότι συμμορφώνονται με τον Κανονισμό (Υποχρέωση Λογοδοσίας).
- Οφείλουν να υιοθετήσουν συστήματα προστασίας δεδομένων «εξ' ορισμού» (by default) και «κατά το σχεδιασμό» (by design).
- Πρέπει να εξασφαλίζουν ειδική προστασία των παιδιών και των ανηλίκων.

Οι νέες διαδικασίες για τις επιχειρήσεις αφορούν:

- Νέα υποχρέωση σχεδιασμού της «εξ' ορισμού» και «κατά το σχεδιασμό» (by default & by design) προστασίας δεδομένων με τη λήψη κατάλληλων τεχνικών και προστασία δεδομένων όπως ψευδωνυμοποίηση, ελαχιστοποίηση και ενσωμάτωση εγγυήσεων.

Ως προς τον όρο της «ψευδωνυμοποίησης», το άρθρο 4 του νέου Κανονισμού ορίζει ότι είναι «η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο».

- Νέα υποχρέωση τήρησης αρχείου δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων.
- Νέες προϋποθέσεις για την ανάθεση της επεξεργασίας δεδομένων σε «εκτελούντα την επεξεργασία» (outsourcing).
- Νέα υποχρέωση «εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων» (Data Protection Impact Assessment-DPIA) και σχετική υποχρέωση διαβούλευσης με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

- Νέα υποχρέωση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για παραβιάσεις προσωπικών δεδομένων
- Υποχρέωση ορισμού ενός προσώπου ως «Υπεύθυνου Προστασίας Δεδομένων» (Data Protection Officer-DPO) με ειδικές αρμοδιότητες για την τήρηση των παραπάνω διαδικασιών

Οι περισσότερες επιχειρήσεις ανησυχούν σχετικά με την εφαρμογή του νέου Κανονισμού, αλλά στην πραγματικότητα αυτό δεν χρειάζεται, διότι ναι μεν καθίστανται αυστηρότεροι κανόνες και μεγαλύτερες ποινές, αλλά οι βασικές αρχές της προστασίας των δεδομένων, παραμένουν ίδιες. Ο ΓΚΠΔ ουσιαστικά, αφορά περισσότερο τους τρόπους και τις διαδικασίες ελέγχου ως προς τη συμμόρφωση στη νομοθεσία, παρά δημιουργεί κάτι εντελώς νέο εξαρχής.

Το ζήτημα του επανασχεδιασμού των πληροφοριακών συστημάτων σαφώς προκαλεί τεράστιο κόστος, ενώ ο GDPR βάζει σε δοκιμασία και στρατηγικές συνεργασίες μεταξύ εταιρειών οι οποίες θα πρέπει να συμμορφωθούν ταυτόχρονα και με την ίδια αυστηρότητα στο νέο Κανονισμό προστασίας δεδομένων.

Για παράδειγμα, η συλλογή, η αποθήκευση και η διαχείριση των δεδομένων θα πρέπει να έχει ενταχθεί στο πληροφοριακό σύστημα της κάθε επιχείρησης από τον σχεδιασμό του ώστε να τηρούνται τα όρια.

Ταυτόχρονα, οι προμηθευτές ή οι πελάτες χοντρικής που έχουν υιοθετήσει το νέο Κανονισμό, θα έχουν φραγμούς στη συσχέτιση βάσεων δεδομένων που θα μπορούσαν να οδηγήσουν σε αναγνώριση του πελάτη με πλήρη στοιχεία.

Αυτό δυνητικά δημιουργεί μια προβληματική συνθήκη για την εξατομίκευση των υπηρεσιών και τη στοχευμένη εμπορική πολιτική που αποσκοπεί στην ικανοποίηση του πελάτη. Όλες οι εταιρείες άλλωστε, αναπτύσσουν ειδικές πολιτικές πώλησης και προνομίων για τους «καλούς» πελάτες τους, ενώ οι διαφημιστικές μέσω του «profiling» επιτυγχάνουν να φτάνει το σωστό μήνυμα στον σωστό παραλήπτη.

Την ίδια ώρα, στον χώρο της επικοινωνίας (επικοινωνίες, εκδόσεις και διαφημιστικές εταιρείες) όπου όλες οι επιχειρήσεις θα πρέπει να συμμορφωθούν με τον Κανονισμό GDPR, επικρατεί έντονος προβληματισμός για το πώς νέα εργαλεία καταγραφής της

συμπεριφοράς και αξιοποίησης της διαφημιστικής στόχευσης δεν θα συγκρούονται ευθέως με τα ρυθμιστικά πλαίσια.

Με την υιοθέτηση του ΓΚΠΔ, τα σημαντικότερα στοιχεία που υφίστανται τροποποιήσεις είναι:

1) Μεγαλύτερο προβάδισμα και εξουσία στα άτομα. Ο νέος Κανονισμός, τοποθετεί τα υποκείμενα των δεδομένων στο κέντρο της προστασίας των δεδομένων. Για παράδειγμα, το δικαίωμα στη φορητότητα των δεδομένων προβλέπει ότι όταν οι πελάτες θέλουν να αλλάξουν πάροχο για τα e-mail τους, θα πρέπει να μπορούν να μεταφέρουν το σύνολο των δεδομένων τους στο νέο πάροχο. Σήμερα, οι καταναλωτές έχουν ήδη τη δυνατότητα να ζητήσουν την διαγραφή των προσωπικών τους στοιχείων, αλλά ο ΓΚΠΔ ενισχύει αυτό το δικαίωμα διαγραφής με το λεγόμενο «δικαίωμα στη λήθη». Ωστόσο, πέρα από τη συμμόρφωση, η μεγαλύτερη αλλαγή θα είναι η μετατόπιση της στάσης του οργανισμού απέναντι στην προστασία της ιδιωτικής ζωής. Η προστασία της ιδιωτικής ζωής τείνει να γίνει αντικείμενο σεβασμού για τις επιχειρήσεις. Στοιχείο-κλειδί θα είναι το να καταφέρουν να κερδίσουν την εμπιστοσύνη των πελατών και να αποκτήσουν ανταγωνιστικό πλεονέκτημα, ακριβώς επειδή οι πελάτες δίνουν μεγάλη αξία στην προστασία της ιδιωτικής τους ζωής. Εκτιμούν, επίσης, τις απλές και διαφανείς διαδικασίες για να την προάσπιση των δικαιωμάτων τους

2) Προστασία της ιδιωτικότητας ήδη από το στάδιο του σχεδιασμού («by design»). Το πρώτο βήμα για κάθε οργανισμό θα είναι μια άσκηση χαρτογράφησης της ροής των δεδομένων στην οποία θα συμμετέχει το σύνολο του οργανισμού, επειδή η προστασία της ιδιωτικότητας ήδη από τον σχεδιασμό προϋποθέτει ότι όλες οι υπηρεσίες θα εξετάσουν τα δεδομένα τους και τον τρόπο με τον οποίο τα χειρίζονται. Αφού εντοπίσουν τα προσωπικά τους δεδομένα και πώς ακριβώς τα χρησιμοποιούν, θα πρέπει να τα διασφαλίσουν με τον σωστό τρόπο. Η εξέταση των δεδομένων των ατόμων και πελατών τους από τη σκοπιά της ιδιωτικότητάς τους, από την ανάπτυξη του προϊόντος σε όλη την αλυσίδα του εφοδιασμού έως τον τελικό πελάτη, είναι ακριβώς η ουσία της νέας νομοθεσίας των προσωπικών δεδομένων. Οι περισσότερες εταιρείες έχουν

ήδη υιοθετήσει ένα σύστημα που είναι σε θέση να προσδιορίζει τα προσωπικά δεδομένα, αφού ήδη πρέπει να έχουν συμμορφωθεί με την υφιστάμενη νομοθεσία για την προστασία των δεδομένων. Η νέα νομοθεσία υποχρεώνει τους οργανισμούς να υιοθετήσουν πιο λεπτομερείς διαδικασίες, αλλά ευτυχώς υπάρχουν πολλές λύσεις που μπορούν να υποστηρίξουν αυτή τη διαδικασία ελέγχου, όπως η χρήση νέων τεχνολογιών και λογισμικών. Η προστασία της ιδιωτικότητας ήδη από τον σχεδιασμό προϋποθέτει επίσης ότι υπάρχει μεγαλύτερη διαφάνεια σχετικά με τα δεδομένα και τη μεταφορά δεδομένων.

3) Περισσότερα μέσα επιβολής κυρώσεων και προστίμων. Με τον νέο Κανονισμό, η επιβολή του νόμου γίνεται αυστηρότερη. Οι Αρχές Προστασίας Προσωπικών Δεδομένων αποκτούν περισσότερους πόρους και θα ενώσουν τις δυνάμεις τους σε ένα νέο πανευρωπαϊκό σώμα που θα εκδίδει δεσμευτικές γνωμοδοτήσεις. Εκτός αυτού, τα πρόστιμα θα είναι τόσο υψηλά - έως και 4% του ετήσιου παγκόσμιου κύκλου εργασιών ενός οργανισμού - που ο νέος Κανονισμός αυτομάτως αφυπνίζει τους οργανισμούς σε όλους τους κλάδους. Ο φόβος της επιβολής προστίμου δεν θα έπρεπε να είναι το βασικό κίνητρο των οργανισμών για συμμόρφωση, αλλά είναι σίγουρα ένας λόγος για να προσέξουν πολύ περισσότερο.

4) Αυξημένη υποχρέωση λογοδοσίας. Ο ΓΚΠΔ καθιστά τους οργανισμούς υπόλογους για την προστασία των προσωπικών δεδομένων. Θα φέρουν το βάρος της απόδειξης όσον αφορά το εάν, το πώς και το πόσο καλά προστάτευσαν τα προσωπικά δεδομένα. Σήμερα υπάρχει μια αρκετά τυπική διαδικασία για την απόκτηση άδειας πρόσβασης σε προσωπικά δεδομένα, που βασίζεται στο είδος των δεδομένων που επεξεργάζονται και στο αν μεταφέρονται σε τρίτους. Στο μέλλον, αυτό που θα μετρά περισσότερο θα είναι το πόσο καλά οργανωμένες είναι οι διαδικασίες των επιχειρήσεων, παρά η απόκτηση τυπικής άδειας πρόσβασης. Στο πλαίσιο αυτό, θα είναι χρήσιμο να υπάρχει κάποιος, είτε εσωτερικά είτε εξωτερικά, που να αντιλαμβάνεται την έννοια του απορρήτου των δεδομένων και γνωρίζει πώς να επιφέρει αλλαγές και να εφαρμόζει τη νομοθεσία.

Μια άλλη παράμετρο που εισάγει ο νέος Κανονισμός, είναι ότι θεσπίζει ένα νόμο σε ολόκληρη την ήπειρο και ένα ενιαίο σύνολο κανόνων που ισχύουν για τις επιχειρήσεις που αναπτύσσουν επιχειρηματικές δραστηριότητες στην ΕΕ. Αυτό σημαίνει ότι η εμβέλεια της νομοθεσίας εκτείνεται πέρα από τα σύνορα της ίδιας της Ευρώπης, καθώς οι εταιρείες που εδρεύουν εκτός της περιοχής αλλά έχουν δραστηριότητα στο «ευρωπαϊκό έδαφος» θα εξακολουθούν να υπόκεινται σε συμμόρφωση με τον Κανονισμό. Η Ευρωπαϊκή Επιτροπή υποστηρίζει ότι, έχοντας μια ενιαία αρχή εποπτείας για ολόκληρη την ΕΕ, θα καταστεί απλούστερη και φθηνότερη η λειτουργία των επιχειρήσεων στην περιοχή. Αυτό σημαίνει ότι, θα διασφαλιστεί ότι οι εγγυήσεις προστασίας δεδομένων ενσωματώνονται σε προϊόντα και υπηρεσίες από το αρχικό στάδιο ανάπτυξης, παρέχοντας «προστασία δεδομένων από το σχεδιασμό» σε νέα προϊόντα και τεχνολογίες. Οι οργανισμοί θα ενθαρρυνθούν επίσης να υιοθετήσουν τεχνικές όπως «ψευδωνυμοποίηση» προκειμένου να επωφεληθούν από τη συλλογή και ανάλυση δεδομένων, ενώ ταυτόχρονα προστατεύεται το απόρρητο των πελατών τους.

3.4.1 Υποχρέωση Γνωστοποίησης παραβιάσεων προσωπικών δεδομένων

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων εισάγει, μεταξύ άλλων, την υποχρέωση γνωστοποίησης τυχόν παραβιάσεων προσωπικών δεδομένων (data breaches). Όλες οι επιχειρήσεις θα έχουν ως καθήκον να αναφέρουν ορισμένες μορφές παραβιάσεων δεδομένων που συνεπάγονται μη εξουσιοδοτημένη πρόσβαση ή απώλεια δεδομένων προσωπικού χαρακτήρα στην αρμόδια εποπτική αρχή.

Σε ορισμένες περιπτώσεις, οι επιχειρήσεις θα υποχρεούνται να ενημερώνουν τα άτομα που επηρεάζονται από την παραβίαση, ειδικά όταν αυτή ενδέχεται να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες των ατόμων και να οδηγήσει σε διακρίσεις, οικονομικές απώλειες, απώλεια εμπιστευτικότητας ή οποιοδήποτε άλλο οικονομικό ή κοινωνικό μειονέκτημα.

Κατευθυντήριες γραμμές για την εφαρμογή των διατάξεων του νέου ΓΚΠΔ αναφορικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα, εξέδωσε η Ομάδα Εργασίας του άρθρου 29. Η Ομάδα Εργασίας του άρθρου 29 είναι ένα ανεξάρτητο συμβουλευτικό σώμα που ασχολείται με την προστασία των δεδομένων

προσωπικού χαρακτήρα και την ιδιωτικότητα στην Ευρωπαϊκή Ένωση. Συστάθηκε με βάση το άρθρο 29 της Οδηγίας 95/46/ΕΚ, ενώ οι αρμοδιότητές του περιγράφονται στο άρθρο 30 της ίδιας Οδηγίας, καθώς και στο άρθρο 15 της Οδηγίας 2002/58/ΕΚ.

Η γνωστοποίηση απευθύνεται προς την αρμόδια εθνική εποπτική αρχή (άρθρο 33) και σε ορισμένες περιπτώσεις, η παραβίαση πρέπει να ανακοινώνεται και στα άτομα, των οποίων τα προσωπικά δεδομένα έχουν επηρεαστεί από αυτήν (άρθρο 34).

Η υποχρέωση γνωστοποίησης παραβιάσεων υφίσταται ήδη για ορισμένους οργανισμούς, όπως οι πάροχοι διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών (όπως ορίζονται στην Οδηγία 2009/136/ΕΚ και τον Κανονισμό 611/2013).

Υπάρχουν επίσης ορισμένα κράτη μέλη της ΕΕ στα οποία έχει ήδη θεσπιστεί υποχρέωση γνωστοποίησης των παραβιάσεων, είτε σε γενικό επίπεδο (π.χ. Ολλανδία) είτε σε πιο ειδικό (π.χ. Γερμανία και Ιταλία), ενώ σε κάποιες χώρες, όπως για παράδειγμα στην Ιρλανδία, εφαρμόζονται σχετικοί κώδικες ορθών πρακτικών (Codes of Practice).

Αν και πολλές αρμόδιες αρχές κρατών μελών της ΕΕ ενθαρρύνουν τους υπευθύνους επεξεργασίας να γνωστοποιούν τέτοιες παραβιάσεις, η Οδηγία 95/46/ΕΚ για την προστασία των δεδομένων, την οποία αντικαθιστά ο ΓΚΠΔ, δεν περιέχει συγκεκριμένη υποχρέωση γνωστοποίησης.

Οι εκτελούντες την επεξεργασία είναι επίσης επιφορτισμένοι με σημαντικό ρόλο, καθώς πρέπει να ενημερώνουν τον υπεύθυνο επεξεργασίας αμέσως μόλις αντιληφθούν κάποια παραβίαση δεδομένων προσωπικού χαρακτήρα.

Η Ομάδα Εργασίας του άρθρου 29 εκτιμά ότι η νέα υποχρέωση γνωστοποίησης έχει μία σειρά από πλεονεκτήματα.

Όταν γνωστοποιούν την παραβίαση στην εποπτική αρχή, οι υπεύθυνοι επεξεργασίας μπορούν να λαμβάνουν συμβουλές και καθοδήγηση σχετικά με το εάν τα πρόσωπα, τα δεδομένα των οποίων έχουν παραβιαστεί, θα πρέπει να ενημερωθούν (άρθρο 34 παρ. 4 και άρθρο 58 παρ. 2).

Η ανακοίνωση της παραβίασης στα υποκείμενα των δεδομένων επιτρέπει στον υπεύθυνο επεξεργασίας να παρέχει πληροφορίες σχετικά με τους κινδύνους που

παρουσιάζονται ως αποτέλεσμα της παραβίασης και τα μέτρα που μπορούν να λάβουν για να προστατευθούν από τις πιθανές συνέπειες.

Στο επίκεντρο οποιασδήποτε παραβίασης πρέπει να βρίσκεται η προστασία των ατόμων και των προσωπικών τους δεδομένων. Συνεπώς, η γνωστοποίηση της παραβίασης πρέπει να θεωρείται ως εργαλείο που ενισχύει τη συμμόρφωση σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα.

Ταυτόχρονα, η μη γνωστοποίηση παραβίασης σε ένα υποκείμενο δεδομένων ή στην εποπτική αρχή ενδέχεται να συνεπάγεται την επιβολή κυρώσεων στον υπεύθυνο επεξεργασίας, σύμφωνα με το άρθρο 83. Επομένως, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες αυτήν, θα πρέπει να καταρτίσουν εκ των προτέρων ένα πλάνο και να θέσουν σε εφαρμογή τις απαιτούμενες διαδικασίες, προκειμένου να είναι σε θέση να εντοπίζουν και να περιορίζουν εγκαίρως τυχόν παραβιάσεις, να προβαίνουν σε εκτίμηση του κινδύνου για τα υποκείμενα των δεδομένων, και εν συνεχεία να αποφασίζουν κατά πόσον είναι απαραίτητο να ειδοποιηθεί η αρμόδια εποπτική αρχή και συγκεκριμένα πρόσωπα.

Σύμφωνα με τη γνωμοδότηση, η γνωστοποίηση στην εποπτική αρχή θα πρέπει να αποτελεί μέρος του σχεδίου αντιμετώπισης περιστατικών παραβίασης δεδομένων. Ο νέος Κανονισμός περιέχει διατάξεις σχετικά με το πότε πρέπει να γνωστοποιηθεί η παραβίαση και σε ποιον, καθώς και ποιες πληροφορίες θα πρέπει να παρέχονται στο πλαίσιο της γνωστοποίησης.

Με άλλα λόγια, σε περίπτωση παραβίασης του ονόματος, της διεύθυνσης, των δεδομένων της γέννησης, των ιατρικών αρχείων, των τραπεζικών στοιχείων ή τυχόν ιδιωτικών δεδομένων σχετικά με τους πελάτες, ο οργανισμός υποχρεούται να ενημερώσει τους ενδιαφερόμενους καθώς και τον αρμόδιο ρυθμιστικό φορέα, για να περιορίσει τη ζημιά.

Για παράδειγμα, σε περίπτωση που μια εταιρεία χάσει δεδομένα, είτε πρόκειται για «κυβερνοεπίθεση», είτε για ανθρώπινο λάθος ή για οτιδήποτε άλλο, η εταιρεία θα υποχρεωθεί να παραδώσει μια γνωστοποίηση παραβίασης. Αυτό πρέπει να περιλαμβάνει κατά προσέγγιση δεδομένα σχετικά με την παραβίαση, συμπεριλαμβανομένων των αριθμών των σχετικών αρχείων προσωπικών δεδομένων, των κατηγοριών των πληροφοριών και του αριθμού των ατόμων που διακυβεύονται τα προσωπικά τους δεδομένα. Οι επιχειρήσεις θα πρέπει επίσης να

παρέχουν μια περιγραφή των πιθανών συνεπειών της παραβίασης των δεδομένων, όπως η κλοπή χρημάτων ή η απάτη ταυτότητας, καθώς και περιγραφή των μέτρων που λαμβάνονται για την αντιμετώπιση της παραβίασης των δεδομένων και για την αντιμετώπιση τυχόν αρνητικών επιπτώσεων που μπορεί να αντιμετωπίσουν τα άτομα. Θα πρέπει επίσης να παρέχονται τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή του βασικού υπευθύνου που έχει αναλάβει την επίλυση του ζητήματος της παραβίασης.

Η παραβίαση πρέπει να αναφέρεται στο αρμόδιο εποπτικό όργανο εντός 72 ωρών από την πρώτη στιγμή που η επιχείρηση ή ο οργανισμός θα λάβει γνώση αυτού. Αυτό θα πρέπει να γίνει μέσω «κοινοποίησης παραβίασης», η οποία θα πρέπει να παραδοθεί απευθείας στα θύματα. Αυτές οι πληροφορίες ενδέχεται να μην κοινοποιούνται μόνο σε δελτίο τύπου, στα κοινωνικά μέσα ή στην ιστοσελίδα της εταιρείας. Πρέπει να είναι μια αλληλογραφία μεταξύ των ατόμων που επηρεάζονται. Επιπλέον, αν η παραβίαση είναι αρκετά σοβαρή ώστε να σημαίνει ότι οι πελάτες ή το κοινό πρέπει να ενημερωθούν, η νομοθεσία του ΓΚΠΔ αναφέρει ότι οι πελάτες πρέπει να γίνονται υπεύθυνοι χωρίς «αδικαιολόγητη καθυστέρηση».

3.4.2 Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (Data Protection Impact Assessment - DPIA)

Σύμφωνα με τον άρθρο 35 του ΓΚΠΔ κάθε δημόσιος ή ιδιωτικός οργανισμός που επεξεργάζεται συγκεκριμένα προσωπικά δεδομένα, υποχρεούται πριν από ην επεξεργασία να εκτελεί μια εκτίμηση των πιθανών επιπτώσεων των κινδύνων που μπορεί να προκύψουν από την επεξεργασία των δεδομένων αυτών.

Πρακτικά, η εκτίμηση του αντικτύπου σχετικά με την προστασία των προσωπικών δεδομένων, αποτελεί μια διαδικασία που πραγματοποιείται κατά τη φάση του σχεδιασμού της εφαρμογής του νέου Κανονισμού. Το γεγονός ότι εκτελείται κατά το αρχικό στάδιο σχεδίασης της εφαρμογής δίνει το πλεονέκτημα της πρόληψης και της αντιμετώπισης των κινδύνων, όπως επίσης και της αποφυγής οικονομικής ζημιάς για τον οργανισμό, σε περίπτωση που οι επιπτώσεις των κινδύνων επεκταθούν σε κάποιον από τους εμπλεκόμενους στην επεξεργασία. Αυτή η εκ των προτέρων εκτίμηση της όλης διαδικασίας της επεξεργασίας ενισχύει την πιθανότητα επιρροής της

DPIA στην σχεδίαση της εφαρμογής, πληρώντας με αυτό τον τρόπο το κριτήριο της ιδιωτικότητας κατά την σχεδίαση (privacy by design).

Με την ολοκλήρωση της διαδικασίας αυτής, συντάσσεται μια έκθεση, η οποία περιλαμβάνει όλα τα στοιχεία και τα χαρακτηριστικά της επεξεργασίας, την εκτίμηση των πιθανών κινδύνων, όπως επίσης και τα ενδεικτικά μέτρα ασφαλείας που θα μπορούσαν να ληφθούν, ώστε να επιτευχθεί ο περιορισμός ή η εξάλειψη αυτών των κινδύνων. Η έκθεση αυτή υπόκειται σε έλεγχο από την εκάστοτε Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ώστε να αξιολογήσει το κατά πόσο η συγκεκριμένη επεξεργασία παρουσιάζει συμμόρφωση με τον Κανονισμό της Ευρωπαϊκής Επιτροπής και έπειτα να εκδώσει την απαραίτητη άδεια επεξεργασίας των συγκεκριμένων δεδομένων.

Σύμφωνα με τη παράγραφο 7 του άρθρου 35, η εκτίμηση επιπτώσεων (DPIA) αποσκοπεί στη συστηματική περιγραφή των διαδικασιών και των σκοπών επεξεργασίας, στην εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων αυτών συγκριτικά με τους σκοπούς της επεξεργασίας, στην εκτίμηση των κινδύνων ως προς τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, και τέλος στη λήψη μέτρων για τη διευθέτηση των κινδύνων και των ζητημάτων ασφάλειας ώστε να διαβεβαιώνεται η προστασία των δεδομένων και η συμμόρφωση με τον ΓΚΠΔ.

Έτσι, η DPIA πρέπει να θεωρείται ένα κομμάτι από μια ευρύτερη διαδικασία διαχείρισης κινδύνων (risk management) που οφείλει να εφαρμόζει ένας οργανισμός. Παρ’ όλο που ονομάζεται εκτίμηση ή αξιολόγηση, η DPIA δεν είναι μια απλή ανάλυση κινδύνων αλλά περιλαμβάνει όλα τα απαραίτητα μέτρα ασφαλείας ή ελέγχου σε σχέση με τους πιθανούς κινδύνους.

3.4.3 Ο GDPR στις ευρωπαϊκές επιχειρήσεις

Σύμφωνα με έρευνες που έχουν πραγματοποιηθεί το τελευταίο διάστημα σε ευρωπαϊκές επιχειρήσεις, ένα μεγάλο ποσοστό αυτών δηλώνει ανησυχία σχετικά με την εφαρμογή του Κανονισμού και τη συμμόρφωσή τους ως προς αυτόν, ενώ δεν

φαίνονται σίγουρες ότι θα καταφέρουν να ενταχθούν σε αυτόν εντός της οριζόμενης προθεσμίας.

Συγκεκριμένα, σύμφωνα με τα αποτελέσματα της έρευνας της Symantec για την Ευρωπαϊκή Επιτροπή Προσωπικών Δεδομένων (European Data Privacy Survey), η οποία πραγματοποιήθηκε μέσω συνεντεύξεων σε 900 επιχειρήσεις και υπευθύνους μηχανογράφησης στη Βρετανία, τη Γαλλία και τη Γερμανία, το 91% των ερωτηθέντων έχει σοβαρές ανησυχίες σχετικά με την ικανότητα συμμόρφωσης.

Η έρευνα αποκάλυψε επίσης ότι μόλις το 22% των επιχειρήσεων θεωρούν ότι η συμμόρφωση αποτελεί ύψιστη προτεραιότητα για τα επόμενα δύο χρόνια, ενώ μόνο το 26% των ερωτηθέντων πιστεύουν ότι η επιχείρησή τους είναι πλήρως προετοιμασμένη για το νέο Ευρωπαϊκό Κανονισμό Προστασίας Δεδομένων (GDPR).

Το 23% δήλωσε ότι η επιχείρησή τους δεν θα είναι καθόλου ή θα είναι εν μέρει συμμορφωμένη μέχρι το 2018. Από το συγκεκριμένο αυτό ποσοστό, μόνο το 20%, πιστεύουν ότι είναι πιθανό να καταστούν πλήρως συμμορφωμένες με τον GDPR, ενώ σχεδόν οι μισοί από αυτούς (49%), πιστεύουν ότι ορισμένα μόνο τμήματα των εταιρειών θα μπορέσουν να συμμορφωθούν, σε αντίθεση με άλλα τμήματα που δε θα μπορέσουν.

Μια άλλη πρόσφατη μελέτη της Forrester με τίτλο «Predictions 2017-A Year of Reckoning», προβλέπει ότι το 80% των επιχειρήσεων που επηρεάζονται από το νόμο GDPR δεν θα έχουν συμμορφωθεί με τις επιταγές του τον επόμενο Μάιο, όταν και θα τεθεί σε ισχύ.

Από αυτές, το 50% θα αγνοήσει σκόπιμα τον ευρωπαϊκό κανονισμό, που σημαίνει ότι «έχουν ζυγίσει το κόστος και τα ρίσκα και αποφάσισαν να ακολουθήσουν εκείνο το μονοπάτι που θεωρούν το πιο συμφέρον για αυτές» αναφέρει η Forrester. Επιπλέον, οι αναλυτές προσθέτουν ότι το άλλο 50% θα προσπαθήσει να συμμορφωθεί, αλλά θα αποτύχει.

Από τα αποτελέσματα των παραπάνω ερευνών προκύπτει συνεπώς, ότι οι επιχειρήσεις, αν και γνωρίζουν για τις αλλαγές, τα νέα μέτρα και τις κυρώσεις που επιφέρει ο νέος Κανονισμός, καθίστανται ασυνεπείς ή ανίκανες να βρουν τρόπους

συμμόρφωσης με αυτόν. Αυτό ενδεχομένως να οφείλεται είτε στην ελλιπή, εις βάθος, ενημέρωσή τους για τις μεθόδους εναρμόνισης με τους κανόνες του GDPR, είτε στην έλλειψη των κατάλληλων ατόμων που θα μπορούσαν να βοηθήσουν στην προετοιμασία τους για την αποδοχή των νέων αλλαγών, είτε ακόμα και στην αδυναμία τους να εφαρμόσουν τη θεωρία του Κανονισμού στην πράξη. Το αποτέλεσμα είναι ένα μεγάλο μέρος των επιχειρήσεων να αδυνατεί να συμβαδίσει με τον Κανονισμό εγκαίρως ή και να «τρέχει» μέχρι τελευταία στιγμή να προφτάσει τις επικείμενες αλλαγές.

3.4.4 Ο GDPR στις ελληνικές επιχειρήσεις

Από την άλλη, οι ελληνικές επιχειρήσεις, ανάλογα με το μέγεθος τους κάθε φορά, παρουσιάζουν μία γενικά θετική εικόνα στην ψηφιακή τους προστασία. Αυτό όμως που λείπει, είναι η εταιρική κουλτούρα, γιατί «ψηφιακή προστασία» δεν σημαίνει μόνο «ασφάλεια των συστημάτων» αλλά και προστασία της ιδιωτικότητας.

Οι επιχειρήσεις θα πρέπει πρώτα οι ίδιες να κατανοήσουν την σπουδαιότητα και την αξία των δεδομένων που έχουν στην διάθεσή τους, αλλά να κατανοήσουν επίσης γιατί οι πολιτικές που ακολουθούνται – από τα ανεξαρτήτως βαθμίδας στελέχη τους – θα πρέπει να συντείνουν σε αυτό το σκοπό, και να επενδύσουν και τυπικά και ουσιαστικά στην υλοποίησή τους. Αν τα κράτη μέλη της ΕΕ θέλουν να είναι όντως ευνομούμενα σε όλες τις εκφάνσεις της διοίκησης τους, πρέπει να θεσπίσουν τα αναγκαία μέτρα και μηχανισμούς. Η τεχνολογική εξέλιξη δεν μπορεί από μόνη της να παράσχει αυτή την προστασία. Άλλωστε, το κάθε τεχνολογικό επίτευγμα εξ ορισμού μπορεί ανά πάσα στιγμή να είναι «παρωχημένο». Η γνώση, η ευαισθητοποίηση και η λογοδοσία πρέπει να γίνουν ο ακρογωνιαίος λίθος για κάθε επιχείρηση που θέλει να προστατεύσει τα προσωπικά δεδομένα, τα οποία αποτελούν το σημαντικότερο περιουσιακό της στοιχείο.

Πολλές από τις μεγάλες ελληνικές επιχειρήσεις και οργανισμούς ασχολούνται με το θέμα της συμμόρφωσης, αλλά πρακτικά ελάχιστες είναι εκείνες που έχουν ολοκληρώσει το συγκεκριμένο έργο, το οποίο απαιτεί συντονισμό μίας μεγάλης ομάδας στελεχών και διαμόρφωση εξειδικευμένων διαδικασιών.

Ωστόσο, στο ζήτημα του GDPR θα πρέπει να επισημανθεί ότι η Ελλάδα δεν βρίσκεται πίσω από τις υπόλοιπες χώρες της ΕΕ, καθώς και εκεί παρουσιάζονται αρκετές καθυστερήσεις.

Κάθε ελληνική επιχείρηση που διατηρεί σε υπολογιστή δεδομένα (offline & online) πρέπει να συντάξει έκθεση διαχείρισης αυτών και να συμβουλευτεί την αρμόδια Αρχή για το εάν θα πρέπει να συμμορφωθεί με το νέο Κανονισμό. Εάν είναι υπόχρεη, θα πρέπει να ορίσει έναν υπεύθυνο διαχείρισης και προστασίας δεδομένων ο οποίος δεν μπορεί να είναι ο τεχνικός Ηλεκτρονικών Υπολογιστών - Δικτύων, δηλαδή ο επικεφαλής του υπάρχοντος Πληροφοριακού Συστήματος, λόγω σύγκρουσης συμφερόντων.

Ο Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer - DPO) θα είναι το «δεξί χέρι» του μάνατζερ και θα πρέπει να συγκροτήσει ομάδα ειδικών και με νομική συμβολή ώστε να απεξαρτηθεί από την πληροφόρηση που προέρχεται από μονάδες και πρόσωπα που μπορεί να προστατεύουν ξεπερασμένα και επικίνδυνα για διαρροές πληροφοριακά συστήματα.

Στη συνέχεια, η εταιρεία πρέπει να εξετάσει την αλλαγή ή και προσαρμογή των πληροφοριακών της συστημάτων για να συμμορφωθεί με τους όρους που θέτει ο Κανονισμός.

3.4.5 Ο GDPR στον Δημόσιο Τομέα

Όσον αφορά την εφαρμογή του GDPR στον Δημόσιο Τομέα, το Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, μέσω της αρμόδια Γενικής Γραμματείας Ψηφιακής Πολιτικής, συνεργάζεται με τα αρμόδια Υπουργεία και τις Ανεξάρτητες και Ρυθμιστικές Αρχές για την άμεση ενσωμάτωση του νέου Κανονισμού.

Στόχος αποτελεί ο σχεδιασμός ενός ολοκληρωμένου σχεδίου ασφαλείας και η ανάπτυξη ενιαίας πλατφόρμας που θα υιοθετεί τα απαιτούμενα τεχνικά, διαδικαστικά και οργανωτικά μέτρα που απαιτούνται για την προστασία των πληροφοριακών συστημάτων.

Η Γενική Γραμματεία θα συντονίσει μεγάλους φορείς, όπως η ΗΔΙΚΑ (Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης), η ΓΓΠΣ (Γενική Γραμματεία Πληροφοριακών Συστημάτων), ο ΕΟΠΥΥ (Εθνικός Οργανισμός Παροχής Υπηρεσιών Υγείας) και το

ΕΔΕΤ (Εθνικό Δίκτυο Έρευνας και Τεχνολογίας), οι οποίοι κατέχουν μεγάλο όγκο προσωπικών δεδομένων, ώστε να εναρμονιστούν με τον Κανονισμό GDPR για την προστασία των προσωπικών δεδομένων.

Επιπλέον, η Γενική Γραμματεία συμμετέχει στην ομάδα εναρμόνισης της Εθνικής νομοθεσίας με την οδηγία NIS (Network and Information Security), αλλά και στο cooperation group, όπου γίνεται ανταλλαγή βέλτιστων πρακτικών μεταξύ των κρατών μελών.

Στο πλαίσιο του συντονισμού της ασφάλειας στον τομέα του Δημοσίου, όλοι οι φορείς καλούνται να ορίσουν Υπεύθυνο Ασφάλειας Πληροφοριών και Δικτύων, ο οποίος θα λειτουργεί ως σύνδεσμος με τη Γενική Γραμματεία Ψηφιακής Πολιτικής και θα εκπροσωπεί το φορέα του.

Μέχρι στιγμής, ουσιαστικές ενέργειες για την πρακτική εφαρμογή του GDPR στον Δημόσιο Τομέα δεν έχουν γίνει ευρέως γνωστές, με αποτέλεσμα η συμμόρφωση των κρατικών υπηρεσιών με τον Κανονισμό αυτό, να μένει ακόμα «πίσω» σε σχέση με τον ιδιωτικό τομέα.

3.5 Ο Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer-DPO)

Καθίσταται σαφές λοιπόν, πως όλοι οι οργανισμοί που με τον έναν ή τον άλλον τρόπο συλλέγουν, αποθηκεύουν και επεξεργάζονται δεδομένα ή συμπεριφορές σε μεγάλη κλίμακα ή είναι δημόσιες αρχές, έχουν να ακολουθήσουν μία μακρά και μη ξεκάθαρα προσδιορισμένη πορεία προς τη συμμόρφωσή τους με τις διατάξεις του Κανονισμού. Στον πυρήνα αυτής της διαδικασίας βρίσκεται ο θεσμός του **Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer)**. Η σχετική πρόβλεψη υπάρχει ρητώς στα άρθρα 37-39 του Κανονισμού, αλλά βρίσκεται διάσπαρτη σε πολλά σημεία του.

Ο Υπεύθυνος Προστασίας Δεδομένων δρα και ενεργεί σε καθεστώς ανεξαρτησίας και ανεξάρτητα από τον ειδικό νομικό χαρακτηρισμό της σύμβασης που τον συνδέει με τον εκάστοτε οργανισμό και από το αν ο οργανισμός αυτός λειτουργεί ως υπεύθυνος επεξεργασίας ή ως εκτελών την επεξεργασία.

Το άρθρο 37 του Κανονισμού ορίζει το θεσμό του Υπευθύνου Προστασίας Δεδομένων ως υποχρεωτικό σε τρεις περιπτώσεις:

1. Όταν η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας,
2. Όταν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή
3. Όταν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα κατά το άρθρο 9 και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο.

Παραδείγματα εταιρειών που επιβάλλεται ο καθορισμός του DPO είναι οργανισμοί και επιχειρήσεις που δραστηριοποιούνται στον τομέα της Υγείας, των Τηλεπικοινωνιών, δημόσιοι φορείς και ΔΕΚΟ, οργανισμοί που επεξεργάζονται Ειδικά Προσωπικά Δεδομένα (π.χ. διαχείριση μισθοδοσίας, οικονομικά στοιχεία κ.ά.), κ.λπ.

Όσον αφορά τις δημόσιες αρχές, μπορεί να διοριστεί ένας ενιαίος Υπεύθυνος Προστασίας Δεδομένων σε μια ομάδα οργανώσεων. Ενώ δεν είναι υποχρεωτικό για τους οργανισμούς, εκτός των ανωτέρω, να ορίσουν έναν DPO, όλοι οι οργανισμοί θα χρειαστεί να εξασφαλίσουν ότι διαθέτουν τις δεξιότητες και το προσωπικό που απαιτείται ώστε να συμμορφώνεται με τη νομοθεσία του νέου Κανονισμού. Και η συμμόρφωση αυτή αποτελεί μία πολύπλοκη, πολυεπίπεδη και διατομεακή διαδικασία, που περιλαμβάνει πολλά στάδια, όπως ταξινόμηση δεδομένων, καταγεγραμμένες διαδικασίες συλλογής, ταξινόμησης, αποθήκευσης, μεταβίβασης και διαμοιρασμού δεδομένων, εκθέσεις αποτίμησης κινδύνου (DPIA), διαδικασίες αντιμετώπισης κινδύνων και άλλα. Δεν υπάρχουν καθορισμένα κριτήρια σχετικά με το ποιος πρέπει να είναι Υπεύθυνος Προστασίας Δεδομένων ή τι είδους προσόντα θα έπρεπε να έχει, αλλά σύμφωνα με το Γραφείο του Επιτρόπου Πληροφόρησης, θα πρέπει να διατίθεται νομοθεσία για την επαγγελματική πείρα και την προστασία των δεδομένων ανάλογα

με το τι εκτελεί ο οργανισμός. Η αδυναμία διορισμού ενός Υπεύθυνου Προστασίας Δεδομένων, σύμφωνα με τον ΓΚΠΔ, θα μπορούσε να οδηγήσει σε πρόστιμο.

3.5.1 Βασικές Δραστηριότητες του DPO

Ο Υπεύθυνος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (DPO) είναι υπεύθυνος για την παρακολούθηση της συμμόρφωσης με τον Κανονισμό και όλες τις σχετικές κανονιστικές απαιτήσεις και αποτελεί το σημείο επίσημης επικοινωνίας του οργανισμού με την εποπτική αρχή (ΑΠΔΠΧ), καθώς και με κάθε υποκείμενο που υπόκειται σε επεξεργασία προσωπικών δεδομένων από τον οργανισμό. Επίσης, είναι αρμόδιος για την ενημέρωση και εκπαίδευση της επιχείρησης στις απαιτήσεις του Κανονισμού, για την παροχή συμβουλών, για την εκτίμηση αντικτύπου (DPIA) καθώς και για την τήρηση των αρχείων καταγραφής.

3.5.2 Απαιτούμενα προσόντα ενός DPO

Ο DPO θα πρέπει να έχει κατανοήσει εις βάθος τις απαιτήσεις του GDPR. Επίσης, θα πρέπει να έχει γνώση και κατανόηση των δραστηριοτήτων που ενέχουν επεξεργασία δεδομένων στον οργανισμό που εκπροσωπεί, καθώς και των τεχνολογιών IT και των μεθόδων ασφαλείας πληροφοριών που εφαρμόζονται.

Η σημαντική του θέση στην εταιρεία, προϋποθέτει ακεραιότητα και επαγγελματικό ήθος τα οποία θα προάγουν την αναγκαιότητα της προστασίας προσωπικών δεδομένων εντός του οργανισμού. Ο ρόλος του στην οργανωτική δομή του οργανισμού θα πρέπει να είναι ανεξάρτητος και να μην έγκειται σε σύγκρουση συμφερόντων με άλλους εργασιακούς ρόλους που τυχόν κατέχει.

Μέχρι σήμερα κανένας φορέας στην Ελλάδα δεν έχει διαπιστευθεί για να πιστοποιεί επίσημα τα επαγγελματικά προσόντα και τις δεξιότητες ενός DPO, ενώ επίσης και ο ΓΚΠΔ, που θα τεθεί σε ισχύ τον Μάϊο του 2018, δεν θέτει κάποια υποχρεωτική απαίτηση για πιστοποίηση του DPO, ούτε ενθαρρύνει σχετική πιστοποίηση σε προαιρετική βάση.

3.5.3 Η ευθύνη ενός DPO

Ο DPO είναι αρμόδιος για την εφαρμογή των απαιτήσεων και την ενημέρωση του οργανισμού στο σύνολό του. Η ευθύνη της μη συμμόρφωσης σύμφωνα με τις

απαιτήσεις του Κανονισμού, αφορά το σύνολο του οργανισμού, συνεπώς ο DPO φέρει την ευθύνη να αποδεικνύει τη συμμόρφωση με τις απαιτήσεις του GDPR.

3.6 Ποινές, κυρώσεις και πρόστιμα

Η Ευρωπαϊκή Ένωση έχει ολοκληρώσει μια εκτεταμένη μεταρρύθμιση του νομοθετικού πλαισίου για την προστασία των δεδομένων στην Ευρώπη, βασιζόμενη σε συγκεκριμένους άξονες: κανόνες με συνοχή, απλουστευμένες διαδικασίες, συντονισμένες ενέργειες, τη συμμετοχή των χρηστών, αποτελεσματικότερη ενημέρωση και τις ισχυρότερες εξουσίες για την εφαρμογή των κανόνων.

Η συνεπής εφαρμογή των κανόνων προστασίας των δεδομένων αποτελεί κεντρικό στοιχείο ενός εναρμονισμένου καθεστώτος προστασίας δεδομένων.

Τα διοικητικά πρόστιμα αποτελούν κεντρικό στοιχείο του νέου καθεστώτος επιβολής που έχει θεσπιστεί με τον GDPR, και ένα ισχυρό εργαλείο στα χέρια των εποπτικών αρχών, μαζί με τα άλλα μέτρα που προβλέπονται στο άρθρο 58, για την εφαρμογή των νέων διατάξεων.

Στο πλαίσιο αυτό, η Ομάδα Εργασίας του Άρθρου 29 δημοσίευσε ένα νέο έγγραφο με κατευθυντήριες γραμμές για την εφαρμογή των διατάξεων του GDPR σχετικά με την επιβολή διοικητικών προστίμων.

Συγκεκριμένα, σύμφωνα με το άρθρο 70, παρ. 1, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB) έχει την εξουσία να εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές, προκειμένου να διασφαλίσει τη συνεκτική εφαρμογή του παρόντος κανονισμού.

Επιπρόσθετα, σύμφωνα με το ίδιο άρθρο, το EDPB εκπονεί κατευθυντήριες γραμμές για τις εποπτικές αρχές όσον αφορά την εφαρμογή των μέτρων που αναφέρονται στο άρθρο 58 παράγραφοι 1, 2 και 3 και τον καθορισμό διοικητικών προστίμων δυνάμει του άρθρου 83.

Προκειμένου να επιτευχθεί μια συνεκτική προσέγγιση στην επιβολή των διοικητικών προστίμων, το EDPB συμφώνησε σε μια κοινή κατανόηση των κριτηρίων αξιολόγησης του άρθρου 83 παρ. 2 του Κανονισμού και επομένως το EDPB και οι εθνικές εποπτικές αρχές συμφωνούν να χρησιμοποιήσουν τις κατευθυντήριες γραμμές ως κοινό έδαφος για μία ενιαία προσέγγιση.

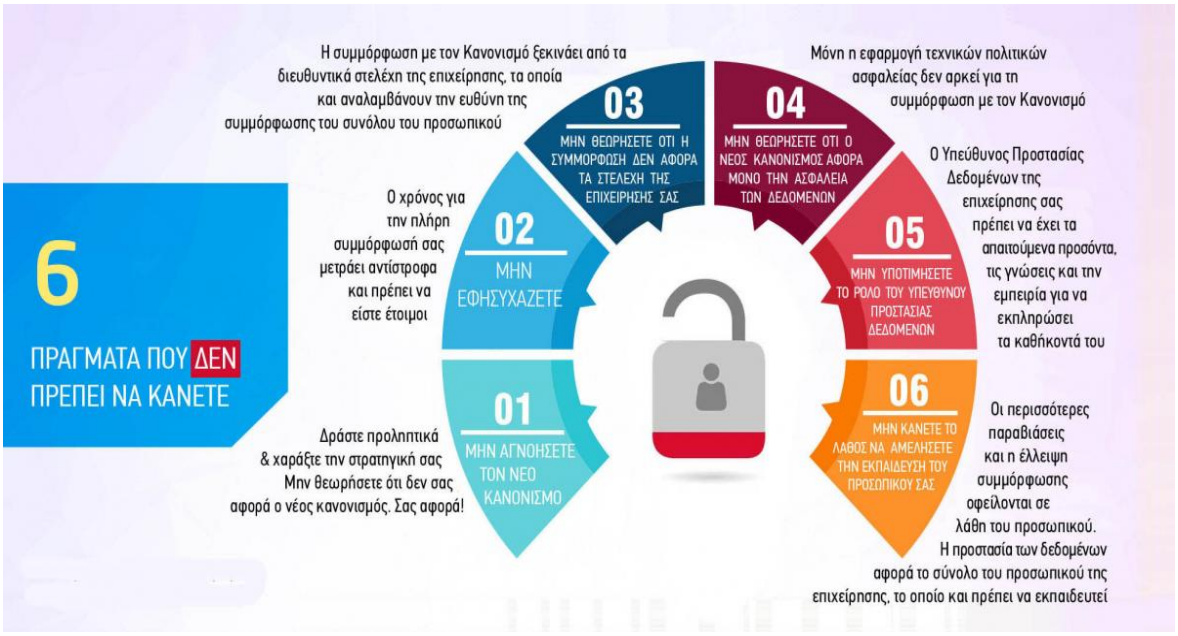
Σύμφωνα με τις διατάξεις του GDPR, η μη συμμόρφωση με τον Κανονισμό μπορεί να οδηγήσει τις εποπτικές αρχές στην επιβολή διοικητικού προστίμου που κυμαίνεται από 20 εκατομμύρια ευρώ έως 4% του παγκόσμιου ετήσιου κύκλου εργασιών της εταιρείας του προηγούμενου οικονομικού έτους, ποσό το οποίο για κάποιους θα μπορούσε να σημαίνει δισεκατομμύρια. Τα πρόστιμα θα εξαρτηθούν από τη σοβαρότητα της παραβίασης και από το εάν η εταιρεία θεωρείται ότι έλαβε σοβαρά υπόψιν της εφαρμοστέα μέτρα και κανόνες σχετικά με την ασφάλεια.

Η έλλειψη συμμόρφωσης μπορεί να συνεπάγεται:

- Ελέγχους και επιβολή κυρώσεων από την Αρχή (συστάσεις, πρόστιμα, απαγορεύσεις, ανακλήσεις αδειών).
- Καταγγελίες από πελάτες – προμηθευτές – συνεργάτες – εργαζομένους σε έτερες δημόσιες αρχές.
- Δικαστικές διαδικασίες (για χρηματική ικανοποίηση λόγω ηθικής βλάβης ή για ποινική ευθύνη).
- Απώλεια πιστοποιήσεων που έχουν οι επιχειρήσεις σε σχέση με πρότυπα λειτουργίας τους

Το ανώτατο πρόστιμο ύψους 20 εκατομμυρίων ευρώ ή το 4% του παγκόσμιου κύκλου εργασιών - όποιο είναι μεγαλύτερο - αφορά παραβιάσεις των δικαιωμάτων των προσώπων στα οποία αναφέρονται τα δεδομένα, μη εξουσιοδοτημένη διεθνή μεταφορά προσωπικών δεδομένων και μη εφαρμογή διαδικασιών ή παραβίαση της πρόσβασης στα αιτήματα για τα δεδομένα τους.

Ένα μικρότερο πρόστιμο ύψους 10 εκατομμυρίων ευρώ ή 2% του παγκόσμιου κύκλου εργασιών θα εφαρμοστεί σε εταιρείες που κακοδιαχειρίζονται δεδομένα με άλλους τρόπους. Περιλαμβάνουν, μεταξύ άλλων, την αδυναμία δήλωσης παραβίασης των δεδομένων, την αδυναμία οικοδόμησης της προστασίας της ιδιωτικής ζωής από το σχεδιασμό, την εξασφάλιση της προστασίας των δεδομένων κατά το πρώτο στάδιο ενός έργου και την αδυναμία συμμόρφωσης ως προς τον διορισμό ενός Υπευθύνου Προστασίας Δεδομένων



Εικόνα 1: *Ενέργειες προς αποφυγή για την μη επιβολή προστίμων*

Για την επιβολή διοικητικού προστίμου, καθώς και σχετικά με το ύψος του διοικητικού προστίμου για κάθε μεμονωμένη περίπτωση, λαμβάνονται υπόψη, μεταξύ άλλων τα ακόλουθα:

1. Η φύση, η βαρύτητα και η διάρκεια της παράβασης, καθώς και ο αριθμός των υποκειμένων που έθιξε η παράβαση και ο βαθμός ζημίας που υπέστησαν.
2. Ο δόλος ή η αμέλεια που προκάλεσε την παράβαση.
3. Οποιεσδήποτε ενέργειες στις οποίες προέβη ο υπεύθυνος επεξεργασίας για να μετριάσει τη ζημία που υπέστησαν τα υποκείμενα των δεδομένων.
4. Ο βαθμός ευθύνης του υπεύθυνου επεξεργασίας, λαμβάνοντας υπόψη τα μέτρα που εφάρμοσε.
5. Ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των επιπτώσεών της.
6. Οι κατηγορίες προσωπικών δεδομένων που επηρέασε η παράβαση.
7. Η τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης.

Ο Κανονισμός αναγνωρίζει το δικαίωμα των υποκειμένων των δεδομένων να υποβάλουν καταγγελία στην εποπτική αρχή καθώς και το δικαίωμά τους για λήψη δικαστικών μέτρων και απαίτηση αποζημιώσεων. Συνεπώς παραβιάσεις όπως πρόσβαση στον εξυπηρετητή από hackers, κλοπή εγγράφων, καταστροφή

πρωτοτύπων, απλή διαρροή δεδομένων μισθοδοσίας ή ονομάτων, όπως για παράδειγμα η πρόσφατη καταγγελία για διαρροή τηλεπικοινωνιακών στοιχείων πελατών από υπάλληλο οργανισμού του ευρύτερου δημόσιου τομέα, αλλά και συλλογή αρχείου τρίτων προσώπων άνευ συναίνεσης άλλης βάσης επεξεργασίας, δύνανται να προκαλέσουν αξιώσεις σοβαρών αποζημιώσεων.

Ασφαλώς, επιχειρήσεις οι οποίες ευθύνονται για μικρές παραβιάσεις του Κανονισμού δεν πρέπει να ανησυχούν για την επιβολή των αυστηρότερων κυρώσεων αλλά ούτε και να τρομοκρατηθούν εξαιτίας των εξαντλητικών κυρώσεων και να θεωρήσουν ότι η εφαρμογή του Κανονισμού αποτελεί την μεγαλύτερη απειλή για τις επιχειρήσεις. Από την άλλη μεριά όμως, αποτελεί παραδεκτό γεγονός ότι ο ΓΚΠΔ παρέχει την εξουσία στις αρχές να επιβάλλουν υψηλά έως και εξοντωτικά πρόστιμα αλλά και μια σειρά άλλων εργαλείων για τον έλεγχο συμμόρφωσης και εφαρμογής του Κανονισμού.

3.7 Η προστασία των παιδιών βάσει του νέου Κανονισμού

Σύμφωνα με το άρθρο 8 παρ. 1 του νέου Κανονισμού, η διάθεση ψηφιακών υπηρεσιών σε παιδιά κάτω των 18 ετών θα επιτρέπεται μόνο αν το παιδί είναι τουλάχιστον 16 ετών, ενώ για παιδιά ηλικίας από 13-16 ετών θα απαιτείται η συναίνεση του γονέα ή κηδεμόνα. Ο νέος κοινός ευρωπαϊκός νόμος δίνει το περιθώριο σε κάθε χώρα-μέλος να νομοθετήσει για ελεύθερη πρόσβαση στο διαδίκτυο παιδιών μικρότερης ηλικίας με κατώτατο επιτρεπόμενο όριο τα 13 έτη. Ήδη κάποιες από τις χώρες-μέλη έχουν πάρει τις οριστικές αποφάσεις για το θέμα και πολύ σύντομα θα διευκρινιστεί και το τοπίο στην Ελλάδα, αφού ληφθούν υπόψη οι εισηγήσεις όλων των εμπλεκόμενων φορέων και αρχών.

Επιπλέον, ο νέος Κανονισμός ορίζει την ευθύνη του Υπευθύνου Επεξεργασίας, ο οποίος οφείλει να καταβάλλει κάθε δυνατή προσπάθεια, προκειμένου να εξακριβώσει την ηλικία του υποκειμένου των δεδομένων, ειδικά όταν πρόκειται για παιδί.

Ωστόσο, ένα θέμα που έχει απασχολήσει ιδιαίτερα τις αρχές της Ελλάδας, είναι η συμμετοχή των παιδιών στις νέες τεχνολογίες και το κατά πόσο είναι εφικτό, επιθυμητό και πρέπον να αφαιρεθεί στα παιδιά το δικαίωμα να συμμετέχουν ελεύθερα στις νέες τεχνολογίες και στις ευκαιρίες που προσφέρει ο ψηφιακός κόσμος.

Στο συνέδριο της 2ης συνάντησης του συμβουλευτικού οργάνου του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου του ΙΤΕ, που πραγματοποιήθηκε στις 18 Οκτωβρίου 2017 με τη συμμετοχή εκπροσώπων της πολιτείας, της βιομηχανίας του ίντερνετ, της ακαδημαϊκής κοινότητας και οργανώσεων προστασίας του παιδιού, ο εκπρόσωπος της Αρχής Προστασίας Προσωπικών Δεδομένων επεσήμανε την αναγκαιότητα συνολικής ενισχυμένης προστασίας προσωπικών δεδομένων, ανεξαρτήτου ηλικίας του χρήστη του διαδικτύου, καθώς δεν είναι λίγοι οι ενήλικοι διαδικτυακώς «αναλφάβητοι» που με πλήρη άγνοια κινδύνου εισέρχονται στο διαδίκτυο. Υπογράμμισε επίσης, την ευθύνη των παρόχων να αναζητήσουν και να εφαρμόσουν αποτελεσματικούς τρόπους ελέγχου της ηλικίας των παιδιών που κάνουν χρήση των κοινωνικών δικτύων έτσι ώστε να διασφαλίζεται το επιτρεπόμενο ηλικιακό όριο, που προς το παρόν τουλάχιστον, είναι τα 13 έτη. Ιδιαίτερη έμφαση τέλος, δόθηκε και στην αλλαγή της μορφής των όρων χρήσης της κάθε εφαρμογής που στην παρούσα φάση χαρακτηρίζονται ατέρμονοι και δυσνόητοι με συνέπεια ο χρήστης να μην κατανοεί σε τι συναινεί. Συνεπώς, είναι επιτακτική ανάγκη η ενημέρωση των παιδιών αλλά και των κηδεμόνων τους, να γίνεται σε γλώσσα απλή και σαφή.

3.8 Σύνοψη

Στο παρόν κεφάλαιο παρουσιάστηκε αναλυτικά ο νέος Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR), όπως θεσπίστηκε από τα κεντρικά όργανα της Ευρωπαϊκής Ένωσης. Μέσω της αναφοράς στο περιεχόμενο και στους ορισμούς του Κανονισμού, περιγράφηκαν οι αλλαγές που θα επιφέρει τόσο στους πολίτες, όσο και στις επιχειρήσεις, ιδιωτικού και δημοσίου τομέα, οι οποίες καλούνται να εναρμονιστούν με αυτές έως τις 25 Μαΐου 2018.

Επίσης, έγινε εκτενής αναφορά στα νέα δεδομένα που εισάγει ο Κανονισμός, όπως η υποχρέωση γνωστοποίησης της παραβίασης δεδομένων στην εποπτική αρχή, η μελέτη εκτίμησης αντικτύπου της παραβίασης αυτής αλλά και ο νέος ρόλος που εισάγεται με τον Κανονισμό, αυτός του Υπευθύνου Προστασίας Δεδομένων.

Ξεχωριστή αναφορά έγινε στις αλλαγές που επιφέρει ο Κανονισμός για την προστασία των παιδιών καθώς και στα πρόστιμα με τα οποία έρχονται αντιμέτωπες οι επιχειρήσεις σε περίπτωση μη συμμόρφωσής τους με τα νέα δεδομένα.

Όλα τα παραπάνω στοιχεία, αποτελούν βασικές και απαραίτητες γνώσεις για την εξοικείωση με το νέο ρυθμιστικό πλαίσιο που εισάγει ο GDPR, καθώς και για την καλύτερη κατανόηση της μεθοδολογίας και του τρόπου συμμόρφωσης με αυτόν, όπως παρουσιάζονται στο επόμενο κεφάλαιο.

4. ΜΕΘΟΔΟΛΟΓΙΑ ΚΑΙ ΠΛΑΝΟ ΕΚΠΑΙΔΕΥΣΗΣ ΓΙΑ ΣΥΜΜΟΡΦΩΣΗ ΜΕ ΤΟΝ GDPR

4.1 Εισαγωγή

Δεν υπάρχει μια ενιαία προσέγγιση που να ταιριάζει σε όλους για την προετοιμασία του GDPR. Αντίθετα, κάθε επιχείρηση θα πρέπει να λάβει μέτρα, αφού εξετάσει τι ακριβώς χρειάζεται να επιτευχθεί για να συμμορφωθεί με το νέο Κανονισμό, καθώς και ποιος είναι ο υπεύθυνος επεξεργασίας δεδομένων ο οποίος έχει αναλάβει την ευθύνη για να εξασφαλίσει ότι θα συμβεί αυτό.

Τα μέτρα αυτά πρέπει να ελαχιστοποιήσουν τον κίνδυνο παραβίασης και να προασπίσουν την προστασία των προσωπικών δεδομένων. Πρακτικά αυτό σημαίνει περισσότερες πολιτικές και διαδικασίες για τους οργανισμούς, αν και πολλές οργανώσεις θα έχουν ήδη θεσπίσει μέτρα σωστής διακυβέρνησης. Αυτό θα μπορούσε να είναι ευθύνη ενός ατόμου σε μια μικρή επιχείρηση ή ακόμα και ενός ολόκληρου τμήματος σε μια πολυεθνική εταιρεία. Είτε έτσι είτε αλλιώς, ο προϋπολογισμός, τα συστήματα και το προσωπικό θα πρέπει να ληφθούν υπόψη για να λειτουργήσουν.

Σύμφωνα με τις διατάξεις του ΓΚΠΔ που προωθούν τη λογοδοσία και τη διακυβέρνηση, οι επιχειρήσεις πρέπει να εφαρμόσουν κατάλληλα τεχνικά και οργανωτικά μέτρα. Αυτά θα μπορούσαν να περιλαμβάνουν διατάξεις για την προστασία των δεδομένων, όπως κατάρτιση του προσωπικού, εσωτερικοί έλεγχοι των δραστηριοτήτων επεξεργασίας και ανασκόπηση των πολιτικών ανθρώπινου δυναμικού, καθώς και τήρηση τεκμηρίωσης σχετικά με τις δραστηριότητες επεξεργασίας. Άλλες τακτικές που μπορούν να εξετάσουν οι οργανισμοί περιλαμβάνουν την ελαχιστοποίηση των δεδομένων και την ψευδωνυμοποίηση ή την άδεια στα άτομα να παρακολουθούν την διαδικασία.

Με αυτό το κεφάλαιο, θα επιδιωχθεί μια πρώτη προσέγγιση της διαδικασίας συμμόρφωσης των επιχειρήσεων με τον GDPR, καθώς και των πρακτικών που μπορούν να ακολουθήσουν για να προετοιμαστούν κατάλληλα για την υποδοχή των νέων δεδομένων.

4.2 Βήματα προετοιμασίας των επιχειρήσεων για τον GDPR

Το νέο περιβάλλον στο οποίο καλούνται να δραστηριοποιηθούν οι επιχειρήσεις απαιτεί την κατάλληλη προετοιμασία και συμμόρφωσή τους με το νέο Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων (GDPR). Σε αυτό το πλαίσιο, οι επιχειρήσεις οφείλουν να επιλέγουν προϊόντα και υπηρεσίες προστασίας για τις πληροφορίες που διαχειρίζονται, τα οποία θα τις βοηθήσουν να αντιμετωπίσουν αποτελεσματικότερα τυχόν μελλοντικά περιστατικά, δημιουργώντας έτσι τις κατάλληλες συνθήκες που θα εξασφαλίσουν την ασφάλεια των εταιριών και την ανάπτυξη της αγοράς της «κυβερνοασφάλειας».

Αρχικά, οι επιχειρήσεις, λαμβάνοντας υπόψιν τα δικαιώματα των υποκειμένων των δεδομένων για την προστασία των προσωπικών τους δεδομένων, οφείλουν να μεριμνήσουν για την αποτελεσματικότερη ανταπόκρισή τους σε αυτά. Πιο συγκεκριμένα, κάθε επιχείρηση και οργανισμός, θα πρέπει να γνωρίζει :

- Το δικαίωμα στη «λήθη» και τις ενέργειες που πρέπει να ακολουθήσει όταν ένα άτομο ζητά τη διαγραφή των δεδομένων του από το αρχείο της
- Το δικαίωμα περιορισμού της επεξεργασίας και τις περιπτώσεις στις οποίες οφείλει να αναπροσαρμόζει την επεξεργασία των προσωπικών δεδομένων των υποκειμένων.
- Το δικαίωμα στη φορητότητα των δεδομένων και τη μορφή στην οποία θα πρέπει να δίνει αντίγραφα όταν το υποκείμενο ζητά πρόσβαση στα δεδομένα του.
- Τους περιορισμούς στην κατάρτιση προφίλ και τις καταστάσεις στις οποίες θα επιτρέπεται η δημιουργία «προφίλ» για το υποκείμενο των δεδομένων.
- Τις περιστάσεις στις οποίες η επιχείρηση οφείλει να ενημερώνει το υποκείμενο των δεδομένων ότι πραγματοποιήθηκε παραβίαση των δεδομένων του.

Εικόνα 2: *Αρχικά βήματα προετοιμασίας για συμμόρφωση με τον GDPR*

Για να μπορέσουν συνεπώς οι επιχειρήσεις να ανταπεξέλθουν στα νέα αυτά δεδομένα που εισάγει ο νέος Κανονισμός, θα πρέπει αρχικά να ακολουθήσουν κάποια βήματα προετοιμασίας, όπως:

1) Να ενημερωθούν μελετώντας τον Κανονισμό και εντοπίζοντας πτυχές που μπορεί να επηρεάζουν τη διάρθρωση, το αντικείμενο ή τις δραστηριότητες της επιχείρησης. Στη συνέχεια, να συζητήσουν τον Κανονισμό με συναδέλφους που ασχολούνται με θέματα προσωπικού ή τεχνικά θέματα μηχανογράφησης ή διαχείρισης βάσεων δεδομένων και αν προκύψουν απορίες, να συμβουλευτούν τους νομικούς συμβούλους της εταιρίας.

2) Να καταγράψουν τις δραστηριότητες του οργανισμού που εμπίπτουν στον Κανονισμό, διότι έτσι διευκολύνεται τόσο η εσωτερική λειτουργία του οργανισμού όσο και η εφαρμογή των Αρχών της Διαφάνειας και της Λογοδοσίας. Οι υπεύθυνοι επεξεργασίας θα έχουν υποχρέωση να

συμμορφώνονται με τον Κανονισμό αλλά και υποχρέωση να επιδεικνύουν τη συμμόρφωσή τους.

3) Να ελέγξουν αν η πληροφόρηση που παρέχεται σε πολίτες, πελάτες ή εταίρους της επιχείρησης, μέσω εντύπων ή μέσω της ιστοσελίδας της, χρειάζεται να διαφοροποιηθεί και να προσαρμοστεί ανάλογα. Επιπλέον, αν η επιχείρηση έχει Πολιτική Προστασίας της Ιδιωτικής Ζωής (Privacy Policy), πρέπει να ελέγξει ποιες πτυχές της χρήζουν εκσυγχρονισμού σε συμμόρφωση με τον Κανονισμό.

4) Να εκπαιδεύσουν κατάλληλα το ανθρώπινο δυναμικό τους, είτε μέσω μελετών περιπτώσεων (case studies), είτε μέσω παρακολούθησης σεμιναρίων επιμόρφωσης των αρμόδιων στελεχών για τους τρόπους συμμόρφωσης με τον Κανονισμό.

5) Να ελέγξουν πώς τα νέα δικαιώματα που δημιουργεί ο ΓΚΠΔ επηρεάζουν τις δραστηριότητες του οργανισμού και να συζητήσουν με το προσωπικό τους, τους τρόπους με τους οποίους οι πολίτες θα μπορούν να ασκούν τα δικαιώματά τους. Με την εφαρμογή του Κανονισμού, ίσως χρειαστεί να υιοθετηθεί και να γνωστοποιηθεί στο κοινό μια τυποποιημένη διαδικασία για την άσκηση των δικαιωμάτων.

6) Να εξασφαλίσουν ότι κάθε δραστηριότητα της επιχείρησης υπακούει στις προϋποθέσεις για νόμιμη επεξεργασία που καθορίζει ο Κανονισμός και να είναι σε θέση να δικαιολογήσουν, εφόσον χρειαστεί, τη νομική βάση στην οποία βασίζεται η κάθε δραστηριότητα της.

7) Να εξασφαλίσουν ότι διαθέτουν κατάλληλα και εκσυγχρονισμένα τεχνικά και διαδικαστικά μέτρα ασφαλείας και ότι εφαρμόζουν τις αναγκαίες πολιτικές για την προστασία των πληροφοριών που χειρίζονται και τα οποία ανταποκρίνονται στις απαιτήσεις του Κανονισμού.

8) Να προσέξουν ιδιαίτερα τις σχετικές πρόνοιες του Κανονισμού για την επεξεργασία «ευαίσθητων» δεδομένων, σε περίπτωση που οι δραστηριότητες του οργανισμού βασίζονται στη συγκατάθεση και να μεριμνήσουν για την

ενσωμάτωση δικλείδων ασφαλείας (data protection by design and by default). Για υπηρεσίες της κοινωνίας των πληροφοριών απευθείας σε παιδιά, θα πρέπει να λαμβάνεται η συγκατάθεση του προσώπου που έχει τη γονική μέριμνα του παιδιού.

9) Να κατανοήσουν τους κινδύνους που δημιουργούνται και να κάνουν αναλύσεις των επιπτώσεων που μπορούν να προκύψουν λόγω παραβίασης της ιδιωτικότητας (Data Privacy Impact Assessment-DPIA).

10) Να σχεδιάζουν προϊόντα και υπηρεσίες λαμβάνοντας υπόψη την προστασία της ιδιωτικότητας.

11) Να ενημερώνουν τις αρμόδιες αρχές ή και τα επηρεαζόμενα πρόσωπα εντός 72 ωρών από τον εντοπισμό συμβάντος παραβίασης συστημάτων ή υποκλοπής βάσεων δεδομένων.

12) Να ορίσουν Υπεύθυνο Προστασίας Δεδομένων (Data Protection Officer-DPO), ο οποίος μπορεί να είναι υπάλληλος του οργανισμού ή εξωτερικός συνεργάτης.

13) Να ορίσουν το κράτος-μέλος της κύριας εγκατάστασης, στο πλαίσιο του μηχανισμού συνεργασίας και συνεκτικότητας, εφ' όσον προβαίνουν σε διασυνοριακή επεξεργασία δεδομένων εντός της ΕΕ. Η εποπτεύουσα Αρχή του κράτους αυτού, θα είναι αρμόδια ως επικεφαλής Αρχή για την εποπτεία της νομιμότητας και της επεξεργασίας εντός της Ένωσης.

14) Να χρησιμοποιούν δεσμευτικούς εταιρικούς κανόνες (BCRs) ή και τυποποιημένες συμβατικές ρήτρες (SCCs) όταν συνάπτουν συμφωνίες με τους συνεργάτες τους, σε περίπτωση που απαιτηθεί, λόγω διαβίβασης δεδομένων σε τρίτες χώρες.

15) Να έχουν πλάνο αντιμετώπισης περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων (Incident Response Plan).

16) Να είναι έτοιμες να αποζημιώσουν τους πελάτες των οποίων τα δεδομένα δεν κατάφεραν να προστατεύσουν.

4.3 Μεθοδολογία συμμόρφωσης με τον GPDR

Ενόψει της εφαρμογής του νέου Ευρωπαϊκού Γενικού Κανονισμού για την Προστασία των Δεδομένων, η κάθε επιχείρηση καλείται, αφού ακολουθήσει τα βήματα προετοιμασίας που αναλύθηκαν προηγουμένως, να εφαρμόσει την κατάλληλη στρατηγική και μεθοδολογία προκειμένου να συμμορφωθεί με το νέο Κανονισμό.

Κατά καιρούς, οι αρμόδιες εποπτικές Αρχές Προστασίας Δεδομένων της ΕΕ, έχουν δημοσιεύσει μεθοδολογίες και εργαλεία για τις επιχειρήσεις, προκειμένου να διευκολύνουν την ομαλή μετάβασή τους στο νέο Κανονισμό, που θα τεθεί σε ισχύ στις 25 Μαΐου 2018.

Εικόνα 3: *Συνοπτικά βήματα μεθοδολογίας συμμόρφωσης με τον GDPR*

Οι μεθοδολογίες αυτές συνοψίζονται στα παρακάτω βήματα:

Βήμα 1: Διορισμός ενός Υπευθύνου Προστασίας Δεδομένων ("DPO")

Συνίσταται, οι επιχειρήσεις και οι οργανισμοί να διορίσουν έναν «ηγέτη» στην πιλοτική διακυβέρνηση της προστασίας των δεδομένων εντός της δομής τους. Αυτό το άτομο

θα εκτελεί εσωτερικά ενημερωτικές, συμβουλευτικές και ελεγκτικές εργασίες. Εν αναμονή της εφαρμογής του GDPR το 2018, οι οργανισμοί μπορούν να διορίσουν νωρίτερα έναν Υπεύθυνο Προστασίας Δεδομένων (DPO), που θα τους επιτρέψει να οργανωθούν καλύτερα και να είναι ένα βήμα μπροστά στο να συμμορφωθούν με τον επερχόμενο Κανονισμό. Ο ορισμός Υπευθύνου Προστασίας δεν είναι πάντοτε υποχρεωτικός. Εξαρτάται από το μέγεθος της εταιρείας, τον τύπο και τον αριθμό των δεδομένων που συλλέγονται, αν η επεξεργασία είναι η κύρια επιχειρηματική δραστηριότητα και αν πραγματοποιείται επεξεργασία δεδομένων σε μεγάλη κλίμακα. Ωστόσο, ο διορισμός ενός DPO ενδείκνυται για τη διασφάλιση της συμμόρφωσης με τον GDPR. Μόλις οι επιχειρήσεις ορίσουν έναν «πιλοτικό» υπεύθυνο για την εφαρμογή των μέτρων συμμόρφωσης με τον Κανονισμό και του παρέχουν ανθρώπινα και οικονομικά μέσα για να εκτελέσει τα καθήκοντά του, ολοκληρώνεται το πρώτο βήμα.

Βήμα 2: Αναγνώριση, κατάταξη και χαρτογράφηση δεδομένων

Για το δεύτερο βήμα, οι οργανισμοί θα πρέπει να αναγνωρίσουν αν τηρούν σε οποιαδήποτε μορφή (φυσική ή ηλεκτρονική) αρχείο με δεδομένα προσωπικού χαρακτήρα και να προσδιορίσουν λεπτομερώς τις δραστηριότητές τους που υπόκεινται σε επεξεργασία δεδομένων. Εκτός από την αναγνώριση της ύπαρξης τέτοιων δεδομένων, ο οργανισμός θα πρέπει να συλλέξει και πληροφορίες σχετικά με την φύση των δεδομένων, την κατηγορία στην οποία ανήκουν, τον σκοπό που εξυπηρετεί η συλλογή τους, τον χρόνο και τα μέσα αποθήκευσής τους. Αυτό, μπορούν να το πράξουν με την κατάρτιση και τη διατήρηση ενός μητρώου δραστηριοτήτων επεξεργασίας δεδομένων (κυρίως οι επιχειρήσεις άνω των 250 ατόμων). Επισημαίνεται, ότι στο πλαίσιο του GDPR, οι οργανισμοί θα πρέπει να διατηρούν πλήρη εσωτερική τεκμηρίωση των δραστηριοτήτων επεξεργασίας δεδομένων τους, κατά προτίμηση διατηρώντας ένα πρότυπο μητρώο δεδομένων.

Οι οργανισμοί μπορούν να προχωρήσουν στο τρίτο βήμα αν:

- Έχουν έρθει σε επαφή με όλες τις κατάλληλες υπηρεσίες και οντότητες που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα στην οργανωτική δομή τους.

- Έχουν καταρτίσει κατάλογο των δραστηριοτήτων επεξεργασίας δεδομένων τους κατά κύριο σκοπό και τους τύπους επεξεργασμένων δεδομένων προσωπικού χαρακτήρα.
- Έχουν εντοπίσει τους υπευθύνους συλλογής και επεξεργασίας δεδομένων που συμμετέχουν σε κάθε δραστηριότητα επεξεργασίας δεδομένων.
- Γνωρίζουν πού μεταφέρονται τα δεδομένα και σε ποιον, πού φιλοξενούνται και για πόσο καιρό διατηρούνται.

Βήμα 3: Κατάταξη και προτεραιότητα στις ενέργειες συμμόρφωσης

Μετά τη σύνταξη του μητρώου στο δεύτερο βήμα, πρέπει να προσδιοριστούν για κάθε δραστηριότητα επεξεργασίας δεδομένων, οι ενέργειες που θα πρέπει να εφαρμοστούν για να συμμορφωθούν οι επιχειρήσεις με τις τρέχουσες και τις μελλοντικές υποχρεώσεις προστασίας δεδομένων. Αυτή η ιεράρχηση πρέπει να πραγματοποιηθεί λαμβάνοντας υπόψιν τους κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

Οι ενέργειες που θα εφαρμοστούν θα πρέπει να περιλαμβάνουν τουλάχιστον:

- Τη διασφάλιση ότι συλλέγονται και υποβάλλονται σε περαιτέρω επεξεργασία μόνο δεδομένα προσωπικού χαρακτήρα που είναι απολύτως απαραίτητα.
- Τον προσδιορισμό της νομικής βάσης για την επεξεργασία δεδομένων.
- Την επανεξέταση των τωρινών ειδοποιήσεων απορρήτου για να συμμορφωθεί ο οργανισμός με τις απαιτήσεις ειδοποίησης που ορίζει ο Κανονισμός.
- Την επιβεβαίωση ότι όλοι οι πάροχοι και επεξεργαστές δεδομένων γνωρίζουν τις νέες υποχρεώσεις και ευθύνες τους στο πλαίσιο του GDPR και ότι στις συμφωνίες παροχής υπηρεσιών εισάγονται κατάλληλες ρήτρες προστασίας της ιδιωτικής ζωής.
- Τον καθορισμό διαδικασίας για τη διεκπεραίωση των αιτημάτων των υποκειμένων των δεδομένων για την άσκηση των δικαιωμάτων προστασίας των δεδομένων τους.
- Την επαλήθευση των μέτρων ασφαλείας προσωπικών δεδομένων που εφαρμόζονται.

Το τρίτο βήμα θα ολοκληρωθεί μόλις οι οργανισμοί εφαρμόσουν μέτρα για την προστασία των υποκειμένων των δεδομένων που σχετίζονται με τις δραστηριότητες επεξεργασίας δεδομένων τους και έχουν εντοπίσει εκείνες τις δραστηριότητες

επεξεργασίας δεδομένων που συνεπάγονται κίνδυνο για την προστασία της ιδιωτικής ζωής.

Βήμα 4: Διαχείριση κινδύνων

Εάν, κατά το προηγούμενο στάδιο, οι οργανώσεις έχουν εντοπίσει δραστηριότητες επεξεργασίας δεδομένων που ενδέχεται να ενέχουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα, θα πρέπει να διενεργήσουν εκτίμηση επιπτώσεων στην ιδιωτική ζωή (DPIA) για καθεμία από αυτές τις δραστηριότητες επεξεργασίας δεδομένων.

Το τέταρτο βήμα θα ολοκληρωθεί μόλις οι οργανισμοί εφαρμόσουν μέτρα για την αντιμετώπιση των κυριότερων κινδύνων και απειλών για την ιδιωτική ζωή των προσώπων στα οποία αναφέρονται τα δεδομένα.

Βήμα 5: Οργάνωση των εσωτερικών διαδικασιών

Στο πλαίσιο του πέμπτου σταδίου της προτεινόμενης μεθοδολογίας, οι επιχειρήσεις πρέπει να επανασχεδιάσουν και να εφαρμόσουν εσωτερικές διαδικασίες για να εγγυώνται την προστασία των δεδομένων ανά πάσα στιγμή, λαμβάνοντας υπόψη όλα τα συμβάντα που μπορεί να προκύψουν κατά τη διάρκεια μιας δραστηριότητας επεξεργασίας δεδομένων (όπως παραβίαση της ασφάλειας των δεδομένων, διαχείριση των αιτημάτων των υποκειμένων των δεδομένων, φύση των δεδομένων που συλλέγονται, αλλαγή του προσωπικού κ.λπ.).

Ειδικότερα, αυτό συνεπάγεται τις ακόλουθες ενέργειες:

- Λήψη αποφάσεων και ανάπτυξη στρατηγικών διαχείρισης των πιθανών απειλών σε συνεργασία με τους αρμόδιους υπευθύνους και τις αρμόδιες Αρχές Προστασίας Δεδομένων κατά το σχεδιασμό μιας εφαρμογής ή μιας δραστηριότητας επεξεργασίας δεδομένων.
- Εφαρμογή τεχνικών μέτρων που να διασφαλίζουν την ακεραιότητα των δεδομένων, όπως ψευδωνυμοποίηση και κρυπτογράφηση ή μεθόδων περισσότερο φιλικών για το χρήστη, όπως η προστασία κατά το σχεδιασμό εξ' ορισμού.
- Αύξηση της ευαισθητοποίησης των εργαζομένων και διασφάλιση της κλιμάκωσης των πληροφοριών στους αρμόδιους υπαλλήλους ή διευθυντές, ιδίως με την ανάπτυξη σχεδίου κατάρτισης και επικοινωνιών.

- Διαρκής εκπαίδευση του προσωπικού στο χειρισμό των καταγγελιών των υποκειμένων των δεδομένων και των αιτημάτων για την άσκηση των δικαιωμάτων προστασίας των δεδομένων.
- Πρόβλεψη των παραβιάσεων ασφαλείας των δεδομένων, διασφαλίζοντας ότι σε ορισμένες περιπτώσεις η παραβίαση θα πρέπει να κοινοποιείται στην Αρχή Προστασίας Δεδομένων εντός 72 ωρών και χωρίς αδικαιολόγητη καθυστέρηση στα θιγόμενα πρόσωπα που επηρεάζονται.

Οι οργανισμοί μπορούν να προχωρήσουν στο τελικό βήμα μόλις εφαρμοστούν οι βέλτιστες πρακτικές για την προστασία των δεδομένων από τις υπηρεσίες που είναι υπεύθυνες για την υλοποίηση δραστηριοτήτων επεξεργασίας δεδομένων και όταν το προσωπικό γνωρίζει τι πρέπει να κάνει και με ποιον θα επικοινωνήσει σε περίπτωση συμβάντος παραβίασης προσωπικών δεδομένων.

Βήμα 6: Διατήρηση της τεκμηρίωσης σχετικά με τα μέτρα συμμόρφωσης

Είναι ευθύνη του οργανισμού που επεξεργάζεται τα δεδομένα να αποδεικνύει την συμμόρφωση του ως προς τις απαιτήσεις του Κανονισμού. Συνεπώς στο τελικό βήμα, οι οργανισμοί πρέπει να συγκεντρώσουν όλα τα απαραίτητα έγγραφα για την επαλήθευση αυτή. Οι ενέργειες και τα έγγραφα που εκπονούνται σε κάθε στάδιο πρέπει να επανεξετάζονται και να ενημερώνονται τακτικά, ώστε να διασφαλίζεται η συνεχής προστασία των δεδομένων.

Ειδικότερα, η τεκμηρίωση αυτή θα πρέπει να περιλαμβάνει:

- Το μητρώο δραστηριοτήτων επεξεργασίας δεδομένων (για τους υπευθύνους επεξεργασίας δεδομένων) ή τις κατηγορίες δραστηριοτήτων επεξεργασίας δεδομένων (για τους εκτελούντες την επεξεργασία των δεδομένων).
- Την εκτίμηση των επιπτώσεων (DPIA) για επεξεργασία δεδομένων υψηλού κινδύνου.
- Τους μηχανισμούς μεταφοράς δεδομένων (π.χ. πρότυπα Ευρωπαϊκής Ένωσης, δεσμευτικοί εταιρικοί κανόνες και πιστοποιήσεις, κ.λπ.).
- Τις ειδοποιήσεις απορρήτου.
- Τα έντυπα συναίνεσης, καθώς και αποδεικτικά στοιχεία ότι τα υποκείμενα των δεδομένων έχουν δώσει τη συγκατάθεσή τους όταν η συναίνεση αποτελεί τη νομική βάση για την επεξεργασία δεδομένων.

- Τις διαδικασίες που εφαρμόζονται για την άσκηση των δικαιωμάτων προστασίας δεδομένων των υποκειμένων των δεδομένων.
- Τις συμβάσεις με τους αρμόδιους παρόχους, επεξεργαστές και υπευθύνους δεδομένων.
- Τις εσωτερικές διαδικασίες που εφαρμόζονται σε περίπτωση παραβίασης των δεδομένων.

Το έκτο βήμα θα ολοκληρωθεί όταν ο έλεγχος και η επαλήθευση καταδείξει τη συμμόρφωση με όλες τις υποχρεώσεις που ορίζει ο ΓΚΠΔ.

Για την υλοποίηση της παραπάνω προτεινόμενης μεθοδολογίας, απαιτείται η άμεση διενέργεια ενός αρχικού ελέγχου (soft audit) επί της υφιστάμενης οργανωτικής δομής της επιχείρησης ή του οργανισμού, των προηγούμενων γνωστοποιήσεων στην Αρχή Προστασίας Δεδομένων, καθώς και των ροών διαβίβασης δεδομένων τόσο σε ενδοεταιρικό ή ενδοομιλικό επίπεδο όσο και μεταξύ εταιρειών σε διαφορετικές χώρες εντός ΕΕ και προς τρίτες χώρες.

4.4 Η συμβολή του DPO στην υλοποίηση της συμμόρφωσης

Σύμφωνα με το κείμενο του GDPR, ο διορισμός ενός, είτε εσωτερικού είτε εξωτερικού, DPO στο εσωτερικό μίας επιχείρησης είναι υποχρεωτικός για συγκεκριμένες κατηγορίες υπευθύνων και εκτελούντων την επεξεργασία. Η παρουσία και η δράση του κρίνεται απαραίτητη σε όλες τις επιχειρήσεις, ακόμη και στις μικρομεσαίες, οι οποίες μπορούν κατά διακριτική ευχέρεια να διορίσουν DPO ο οποίος θα έχει κομβικό ρόλο ως προς την συμμόρφωση του υπευθύνου και εκτελούντος την επεξεργασία προς το ισχύον κανονιστικό πλαίσιο.

4.4.1 Ο κρίσιμος ρόλος του DPO

Ο ρόλος του στο εσωτερικό μίας επιχείρησης, ανεξαρτήτως του μεγέθους αυτής, μπορεί να συμβάλλει αποφασιστικά στην ενδυνάμωση της συμμόρφωσής της, η ύπαρξη της οποίας αποτελεί σήμερα σημαντικό ανταγωνιστικό πλεονέκτημα στην αγορά έναντι άλλων επιχειρήσεων

1. Ο DPO πρέπει να συμμετέχει ενεργά σε όλα τα ζητήματα που αφορούν την προστασία δεδομένων προσωπικού χαρακτήρα, ενώ η επιχείρηση θα πρέπει να διασφαλίζει αντιστοίχως την πρόσβαση του σε κάθε απαραίτητη για τον σκοπό αυτό πληροφορία σχετικά με προσωπικά δεδομένα και τις διαδικασίες επεξεργασίας τους.

2. Ο DPO πρέπει να έχει την αμέριστη υποστήριξη της επιχείρησης η οποία οφείλει να τον εφοδιάζει με όλα τα απαραίτητα μέσα για την επιτυχή εκπλήρωση των αρμοδιοτήτων του.

3. Ο DPO πρέπει να είναι σε θέση να δρα και να λειτουργεί αυτόνομα στο εσωτερικό της επιχείρησης.

4. Σε καμία περίπτωση δεν θα πρέπει ο ρόλος του DPO και η συνέπεια προς αυτόν να επιφέρει την τιμωρία του τελευταίου ή την απαλλαγή του εκ των καθηκόντων του εκ μέρους του υπευθύνου ή του εκτελούντος την επεξεργασία.

5. Η επιχείρηση οφείλει να μην αναθέτει στον DPO καθήκοντα τα οποία ενδέχεται να συγκρούονται με εκείνα τα οποία ο ίδιος έχει αναλάβει ως Υπεύθυνος Προστασίας Δεδομένων (π.χ. καθήκοντα θέσης Οικονομικού Διευθυντή, Διευθυντή τμήματος HR, Ιατρικού Διευθυντή κ.λπ)

6. Ο DPO μπορεί να συμβάλλει δυναμικά στην καταγραφή και τήρηση αρχείου αναφορικά με τις διαδικασίες επεξεργασίας που λαμβάνουν χώρα εντός της επιχείρησης, σύμφωνα πάντα με τις πληροφορίες που θέτουν υπόψιν του ο υπεύθυνος ή ο εκτελών την επεξεργασία. Με αυτόν τον τρόπο μπορεί να ενδυναμωθεί η συμμόρφωση της επιχείρησης μέσω της συχνής πληροφόρησης και αναφοράς στον DPO.

Ένα ισχυρό πρόγραμμα συμμόρφωσης με τον ΓΚΠΔ, εποπτευόμενο από έναν κατάλληλο DPO μπορεί να συμβάλει στην ελαχιστοποίηση του κινδύνου παραβίασης προσωπικών δεδομένων και συνεπώς στην αποφυγή προστίμων και λοιπών κυρώσεων και αξιώσεων αποζημίωσης από τα υποκείμενα των δεδομένων σε περίπτωση παραβίασης των δεδομένων τους. Μπορεί, τέλος, να ενισχύσει την αφοσίωση του προσωπικού της εταιρείας που το υιοθετεί, καθώς επίσης και τη φήμη και την αξιοπιστία της, βοηθώντας την να κερδίσει νέες ευκαιρίες.

4.4.2 Προκλήσεις που καλείται να αντιμετωπίσει ο DPO

Ο ΓΚΠΔ καθιστά σαφές ότι βασικός υπόχρεος συμμόρφωσης προς το συγκεκριμένο κανονιστικό πλαίσιο είναι όχι ο DPO αλλά ο ίδιος ο Υπεύθυνος Επεξεργασίας, ο οποίος και καλείται να εφαρμόσει όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να είναι σε θέση να αποδείξει ότι η επεξεργασία προσωπικών δεδομένων λαμβάνει χώρα σε συμμόρφωση με τις επιταγές του Κανονισμού. Αναδεικνύεται, έτσι, ένα ιδιαιτέρως σημαντικό ζήτημα, ήτοι ότι η συμμόρφωση προς το κανονιστικό πλαίσιο για την προστασία προσωπικών δεδομένων αποτελεί πρωταρχική εταιρική ευθύνη του ίδιου του υπευθύνου επεξεργασίας και όχι του DPO.

Ωστόσο, ο ρόλος του τελευταίου στο εσωτερικό μίας επιχείρησης θα αποτελέσει προϋπόθεση επίτευξης ενός υψηλού επιπέδου συμμόρφωσης, γεγονός που, αν μη τι άλλο, τον καθιστά αδιαμφισβήτητα απαραίτητο αλλά και αντιμέτωπο με μια σειρά προκλήσεων όπως:

- Να εκπροσωπήσει την Επιχείρηση έναντι των Αρχών, Εθνικών και Ευρωπαϊκών, ως διαμεσολαβητής.
- Να διασφαλίσει την εναρμόνιση της λειτουργίας της επιχείρησης σε ότι αφορά τις πολιτικές πρακτικές και τις μεθοδολογίες επεξεργασίας, αποθήκευσης και μεταφοράς Δεδομένων Προσωπικού Χαρακτήρα με το νέο αυστηρό νομοθετικό πλαίσιο.
- Να δημιουργήσει την κατάλληλη κουλτούρα στο ανθρώπινο δυναμικό της εταιρείας.
- Να εκπαιδεύσει το προσωπικό σχετικά με τις σημαντικές απαιτήσεις συμμόρφωσης του GDPR, την επεξεργασία δεδομένων και τη διενέργεια τακτικών ελέγχων ασφάλειας.
- Να προστατέψει την επιχείρηση από τους κινδύνους επιβολής των βαρύτατων διοικητικών προστίμων που προβλέπει ο Κανονισμός, τα οποία ξεκινούν από 10 εκατομμύρια ευρώ ή στο 2% του παγκόσμιου τζίρου εάν πρόκειται για διεθνή όμιλο και φτάνουν σε περίπτωση παράβασης βασικών διατάξεων του Κανονισμού στα 20 εκατομμύρια ευρώ ή στο 4% του παγκόσμιου τζίρου.

Επιπλέον, ο DPO θα πρέπει να έχει τις κατάλληλες γνώσεις και δεξιότητες για να ανταποκριθεί στον ρόλο του, με αποδεδειγμένη (πιστοποιημένη από ανεξάρτητο

φορέα) γνώση και εμπειρία στη νομοθεσία και πρακτική εφαρμογή των διαδικασιών διαχείρισης προσωπικών δεδομένων. Ακόμα θα έχει εχέγγυα ανεξαρτησίας και θα αναφέρεται απευθείας στον Διευθυντή ή σε μέλος του Δ.Σ της εταιρείας.

4.4.3 Προβληματισμοί σχετικά με το διορισμό ενός DPO

Λόγω της εμβέλειας του GDPR και εκτός Ευρωπαϊκής Ένωσης, πολλές εταιρείες θα πρέπει να ξοδεύουν χρήματα είτε σε έναν εσωτερικό DPO είτε σε έναν τρίτο φορέα, όπως μια δικηγορική εταιρεία ή μια επιχείρηση πληροφορικής που θα ενεργεί ως εξωτερικός Υπεύθυνος Προστασίας Δεδομένων. Σύμφωνα με μελέτες, περισσότεροι από 28.000 νέοι Υπεύθυνοι Προστασίας Δεδομένων πρέπει να προσληφθούν μέχρι το 2018, και αυτό ισχύει μόνο στην ΕΕ και στις Η.Π.Α. Σε παγκόσμιο επίπεδο όμως, ο αριθμός αυξάνεται στους 75.000. Με την έλλειψη λοιπόν ατόμων που εκπαιδεύονται στη διαχείριση των ευθυνών του DPO, είναι πιθανό ότι πολλές επιχειρήσεις θα αναζητήσουν την πρόσληψη ενός εξωτερικού DPO τρίτου.

Ωστόσο, πριν από την πρόσληψη ενός εξωτερικού DPO, οι επιχειρήσεις πρέπει να εξετάσουν τα ακόλουθα θέματα:

1. Δικαιολογείται το κόστος πρόσληψης ενός DPO με τη συμμετοχή του στο πρόγραμμα προστασίας προσωπικών δεδομένων μιας επιχείρησης;

Τα καθήκοντα του DPO δεν αφορούν μόνο την αντιμετώπιση καταστάσεων παραβίασης και τη συνεργασία με τις εποπτικές αρχές αλλά περιλαμβάνουν και αρμοδιότητες όπως την παρακολούθηση της συμμόρφωσης της επιχείρησης με τον GDPR, την παροχή συμβουλών κατά τη διενέργεια εκτιμήσεων αντικτύπου προστασίας δεδομένων και την ενημέρωση της επιχείρησης και των εργαζομένων της για υποχρεώσεις προστασίας δεδομένων. Επιπλέον, ένας DPO πρέπει να συμμετέχει τακτικά σε συνεδριάσεις με ανώτερα και μεσαία στελέχη και πρέπει επίσης να είναι εύκολα προσβάσιμος εντός του οργανισμού. Οι δικηγορικές εταιρίες και οι εταιρείες παροχής συμβούλων πληροφορικής είτε χρεώνουν ανά ώρα είτε έχουν σταθερό προϋπολογισμό για να παρέχουν τις υπηρεσίες τους. Έτσι, είναι σημαντικό να ληφθεί υπόψιν ότι ορισμένες ευθύνες, όπως η παρακολούθηση συναντήσεων και η παρακολούθηση της συμμόρφωσης της επιχείρησης με τον GDPR, μπορεί να είναι εξαιρετικά χρονοβόρες και δαπανηρές ανά ώρα. Ορισμένες εταιρείες παροχής

υπηρεσιών δημιούργησαν μια ρύθμιση σταθερού τέλους που μπορεί να προσφέρει εξοικονόμηση κόστους, αλλά με κίνδυνο να θυσιάσει την ποιότητα, θέτοντας λιγότερο εξειδικευμένα και έμπειρα άτομα σε ρόλους DPO. Συνεπώς, σε μια ωριαία αμοιβή ή μισθολογική συμφωνία, μια επιχείρηση θα πρέπει να εξετάσει τις υπηρεσίες που περιλαμβάνονται συγκριτικά με την εμπειρία των ατόμων που θα εκτελούν αυτές τις υπηρεσίες.

2. Μπορεί ο πάροχος υπηρεσιών να ενεργεί ανεξάρτητα κατά την εκτέλεση των καθηκόντων του ως DPO;

Σύμφωνα με τις κατευθυντήριες γραμμές του GDPR του άρθρου 38 παράγραφος 3 και του άρθρου 29, ο DPO πρέπει να εκτελεί τα καθήκοντά του με ανεξάρτητο και αδιάβλητο τρόπο, δηλαδή δεν πρέπει να ενημερώνεται σχετικά με τον τρόπο αντιμετώπισης ενός θέματος και δεν μπορεί να του δοθεί εντολή να λάβει θέση σχετικά με το θέμα της προστασίας της ιδιωτικής ζωής των δεδομένων. Ωστόσο, για πολλούς παρόχους τρίτων, αυτό θα μπορούσε να είναι ένα πιθανό ζήτημα, ειδικά εάν ο πάροχος υπηρεσιών έχει πολλές δεσμεύσεις με την εν λόγω επιχείρηση. Εάν μια επιχείρηση έχει στενή σχέση με τον πάροχο υπηρεσιών, η γραμμή μπορεί να είναι πολύ «λεπτή» και μπορεί να οδηγήσει σε περιπτώσεις όπου μπορεί να ζητηθεί ή να ασκηθεί πίεση στον πάροχο υπηρεσιών να λάβει θέση με οποιονδήποτε τρόπο.

3. Έχει ο DPO άλλες δεσμεύσεις σχετικά με την προστασία της ιδιωτικής ζωής, την ασφάλεια των δεδομένων ή τις σχετικές με την πληροφορική τεχνογνωσίες με την επιχείρηση, οι οποίες θα μπορούσαν ενδεχομένως να δημιουργήσουν σύγκρουση συμφερόντων;

Σύμφωνα με τις κατευθυντήριες γραμμές του GDPR του άρθρου 38 παράγραφος 6 και του άρθρου 29, επιτρέπεται στον DPO να εκπληρώνει άλλα καθήκοντα, τα οποία όμως να μην οδηγούν σε σύγκρουση συμφερόντων με τα καθήκοντά του όσον αφορά τη θέση του σαν DPO. Για πολλές εταιρείες παροχής υπηρεσιών, αυτό μπορεί να αποτελεί πρόβλημα, ειδικά εάν είχαν συνεργαστεί με τη διοίκηση της επιχείρησης και κατά το σχεδιασμό του προγράμματος προστασίας προσωπικών δεδομένων της ή τη βοήθησαν να ερμηνεύσει τους κανόνες και τους κανονισμούς απορρήτου. Οι πάροχοι υπηρεσιών ενδέχεται να αισθάνονται άβολα όταν κάνουν διαπιστώσεις που αντιβαίνουν στις συμβουλές που παρείχαν σε προηγούμενη δέσμευση.

Συνεπώς ερωτήματα που θα πρέπει να εξετάζει μια επιχείρηση πριν τον διορισμό ενός εξωτερικού Υπευθύνου Προστασίας Δεδομένων είναι:

- Τι είδους σύμβαση αμοιβής προσφέρει ο εξωτερικός DPO;
- Εάν το ποσό αμοιβής είναι σταθερό: είναι οι παρεχόμενες υπηρεσίες επαρκείς για την επιχείρηση; Είναι κατάλληλα τα άτομα που χειρίζονται τα καθήκοντα ως DPO;
- Εάν το ποσό αμοιβής είναι ανά ώρα: είναι οι τιμές ανάλογες της εμπειρίας των ατόμων που εκτελούν καθήκοντα DPO; Υπάρχουν δυνατότητες έκπτωσης στην τιμή σε περίπτωση προκαταβολής του ποσού; Τι είδους καθήκοντα αναμένει η επιχείρηση να εκτελεί ο DPO;
- Ο DPO εκπροσωπεί και άλλες επιχειρήσεις στον ίδιο κλάδο;
- Η επιχείρηση έχει στενή σχέση με τον εξωτερικό DPO σε σημείο που μπορεί να προκαλέσει προβλήματα ανεξαρτησίας;
- Έχει ο εξωτερικός DPO εμπλακεί στο παρελθόν σε οποιαδήποτε εργασία προστασίας προσωπικών δεδομένων για την επιχείρηση; Μπορεί το έργο αυτό να προκαλέσει σύγκρουση συμφερόντων;

4.5 Πλάνο εκπαίδευσης του ανθρώπινου δυναμικού

Οι περισσότερες παραβιάσεις προσωπικών δεδομένων συμβαίνουν στην πραγματικότητα λόγω ανθρώπινου λάθους, ως αποτέλεσμα των εργαζομένων που κάνουν απλά κάτι που δεν πρέπει να κάνουν.

Ενώ η κατάρτιση του προσωπικού αποτελούσε πάντοτε σημαντικό στοιχείο της συμμόρφωσης με την Προστασία Δεδομένων, η επικείμενη εισαγωγή του Γενικού Κανονισμού Προστασίας Δεδομένων από τον Μάιο του 2018 θα καταστήσει ακόμη πιο απαραίτητη την εκπαίδευση του προσωπικού, δεδομένου ότι τα πρόστιμα βάσει του ΓΚΠΔ για μη συμμόρφωση αναμένονται «τσουχτερά».

Επίσης, οι εταιρείες θα πρέπει τώρα να αποδείξουν τη συμμόρφωσή τους με τον Κανονισμό και ως εκ τούτου η κατάρτιση του προσωπικού και η καταγραφή και παρακολούθηση της εκπαίδευσης του προσωπικού θα είναι μια βασική πτυχή της απόδειξης ότι ο οργανισμός συμμορφώνεται με το GDPR.

Στη συνέχεια ακολουθούν ορισμένες συμβουλές για την καλύτερη εκπαίδευση του προσωπικού:

1) Κατανόηση του Γενικού Κανονισμού Προστασίας Δεδομένων

Οι εργαζόμενοι πρέπει να κατανοήσουν τους οικονομικούς κινδύνους και τους κινδύνους υπόληψης της επιχείρησης, καθώς και τον κίνδυνο ενδεχόμενων πειθαρχικών μέτρων ή ακόμη και της απόλυσης σε περίπτωση υπαιτιότητάς τους για παραβίαση δεδομένων που βλάπτει την επιχείρηση.

Όταν οι κίνδυνοι συσχετίζονται με την ιδέα πίσω από τον GDPR, οι εργαζόμενοι μπορούν ευκολότερα να αρχίσουν να κατανοούν τη σημασία των νόμων περί προστασίας δεδομένων, τους λόγους που υπάρχουν ορισμένες πολιτικές και διαδικασίες και γιατί πρέπει να συμμορφώνονται με αυτές τις πολιτικές. Αυτό μπορεί να επιτευχθεί μέσω της παροχής στοχοθετημένων πρωτοβουλιών ευαισθητοποίησης του προσωπικού στον τρόπο που αντιμετωπίζουν βασικούς επιχειρηματικούς στόχους.

2) Συνεχής και εμπεριστατωμένη εκπαίδευση

Η εκπαίδευση πρέπει να είναι πολύ συγκεκριμένη, έτσι ώστε οι υπάλληλοι να μπορούν να συσχετίζουν τις πολιτικές και τις διαδικασίες που εφαρμόζει ο οργανισμός γύρω από τη συμμόρφωση με τον ΓΚΠΔ στους καθημερινούς τους ρόλους.

Ενδεικτικά, μπορεί να περιλαμβάνει ενημέρωση σχετικά με τη σημασία της υιοθέτησης «ισχυρών» κωδικών πρόσβασης και της συχνής αλλαγής αυτών, μέχρι πρακτικές για την ασφαλή καταστροφή και κρυπτογράφηση δεδομένων και διατήρηση ασφαλών και εμπιστευτικών φακέλων στο χώρο του γραφείου.

3) Εκπαίδευση ανάλογα με τη θέση και τις αρμοδιότητες στην επιχείρηση

Ο τρόπος που εκπαιδεύεται το προσωπικό, πρέπει να αντικατοπτρίζει τις αρμοδιότητες και να λαμβάνει υπόψιν τις διαφορετικές θέσεις και τους πολλαπλούς ρόλους που υπάρχουν μέσα στον ίδιο οργανισμό..

Συγκεκριμένα, όσοι χειρίζονται χρηματοοικονομικές πληροφορίες, πρέπει να εξασκήσουν τις δεξιότητες που απαιτούνται για την εξασφάλιση δεδομένων πιστωτικών καρτών και όλων των πηγών χρηματοοικονομικών δεδομένων, όπως

ακριβώς και οι νοσηλευτές και οι επαγγελματίες του τομέα υγείας πρέπει να προστατεύσουν τις εμπιστευτικές πληροφορίες για την υγεία.

Οι διευθυντές και τα στελέχη πρέπει να κατανοήσουν ότι η αυξημένη πρόσβασή τους στις πληροφορίες, τους καθιστά στόχους

Το προσωπικό πληροφορικής χρειάζεται ειδική εκπαίδευση, όχι μόνο για την προνομιακή πρόσβαση στα δεδομένα αλλά και για το ρόλο που διαδραματίζουν ως πρεσβευτές στην κατανόηση και τη χρήση της τεχνολογίας των πληροφοριών για την προστασία των πληροφοριών.

Με αυτόν το διαχωρισμό, καθίσταται ευκολότερη η εκπαίδευση και ο σχεδιασμός ενός πλάνου που προσαρμόζεται σε όλες τις εργασιακές θέσεις.

4) Εκπαίδευση με φυσική παρουσία των εργαζομένων

Ενώ η online ή εξ' αποστάσεως εκπαίδευση είναι μια βιώσιμη επιλογή, τίθεται το ερώτημα σε ποιο βαθμό «απορροφάται» πλήρως από τους εργαζόμενους και σε ποιο βαθμό οι εργαζόμενοι μπορούν να συνδέσουν τις «εξ' αποστάσεως» αυτές πληροφορίες εκπαίδευσης στους καθημερινούς τους ρόλους.

Συνεπώς, προτείνεται να εκτελούνται εκπαιδευτικές συναντήσεις με φυσική παρουσία των ενδιαφερομένων, ώστε να δίνεται η ευκαιρία στους υπαλλήλους να θέτουν συναφείς ερωτήσεις και να επωφελούνται από τον διάλογο που οδηγεί αυτά τα ερωτήματα στη συσχέτισή τους με αυτό που κάνουν σε καθημερινή βάση.

5) Εκπαίδευση εντοπισμού παραβιάσεων προσωπικών δεδομένων

Μία από τις νέες πτυχές του GDPR, θα είναι η υποχρέωση των εργαζομένων να αναφέρουν παραβιάσεις δεδομένων εντός προθεσμίας 72 ωρών στις αρμόδιες εποπτικές αρχές πληροφόρησης, καθώς και να τις γνωστοποιούν στα άτομα που τέθηκαν τα δεδομένα τους σε κίνδυνο, μια υποχρέωση που μέχρι πρότινος δεν υφίστανται στον ιδιωτικό τομέα.

Το προσωπικό συνεπώς, πρέπει να είναι σε θέση να εντοπίσει πότε έχει σημειωθεί πιθανή παραβίαση, πώς αναφέρουν ότι υπάρχει πιθανή παραβίαση εσωτερικά, στον Υπεύθυνο Προστασίας Δεδομένων του οργανισμού, και εντός ποιου χρονικού διαστήματος. Δεδομένου ότι οι εργαζόμενοι θα είναι συχνά οι πρώτοι που θα έχουν επίγνωση ότι έχει σημειωθεί παραβίαση, πρέπει να υπάρχει σαφής πολιτική για την

αναφορά της πιθανής παραβίασης, ώστε ο οργανισμός να μπορεί να συμμορφωθεί με τις υποχρεώσεις υποβολής εκθέσεων και αναφορών.

Έτσι, εάν η εκπαίδευση σχετίζεται με το τι κάνει μια συγκεκριμένη επιχείρηση στην πράξη, τότε σε καταστάσεις «εκτάκτου κινδύνου» καθίσταται ευκολότερο για τους εργαζομένους να εντοπίζουν και να μεταβιβάζουν στο κατάλληλο άτομο τις πληροφορίες, μειώνοντας σημαντικά τον πιθανό κίνδυνο μη συμμόρφωσης.

6) Υιοθέτηση κοινής κουλτούρας για την προστασία των προσωπικών δεδομένων

Είναι σημαντικό να υπάρχει διαφάνεια και να ενισχύεται η προβολή των προσπαθειών για την προώθηση της προστασίας των πληροφοριών, καθώς είναι ζωτικής σημασίας για την ανάπτυξη μιας κουλτούρας που σέβεται την προστασία της ιδιωτικής ζωής μέσα στον οργανισμό ή την επιχείρηση. Αυτή είναι η ευκαιρία να βεβαιωθεί η επιχείρηση ότι ο κάθε εργαζόμενος κάνει την προστασία, της ιδιωτικής ζωής και των δεδομένων, ευθύνη του.

7) Άμεση έναρξη της εκπαίδευσης και διασφάλισης συνέχειάς της

Δεδομένου ότι δεν υπάρχει περίπτωση παράτασης της περιόδου «χάριτος» για συμμόρφωση με το νέο Κανονισμό πριν ξεκινήσουν οι ενέργειες επιβολής του, οι οργανισμοί πρέπει να εναρμονιστούν πλήρως με τους κανόνες έως τον Μάιο του 2018, αν όχι νωρίτερα.

Έτσι, όσο πιο οργανωμένη και έτοιμη είναι μια επιχείρηση ως προς τη συμμόρφωση με τον GDPR, τόσο μικρότερος είναι ο κίνδυνος παραβιάσεων που συμβαίνουν όταν αρχίσουν να ισχύουν οι κανόνες του GDPR.

Ωστόσο, οι επιχειρήσεις δεν πρέπει να επαναπαύονται απλά στην εκπαίδευση των εργαζομένων τους, αλλά η κατάρτιση αυτή πρέπει να είναι συνεχής και αδιάλειπτη, ώστε να συμπεριληφθούν και τα νέα μέλη του προσωπικού. Επιπλέον, το προσωπικό θα πρέπει να εκπαιδεύεται σε θέματα του ΓΚΠΔ ως μέρος της συνεχούς εξέλιξής του, ώστε να ενστερνιστεί πλήρως τους νέους κανόνες και να οδηγηθεί πραγματικά στην υιοθέτηση και την εφαρμογή τους. Με αυτό τον τρόπο, οι εργαζόμενοι θα είναι προετοιμασμένοι να χειριστούν και να αποφύγουν τυχόν παραβιάσεις προσωπικών δεδομένων.

4.6 Συνεχής παρακολούθηση και επικαιροποίηση του GDPR

Το σημαντικότερο κομμάτι μετά το πέρας της διαδικασίας εναρμόνισης της εταιρείας με τους κανονισμούς του GDPR και την κατάλληλη εκπαίδευση του προσωπικού, είναι η διαμόρφωση μιας ορθής και ηθικής νοοτροπίας. Αν μια εταιρεία δεν υιοθετήσει μια τέτοια νοοτροπία, η εστιασμένη προσέγγισή της στη συμμόρφωση για την εξάλειψη ανήθικων συμπεριφορών ενδέχεται να ανακόψει τις προσπάθειές της να καινοτομεί και να λαμβάνει τα αναμενόμενα υγιή ρίσκα.

Σύμφωνα με έρευνες, η συνεχής επένδυση σε εκπαίδευση και επιμόρφωση σε θέματα συμμόρφωσης με τον ΓΚΠΔ, ενθαρρύνει τον υγιή ανταγωνισμό και την εξωστρέφεια των επιχειρήσεων, ευθυγραμμίζει την εταιρική νοοτροπία με αυτή των επιχειρήσεων του εξωτερικού και έχει ως αποτέλεσμα την αδιαπραγμάτευτη ανάπτυξη και εδραίωση της θέσης της επιχείρησης στην αγορά καθώς και τη δημιουργία συνεργασιών εμπιστοσύνης εντός και εκτός Ελλάδος. Το τελευταίο ίσως αποτελεί και το σημαντικότερο όφελος μιας ολοκληρωμένης Στρατηγικής Συμμόρφωσης.

Συνεπώς, μετά το πέρας της διαδικασίας συμμόρφωσης με τον Κανονισμό, τόσο η εταιρεία όσο και οι εργαζόμενοί της, θα πρέπει να βρίσκονται σε μια συνεχή παρακολούθηση των γεγονότων γύρω από τον GDPR και να επικαιροποιούν τις γνώσεις, τις δεξιότητες, τα επαγγελματικά τους προσόντα και τις εμπειρίες τους με νέες, είτε μέσω συμμετοχής σε σεμινάρια επιμόρφωσης είτε μέσω παρακολούθησης ειδικά διαμορφωμένων εκπαιδευτικών προγραμμάτων.

Τα προγράμματα αυτά μπορεί να περιλαμβάνουν μελέτες περιπτώσεων (case studies), και χρήση οδηγών, οι οποίοι αποτελούν βασικά εργαλεία των DPOs, για την δημιουργία μελέτης επιπτώσεων παραβίασης προσωπικών δεδομένων (DPIA) και άμεσης ανταπόκρισης σε αυτήν. Η παρακολούθησή τους, θα βοηθήσει τους εργαζόμενους να ακολουθούν αποτελεσματικά τις εξελίξεις και να γίνουν πιο ανταγωνιστικοί στη συνεχώς μεταβαλλόμενη και τεχνολογικά εξελισσόμενη αγορά εργασίας. Επιπλέον, θα αναβαθμίσουν τα ατομικά τους χαρακτηριστικά (γνώσεις, δεξιότητες, συμπεριφορές) προς όφελος της επαγγελματικής τους εξέλιξης, θα μάθουν να διαχειρίζονται τις συνεχείς μεταβολές στον εργασιακό τους χώρο, βελτιώνοντας την ευελιξία και την προσαρμοστικότητα τους σε αυτές, και θα αποκτήσουν όλα τα

απαραίτητα εφόδια για να εκτελούν με επιτυχή και παραγωγικό τρόπο την εργασία που τους ανατίθεται, τονώνοντας παράλληλα την απόδοση της επιχείρησης.

Συνεπώς, η συνεχής εκπαίδευση των εργαζομένων και μετά την ολοκλήρωση της διαδικασίας συμμόρφωσης με τον ΓΚΠΔ, είναι ζωτικής σημασίας για την επιχείρηση μιας και μέσω αυτής, δημιουργείται μια ευρύτερη οργανωτική κουλτούρα, η επιχείρηση αποκτά ανταγωνιστικό πλεονέκτημα, εξελίσσεται, δείχνει τη δυναμική της και ικανοποιεί τους στρατηγικούς της στόχους.

Είναι άλλωστε γνωστό, ότι οι εταιρείες δεν είναι εντελώς ενάρετες ούτε όμως και δίχως αξίες. Ο στόχος για αυτές είναι να γίνουν καλύτερες απ' όσο υπήρξαν και για τους ηγέτες τους να διδάξουν την αρμόζουσα συμπεριφορά με το δικό τους παράδειγμα. Ως εκ τούτου, η πορεία προς την Αριστεία, δεν είναι μια πράξη από μόνη της, αλλά μια συνήθεια που επιτυγχάνεται με συνεχή προσπάθεια και θέληση για εξέλιξη και μάθηση.

4.7 Σύνοψη

Με την κατάλληλη προετοιμασία και κατανόηση της μεθοδολογίας σε θεωρητικό επίπεδο, που παρουσιάστηκε σε αυτό το κεφάλαιο, οι επιχειρήσεις βρίσκονται ένα βήμα πιο κοντά στον αποτελεσματικότερο σχεδιασμό της στρατηγικής τους για την εφαρμογή του GDPR. Μέσω της εφαρμογής των κατάλληλων τεχνικών και της εκπαίδευσης του ανθρώπινου δυναμικού τους, ενισχύουν την ασφάλεια των προσωπικών τους δεδομένων και εξασφαλίζουν τη συνεχή προστασία αυτών.

Βέβαια, όλα τα παραπάνω απαιτούν και τα κατάλληλα τεχνολογικά και υποστηρικτικά μέτρα και συστήματα, που θα διευκολύνουν την επιχείρηση στη γρηγορότερη και ασφαλέστερη μετάβαση στον GDPR. Μερικά από αυτά τα συστήματα, περιγράφονται αναλυτικά στο κεφάλαιο που ακολουθεί.

5. ΛΟΓΙΣΜΙΚΑ ΥΠΟΣΤΗΡΙΞΗΣ ΚΑΙ ΕΝΣΩΜΑΤΩΣΗΣ ΤΟΥ ΝΕΟΥ ΚΑΝΟΝΙΣΜΟΥ

5.1 Εισαγωγή

Οι οργανισμοί συνήθως, έχουν πολλαπλά επίπεδα ασφάλειας γύρω από τη βάση δεδομένων τους είτε χρησιμοποιώντας τείχος προστασίας (firewall), είτε συστήματα ανίχνευσης εισβολών και κατάλληλη κατάτμηση δικτύων, επιδιώκοντας έτσι οι εισβολείς να μην καταφέρουν να φτάσουν απευθείας στις βάσεις δεδομένων της επιχείρησης. Ωστόσο, καθώς οι συνήθεις περίμετροι του δικτύου γίνονται πιο πολύπλοκες και ο αριθμός των ατόμων (διαχειριστές, προγραμματιστές και συνεργάτες) που έχουν άμεση πρόσβαση στις βάσεις δεδομένων όλο και αυξάνεται, καθίσταται πολύ σημαντική η άμεση διασφάλιση των βάσεων δεδομένων. Προκειμένου να περιοριστούν οι «ευάλωτες» περιοχές και να μειωθεί ο αριθμός των τρόπων με τους οποίους οι «επιτιθέμενοι εισβολείς» μπορούν να φτάσουν στις βάσεις δεδομένων, είναι εξαιρετικά σημαντικό να επιβάλλεται η ασφάλεια όσο το δυνατόν πιο κοντά στα δεδομένα.

Μία από τις προκλήσεις κατά την αξιολόγηση της φύσης των κινδύνων είναι να προσδιοριστεί τι πρέπει να αξιολογηθεί, επειδή οι εφαρμογές βάσεων δεδομένων περιέχουν συνήθως διάφορα σημεία εισόδου από δίκτυα, λειτουργικά συστήματα, βάσεις δεδομένων αλλά και την ίδια την εφαρμογή. Οι κακόβουλοι εισβολείς μπορούν να εκμεταλλευτούν τις αδυναμίες σε οποιοδήποτε από αυτά τα σημεία εισόδου ή ακόμα και να στοχεύσουν εργαζόμενους και μεσολαβητές που είναι υπεύθυνοι για τη χρήση, διαχείριση, δοκιμή και συντήρηση του συστήματος.

Συνεπώς, οι επιχειρήσεις και οι οργανισμοί, πέραν της προετοιμασίας και των μεθοδολογιών που πρέπει να ακολουθήσουν, οφείλουν να εξετάσουν και τον τρόπο με τον οποίο αναπτύσσονται τα συστήματά τους, συμπεριλαμβανομένου του cloud και της χρήσης εφαρμογών παλαιού τύπου, όπου ενδέχεται να μην έχουν τον πηγαίο κώδικά τους και να εξαρτώνται από τρίτους, είτε εντός είτε εκτός της ΕΕ.

Για τους παραπάνω λόγους, λοιπόν, κάποιες από τις μεγαλύτερες εταιρείες hardware και software λογισμικών, είτε έχουν αναπτύξει έτοιμα προγράμματα και βάσεις δεδομένων που ενσωματώνουν το νέο Κανονισμό, είτε έχουν αναβαθμίσει τα

προγράμματά τους, ώστε να συμπεριλάβουν αυτόματα και τις εταιρίες που τα χρησιμοποιούν ήδη, είτε παρέχουν έτοιμες λύσεις και μεθοδολογίες, προκειμένου να διευκολύνουν και να υποστηρίξουν τους οργανισμούς στη γρηγορότερη μετάβαση και συμμόρφωση με τον ΓΚΠΔ.

Στις επόμενες ενότητες, θα γίνει προσπάθεια να περιγραφούν οι βασικότερες τεχνολογίες και οι έλεγχοι των λειτουργικών συστημάτων των οργανισμών, που προσφέρουν μερικές από τις πιο γνωστές εταιρίες λογισμικών στη συμμόρφωση με τον ΓΚΠΔ, για την αξιολόγηση της ασφάλειας, της πρόληψης και της ανίχνευσης «επιθέσεων». Επιπλέον, θα γίνει αναφορά στις μεθόδους και στις υπηρεσίες που παρέχουν εταιρείες τρίτων για τη διευκόλυνση των επιχειρήσεων και οργανισμών στην ενσωμάτωση του GDPR στο εσωτερικό τους.

5.2 Συστήματα και λογισμικά της εταιρείας SYMANTEC

Η εταιρεία Symantec είναι μία από τις μεγαλύτερες εταιρείες παγκόσμιας ασφάλειας στον κυβερνοχώρο και παρέχει ολοκληρωμένες λύσεις για την προστασία από επιθέσεις σε clouds, υποδομές πληροφορικής και λειτουργικά συστήματα, ενώ εκμεταλλεύεται ένα από τα μεγαλύτερα δίκτυα μη κυβερνητικών πληροφοριών, που της επιτρέπει να βλέπει και να προστατεύει από τις πιο εξελιγμένες απειλές.

Με την χρήση της Symantec Control Compliance Suite (CCS), η Symantec επιδιώκει να βοηθήσει τους πελάτες της σε δύο στάδια:

1) Αρχική αξιολόγηση της ετοιμότητας: Το περιεχόμενο του Symantec CCS GDPR Readiness Assessment θα βοηθήσει τους οργανισμούς να αξιολογήσουν το επίπεδο κατανόησης του κανονισμού και να εκτιμήσουν την τρέχουσα ετοιμότητά τους για την πορεία προς τη συμμόρφωση με το GDPR. Το συνολικό αποτέλεσμα αυτής της αξιολόγησης θα βοηθήσει τους οργανισμούς να εκτιμήσουν πόσο απέχουν από την εκπλήρωση ορισμένων σημαντικών απαιτήσεων του GDPR. Βάσει των αποτελεσμάτων της αξιολόγησης, μπορούν να τεθούν σε εφαρμογή σχέδια δράσης. Αυτή η αξιολόγηση μπορεί να επαναληφθεί πολλές φορές μέχρι να δουν οι επιχειρήσεις την εξέλιξη.
2) Αυτοματοποίηση συμμόρφωσης: Ο απώτερος στόχος της Symantec Control Compliance Suite είναι να βοηθήσει τους οργανισμούς να εφαρμόσουν μια

αποδοτική, ολιστική προσέγγιση στη διαδικασία αυτοματοποίησης συμμόρφωσης, παρακολουθώντας και καταγράφοντας την πρόοδο με την αξιοποίηση των παρακάτω λειτουργικών εργαλείων της CCS:

- **Symantec CCS Policy Manager**: Αυτοματοποιεί τον ορισμό της πολιτικής και της διαχείριση του κύκλου ζωής της. Οι πελάτες χρησιμοποιούν το Policy Manager για να εντοπίζουν παρόμοιους ελέγχους σε πολλαπλές εντολές, να αναβαθμίζουν τακτικά τις ενημερώσεις του περιεχομένου και των τεχνικών προτύπων και να διαχειρίζονται τον κύκλο ζωής των πολιτικών ασφαλείας, των προτύπων και των ελέγχων.
- **Symantec CCS Assessment Manager**: Χρησιμοποιείται για να συλλέξει πληροφορίες για την ανταπόκριση τόσο στην ετοιμότητα όσο και στο πλήρες ερωτηματολόγιο περιεχομένου του GDPR. Οι πελάτες το χρησιμοποιούν για να αξιολογήσουν την αποτελεσματικότητα των διαδικαστικών ελέγχων ασφαλείας στο κέντρο δεδομένων, για να αξιολογήσουν την επίγνωση των εργαζομένων σχετικά με την ασφάλεια των δεδομένων και για να υποστηρίξουν την εκπαίδευση για την κινητοποίηση σχετικά με την ασφάλεια.
- **Symantec CCS Standards Manager**: Χρησιμοποιείται για τη συλλογή τεχνικών στοιχείων σχετικά με την επιβολή της ασφάλειας των δεδομένων. Οι επιχειρήσεις προσλαμβάνουν τον Διαχειριστή Προτύπων (Standards Manager) για να ανακαλύψουν και να εντοπίσουν παρωχημένα και εσφαλμένα στοιχεία, να ανιχνεύσουν παραμορφώσεις παραμέτρων και να αξιολογήσουν εάν τα συστήματα είναι ασφαλή, διαμορφωμένα και προσαρμοσμένα σύμφωνα με τα πρότυπα ασφαλείας του πελάτη.

Ένα άλλο εργαλείο της Symantec που διασφαλίζει την προστασία των προσωπικών δεδομένων σύμφωνα με τις απαιτήσεις του GDPR είναι το **Information Centric Security**. Με αυτό το εργαλείο, επιτυγχάνεται ένας καινοτόμος συνδυασμός βασικής τεχνολογίας προστασίας δεδομένων και αναλυτικών στοιχείων, ώστε οι οργανισμοί να μπορούν να εντοπίζουν, να παρακολουθούν και να προστατεύουν ευαίσθητα δεδομένα, συμπεριλαμβανομένων των δεδομένων που μετακινούνται στο cloud και χρησιμοποιούνται από οργανισμούς τρίτων. Έτσι, σε περίπτωση που τα δεδομένα έχουν πέσει σε λάθος χέρια, οι επιχειρήσεις μπορούν να χρησιμοποιήσουν τα

δεδομένα αναλυτικών στοιχείων για να επισημάνουν τους επικίνδυνους χρήστες και να ενεργοποιήσουν εξ' αποστάσεως σε πραγματικό χρόνο τους ελέγχους πρόσβασης για τον αποκλεισμό των ανεπιθύμητων χρηστών.

5.3 Συστήματα και λογισμικά της εταιρείας IBM

Η IBM διαθέτει έναν από τους μεγαλύτερους στον κόσμο οργανισμό έρευνας, ανάπτυξης και διάθεσης λύσεων στον τομέα της ασφάλειας των πληροφοριακών συστημάτων. Για να βοηθήσει τις επιχειρήσεις να αντιμετωπίσουν με επιτυχία και χωρίς επιπτώσεις οποιαδήποτε κυβερνοεπίθεση ή επιχειρησιακή κρίση σύμφωνα με το νέο Ευρωπαϊκό Κανονισμό GDPR, δημιούργησε από τα πιο εξελιγμένα και ολοκληρωμένα χαρτοφυλάκια προϊόντων και υπηρεσιών ασφαλείας, το **IBM Resilient**. Τα εργαλεία που παρέχει το συγκεκριμένο σύστημα είναι:

- Το **Resilient GDPR Preparatory Guide**, ένα διαδραστικό εργαλείο με οδηγίες για την ετοιμότητα της επιχείρησης ως προς τον Κανονισμό GDPR, το οποίο αξιοποιεί την ευελιξία της πλατφόρμας Resilient IRP (Incident Response Platform) και κάνει την προετοιμασία και το σχεδιασμό μια διαδραστική και δυναμική διαδικασία. Οι εργασίες στον οδηγό μπορούν να τροποποιηθούν ή να ανατεθούν ώστε η επιχείρηση να μπορεί να διαχειρίζεται πιο αποτελεσματικά τη ροή εργασιών, πέρα από την υποχρέωση ενημέρωσης σε περίπτωση παραβίασης. Ο οδηγός καλύπτει όλες τις πλευρές της προετοιμασίας, οι οποίες αποτυπώνονται αναλυτικά, διευκολύνοντας τη μελλοντική παρακολούθηση και τεκμηρίωση.
- Το **Resilient GDPR Simulation**, μια νέα λειτουργία της πλατφόρμας Resilient IRP που βοηθά τους αναλυτές ασφάλειας της επιχείρησης να προσομοιάσουν τις ενέργειες στις οποίες θα χρειαστεί να προβούν σε περίπτωση παραβίασης, όπως η γνωστοποίηση παραβίασης των δεδομένων εντός 72 ωρών, η εκτίμηση του κινδύνου δυσμενών επιπτώσεων ή η επικοινωνία με τον Υπεύθυνο Προστασίας Δεδομένων (Data Protection Officer - DPO) και την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Data Protection Authority - DPA). Στο πλαίσιο της προσομοίωσης, οι αναλυτές αξιολογούν ένα περιστατικό ως υψηλού, μεσαίου ή χαμηλού κινδύνου και ακολουθούν τα ενδεδειγμένα

βήματα για την ενημέρωση της εποπτικής αρχής και των καταναλωτών των οποίων τα δεδομένα παραβιάστηκαν.

- **To Resilient GDPR-Enhanced Privacy Module**, μια παγκόσμια βάση δεδομένων για την προστασία της ιδιωτικότητας, όπου η IBM προσθέτει συνεχώς ενημερώσεις σχετικά με τις απαιτήσεις του Κανονισμού GDPR και στην οποία οι πελάτες που χρησιμοποιούν την πλατφόρμα IBM Resilient μπορούν να έχουν πρόσβαση στις σχετικές οδηγίες και κανονισμούς του GDPR.
- **To Incident Response Platform (IRP),** μια πλατφόρμα που δίνει στις ομάδες ασφαλείας της επιχείρησης τα απαραίτητα εργαλεία για να αναλύουν, να αντιμετωπίζουν και να εξουδετερώνουν τα περιστατικά γρηγορότερα, εξυπνότερα και αποτελεσματικότερα, ενώ δίνει τη δυνατότητα στις ομάδες ασφαλείας να συντονίζουν ανθρώπους, διαδικασίες και τεχνολογίες σε ένα ενιαίο μέτωπο άμυνας απέναντι στις απειλές.

5.4 Συστήματα και λογισμικά της εταιρείας SAP

Μια άλλη εταιρεία παροχής υπηρεσιών υποστήριξης και λογισμικών, η SAP, ανακοίνωσε τα βήματα με τα οποία οι επιχειρήσεις μπορούν να προετοιμάσουν τα συστήματα SAP τους για να συμβαδίζουν με τους κανόνες του ΓΚΠΔ. Ουσιαστικά, δεν δημιουργεί εκ νέου εφαρμογές που ακολουθούν το νέο Κανονισμό, αλλά ενσωματώνει λειτουργίες στα ήδη υπάρχοντα συστήματα και προγράμματά της, έτσι ώστε αυτά να εμπεριέχουν από εδώ και στο εξής τους κανόνες συμμόρφωσης του GDPR.

Ένα σχέδιο προετοιμασίας ξεκινά με τον εντοπισμό όλων των περιβαλλόντων SAP, των πελατών, των βασικών αρχείων δεδομένων και των πεδίων που περιέχουν προσωπικές πληροφορίες των υποκειμένων. Όλα τα συστήματα SAP, όπως το κεντρικό στοιχείο SAP ERP (ECC), η επιχειρησιακή ευφυΐα (BI), η διαχείριση σχέσεων πελατών (CRM) και άλλες εφαρμογές θα πρέπει να συμπεριληφθούν στο σχέδιο προετοιμασίας. Τα αντίγραφα ασφαλείας, τα παλαιότερα συστήματα και τα αρχεία των βάσεων δεδομένων SAP πρέπει επίσης να συμπεριληφθούν στον προγραμματισμό της προετοιμασίας, καθώς και τα ψηφιοποιημένα έγγραφα που περιέχουν ιδιωτικές πληροφορίες.

Το αποθετήριο του συστήματος πληροφοριών στο SAP ABAP μπορεί να χρησιμοποιηθεί για να απαριθμήσει όλους τους πίνακες που περιέχουν πεδία με προσωπικές πληροφορίες, ωστόσο η μείωση της ποσότητας των προσωπικών πληροφοριών θα διευκολύνει την προετοιμασία με τον μετριασμό του κινδύνου στο σύστημα SAP.

Οι 3 βασικές ενέργειες που πρέπει να γίνουν είναι:

1) Ο έλεγχος των συστημάτων για τρωτά σημεία ασφαλείας από μια αξιολόγηση ασφαλείας SAP και ενίσχυση της ασφάλειας ώστε αυτά να μην παραβιάζονται.

2) Παρακολούθηση ασφάλειας SAP σε πραγματικό χρόνο, έτσι ώστε αν κάποιος εσωτερικός χρήστης χρησιμοποιεί κατά λάθος τα συστήματα ή ένας εξωτερικός προσπαθεί να επιτεθεί στα συστήματα, να μπορεί να εξουδετερωθεί η επίθεση πριν γίνει η παραβίαση.

3) Δυνατότητες διατήρησης και ανάλυσης του αρχείου καταγραφής ασφαλείας SAP συγκεντρωτικά.

Ένας πιο ώριμος τρόπος διαχείρισης της ασφάλειας είναι η εφαρμογή δραστηριοτήτων ή διαδικασιών ασφαλείας που ικανοποιούν τους στόχους ασφαλείας της εταιρείας. Οι δραστηριότητες χρησιμοποιούν τους προαναφερθέντες μηχανισμούς ασφαλείας και παράγουν αποτελέσματα που έχουν νόημα για την παροχή ασφάλειας. Οι δραστηριότητες ασφαλείας που αφορούν ειδικά τα περιβάλλοντα SAP περιγράφονται ενδεικτικά στο πλαίσιο SAP Cybersecurity Framework (SCSF). Το συγκεκριμένο πλαίσιο, δημιουργήθηκε για να αποτελέσει μια εννοιολογική γέφυρα μεταξύ της ολοκληρωμένης προσαρμοστικής αρχιτεκτονικής ασφάλειας και των ενεργειών. Το SCSF περιγράφει τέσσερις κατηγορίες για τις διαδικασίες προστασίας του SAP: πρόβλεψη (predict), πρόληψη (prevent), ανίχνευση (detect) και ανταπόκριση (respond). Το πλαίσιο διαρθρώνει κρίσιμους τομείς δράσεων για την καθιέρωση της ασφάλειας των συστημάτων ERP, περιγράφει τα επιθυμητά αποτελέσματα και παρέχει προσέγγιση σε 3 στάδια για να πετύχει σε κάθε περιοχή.

Κάθε κατηγορία περιγράφει συγκεκριμένες διαδικασίες προστασίας, όπως τη διαχείριση περιουσιακών στοιχείων, τη διαχείριση περιστατικών ή την απειλή πληροφοριών. Όλες οι διαδικασίες είναι σύμφωνες με αναγνωρισμένα πλαίσια και

προσεγγίσεις από τις NIST, SANS, ISO, CIS, αλλά αντικατοπτρίζουν τις ιδιαιτερότητες των συστημάτων ERP.

Το SAP Cybersecurity Framework παρέχει έναν οδικό χάρτη τριών βημάτων για την υλοποίηση κάθε διαδικασίας ασφάλειας ERP: Η εφαρμογή του πρώτου βήματος είναι το ελάχιστο. Το δεύτερο βήμα παρέχει επαρκές επίπεδο ασφάλειας και απαιτεί μεσαία προσπάθεια. Το τρίτο βήμα περιλαμβάνει όλα τα παραπάνω βήματα όπως αυτοματοποίηση και άλλα πράγματα, τα οποία προσφέρουν τις τελευταίες δυνατότητες ασφάλειας. Αυτή η πολυεπίπεδη προσέγγιση, από τις απαιτήσεις σε ελέγχους και περαιτέρω σε μηχανισμούς, επιτρέπει τη συνεχή συμμόρφωση με κάθε συμβατική νομοθεσία και κανονιστικές υποχρεώσεις.

Προκειμένου να εξασφαλιστεί η μακροπρόθεσμη προστασία της ιδιωτικής ζωής των δεδομένων, πρέπει να διατηρηθεί το μοντέλο ασφαλείας του συστήματος SAP ή, με άλλα λόγια, οι επιχειρήσεις να διαχειριστούν τον κύκλο ζωής των προσωπικών δεδομένων.
Αυτό επιτυγχάνεται με 2 τρόπους:

1) Προστασία δεδομένων σε διάφορα στάδια:
   - Στάδιο επεξεργασίας: τα προσωπικά δεδομένα πρέπει να είναι προσιτά για τον επιδιωκόμενο σκοπό, π.χ. σύμβαση, παράδοση και πληρωμή.
   - Στάδιο αποκλεισμού: τα δεδομένα διατηρούνται για νομικές υποχρεώσεις αναφοράς και είναι προσβάσιμα μόνο για χρήστες με ρητή άδεια.
   - Ολοκλήρωση δέσμευσης: σε περίπτωση λήξης του σκοπού ή και των φορολογικών-νομικών περιόδων δέσμευσής τους, τα δεδομένα πρέπει να διαγραφούν.
   - Διατήρηση σταθερού μοντέλου ασφαλείας: εξασφαλίζοντας ότι τα στοιχεία ελέγχου ασφαλείας και η περιγραφή τους είναι ενημερωμένα.

2) Προσδιορισμός ευαίσθητων προσωπικών πληροφοριών που αποθηκεύονται, επεξεργάζονται, μεταφέρονται και διαγράφονται σε συστήματα SAP
   - Περιορισμός της πρόσβασης στις προσωπικές πληροφορίες και τη διαθεσιμότητά τους όσο απαιτείται.
   - Εφαρμογή ελέγχων για την αποτροπή της λήψης προσωπικών πληροφοριών.

- Εφαρμογή βέλτιστων πρακτικών για τη μεταφορά και τη διαγραφή προσωπικών δεδομένων σε ένα σύστημα SAP σε παραγωγικά και μη παραγωγικά περιβάλλοντα.

5.5 Συστήματα και λογισμικά της εταιρείας MICROSOFT

Η εταιρεία Microsoft, κινούμενη σε παρόμοιο επίπεδο με τη SAP που περιγράφηκε παραπάνω, συνιστά την έναρξη της συμμόρφωσης με το GDPR εστιάζοντας σε τέσσερα βασικά βήματα:

1) Ανακάλυψη (Discover): Προσδιορισμός τους είδους των προσωπικών δεδομένων που κατέχει η εταιρεία και αξιολόγηση εάν το GDPR ισχύει για αυτήν και σε ποιο βαθμό.
2) Διαχείριση (Manage): Καθορισμός του τρόπου χρήσης και πρόσβασης των προσωπικών δεδομένων.
3) Προστασία (Protect): Δημιουργία στοιχείων ελέγχου ασφάλειας για την πρόληψη, ανίχνευση και αντιμετώπιση των αδύναμων σημείων και των παραβιάσεων δεδομένων.
4) Υποβολή έκθεσης (Report): Εκτέλεση σε αιτήματα δεδομένων, παραβίαση δεδομένων αναφοράς και διατήρηση της απαιτούμενης τεκμηρίωσης.

Τα προϊόντα και οι υπηρεσίες της Microsoft, όπως τα Azure, Dynamics 365, Enterprise Mobility + Security, Office 365 και Windows 10, αποτελούν σήμερα λύσεις που βοηθούν τους οργανισμούς να ανιχνεύσουν και να αξιολογήσουν τις απειλές και τις παραβιάσεις της ασφάλειας και να εκπληρώσουν τις υποχρεώσεις γνωστοποίησης παραβίασης του GDPR.

Azure

Το Microsoft Azure είναι μια πλήρως διαχειριζόμενη υπηρεσία cloud που λειτουργεί ως σύστημα εγγραφής και ανίχνευσης για τις πηγές δεδομένων του οργανισμού. Μόλις μια πηγή δεδομένων καταχωρηθεί με το Azure Data Catalog, τα μεταδεδομένα της είναι κατηγοριοποιημένα από την υπηρεσία, έτσι ώστε να μπορούν εύκολα να αναζητηθούν. Με το Azure Active Directory διαχειρίζεται η ταυτότητα των δεδομένων και ελέγχεται η πρόσβαση στο Azure, και σε άλλα clouds, δεδομένα και εφαρμογές.

Επίσης, μπορούν να εκχωρηθούν προσωρινά δικαιώματα διαχείρισης Just-In-Time (JIT) σε κατάλληλους χρήστες για τη διαχείριση πόρων στο Azure.

Με το Azure Role-Based Access Control (RBAC) δίνεται η δυνατότητα χορήγησης πρόσβασης στα δεδομένα βάσει του ρόλου που έχει αναθέσει ο χρήστης, καθιστώντας ευκολότερη τη χορήγηση μόνο των απαιτούμενων δικαιωμάτων που χρειάζονται οι χρήστες για να εκτελέσουν τις εργασίες τους. Το RBAC μπορεί να προσαρμοστεί ανάλογα με το επιχειρηματικό μοντέλο της επιχείρησης και την ανοχή κινδύνου.

Επιπλέον, με το Azure Security παρακολουθούνται συνεχώς οι πόροι της επιχείρησης και παρέχονται χρήσιμες συστάσεις ασφαλείας μέσω της διαδικασίας υλοποίησης των απαιτούμενων στοιχείων ελέγχου, όπως για παράδειγμα, επιτρέποντας την κρυπτογράφηση antimalware ή δίσκου για τους πόρους.

Η κρυπτογράφηση δεδομένων στο Azure εξασφαλίζει τα δεδομένα σε κατάσταση αδράνειας και κατά τη μεταφορά. Μπορεί να χρησιμοποιηθεί το Azure Disk Encryption για την κρυπτογράφηση των λειτουργικών συστημάτων και των δίσκων δεδομένων που χρησιμοποιούνται από τα λειτουργικά συστήματα Windows και Linux. Τα δεδομένα προστατεύονται κατά τη μεταφορά μεταξύ μιας εφαρμογής και του Azure, ώστε να παραμένουν πάντα ασφαλή.

Το Azure Key Vault επιτρέπει την προστασία των κρυπτογραφικών κλειδιών, χρησιμοποιώντας μονάδες ασφαλείας υλικού (HSM) και έχει σχεδιαστεί έτσι ώστε να διατηρείται ο έλεγχος των κλειδιών και συνεπώς και των δεδομένων της επιχείρησης, συμπεριλαμβανομένης της διασφάλισης ότι η Microsoft δεν μπορεί να δει ή να εξαγάγει τα κλειδιά.

Οι ολοκληρωμένες υπηρεσίες με το Azure επιτρέπουν την ταχύτερη και ευκολότερη κατανόηση της γενικής στάσης ασφαλείας, καθώς και την ανίχνευση και διερεύνηση απειλών στο περιβάλλον του cloud. Το Azure Security Center χρησιμοποιεί προηγμένα συστήματα ανάλυσης ασφαλείας, όπως το Azure Log Analytics που παρέχει ρυθμιζόμενες επιλογές ελέγχου και καταγραφής ασφάλειας, βοηθώντας στη συλλογή και ανάλυση δεδομένων που παράγονται από πόρους σε περιβάλλοντα cloud ή σε χώρους εγκατάστασης. Επίσης, παρέχει πληροφορίες σε πραγματικό χρόνο, χρησιμοποιώντας ολοκληρωμένες έρευνες και προσαρμοσμένους πίνακες ελέγχου, για την εύκολη ανάλυση εκατομμυρίων αρχείων σε όλα τα φορτία και τους διακομιστές, ανεξάρτητα από τη φυσική τους θέση και βοηθά στη διευκόλυνση της

γρήγορης ανταπόκρισης και της ενδελεχούς διερεύνησης για τυχόν συμβάντα ασφαλείας.

Dynamics 365

Το Dynamics 365 παρέχει αρκετές δυνατότητες προβολής και ελέγχου που μπορούν να χρησιμοποιηθούν μέσω των εργαλείων αναφοράς του Reporting & Analytics του Dynamics 365 για τον εντοπισμό προσωπικών δεδομένων. Περιλαμβάνει έναν Οδηγό αναφοράς για την εύκολη δημιουργία αναφορών χωρίς τη χρήση ερωτημάτων που βασίζονται σε XML ή SQL, ενώ με το Microsoft Power BI, μια αυτοματοποιημένη πλατφόρμα επιχειρηματικής ευφυΐας (BI), οι επιχειρήσεις μπορούν να ανιχνεύσουν, να αναλύσουν και να απεικονίσουν δεδομένα και να τα μοιραστούν με τρίτους.

Επιπλέον, δίνεται η δυνατότητα προστασίας της ακεραιότητας και του απορρήτου των δεδομένων αλλά και η εφαρμογή ασφαλείας βάσει ρόλων, βάσει εγγραφών ή βάσει πεδίου, για τον καθορισμό της συνολικής πρόσβασης στις πληροφορίες που έχουν οι χρήστες στον οργανισμό.

• Η ασφάλεια βάσει ρόλων στο Dynamics 365 επιτρέπει την ομαδοποίηση ενός συνόλου προνομίων που περιορίζουν τις εργασίες που μπορούν να εκτελεστούν από έναν συγκεκριμένο χρήστη. Αυτή είναι μια σημαντική δυνατότητα, ειδικά όταν οι άνθρωποι αλλάζουν ρόλους μέσα σε έναν οργανισμό.

• Η ασφάλεια που βασίζεται σε εγγραφές επιτρέπει τον περιορισμό της πρόσβασης σε συγκεκριμένες εγγραφές.

• Η ασφάλεια επιπέδου πεδίου επιτρέπει τον περιορισμό της πρόσβασης σε συγκεκριμένα πεδία «υψηλού κινδύνου», όπως πληροφορίες προσωπικής ταυτοποίησης.

Enterprise Mobility + Security (EMS) Suite

Το Enterprise Mobility + Security διαθέτει τεχνολογίες ασφαλείας που βοηθούν τις επιχειρήσεις να ανακαλύψουν, να ελέγξουν και να διαφυλάξουν τα προσωπικά δεδομένα που κατέχουν, να εντοπίσουν τυχόν «τυφλά» σημεία και να προσδιορίσουν πότε συμβαίνουν παραβιάσεις δεδομένων.

Στην πλειονότητα των παραβιάσεων δεδομένων, οι επιτιθέμενοι αποκτούν πρόσβαση στο εταιρικό δίκτυο μέσω αδύναμων, προεπιλεγμένων ή κλεμμένων διαπιστευτηρίων χρηστών. Με το συγκεκριμένο εργαλείο, η ασφάλεια αρχίζει με την προστασία της

ταυτότητας κατά την είσοδο του χρήστη, παρέχοντάς του πρόσβαση υπό όρους ανάλογα με τον κίνδυνο. Το EMS Suite προβάλλει τις δραστηριότητες των χρηστών, των συσκευών και των δεδομένων στις βάσεις δεδομένων και στο cloud και βοηθά στην προστασία των δεδομένων με επιβολή ισχυρών ελέγχων. Για την ολοκληρωμένη πληροφόρηση σχετικά με επιθέσεις και απειλές χρησιμοποιεί αναλύσεις συμπεριφοράς και τεχνολογίες ανίχνευσης αιχμής για τον εντοπισμό και την ανακάλυψη ύποπτων δραστηριοτήτων.

Office 365

Η πλατφόρμα Office 365 ενσωματώνει ασφάλεια σε όλα τα επίπεδα, από την ανάπτυξη εφαρμογών έως τα φυσικά κέντρα δεδομένων και την πρόσβαση των τελικών χρηστών. Οι εφαρμογές του Office 365 περιλαμβάνουν και ενσωματωμένα χαρακτηριστικά ασφαλείας που απλοποιούν τη διαδικασία προστασίας δεδομένων και την ευελιξία στις επιχειρήσεις να ρυθμίσουν, να διαχειριστούν και να ενσωματώσουν την ασφάλεια με τρόπους που έχουν νόημα για τις επιχειρηματικές τους ανάγκες.

Για παράδειγμα, με τη χρήση του Data Loss Prevention (DLP) στο Office και στο Office 365 μπορούν να εντοπιστούν πάνω από 80 κοινοί ευαίσθητοι τύποι δεδομένων, συμπεριλαμβανομένων των οικονομικών, ιατρικών και προσωπικά αναγνωρίσιμων πληροφοριών. Επιπλέον, το DLP επιτρέπει στους οργανισμούς να ρυθμίζουν τις ενέργειες που πρέπει να αναληφθούν κατά την ταυτοποίηση για να προστατεύσουν τις ευαίσθητες πληροφορίες και να αποτρέψουν την τυχαία αποκάλυψή τους.

Πολλοί έλεγχοι ασφαλείας είναι διαθέσιμοι από προεπιλογή. Το SharePoint και το OneDrive for Business, για παράδειγμα, χρησιμοποιούν κρυπτογράφηση για δεδομένα σε μεταφορά και σε κατάσταση αδράνειας. Με τη βοήθειά τους, οι επιχειρήσεις μπορούν να διαμορφώσουν και να αναπτύξουν ψηφιακά πιστοποιητικά για την απόκρυψη προσωπικών δεδομένων ώστε να περιορίσουν την πρόσβαση σε προσωπικά δεδομένα.

Επιπλέον, τα αρχεία καταγραφής ελέγχου του Office 365 επιτρέπουν την παρακολούθηση και τον έλεγχο των δραστηριοτήτων του χρήστη και του διαχειριστή σε όλα τα επίπεδα εργασίας στο Office 365 και βοηθούν στην έγκαιρη ανίχνευση και διερεύνηση ζητημάτων ασφάλειας και συμμόρφωσης.

SQL Server & Azure SQL Database

Οι βάσεις δεδομένων SQL Server και Azure SQL παρέχουν ελέγχους για τη διαχείριση της πρόσβασης και της εξουσιοδότησης βάσεων δεδομένων σε διάφορα επίπεδα. Συγκεκριμένα, το τείχος προστασίας του Azure SQL Database περιορίζει την πρόσβαση σε μεμονωμένες βάσεις δεδομένων στο διακομιστή βάσης δεδομένων Azure SQL, περιορίζοντας την πρόσβαση αποκλειστικά σε εξουσιοδοτημένες συνδέσεις. Ο έλεγχος ταυτότητας του SQL Server βοηθά στη διασφάλιση ότι μόνο οι εξουσιοδοτημένοι χρήστες με έγκυρα διαπιστευτήρια έχουν πρόσβαση στον διακομιστή της βάσης δεδομένων.

Το Dynamic data masking (DDM) είναι μια ενσωματωμένη δυνατότητα που μπορεί να χρησιμοποιηθεί για τον περιορισμό της ευαίσθητης έκθεσης δεδομένων, αποκρύπτοντας τα δεδομένα όταν έχουν πρόσβαση μη προνομιακοί χρήστες ή εφαρμογές. Τα καθορισμένα πεδία δεδομένων καλύπτονται από τα αποτελέσματα των ερωτημάτων, ενώ τα δεδομένα στη βάση δεδομένων παραμένουν αμετάβλητα. Για τους χρήστες του Azure SQL Database, μπορεί να ανακαλύψει αυτόματα δυνητικά ευαίσθητα δεδομένα και να προτείνει την εφαρμογή των κατάλληλων «μασκών».

Το Row-level security (RLS) είναι επίσης μια πρόσθετη ενσωματωμένη δυνατότητα που επιτρέπει στους πελάτες SQL Server και SQL Database να εφαρμόσουν περιορισμούς στην πρόσβαση των δεδομένων. Το RLS μπορεί να χρησιμοποιηθεί για να επιτρέψει την εύκολη πρόσβαση σε γραμμές σε έναν πίνακα βάσης δεδομένων, για μεγαλύτερο έλεγχο των χρηστών που έχουν πρόσβαση στα δεδομένα. Δεδομένου ότι η λογική περιορισμού πρόσβασης βρίσκεται στη βαθμίδα βάσης δεδομένων, αυτή η δυνατότητα απλοποιεί σε μεγάλο βαθμό το σχεδιασμό και την εφαρμογή της ασφάλειας εφαρμογών.

Το Always Encrypted είναι μια πρώτη βιομηχανική λειτουργία που έχει σχεδιαστεί για την προστασία ιδιαίτερα ευαίσθητων δεδομένων σε SQL Server και SQL Database. Το Always Encrypted επιτρέπει στους πελάτες να κρυπτογραφούν ευαίσθητα δεδομένα εντός των εφαρμογών του πελάτη και να μην αποκαλύπτουν ποτέ τα κλειδιά κρυπτογράφησης στη μηχανή βάσης δεδομένων. Η κρυπτογράφηση και η αποκρυπτογράφηση των δεδομένων γίνεται με διαφάνεια σε ένα πρόγραμμα οδήγησης πελάτη που είναι πάντα κρυπτογραφημένο.

Το SQL Database Threat Detection εντοπίζει ανώμαλες δραστηριότητες βάσεων δεδομένων που υποδηλώνουν πιθανές απειλές ασφαλείας στη βάση δεδομένων. Η ανίχνευση απειλών χρησιμοποιεί ένα προηγμένο σύνολο αλγορίθμων για τη συνεχή εκμάθηση και καταγραφή της συμπεριφοράς της εφαρμογής και ενημερώνει αμέσως μόλις εντοπιστεί μια ασυνήθιστη ή ύποπτη δραστηριότητα. Η ανίχνευση απειλών μπορεί να βοηθήσει την επιχείρηση να ανταποκριθεί στην απαίτηση για γνωστοποίηση της παραβίασης δεδομένων σύμφωνα με τον GDPR.

Windows & Windows Server

Τα Windows 10 και Windows Server 2016 περιλαμβάνουν πρωτοποριακές τεχνολογίες κρυπτογράφησης και λύσεις ταυτότητας και πρόσβασης που επιτρέπουν τη μετακίνηση από κωδικούς πρόσβασης σε πιο ασφαλείς μορφές ελέγχου ταυτότητας:

- Το Windows Defender Antivirus εντοπίζει γρήγορα και προστατεύει από το αναδυόμενο κακόβουλο λογισμικό και μπορεί να βοηθήσει άμεσα στην προστασία των συσκευών όταν παρατηρηθεί μια απειλή σε οποιοδήποτε μέρος του περιβάλλοντος της επιχείρησης.
- Το Windows Defender Advanced Threat Protection, επιτρέπει στις ομάδες λειτουργιών ασφαλείας να εντοπίζουν, να ερευνούν και να ανταποκρίνονται σε παραβιάσεις δεδομένων στο δίκτυο της επιχείρησης. Με το Windows Defender ATP, η επιχείρηση αποκτά προηγμένες δυνατότητες ανίχνευσης, διερεύνησης και απόκρισης με ιστορικά δεδομένα έως και 6 μηνών, ακόμη και όταν τα τελικά σημεία είναι εκτός σύνδεσης, έξω από τον τομέα δικτύου, έχουν επαναληφθεί ή δεν υπάρχουν πια. Το Windows Defender ATP βοηθά τους οργανισμούς να εκπληρώσουν μια βασική απαίτηση του GDPR, το οποίο διαθέτει σαφείς διαδικασίες ανίχνευσης, διερεύνησης και αναφοράς παραβιάσεων δεδομένων.
- Το αρχείο καταγραφής συμβάντων (Windows Event Log) παρέχει πλούσιες δυνατότητες καταγραφής συμβάντων που επιτρέπουν στους διαχειριστές να προβάλλουν καταγεγραμμένες πληροφορίες σχετικά με τις λειτουργίες του λειτουργικού συστήματος, τις εφαρμογές και τις λειτουργίες των χρηστών. Αυτό το σύστημα καταγραφής μπορεί να ρυθμιστεί ώστε να ελέγχει λεπτομερείς ενέργειες

χρηστών και εφαρμογών, συμπεριλαμβανομένης της πρόσβασης σε αρχεία, χρήση εφαρμογών και αλλαγές πολιτικών. Το αρχείο καταγραφής συμβάντων των Windows επιτρέπει επίσης στους διαχειριστές να προωθούν γεγονότα από πελάτες και διακομιστές σε κεντρική τοποθεσία για σκοπούς αναφοράς και ελέγχου.

Υπηρεσίες Microsoft Cloud

Οι υπηρεσίες cloud της Microsoft λαμβάνουν αυστηρά μέτρα για να προστατεύσουν τα δεδομένα των πελατών των εταιρειών από ακατάλληλη πρόσβαση ή χρήση από μη εξουσιοδοτημένα άτομα. Αυτά τα μέτρα περιλαμβάνουν τον περιορισμό της πρόσβασης του προσωπικού της Microsoft και των υπεργολάβων και τον προσεκτικό καθορισμό των απαιτήσεων για την ανταπόκριση σε κυβερνητικά αιτήματα για δεδομένα πελατών. Το cloud της Microsoft είναι ειδικά σχεδιασμένο για να βοηθήσει να κατανοήσουν οι επιχειρήσεις τους κινδύνους και να τους αντιμετωπίσουν, και είναι σαφώς ασφαλέστερα από τα περιβάλλοντα υπολογιστών που βρίσκονται στο χώρο εργασίας.

5.6 Συστήματα και λογισμικά της εταιρείας ORACLE

Η Oracle υπήρξε αδιαμφισβήτητος ηγέτης στην ασφάλεια των δεδομένων για δεκαετίες και έχει αναπτύξει καινοτόμα προϊόντα ασφάλειας δεδομένων για να βοηθήσει τις επιχειρήσεις να αντιμετωπίσουν επιθέσεις από διάφορους φορείς απειλών. Ήταν η πρώτη που εισήγαγε ελέγχους, όπως την «ασφάλεια επιπέδου γραμμής» (Row-level security), την κρυπτογράφηση δεδομένων (Transparent data encryption) για τον περιορισμό της προνομιακής πρόσβασης των χρηστών σε ευαίσθητες πληροφορίες, την προνομιακή ανάλυση (Privilege Analysis) και το τείχος προστασίας δεδομένων (Database Firewall).

Οι τεχνολογίες και τα προϊόντα της Oracle μπορούν να βοηθήσουν τους οργανισμούς να επιταχύνουν τη συμμόρφωση με τον GDPR αντιμετωπίζοντας τις προκλήσεις μέσω της αυτόματης, ολοκληρωμένης και αποδοτικής σουίτας τεχνολογίας και προϊόντων.

Τα προϊόντα της Oracle καλύπτουν 3 βασικές παραμέτρους για τη συμμόρφωση με τον ΓΚΠΔ: την Αξιολόγηση (Assess), την Πρόληψη (Prevent) και την Ανίχνευση (Detect), που αν συνδυαστούν κατάλληλα, οδηγούν στη Μέγιστη Προστασία (Maximum Protection) των προσωπικών δεδομένων.

1) **Αξιολόγηση (Assess)**

Όσον αφορά τον πρώτο άξονα, δηλαδή την Αξιολόγηση των κινδύνων ασφαλείας, το άρθρο 35 του νέου Κανονισμού προβλέπει εκτίμηση των επιπτώσεων για την προστασία των δεδομένων για ορισμένους τύπους επεξεργασίας δεδομένων. Μία από τις προκλήσεις είναι να προσδιοριστεί τι πρέπει να αξιολογηθεί, επειδή οι εφαρμογές βάσεων δεδομένων περιέχουν συνήθως πολλά σημεία εισόδου και έχουν προσωπικά δεδομένα κατανεμημένα σε πολλαπλές στήλες και πίνακες με «χαλαρά» καθορισμένο έλεγχο πρόσβασης.

Η τεχνολογία και τα προϊόντα της Oracle Database Security βοηθούν στην αντιμετώπιση αυτής της πρόκλησης παρέχοντας εργαλεία για την αξιολόγηση πολλών πτυχών των δεδομένων της εφαρμογής, όπως:

- Ανακάλυψη πινάκων και στηλών που περιέχουν «προσωπικά δεδομένα»
- Διαμόρφωση των βάσεων δεδομένων για τον προσδιορισμό του συνολικού προφίλ ασφαλείας
- Ανάλυση των ρόλων και των δικαιωμάτων των βάσεων δεδομένων για τον καθορισμό του τρόπου με τον οποίο οι ελεγκτές, οι επεξεργαστές, τα τρίτα μέρη, τα δεδομένα και οι παραλήπτες μπορούν να έχουν πρόσβαση σε προσωπικά δεδομένα

Τα εργαλεία που παρέχει η Oracle για την αξιολόγηση είναι:

- **Oracle Application Data Modeling:** Αξιολόγηση ευαίσθητων δεδομένων

Το συγκεκριμένο εργαλείο αυτοματοποιεί τον εντοπισμό των στηλών που περιέχουν ευαίσθητα δεδομένα προσωπικού χαρακτήρα και τις αντίστοιχες σχέσεις γονέα-παιδιού που ορίζονται στη βάση δεδομένων, χρησιμοποιώντας ενσωματωμένα πρότυπα, όπως αριθμούς πιστωτικών καρτών και εθνικά αναγνωριστικά, για να δειγματοληφθούν τα δεδομένα και να προσδιοριστούν οι ευαίσθητες στήλες. Μόλις εντοπιστούν τα προσωπικά δεδομένα, τότε είναι δυνατή η εφαρμογή των σχετικών

ελέγχων, είτε προληπτικά είτε αναγνωριστικά. Το αποτέλεσμα είναι ένα πλήρες σύνολο «ευαίσθητων» στηλών μαζί με τις σχέσεις τους, εξασφαλίζοντας ότι η ακεραιότητα της εφαρμογής διατηρείται από τους ελέγχους προστασίας δεδομένων.

- **Oracle Database Vault Privilege Analysis:** Αξιολόγηση της Προνομιακής Πρόσβασης

Μόλις προσδιοριστούν τα προσωπικά δεδομένα, είναι σημαντικό να εντοπιστούν οι χρήστες, συμπεριλαμβανομένων και των διαχειριστών, οι οποίοι μπορούν όχι μόνο να έχουν πρόσβαση αλλά και να επεξεργάζονται τα προσωπικά δεδομένα. Ωστόσο, κατά τη διάρκεια της διαδικασίας σχεδιασμού και συντήρησης της εφαρμογής, ενδέχεται να χορηγηθούν εκ παραδρομής πρόσθετα δικαιώματα στους χρήστες. Έτσι, με τη χρήση της Oracle Database Vault Privilege Analysis επιτυγχάνεται αύξηση της ασφάλειας των εφαρμογών, αφού αναγνωρίζει τα πραγματικά δικαιώματα των χρηστών που χρησιμοποιούνται κατά την εκτέλεση. Τα δικαιώματα που έχουν αναγνωριστεί ως αχρησιμοποίητα μπορούν να αξιολογούνται για πιθανή ανάκληση, συμβάλλοντας στην επίτευξη ενός «μοντέλου ελαχίστων προνομίων».

- **Oracle Database Lifecycle Management Pack:** Αξιολόγηση της ρύθμισης των παραμέτρων της βάσης δεδομένων

Όλες οι βάσεις δεδομένων αποτελούνται από ένα πλήθος παραμέτρων διαμόρφωσης για να ανταποκρίνονται στις ευρείες απαιτήσεις ασφαλείας. Έτσι, οι επιχειρήσεις πρέπει να ελέγξουν όλες τις ρυθμίσεις των βάσεων δεδομένων που σχετίζονται με την ασφάλεια, συμπεριλαμβανομένων των προεπιλεγμένων κωδικών πρόσβασης των λογαριασμών, την κατάσταση και τα προφίλ του λογαριασμού. Με το συγκεκριμένο εργαλείο, μπορούν να εκτελεστούν περισσότεροι από 100 έλεγχοι πολιτικής στις βάσεις δεδομένων της Oracle, να εντοπιστούν οι τάσεις και να πραγματοποιηθούν εξατομικευμένοι έλεγχοι διαμόρφωσης για να συμπληρώσουν τους ελέγχους που παρέχει η Oracle.

- **Oracle Database Security Assessment Tool:** Αξιολόγηση του προφίλ ασφάλειας των βάσεων δεδομένων

Σύμφωνα με το άρθρο 36 του GDPR, ανάλογα με την ευαισθησία των δεδομένων, οι επιχειρήσεις ενδέχεται να χρειαστούν την έγκριση μιας Εποπτικής Αρχής πριν από την

επεξεργασία ορισμένων προσωπικών πληροφοριών. Η πρόκληση είναι να δημιουργηθεί γρήγορα μια ευδιάκριτη έκθεση αναφοράς σχετικά με την προστασία της ιδιωτικής ζωής και της ασφάλειας για να υποβληθεί στην Εποπτική Αρχή. Με το συγκεκριμένο εργαλείο αναλύεται όχι μόνο η διαμόρφωση αλλά και ο τρόπος εφαρμογής ορισμένων πολιτικών ασφαλείας. Στη συνέχεια, παρουσιάζονται τα ευρήματά του ιεραρχημένα ώστε να μπορούν να υποβληθούν στην Εποπτική Αρχή. Αυτές οι πληροφορίες μπορούν να συμβάλουν σημαντικά στη μελέτη της εκτίμησης των επιπτώσεων στην προστασία των δεδομένων.

2) **Πρόληψη (Prevent)**

Η Oracle παρέχει μια εύκολη στη χρήση σειρά προληπτικών ελέγχων που βοηθά τους οργανισμούς να εφαρμόσουν τις βασικές προληπτικές τεχνικές σύμφωνα με το GDPR, συμπεριλαμβανομένης της κρυπτογράφησης, της ψευδωνυμοποίησης, της ανωνυμίας, του προνομιακού ελέγχου των χρηστών, του λεπτομερούς ελέγχου πρόσβασης και της απόκρυψης δεδομένων.

- **Transparent Data Encryption (TDE):** Κρυπτογράφηση δεδομένων

Το άρθρο 32 και η αιτιολογική σκέψη 83 του GDPR συνιστούν την κρυπτογράφηση ως μία από τις τεχνικές προστασίας δεδομένων. Μία από τις προκλήσεις που αντιμετωπίζουν οι οργανισμοί κατά την εφαρμογή της κρυπτογράφησης δεδομένων είναι η διασφάλιση όχι μόνο της κρυπτογράφησης των προσωπικών δεδομένων στους πίνακες, αλλά και των αντιγράφων ασφαλείας και των αρχείων καταγραφής. Το συγκεκριμένο εργαλείο, αντιμετωπίζει αυτή την πρόκληση με την κρυπτογράφηση όλων των δεδομένων απευθείας στη βάση δεδομένων. Κρυπτογραφεί τα δεδομένα αυτόματα όταν είναι καταγεγραμμένα στο χώρο αποθήκευσης, συμπεριλαμβανομένων των αντιγράφων ασφαλείας, των εξαχθέντων δεδομένων και των αρχείων καταγραφής. Τα κρυπτογραφημένα δεδομένα αντίστοιχα αποκρυπτογραφούνται όταν διαβάζονται από το χώρο αποθήκευσης. Αυτή η δυνατότητα αυτόματης κρυπτογράφησης-αποκρυπτογράφησης σε επίπεδο βάσης δεδομένων καθιστά τη λύση διαφανή σε εφαρμογές βάσης δεδομένων. Τα στοιχεία ελέγχου πρόσβασης που επιβάλλονται στη βάση δεδομένων και τα επίπεδα εφαρμογής παραμένουν σε ισχύ. Τα ερωτήματα SQL δεν τροποποιούνται ποτέ και, επομένως, δεν απαιτείται κανένας κώδικας εφαρμογής ή αλλαγές διαμόρφωσης. Η

διαδικασία κρυπτογράφησης και αποκρυπτογράφησης είναι εξαιρετικά γρήγορη, καθώς το TDE αξιοποιεί τις βελτιστοποιήσεις της κρυπτογράφησης δεδομένων της Oracle Database και χρησιμοποιεί επιτάχυνση υλικού βασισμένη στους επεξεργαστές της Intel (AES-NI) και της Oracle (SPARC).

- **Oracle Key Vault (OKV):** Διαχείριση κεντρικών κλειδιών κρυπτογράφησης

Το Oracle Key Vault (OKV) παρέχει κεντρικό έλεγχο στα δεδομένα που είναι κρυπτογραφημένα με το προηγούμενο εργαλείο (TDE). Το TDE παρέχει διαχείριση κλειδιού κρυπτογράφησης δύο επιπέδων, με κλειδιά κρυπτογράφησης δεδομένων και κύρια κλειδιά κρυπτογράφησης. Τα κύρια κλειδιά κρυπτογράφησης μπορούν να ελέγχονται κεντρικά και να διαχειρίζονται με τη χρήση του Oracle Key Vault, που επιτρέπει την ταχεία ανάπτυξη κρυπτογράφησης, τη δυνατότητα αναστολής της πρόσβασης στο κύριο κλειδί και την αποσαφήνιση των κρυπτογραφημένων δεδομένων σε περίπτωση παραβίασης δεδομένων ή ύποπτης δραστηριότητας.

- **Oracle Database Network Encryption and Data Integrity:** Κρυπτογράφηση δεδομένων σε μεταφορά

Για να πληρούνται οι απαιτήσεις του άρθρου 32 του GDPR για την προστασία των προσωπικών δεδομένων στη μετάδοση, η συγκεκριμένη εφαρμογή βοηθά τις επιχειρήσεις και τους υπευθύνους να κρυπτογραφούν δεδομένα και να αποτρέπουν την απώλεια δεδομένων, την επανάληψη και τις ενδιάμεσες επιθέσεις. Η Oracle παρέχει κρυπτογράφηση δικτύου με κρυπτογράφηση μη αυτόματου δικτύου και κρυπτογράφηση δικτύου με βάση την ασφάλεια μεταφοράς επιπέδου (TLS) για οργανισμούς με υποδομή PKI. Η Oracle παρέχει επίσης υποστήριξη για παγκόσμιους αλγόριθμους κρυπτογράφησης, όπως το AES.

- **Data Redaction:** Ψευδωνυμοποίηση δεδομένων

Βάσει του άρθρου 32 και της αιτιολογικής σκέψης 28 του GDPR συνίσταται η ψευδωνυμοποίηση. Για παράδειγμα, ένα χαρακτηριστικό γνώρισμα σε μια στήλη πίνακα που αντιπροσωπεύει ένα υποκείμενο δεδομένων μπορεί να τροποποιηθεί ή ένας πίνακας που περιέχει πολλαπλά χαρακτηριστικά που μπορούν να βοηθήσουν στη δημιουργία του συνδέσμου με το αρχικό υποκείμενο δεδομένων μπορεί να προστατευθεί με τέτοιο τρόπο ώστε να μην είναι δυνατή η σύνδεση του συνόλου δεδομένων με το υποκείμενο των δεδομένων.

Μία από τις προκλήσεις κατά την εφαρμογή ψευδωνυμοποίησης είναι ο τρόπος υποκλοπής ερωτημάτων εφαρμογής στη βάση δεδομένων και η μετατροπή των δεδομένων χωρίς να επηρεάζεται η βάση δεδομένων της εφαρμογής ή της βάσης δεδομένων.

Η χρήση του Data Redaction μπορεί να βοηθήσει στην αντιμετώπιση αυτής της ανησυχίας, παρέχοντας επιλεκτική και άμεση επεξεργασία των προσωπικών δεδομένων στα αποτελέσματα των ερωτημάτων SQL πριν επιστρέψει στις εφαρμογές, ώστε οι μη εξουσιοδοτημένοι χρήστες να μην μπορούν να δουν τα δεδομένα. Επιπλέον, ελαχιστοποιεί τις αλλαγές στις εφαρμογές επειδή δεν μεταβάλλει τα πραγματικά δεδομένα, διατηρώντας παράλληλα τον αρχικό τύπο δεδομένων και τη μορφοποίηση, όταν τα μετασχηματισμένα δεδομένα επιστρέφονται στην εφαρμογή. Το συγκεκριμένο πρόγραμμα δεν επηρεάζει τις λειτουργικές δραστηριότητες της βάσης δεδομένων, όπως η δημιουργία αντιγράφων ασφαλείας και η επαναφορά, η αναβάθμιση και η ενημερωμένη έκδοση κώδικα, καθώς δεν μεταβάλλονται τα σταθερά δεδομένα. Οι πολιτικές της Oracle Data Redaction επιβάλλονται απευθείας στον πυρήνα της βάσης δεδομένων, οδηγώντας σε αυστηρότερη ασφάλεια και καλύτερη απόδοση. Επιτρέπει επίσης στο διαχειριστή να καθορίσει τις συνθήκες υπό τις οποίες τα πραγματικά δεδομένα πρέπει να επιστραφούν στους εξουσιοδοτημένους αποδέκτες.

- **Oracle Data Masking and Subsetting:** Ανωνυμοποίηση και ελαχιστοποίηση

Το συγκεκριμένο εργαλείο μπορεί να χρησιμοποιηθεί για την αποδέσμευση των προσωπικών δεδομένων του Υπευθύνου Προστασίας Δεδομένων και για τον περιορισμό της έκθεσης προσωπικών δεδομένων σε λιγότερο προστατευμένα περιβάλλοντα. Μία από τις προκλήσεις της ανωνυμοποίησης είναι ότι αν δεν γίνει σωστά, τα μη-ταυτοποιημένα ή κωδικοποιημένα δεδομένα ενδέχεται να μην είναι χρησιμοποιήσιμα για τους επεξεργαστές και τους προγραμματιστές. Επιπλέον, θα μπορούσε να σπάσει την ακεραιότητα των δεδομένων των εφαρμογών και των βάσεων δεδομένων.

Το Oracle Data Masking and Subsetting αντιμετωπίζει αυτές τις προκλήσεις παρέχοντας μια ολοκληρωμένη και επεκτάσιμη βιβλιοθήκη με μορφές ανωνυμοποίησης και κάλυψης, μετασχηματισμούς και πρότυπα εφαρμογών. Τα προσωπικά δεδομένα και άλλες σημαντικές πληροφορίες, όπως αριθμοί πιστωτικών

καρτών, εθνικά αναγνωριστικά στοιχεία και άλλες πληροφορίες προσωπικής ταυτοποίησης (PII), μπορούν εύκολα να καλυφθούν με μια άλλης μορφής βιβλιοθήκη κάλυψης και ανωνυμοποίησης.

Επιπλέον, παρέχει αυτοματοποιημένη δυνατότητα εντοπισμού, διαγραφής ή εξαγωγής ενός υποσυνόλου δεδομένων από ένα μεγάλο σύνολο δεδομένων, διατηρώντας την ακεραιότητα του συνόλου δεδομένων, έτσι ώστε να συμβαδίζει με το άρθρο 5 του GDPR που απαιτεί την «μείωση» του όγκου συλλογής, επεξεργασίας και διατήρησης των προσωπικών δεδομένων. Έτσι τα δεδομένα μπορούν να μοιραστούν με ασφάλεια με τους επεξεργαστές ή τρίτους συνεργάτες, διασφαλίζοντας παράλληλα τη συνέχεια των εφαρμογών.

- **Oracle Database Vault:** Έλεγχος των Προνομιακών Χρηστών και επιβολή του Διαχωρισμού των Υποχρεώσεων

Το Oracle Database Vault ενσωματώνει τον έλεγχο πρόσβασης των χρηστών εντός της βάσης δεδομένων της Oracle, δημιουργώντας πυρήνες που περιορίζουν την πρόσβαση στα δεδομένα μόνο σε εξουσιοδοτημένο προσωπικό και υπό ορισμένες συνθήκες. Ταυτόχρονα επιτρέπει στις βάσεις δεδομένων να εκτελούν τις κανονικές λειτουργικές τους δραστηριότητες, όπως την επιδιόρθωση, την εισαγωγή, την εξαγωγή και την δημιουργία αντιγράφων ασφαλείας χωρίς πρόσβαση στα προσωπικά δεδομένα. Για παράδειγμα, ο χρήστης της εφαρμογής θα μπορούσε να διαβάσει όλα τα χαρακτηριστικά γνωρίσματα των δεδομένων (σε πολλούς πίνακες) ενώ οι διαχειριστές βάσεων δεδομένων ή άλλοι χρήστες θα μπορούσαν να δουν μόνο τα κύρια χαρακτηριστικά στον μητρικό πίνακα, καθιστώντας έτσι δύσκολη τη σύνδεση με το υποκείμενο των δεδομένων.

- **Oracle Virtual Private Database:** Επιλεκτική απόκρυψη δεδομένων

Η συγκεκριμένη εφαρμογή παρέχει προσωρινές προληπτικές τεχνικές, όπως φιλτράρισμα και απόκρυψη ενός υποσυνόλου δεδομένων για την αντιμετώπιση περιπτώσεων υποκλοπής δεδομένων ή εμφάνισής τους σε μη εξουσιοδοτημένους χρήστες. Υπολογίζει μια πρόβλεψη ή μια ρήτρα που προσαρτάται αυτόματα στις εισερχόμενες εντολές SQL, περιορίζοντας την πρόσβαση σε γραμμές και στήλες μέσα στον πίνακα. Αυτό περιορίζει το μέγεθος της ζημιάς, σε περίπτωση που υπάρχει ένα

σφάλμα προγραμματισμού που επιτρέπει στους χρήστες να μην βλέπουν μόνο τα δικά τους δεδομένα, αλλά και τα δεδομένα άλλων χρηστών.

- **Oracle Label Security:** Έλεγχος Πρόσβασης

Το Oracle Label Security (OLS) βοηθά τους οργανισμούς να ταξινομούν τα στοιχεία Προσωπικών Δεδομένων αναθέτοντας ετικέτες με βάση την εμπιστευτικότητα (όπως οι δημόσιες, ευαίσθητες ή εξαιρετικά εμπιστευτικές πληροφορίες) ή περιοχές (όπως Βόρεια Αμερική, Ευρώπη ή Ασία-Ειρηνικός). Το OLS καθιστά ευκολότερη τη δήλωση στοιχείων ελέγχου πρόσβασης βάσει ταξινόμησης δεδομένων, απλοποιώντας έτσι το μοντέλο πολυεπίπεδης ασφάλειας (MLS), το οποίο είναι συνήθως υποχρεωτικό για πολλές κυβερνητικές και αμυντικές οργανώσεις.

- **Oracle Real Application Security (RAS):** Διευκόλυνση της ολοκλήρωσης του ελέγχου πρόσβασης

Σύμφωνα με την αιτιολογική σκέψη 64 του GDPR, ο υπεύθυνος επεξεργασίας πρέπει να επαληθεύσει την ταυτότητα του αιτούντος υποκειμένου δεδομένων στο πλαίσιο των ηλεκτρονικών υπηρεσιών, προτού δώσει πρόσβαση στα προσωπικά δεδομένα. Στις σύγχρονες εφαρμογές τριών επιπέδων, η επαλήθευση του διαδικτυακού πλαισίου της ταυτότητας ενός χρήστη αποτελεί πρόκληση, επειδή συνήθως οι εφαρμογές και οι διακομιστές εφαρμογών συνδέονται στη βάση δεδομένων ως ένας χρήστης μιας βάσης δεδομένων που καθιστά δύσκολο τον εντοπισμό του δημιουργού χρήστη.

Το Oracle Real Application Security (RAS) αντιμετωπίζει αυτή την ανησυχία παρέχοντας ένα μοντέλο εξουσιοδότησης βάσει πολιτικής που αναγνωρίζει τους χρήστες, τα δικαιώματα και τους ρόλους σε επίπεδο εφαρμογής μέσα στη βάση δεδομένων. Με την ενσωματωμένη υποστήριξη για την ασφαλή διάδοση των πληροφοριών των χρηστών στη βάση δεδομένων, το RAS επιτρέπει στις πολιτικές ασφαλείας των δεδομένων να εκφράζονται απευθείας από την άποψη των χρηστών της εφαρμογής, των ρόλων τους και των πλαισίων ασφαλείας. Μέσω των ACL, το RAS μπορεί να ελέγχει ποιος μπορεί να αποκτήσει πρόσβαση σε προσωπικά δεδομένα.

3) Παρακολούθηση εντοπισμού παραβιάσεων (DETECT)

Τα άρθρα 30 και 33 του GDPR ορίζουν ότι οι οργανισμοί πρέπει να τηρούν αρχείο των δραστηριοτήτων επεξεργασίας τους.

Αυτό μπορεί να επιτευχθεί μόνο με τη συνεχή παρακολούθηση και τον έλεγχο δραστηριοτήτων σχετικά με τα προσωπικά δεδομένα. Αυτά τα δεδομένα μπορούν στη συνέχεια να χρησιμοποιηθούν για την έγκαιρη ενημέρωση των αρχών σε περίπτωση παραβίασης. Εκτός από τον υποχρεωτικό έλεγχο και τις έγκαιρες ειδοποιήσεις, ο GDPR απαιτεί επίσης οι οργανισμοί να τηρούν τα αρχεία ελέγχου υπό τον έλεγχό τους. Ένας κεντρικός έλεγχος των αρχείων ελέγχου αποτρέπει τους εισβολείς ή τους κακόβουλους χρήστες να καλύψουν τα ίχνη της ύποπτης δραστηριότητάς τους διαγράφοντας τα αρχεία τοπικού ελέγχου.

Η Oracle Database Security παρέχει έναν εκτεταμένο μηχανισμό συλλογής και υποβολής εκθέσεων για την κάλυψη των απαιτήσεων παρακολούθησης του GDPR.

Το Oracle Audit Vault and Database Firewall (AVDF) είναι μια πλατφόρμα ελέγχου και προστασίας νέας γενιάς που παρέχει ολοκληρωμένη και ευέλικτη παρακολούθηση μέσω της ενοποίησης δεδομένων ελέγχου από βάσεις δεδομένων Oracle και μη Oracle, λειτουργικά συστήματα, συστήματα αρχείων και εφαρμογή συγκεκριμένων δεδομένων ελέγχου. Ταυτόχρονα, το Oracle Database Firewall μπορεί να λειτουργήσει ως η πρώτη γραμμή υπεράσπισης στο δίκτυο, επιβάλλοντας την αναμενόμενη συμπεριφορά των εφαρμογών, βοηθώντας στην πρόληψη της εισόδου SQL, της παράκαμψης εφαρμογής και άλλων κακόβουλων δραστηριοτήτων από την πρόσβαση στη βάση δεδομένων.

Επιπλέον, μπορεί να ενοποιήσει τα δεδομένα ελέγχου από πολλαπλές βάσεις δεδομένων και να παρακολουθήσει την κυκλοφορία των εντολών που δεν είναι εξουσιοδοτημένες. Οι υπεύθυνοι προστασίας δεδομένων και οι υπεύθυνοι επεξεργασίας μπορούν να καθορίσουν τις συνθήκες υπό τις οποίες μπορούν να εγγραφούν οι ειδοποιήσεις σε πραγματικό χρόνο, προσπαθώντας να προσελκύσουν τους εισβολείς με τις μη φυσιολογικές δραστηριότητες. Δεκάδες αναφορές σε συνδυασμό με μια προσαρμοσμένη διεπαφή αναφοράς, παρέχουν μια ολοκληρωμένη εικόνα της δραστηριότητας της βάσης δεδομένων σε ολόκληρη την επιχείρηση, είτε

παρατηρείται μέσω του δικτύου είτε μέσω των αρχείων καταγραφής ελέγχου. Το Oracle AVDF υποστηρίζει βάσεις δεδομένων Oracle, Microsoft SQL Server, IBM DB2 για LUW, SAP Sybase ASE και Oracle MySQL.

4) **Μέγιστη προστασία με διαφάνεια, ακρίβεια, απόδοση και κλίμακα (MAXIMUM PROTECTION)**

Δεδομένου ότι οι σύγχρονες εφαρμογές περιέχουν πολλά στοιχεία, όπως πύλες ιστού, διακομιστές μεσολάβησης, διακομιστές εφαρμογών και διακομιστές βάσεων δεδομένων, ο καθορισμός και η εφαρμογή όλων των ελέγχων ασφαλείας σε περιβάλλον πολλαπλών στρωμάτων είναι ένα δύσκολο έργο. Η συγκέντρωση όλων αυτών των διαφορετικών ελέγχων ασφάλειας και τεχνολογιών από διάφορους προμηθευτές αποτελεί πρόκληση ενοποίησης και διαχείρισης για τους οργανισμούς. Η Oracle Database Security αντιμετωπίζει αυτή την πρόκληση ορίζοντας τα στοιχεία ελέγχου πιο κοντά στα δεδομένα και επιβάλλοντας την ασφάλεια στις βάσεις δεδομένων. Οι περισσότεροι έλεγχοι προστασίας δεδομένων που προσφέρει η Oracle ενσωματώνονται στη βάση δεδομένων της Oracle, απλοποιώντας έτσι το σχεδιασμό και την ανάπτυξη, βελτιώνοντας την ακρίβεια της προστασίας και ελαχιστοποιώντας την κλίμακα της επίθεσης.

Το Oracle Key Vault και το Oracle Audit Vault and Database Firewall συμπληρώνουν την προστασία δεδομένων στην βάση δεδομένων, συγκεντρώνοντας τον έλεγχο και τη διαχείριση. Είτε πρόκειται για χιλιάδες κλειδιά κρυπτογράφησης και εκατομμύρια αρχεία ελέγχου, είτε για διαφορετικούς τύπους πολιτικών ασφαλείας, αυτά τα στοιχεία μπορούν να διαχειρίζονται κεντρικά, απλοποιώντας σε μεγάλο βαθμό τις εργασίες που σχετίζονται με τη διοίκηση. Επίσης μέσω του Oracle Enterprise Manager (EM) παρέχεται ένα ενιαίο γραφικό περιβάλλον για τη διαχείριση των στοιχείων της Oracle Database Security.Το σημαντικότερο είναι ότι όλα τα στοιχεία ελέγχου της Oracle Database Security είναι καλά ενσωματωμένα για την προστασία των Προσωπικών Δεδομένων.

Στην Ελλάδα, πρόσφατο παράδειγμα αξιοποίησης των εργαλείων της Oracle είναι η συνεργασία της με την εταιρεία παροχής τηλεπικοινωνιών Wind Ελλάς, η οποία

ολοκλήρωσε επιτυχώς ένα έργο στρατηγικής σημασίας σχετικά με το νέο Γενικό Κανονισμό για την Προστασία των Δεδομένων (GDPR) της ΕΕ.

Το έργο περιελάμβανε, στην πρώτη του φάση, υλοποίηση τεχνολογίας κρυπτογράφησης της Oracle Database στα πιο κρίσιμης σημασίας IT συστήματα της Wind, σύμφωνα με το Αρθρο 32 του νέου Κανονισμού, και στη συνέχεια υλοποίηση τεχνολογίας Oracle Cloud Access Security Broker Service (CASB) για την παρακολούθηση κινδύνου και τη διακυβέρνηση κρίσιμης σημασίας SaaS εφαρμογών, καθώς και την ανακάλυψη Shadow IT εφαρμογών. Το έργο αυτό ήταν μέρος της συνολικής υπάρχουσας στρατηγικής της WIND για τη συμμόρφωσή της με το πλαίσιο GDPR της ΕΕ και πραγματοποιήθηκε με τη συνεργασία του τμήματος Συμβουλευτικών Υπηρεσιών της Oracle.

Τα εργαλεία που επέλεξε η Wind είναι το Oracle CASB Service και το Oracle Advanced Security για την ελαχιστοποίηση της έκθεσης σε κίνδυνο και τη διασφάλιση του ελέγχου, που θα της επιτρέψουν να εντοπίσει τυχόν απειλές, ενισχύοντας τα χαρακτηριστικά ασφαλείας του περιβάλλοντος cloud αναφορικά και με το νέο Κανονισμό, με την ελάχιστη δυνατή επίδραση στην απόδοση των IT συστημάτων της.

5.7 Άλλες λύσεις και υπηρεσίες

Εκτός των προαναφερθέντων εφαρμογών και λύσεων για την προσαρμογή των συστημάτων των επιχειρήσεων στα νέα δεδομένα του Κανονισμού, υπάρχουν και εταιρείες όπως για παράδειγμα η KPMG, που αναλαμβάνουν ρόλο συμβούλου, διαμεσολαβητή και εκπαιδευτή στη συμμόρφωση των επιχειρήσεων με τον ΓΚΠΔ.

Τέτοιου είδους εταιρείες, με τη θέσπιση του Κανονισμού, δραστηριοποιούνται άμεσα προσπαθώντας καταρχήν να κατανοήσουν σε βάθος τις παραμέτρους του Κανονισμού, εγείροντας ερωτήματα και λύσεις. Στη συνέχεια, ξεκινούν την εφαρμογή αυτών των πρακτικών και την συμμόρφωση στις επιταγές του Κανονισμού στον δικό τους οργανισμό, με πρωταρχικό μέλημα την εκπαίδευση του προσωπικού τους, η οποία πραγματοποιείται σε τακτικά χρονικά διαστήματα. Με αυτό τον τρόπο δοκιμάζουν στην πράξη την εφαρμογή και τα αποτελέσματα του Κανονισμού, ώστε να μπορέσουν μετέπειτα να συνεισφέρουν στην περαιτέρω επιμόρφωση και των

υπολοίπων που διατηρούν προσωπικά δεδομένα, όπως κοινωνικούς εταίρους, υπαλλήλους, συνεργάτες, πελάτες, οποιουσδήποτε τρίτους με τους οποίους έχουν επικοινωνίες.

5.5.1 Παροχή υπηρεσιών της εταιρείας PRIORITY σε συνεργασία με την ALGOSYSTEMS

Η εταιρεία Priority εξειδικεύεται από το 1995 στον τομέα της ανάλυσης και βελτίωσης των επιχειρησιακών διαδικασιών που ικανοποιούν απαιτήσεις κανονιστικής συμμόρφωσης αλλά και προσθέτουν αξία στην επιχείρηση, ιδιαίτερα στον τομέα της διακυβέρνησης πληροφορικής, της ασφάλειας δεδομένων και της αξιολόγησης κινδύνων.

Η Priority μπορεί να υποστηρίξει τους πελάτες της με τις ακόλουθες υπηρεσίες:

- Διάγνωση και αποτύπωση του επιπέδου συμμόρφωσης με τον GDPR με δημιουργία του αρχείου δραστηριοτήτων.
- Αξιολόγηση επιπτώσεων (DPIA) σχετικά με την προστασία των δεδομένων για τον εντοπισμό των σημαντικότερων κινδύνων.
- Πρόταση μέτρων αντιμετώπισης και σχεδίου συμμόρφωσης με τον Κανονισμό, συνεχή υποστήριξη και καθοδήγηση στην υλοποίησή του.
- Ανάπτυξη όλων των απαιτούμενων πολιτικών και διαδικασιών προστασίας προσωπικών δεδομένων, σε ένα πλήρες Σύστημα Διαχείρισης Προσωπικών Δεδομένων.
- Ορισμό εξωτερικού DPO ή υποστήριξη του υφιστάμενου DPO.
- Επιθεωρήσεις ετοιμότητας ως προς τον GDPR.
- Προετοιμασία για πιστοποίηση και επαλήθευση της συμμόρφωσης με βάση διεθνή πρότυπα.

Από την άλλη, η εταιρεία Algosystems, έχει υλοποιήσει δεκάδες έργα αναφορικά με την ασφάλεια των δεδομένων μιας επιχείρησης και εξακολουθεί να καλύπτει τις ολοένα αυξανόμενες ανάγκες σε τεχνολογικές λύσεις των πελατών της. Με τη συνεργασία μεταξύ Algosystems και Priority, επιτυγχάνεται η παροχή μιας συνολικής λύσης αναφορικά με τη συμμόρφωση στον GDPR, αφού η Priority αναλαμβάνει την

εκπόνηση μελέτης για το εντοπισμό των σημείων που η εταιρεία βρίσκεται εκτεθειμένη έναντι του GDPR και η Algosystems προτείνει τεχνολογικές λύσεις κάλυψης των κενών που προέκυψαν από τη μελέτη και αναλαμβάνει την εκτέλεσή τους.

5.5.2 Παροχή υπηρεσιών της εταιρείας SYNTAX

Ο όμιλος SYNTAX επικεντρώνεται στην ενεργοποίηση και την εξέλιξη της επιχειρηματικής δραστηριότητας των πελατών, συνδυάζοντας την τεχνολογία λογισμικού τελευταίας τεχνολογίας και τις βέλτιστες πρακτικές. Παρέχει συμβουλευτικές υπηρεσίες, σχεδιασμό λύσεων, ενεργοποίηση, εξωτερική ανάθεση και διαχειριζόμενες υπηρεσίες.

Στην παροχή υποστήριξης σχετικά με τον GDPR, επιδιώκει να συνεισφέρει στα προβλήματα που αντιμετωπίζουν οι οργανισμοί, καθώς οι περισσότεροι δεν γνωρίζουν τι πληροφορίες διατηρούν και ποιες από αυτές έχουν κάποια αξία, πού βρίσκονται τα ευαίσθητα δεδομένα, ούτε ποιος έχει πρόσβαση σε αυτά και όταν υπάρχει ανάγκη αναζήτησης, αυτή είναι ιδιαίτερα χρονοβόρα με τα αποτελέσματα να μην είναι πλήρη ούτε ορθά.

Λαμβάνοντας υπόψη όχι μόνο το νέο κανονιστικό πλαίσιο, αλλά και τις ανάγκες του οργανισμού όπως αυτές καθορίζονται από το επιχειρησιακό περιβάλλον, η SYNTAX εφαρμόζει μια δομημένη προσέγγιση τεσσάρων σταδίων:

1) Ανακάλυψη (Discover), όπου “ανακαλύπτονται” τα δεδομένα του οργανισμού, αντιστοιχούνται σε ιδιοκτήτες και κατηγοριοποιούνται ανάλογα με την αξία τους και το βαθμό ευαισθησίας τους.
2) Προστασία (Protect), όπου υλοποιούνται μηχανισμοί προστασίας των δεδομένων τόσο αναφορικά με την διατήρηση της εμπιστευτικότητας και ακεραιότητας, όσο και από μη εξουσιοδοτημένη πρόσβαση.
3) Έλεγχος (Control), όπου υλοποιούνται μηχανισμοί ελέγχου της πρόσβασης στην πληροφορία και της αποτροπής διαρροών και μη ορθής χρήσης.
4) Αναζήτηση (Investigate), όπου υλοποιούνται μηχανισμοί παρακολούθησης των παραπάνω, καθώς και αναζήτησης πληροφοριών.

Τα παραπάνω στάδια, η υλοποίηση των οποίων αποτελεί συνδυασμό τεχνολογικών λύσεων και συμβουλευτικών υπηρεσιών, υλοποιούνται βασισμένα τόσο σε υπηρεσίες

στρατηγικού σχεδιασμού και εξασφάλισης (assurance), όσο και παροχής υπηρεσιών Interim (Chief) Data Protection Officer.

Επιπλέον, η SYNTAX Πληροφορική, με την παραπάνω προσέγγιση δίνει στον οργανισμό, εκτός της δυνατότητας συμμόρφωσης με το νέο κανονιστικό πλαίσιο, τη δυνατότητα βέλτιστης αξιοποίησης την επιχειρησιακής πληροφορίας. Ουσιαστικά, προσφέρει στον οργανισμό τη δυνατότητα μεγιστοποίησης του ROI (Return on Information), σε αντιδιαστολή με το γνωστό Return on Investment

Η μεγιστοποίηση της προσδοκώμενης αξίας των δεδομένων του οργανισμού επιτυγχάνεται μέσω της:

1) Ελαχιστοποίησης των φυσικών εγγραφών.
2) Ελαχιστοποίησης των διατηρούμενων δεδομένων στο αναγκαίο για την υποστήριξη των επιχειρησιακών λειτουργιών και στόχων.
3) Δημιουργίας χρονοπρογραμματισμού διατήρησης των απαραίτητων δεδομένων σε συμμόρφωση με το κανονιστικό πλαίσιο.
4) Δημιουργίας ενός επιχειρησιακού σχεδίου κατηγοριοποίησης / ταξινόμησης των δεδομένων.
5) Ελαχιστοποίησης των κινδύνων κανονιστικής μη συμμόρφωσης.

5.5.3 Παροχή υπηρεσιών της εταιρείας INTRACOM TELECOM

Η Intracom Telecom, ένας από τους κορυφαίους κατασκευαστές τηλεπικοινωνιακών συστημάτων και προμηθευτής ολοκληρωμένων λύσεων και επαγγελματικών υπηρεσιών για τηλεπικοινωνιακούς οργανισμούς σταθερής και κινητής, έχει δημιουργήσει μια έμπειρη και αποδοτική ομάδα εμπειρογνωμόνων, για την καλύτερη υποστήριξη των συνεργατών της στην ενσωμάτωση του GDPR. Η ομάδα της INTRACOM αποτελείται από:

1) Νομικούς εμπειρογνώμονες με σχετικό υπόβαθρο και μακρά εμπειρία στην προστασία προσωπικών δεδομένων.
2) Εμπειρογνώμονες διακυβέρνησης και συμμόρφωσης.
3) Εμπειρογνώμονες και Συμβούλους Πεδίου Ασφαλείας και Ευελιξίας Πληροφοριών.

4) Ειδικούς πληροφοριακών συστημάτων με σχετικό υπόβαθρο σε εφαρμογές, βάσεις δεδομένων, συστήματα, δίκτυα, επικοινωνίες και υποδομές.
5) Διαχειριστές προγραμμάτων και έργων σε επίπεδο εμπειρογνωμόνων με εξαιρετική εμπειρία.

Η προσέγγιση της Intracom για τον ΓΚΠΔ έχει ως σκοπό την ανακάλυψη προσωπικών δεδομένων, την κατηγοριοποίηση και την ταξινόμησή τους, την προστασία τους και την διασφάλιση της ιδιωτικότητάς τους. Πιο συγκεκριμένα, εφαρμόζει τις παρακάτω φάσεις στη διαδικασία συμμόρφωσης της εταιρείας με την οποία αναλαμβάνει να συνεργαστεί:

1) Έναρξη Έργου, Ομάδα & Δέσμευση: Καθορισμός των αναγκών του έργου σχετικά με το πεδίο εφαρμογής του, των στόχων, της έκτασης και των πόρων του (π.χ. προϋπολογισμός, ανθρώπινο δυναμικό, κ.λπ.). Δημιουργία ομάδας έργου, ευαισθητοποίηση και κατάρτιση των εργαζομένων.
2) Εκτέλεση χαρτογράφησης περιβάλλοντος: Κατανόηση των εννοιών των ελεγκτών, των επεξεργαστών και των προσωπικών δεδομένων. Προσδιορισμός όλων των ειδών επεξεργασμένων δεδομένων (μέσω συστημάτων πληροφορικής, διεργασιών κ.λπ.) και ανακάλυψη δεδομένων. Προσδιορισμός όλων των σχετικών ροών δεδομένων και πληροφοριών και των εφαρμόσιμων απαιτήσεων του GDPR.
3) Εκτέλεση ανάλυσης ελλείψεων (GAP Analysis): Προσδιορισμός της τρέχουσας κατάστασης έναντι των απαιτήσεων τους GDPR, λαμβάνοντας υπόψιν τους τύπους δεδομένων, τις πολιτικές και διαδικασίες που εφαρμόζονται, την επεξεργασία των δεδομένων από τρίτους και τις ροές εντός και εκτός της ΕΕ.
4) Προσδιορισμός των κινδύνων και αξιολόγηση των επιπτώσεων τους στην ιδιωτική ζωή (DPIA): Ανάλυση των πιθανών κινδύνων και καθορισμός των επιπτώσεων και των αποτελεσμάτων της συλλογής, συντήρησης, χρήσης και διάδοσης των προσωπικών δεδομένων σύμφωνα με τις απαιτήσεις του GDPR. Προσδιορισμός και αξιολόγηση των υφιστάμενων ελέγχων και διαδικασιών (τόσο τεχνικών όσο και οργανωτικών).
5) Πρόταση σχεδίου για περιορισμό των κινδύνων και συμμόρφωση: Καθορισμός του οδικού χάρτη πορείας (Roadmap) και πρόταση σχεδίου εφαρμογής για τον

περιορισμό των δυνητικών κινδύνων στην προστασία της ιδιωτικής ζωής και της ασφάλειας.

6) Αρχιτεκτονική και σχεδιασμός πλαισίου: Πλάνο σχεδιασμού με αμοιβαία συμφωνημένα μέτρα (έλεγχοι / διαδικασίες τόσο τεχνικές όσο και οργανωτικές) για την αντιμετώπιση πιθανών κινδύνων για την ιδιωτικότητα και την ασφάλεια.
7) Παράδοση υλοποίησης: Μέτρα και τεχνικές εκτέλεσης της υλοποίησης και των ελέγχων για τον περιορισμό των δυνητικών κινδύνων στην προστασία της ιδιωτικότητας.
8) Επιβεβαίωση συμμόρφωσης διακυβέρνησης, Παρακολούθηση & Υποστήριξη: Αναθεώρηση GAP ανάλυσης, έλεγχος λειτουργίας συστήματος παρακολούθησης και διαχείρισης. Παροχή υποστήριξης και συμβουλευτικών υπηρεσιών για την εταιρεία.

5.8 Σύνοψη

Στο συγκεκριμένο κεφάλαιο, περιγράφηκαν μερικά από τα πιο γνωστά πληροφοριακά συστήματα και εφαρμογές και διαπιστώθηκε η ιδιαίτερη συμβολή των λειτουργικών συστημάτων στην εναρμόνιση των επιχειρήσεων με τον GDPR, μέσω των εξειδικευμένων εργαλείων που παρέχουν, αλλά και η ουσιαστική συνεισφορά εξωτερικών εταιρειών στην παροχή υπηρεσιών συμμόρφωσης και εκπαίδευσης.

Είναι φανερό, ότι οι εταιρείες που σχεδίασαν εξαρχής εξειδικευμένα συστήματα και υπηρεσίες για τη συμμόρφωση με τον GDPR είναι ελάχιστες, ενώ η πλειοψηφία επιλέγει να προσαρμόσει, με μικρές προσθήκες, τα ήδη υπάρχοντα λογισμικά της ώστε να εμπεριέχουν και τα νέα δεδομένα του Κανονισμού.

Με αυτόν τον τρόπο, η κάθε επιχείρηση έχει τη δυνατότητα να επιλέξει από μια μεγάλη ποικιλία προϊόντων και υπηρεσιών, αυτό που της ταιριάζει καλύτερα στην υλοποίηση της στρατηγικής της για την αποτελεσματικότερη συμμόρφωσή της με τον GDPR.

6. ΕΦΑΡΜΟΓΗ ΜΕΘΟΔΟΛΟΓΙΑΣ ΣΥΜΜΟΡΦΩΣΗΣ ΣΕ ΕΛΛΗΝΙΚΗ ΕΤΑΙΡΙΑ

6.1 Εισαγωγή

Στο παρόν κεφάλαιο, γίνεται μια προσπάθεια συγκέντρωσης και αξιοποίησης όλων των προηγούμενων πληροφοριών και τεχνικών για τη συμμόρφωση των επιχειρήσεων με τον GDPR. Επιδιώκεται η ανάλυση των προβλημάτων και προκλήσεων που αντιμετωπίζουν οι φαρμακοβιομηχανίες με την εφαρμογή του νέου Κανονισμού και μελετάται η πρακτική εφαρμογή της μεθοδολογίας που περιγράφηκε στα προηγούμενα κεφάλαια στην ελληνική φαρμακευτική εταιρεία ΒΙΑΝΕΞ.

6.2 Η επίδραση του GDPR στις φαρμακοβιομηχανίες

Στη φαρμακευτική αγορά τα προσωπικά δεδομένα είναι προσβάσιμα τόσο σε άμεση αναγνώριση όσο και σε κωδικοποιημένη μορφή. Μπορούν να διακριθούν σε:

- Δεδομένα πελάτη και εταιρικών υπευθύνων
- Δεδομένα φαρμακείων, νοσοκομείων και συνεργαζόμενων εταιρειών
- Δεδομένα συνταγογράφησης
- Δεδομένα για την υγεία και την κοινωνική ασφάλιση
- Φορητά δεδομένα υγείας (από εφαρμογές, κινητές συσκευές, φορητές συσκευές ελέγχου και monitors)
- Δεδομένα από εφαρμογές υγείας (Health Apps)
- Ιατρικά αρχεία και ιστορικά ασθενών
- Δεδομένα ερευνών αγοράς
- Στοιχεία που αναφέρθηκαν από τους ασθενείς
- Επιχειρησιακά Δεδομένα (υπάλληλοι κ.λ.π.)
- Δεδομένα από Μέσα Κοινωνικής Δικτύωσης (Social Media)
- Δεδομένα των Καταναλωτών-Μητρώα Ασθενών
- Δεδομένα Κλινικών Δοκιμών
- Μελέτες Φάσης V-Ασφάλειας
- Δεδομένα που προέρχονται από δείγματα Βιοτραπεζών (βιοδείκτες, κυτταρικοί ιστοί, RNA, DNA, αίμα κλπ.), όπου προκύπτουν και ζητήματα βιοηθικής

Είναι συνεπώς φανερό ότι σε μια φαρμακευτική εταιρεία, η ανάγκη προστασίας τέτοιου είδους δεδομένων είναι άμεση και επιτακτική ανάγκη, διότι διακινούνται ευαίσθητα προσωπικά δεδομένα, άμεσα συσχετισμένα με την προσωπική υγεία και το ιατρικό απόρρητο των ασθενών και των υποκειμένων.

Ωστόσο, σύμφωνα με έρευνες που πραγματοποιήθηκαν τον Αύγουστο του 2017, ο κλάδος της φαρμακοβιομηχανίας, όπως και οι περισσότερες ευρωπαϊκές και κυρίως ελληνικές επιχειρήσεις, δεν είναι ακόμα πλήρως έτοιμες για να ενσωματώσουν τον ΓΚΠΔ.

Λαμβάνοντας υπόψιν τις ρυθμίσεις που περιλαμβάνονται στον νέο Κανονισμό, καθώς και τις κυρώσεις για τη μη συμμόρφωση, είναι κατανοητό ότι η βιομηχανία φαρμάκων πρέπει να ανησυχεί. Τα κριτήρια μη-ταυτοποίησης και ανωνυμοποίησης των κλινικών δεδομένων έχουν περιγραφεί και αξιολογηθεί για απλές περιπτώσεις, όπως η συλλογή δεδομένων με τη χρήση ηλεκτρονικού εντύπου αναφοράς περίπτωσης (eCRF). Οι ερευνητικοί οργανισμοί μπορούν να ανιχνεύσουν αυτόματα τα δεδομένα των ασθενών στην περιοχή, να αποτυπώσουν τις ημερομηνίες γέννησης και να επεξεργαστούν τα ευαίσθητα δεδομένα.

Αξίζει όμως να σημειωθεί ότι η πραγματική ανησυχία είναι η μετάδοση των αποκαλούμενων "μη CRF δεδομένων". Αυτά είναι τα δεδομένα από ηλεκτροεγκεφαλογραφήματα (EEG), παθολογικές διαφάνειες, ηλεκτροκαρδιογραφήματα, δεδομένα απεικόνισης και εργαστηριακά δεδομένα. Αυτά τα δεδομένα τυπικά δεν εισάγονται απευθείας στο eCRF, αλλά αποστέλλονται για ανάλυση από εμπειρογνώμονες, αφού περιέχουν ευαίσθητα δεδομένα που είναι απαραίτητα για την επιστημονική αξία της μελέτης. Η συμμόρφωση σε αυτές τις περιπτώσεις θα περιλαμβάνει νοσοκομεία, εταιρείες παροχής ιατρικών συσκευών και προμηθευτές λογισμικού που προσδιορίζουν μεθόδους. Επομένως, η απλή επεξεργασία των δεδομένων μπορεί να μην είναι πάντα η σωστή λύση. Πολλά νοσοκομεία, εταιρείες ιατρικών συσκευών και πωλητές λογισμικού δεν συμμορφώνονται και ο διαθέσιμος χρόνος για τη λήψη διορθωτικών ενεργειών εξαντλείται.

Η ακεραιότητα των δεδομένων και η ποιότητα των δεδομένων είναι κρίσιμα ζητήματα για κάθε εταιρεία που εκτελεί κλινική έρευνα. Παράλληλα όμως, ο κλάδος αυτός είναι

παγκόσμιος και δεν υπάρχουν όρια όσον αφορά τα δεδομένα που συλλέγονται, επεξεργάζονται και διαβιβάζονται προτού ενσωματωθούν σε μια παγκόσμια βάση δεδομένων κλινικών δοκιμών. Τα δεδομένα πηγαίνουν παντού και με την τεχνολογία που υπάρχει σήμερα, κινούνται επίσης πολύ γρήγορα.

Επίδραση της ιδιωτικότητας και του αυτοματισμού

Η μετακίνηση δεδομένων ήταν πάντα μια περίπλοκη διαδικασία για τα Βιοϊατρικά Συστήματα. Με την εισαγωγή του GDPR, τίθεται το ερώτημα πώς οι επιχειρήσεις που δραστηριοποιούνται στην Ευρωπαϊκή Ένωση θα συνεχίσουν να διεξάγουν δοκιμές, αφού ο νέος Κανονισμός θα δυσχεραίνει τις επιχειρήσεις να αποκτήσουν τα απαιτούμενα δεδομένα και να τα μοιραστούν με τους ερευνητές που πρέπει να τα ερμηνεύσουν.

Ο νέος Κανονισμός δεν αφορά απλώς την παράνομη απελευθέρωση δεδομένων, όπως μια παραβίαση, αλλά την προστασία της αναμενόμενης και προγραμματισμένης διακίνησης δεδομένων από εταιρείες που χρησιμοποιούν δεδομένα με τρόπους που ο ασθενής δεν συνειδητοποιεί ότι θα μπορούσαν να χρησιμοποιηθούν.

Μεγάλο μέρος αυτού του προβλήματος έχει πολιτιστικό χαρακτήρα. Στην Ευρώπη, όλες οι προσωπικές πληροφορίες θεωρούνται ότι ανήκουν στον ασθενή και το ιδιωτικό απόρρητο δεδομένων θεωρείται ανθρώπινο δικαίωμα. Ως εκ τούτου, οι ασθενείς έχουν το δικαίωμα να ελέγχουν τα δεδομένα τους. Για το λόγο αυτό, οι ασθενείς πρέπει να επιλέξουν τη διαδικασία συλλογής δεδομένων, χωρίς να χρειάζεται να αποχωρήσουν από αυτό. Ωστόσο, ο GDPR θέτει το ζήτημα ένα βήμα παραπέρα, δηλώνοντας ότι οι ασθενείς έχουν επίσης το δικαίωμα να απομακρύνουν τα δεδομένα τους από τις εταιρείες, διαγράφοντάς τα («δικαίωμα στη λήθη»). Εκεί βρίσκεται ένα σημαντικό πρόβλημα: ο GDPR δεν διευκρινίζει τι θα συμβεί όταν μια εταιρεία βρίσκεται μεταξύ των εθνικών κανονισμών και των ασθενών που θέλουν να διαγράψουν τα δεδομένα τους.

Ωστόσο, ο πολιτισμός δεν είναι το μόνο θέμα. Ο αυτοματισμός περιπλέκει το πρόβλημα. Παλαιότερα, ένα δοκιμαστικό κύριο αρχείο (TMF) θα βρισκόταν σε ένα συρτάρι στο γραφείο του διαχειριστή. Τώρα υπάρχει ηλεκτρονικά ως eTMF σε ένα

δίκτυο. Όταν υπήρχαν πληροφορίες σε ένα χαρτί, ήταν εύκολο να ελεγχθούν. Όταν όμως πληροφορίες οποιουδήποτε είδους βρίσκονται σε αρχείο δεδομένων, ειδικά σε ένα σύστημα συνδεδεμένο στο Internet, δεν υπάρχει το ίδιο επίπεδο ελέγχου. Αν και τα δεδομένα ελέγχονται, είναι επίσης αποκεντρωμένα. Οι ερευνητές γενικά δεν διαμένουν στην ίδια χώρα όπου διεξήχθη η δοκιμή, με αποτέλεσμα όταν τα δεδομένα χρησιμοποιούνται και αποθηκεύονται σε διαφορετικά μέρη, η συγκέντρωση και άντληση τους σε ένα μέρος να είναι αδύνατη.

Αντιμετώπιση προβλήματος

Για να μπορέσουν να ξεπεραστούν οι παραπάνω προβληματισμοί, θα πρέπει αρχικά οι φαρμακευτικές εταιρείες να έχουν περισσότερες συζητήσεις και διαπραγματεύσεις με τις ομάδες προβληματισμού του κλάδου που περιλαμβάνουν τη συμμετοχή των ρυθμιστικών και εποπτικών αρχών, της ΕΕ και των ενδιαφερομένων, όπως εταιρείες χορηγών, ιστοσελίδες, ερευνητικών οργανισμών και προμηθευτών λογισμικού και συστημάτων υποστήριξης.

Επιπλέον, θα πρέπει να κατανοήσουν τι σημαίνει η μη-ταυτοποίηση της πληροφορίας. Εάν μια εξέταση καταλήγει στο να αναγνωρίζει έναν ασθενή, τότε πραγματικά δεν υπάρχει τρόπος να διαγραφούν αυτές οι πληροφορίες. Είναι μεν δυνατόν να αφαιρεθούν τα αρχικά του ασθενούς, μια διαδικασία γνωστή ως ψευδωνυμοποίηση, αλλά η κατάργηση άλλων πληροφοριών, όπως το φύλο ή η ημερομηνία γέννησης, θα επηρεάσει τα αποτελέσματα της δοκιμής. Για παράδειγμα, η ηλικία ενός ασθενούς είναι κρίσιμη σε μελέτες που αφορούν ασθενείς που μεγαλώνουν γρήγορα. Συνεπώς, η περίοδος από την ημερομηνία γέννησης έως την ημερομηνία της δοκιμής είναι ο τρόπος με τον οποίο καθορίζεται με μεγαλύτερη ακρίβεια η ηλικία.

Ο μόνος τρόπος να επιλυθεί ένα τέτοιο πρόβλημα είναι να επιτραπεί η πλήρης αποκάλυψη δεδομένων μεταξύ των μερών που έχουν ελεγχθεί και θεωρείται ότι τους επιτρέπεται να τα δουν και να τα χρησιμοποιήσουν. Αυτή είναι η πιο λογική προσέγγιση αλλά προς το παρόν επικρατεί μια σύγχυση, η οποία πρέπει να ξεπεραστεί άμεσα διότι τα άτομα που θα εφαρμόσουν αυτόν τον Κανονισμό θα πρέπει να γνωρίζουν και τι απαιτείται.

6.3 Υλοποίηση του GDPR σε μια ελληνική φαρμακευτική εταιρία

Για την καλύτερη κατανόηση όλων των παραπάνω εννοιών, μεθοδολογιών και βημάτων, παρατίθεται στη συνέχεια το πλάνο υλοποίησης και συμμόρφωσης με τον GDPR της ελληνικής φαρμακευτικής εταιρίας ΒΙΑΝΕΞ, το οποίο αποτελεί μια πρόταση εφαρμογής μεθοδολογίας συμμόρφωσης για όλο τον κλάδο.

Η συγκεκριμένη εταιρεία είναι η μεγαλύτερη φαρμακοβιομηχανία στην Ελλάδα με ετήσιες πωλήσεις 259.000.000€. Διαθέτει 4 εργοστάσια παραγωγής στην Ελλάδα, ενώ απασχολεί 1.127 άμεσα εργαζομένους στην Ελλάδα, σε 8 περιφερειακά γραφεία. Επιπλέον, εξάγει προϊόντα σε 37 χώρες του κόσμου και συνεργάζεται με 30 από τις καλύτερες φαρμακευτικές εταιρίες παγκοσμίως. Τέλος, αποτελείται από 34 διευθύνσεις και τμήματα, 1 κέντρο Έρευνας & Ανάπτυξης, ενώ οι πελάτες της σε Ελλάδα και εξωτερικό ανέρχονται σε πάνω από 42.342.

Με τα παραπάνω στοιχεία λοιπόν, γίνεται κατανοητό ότι μια τέτοιου μεγέθους εταιρεία, με τόσο πολύπλοκη οργανωτική και επιχειρησιακή δομή, απαιτεί μια πολύ καλή προετοιμασία και οργάνωση για να μπορέσει να ενσωματώσει αποτελεσματικά τους κανονισμούς του GDPR.

6.3.1 Στρατηγικό και τακτικό πλάνο (Data Privacy Program Management)

Αρχικά, η συγκεκριμένη φαρμακευτική εταιρεία επεδίωξε την κατανόηση των νέων δεδομένων του Κανονισμού. Για να το επιτύχει αυτό, προσπάθησε να δει την εισαγωγή του νέου Ευρωπαϊκού Κανονισμού σαν ένα νέο φαρμακευτικό προϊόν. Το συγκεκριμένο λοιπόν προϊόν, απαιτεί μια πανευρωπαϊκή έγκριση, η οποία σε περίπτωση που δεν αποδοθεί εντός της προθεσμίας, θα της κοστίσει 20.000.000€ ή 4% του ετήσιου τζίρου της. Συνεπώς, παρομοιάζει τον GDPR σαν ένα φάρμακο υψηλού κόστους, το οποίο πρέπει να έχει κυκλοφορήσει στην αγορά μέχρι τις 25 Μαΐου 2018.

Αφού λοιπόν, συνειδητοποίησε την έννοια και τη σημασία του νέου Κανονισμού, άρχισε να διαμορφώνει ένα στρατηγικό και τακτικό σχέδιο προετοιμασίας, ώστε να πετύχει την ενσωμάτωση του ΓΚΠΔ στα συστήματά της.

Ο Οδικός Χάρτης Προετοιμασίας του GDPR (GDPR Roadmap)

Το πρώτο βήμα της υλοποίησης του GDPR, ξεκίνησε με τη δημιουργία ενός οδικού χάρτη σε μορφή πυραμίδας, που βοήθησε τη φαρμακευτική εταιρία να οργανωθεί καλύτερα.

Συγκεκριμένα, στο πρώτο στάδιο η εταιρεία διαμόρφωσε τη στρατηγική της για την προετοιμασία και τη συμμόρφωσή της με τον GDPR. Σε αυτό το στάδιο έπρεπε να διαμορφώσει το όραμα και την αποστολή της, ώστε να εξασφαλίζονται οι ανάγκες των πελατών της, εσωτερικών και εξωτερικών.

Στη συνέχεια, έπρεπε να λάβει υπόψιν της την οργάνωση και τη λογοδοσία στο εσωτερικό κομμάτι της επιχείρησης και μετέπειτα να εξασφαλίσει όλα εκείνα τα μέτρα που θα δημιουργούσαν την αναγκαία οργανωσιακή και επιχειρησιακή κουλτούρα εντός της επιχείρησης, μέσω της κατάλληλης επικοινωνίας, εκπαίδευσης και κινητοποίησης των στελεχών και εργαζομένων της.

Στο επόμενο στάδιο, συγκρότησε τα διάφορα βήματα, τις πολιτικές, και τις διαδικασίες που θα έπρεπε να κάνει για τη διαχείριση και μεταφορά των προσωπικών δεδομένων, ώστε να μπορέσει να περάσει στο στάδιο της αντιμετώπισης των διαφόρων παρεμβάσεων της ιδιωτικότητας, με σημαντικότερη την εκτίμηση των επιπτώσεων της προστασίας των δεδομένων (DPIA).

Στο τελικό στάδιο, αφού εξασφαλίσει τα απαραίτητα πληροφοριακά συστήματα και λογισμικά υποστήριξης, θα μπορέσει να κάνει την επεξεργασία και την απογραφή των δεδομένων που χρειάζεται.

***Εικόνα 4**: Οδικός Χάρτης Ετοιμότητας της ΒΙΑΝΕΞ για τον GDPR*

Το Όραμα και η Αποστολή για το GDPR

Έχοντας έτσι κατά νου το παραπάνω διάγραμμα, και θέτοντας διάφορους στόχους και οράματα, κατέληξε στο ακόλουθο όραμα για τους πελάτες της:

- Σεβασμός του θεμελιώδους δικαιώματος της ιδιωτικότητάς τους.
- Πραγματοποίηση όλων των αναγκαίων διασφαλίσεων για την προστασία της ασφάλειας και της εμπιστευτικότητας των προσωπικών δεδομένων που συγκεντρώνονται, χρησιμοποιούνται ή δημοσιοποιούνται στο πλαίσιο των αλληλεπιδράσεων.
- Περιορισμός των προσωπικών δεδομένων που συγκεντρώνονται στο ελάχιστο δυνατόν, προκειμένου να προσφέρονται καλύτερες υπηρεσίες.
- Άδεια μόνο σε κατάλληλα εκπαιδευμένο, εξουσιοδοτημένο προσωπικό να έχει πρόσβαση σε αυτά.
- Να μη δημοσιοποιούνται τα προσωπικά τους στοιχεία σε εξωτερικά μέρη, εκτός αν συναινούν οι ίδιοι οι πελάτες ή έχουν προηγουμένως πληροφορηθεί από την εταιρεία ή απαιτείται εκ του νόμου.

6.3.2 Φάσεις έργου συμμόρφωσης με τον GDPR

Με την ολοκλήρωση της αποδοχής ενός κοινού οράματος για όλο το ανθρώπινο δυναμικό της εταιρείας, σχεδιάστηκαν και οι φάσεις του έργου για τη συμμόρφωση με τον GDPR.

Οι φάσεις αυτές, όπως φαίνονται και στο παρακάτω διάγραμμα, χωρίζονται:

1) Στην 1η φάση, της προετοιμασίας και της οργάνωσης της εταιρίας για την ενσωμάτωση του Κανονισμού (Awareness), όπου μελετάται η Νομοθεσία και κατανοούνται οι οδηγίες του ΓΚΠΔ.
2) Στη 2η φάση, της εκτίμησης των επιπτώσεων και της διάγνωσης των τομέων που χρήζουν αλλαγών για την ομαλή μετάβαση στον ΓΚΠΔ (Assessment)
3) Στην 3η φάση, που είναι η υλοποίηση του στρατηγικού πλάνου και σχεδίου προετοιμασίας, με σκοπό την ετοιμότητα για εφαρμογή του ΓΚΠΔ στην προστασία των δεδομένων (Implementation).

***Εικόνα 5**: Φάσεις έργου συμμόρφωσης με τον GDPR*

1) Πρώτη φάση: Προετοιμασία και Οργάνωση

- **Δημιουργία Ομάδας Έργου και DPO**

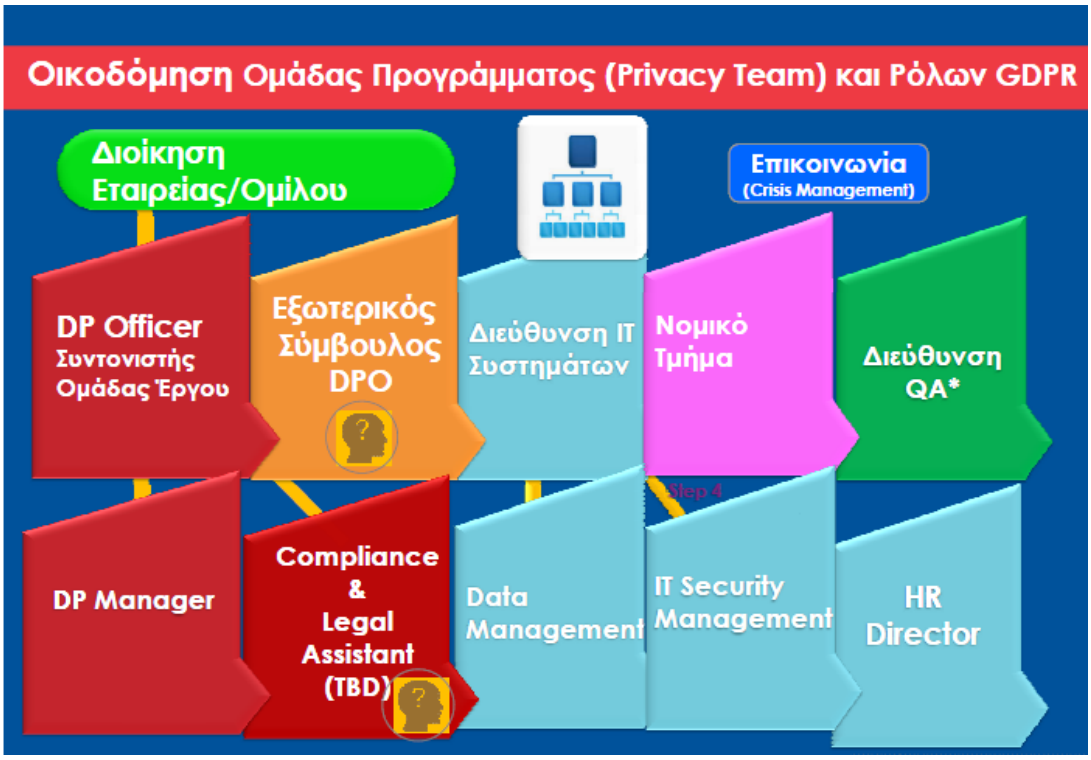
Στη συγκεκριμένη φάση, απαιτείται η δέσμευση και η στήριξη της Διοίκησης και των Ανώτατων Στελεχών για την εκπλήρωση του έργου, διότι χωρίς αυτά, ό,τι αλλαγή και προσπάθεια να γίνει στην εταιρεία, δεν θα έχει αποτέλεσμα. Η Ανώτατη Διοίκηση οφείλει να κατανοήσει ότι είναι υπεύθυνη για τη λογοδοσία και για την εξασφάλιση και έγκριση των απαραίτητων πόρων (ανθρώπινων, υλικών, τεχνολογικών, χρόνου κλπ.) που θα συμμετέχουν στην υλοποίηση του έργου.

Επιπλέον, καθορίζονται οι ευθύνες και οι αρμοδιότητες για κάθε μέλος της ΒΙΑΝΕΞ. Ορίζεται υποχρεωτικά ο Υπεύθυνος Προστασίας των Δεδομένων (DPO) και η ομάδα υποστήριξης του προγράμματος και δημιουργούνται ενδοτμηματικά οι σύνδεσμοι και οι «Πρεσβευτές» για την παρακολούθηση και συγκρότηση του έργου.

Η ΒΙΑΝΕΞ έχει δημιουργήσει την ομάδα έργου της (Privacy Team) με βάση το διάγραμμα που ακολουθεί. Σε αυτό φαίνεται ότι συμμετέχουν, τόσο η Διοίκηση της εταιρείας και του Ομίλου, όσο και:

- Ο εσωτερικός Υπεύθυνος Προστασίας Δεδομένων (DPO) που είναι και ο συντονιστής του έργου.
- Ο Διαχειριστής των δεδομένων (DP Manager).
- Ο εξωτερικός Υπεύθυνος Προστασίας Δεδομένων (DPO) που παρακολουθεί την όλη διαδικασία και παρέχει συμβουλές σχετικά με την πορεία και εξέλιξή της.
- Ο βοηθός συμμόρφωσης και παροχής νομικών υπηρεσιών (TBD).
- Η διεύθυνση των πληροφοριακών συστημάτων και λογισμικών.
- Το τμήμα διαχείρισης των δεδομένων.
- Το τμήμα διασφάλισης και προστασίας των πληροφοριακών συστημάτων.
- Το νομικό τμήμα, για την διευκόλυνση ερμηνείας των όρων και κανόνων του GDPR.
- Ο Διευθυντής Ανθρώπινου Δυναμικού.

- Η Διεύθυνση Διασφάλισης Ποιότητας (Quality Assurance), η οποία έχει ως στόχο το συνεχή έλεγχο για τη διασφάλιση της τήρησης των κανόνων του έργου και τη συνεχή πιστοποίηση του σε συνεργασία με τον DPO, και τέλος
- Ο υπεύθυνος επικοινωνίας, για την ενημέρωση της κοινής γνώμης σε περίπτωση διαχείρισης κρίσεων από τυχόν διώξεις πελατών ως προς την εταιρεία ή κυρώσεων της Αρχής Προστασίας Δεδομένων. Για την αντιμετώπιση τέτοιων περιστατικών, η ΒΙΑΝΕΞ διοργανώνει σεμινάρια διαχείρισης κρίσεων για το προσωπικό της, ώστε να είναι έτοιμο με την ισχύ του ΓΚΠΔ.



***Εικόνα 6**: Δημιουργία Ομάδας Έργου*

- **<u>Κατανομή ρόλων και αρμοδιοτήτων στην Ομάδα Έργου GDPR</u>**

Στη διάρκεια της πρώτης φάσης του έργου συμμόρφωσης με τον GDPR, η εταιρεία κατανέμει ανά τακτά χρονικά διαστήματα τις σημαντικότερες αρμοδιότητες που πρέπει να διεκπεραιώσει η ομάδα έργου (Privacy Team). Μερικές από αυτές αφορούν:

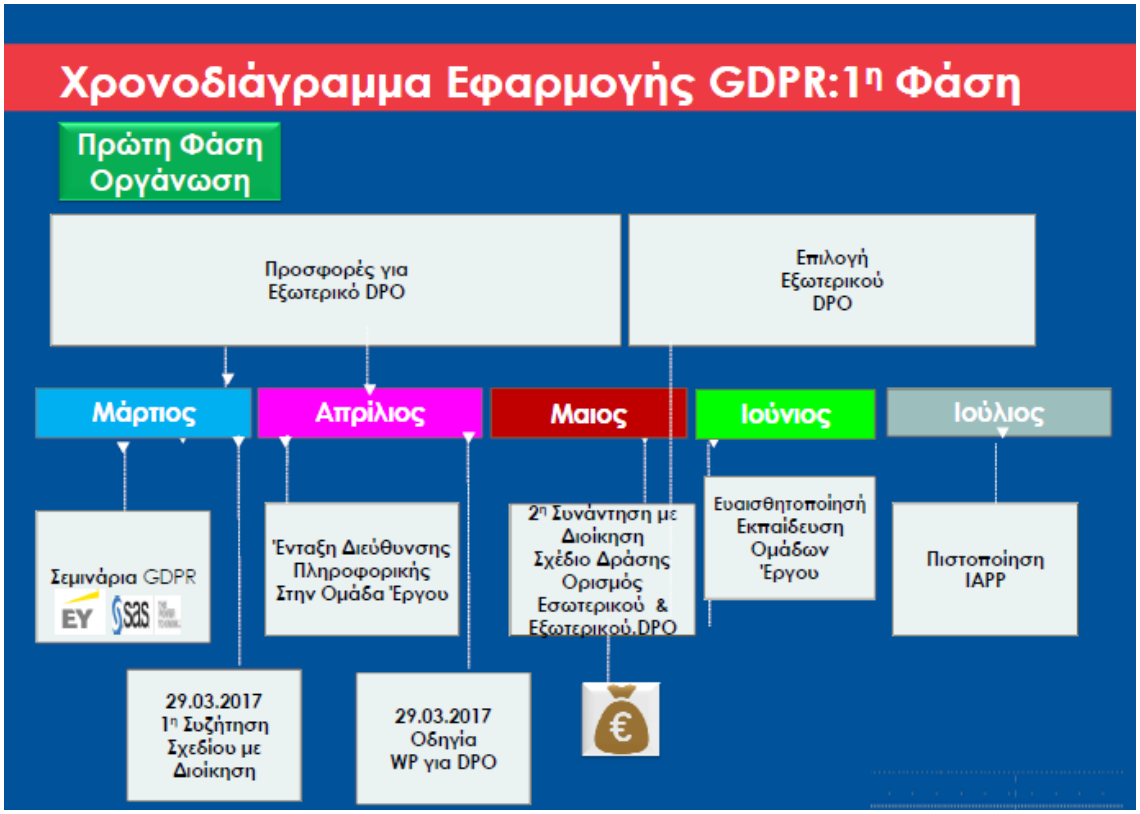
- Τις διαδικασίες, τις πολιτικές και την οργάνωση του έργου.
- Τη συνεχή ενημέρωση του ανθρώπινου δυναμικού και την εκπαίδευσή του.
- Την ανταπόκριση και την ετοιμότητα του προσωπικού σε έκτακτα συμβάντα.
- Το σχεδιασμό και την εκτέλεση των ελέγχων απορρήτου.

- Τον έλεγχο απορρήτου για υπάρχοντα προϊόντα και υπηρεσίες.
- Την εκτέλεση εκτίμησης επιπτώσεων για την προστασία των δεδομένων (DPIA).

- **Αλλαγή Κουλτούρας**

Το σημαντικότερο ωστόσο σημείο στη διάρκεια του έργου είναι η αλλαγή κουλτούρας, η αλλαγή νοοτροπίας των εργαζομένων και η δημιουργία ενός «ανθεκτικού» περιβάλλοντος, όπου θα εργάζονται όλοι για τον ίδιο σκοπό. Αν δεν υπάρχει η διαμόρφωση κουλτούρας στηριζόμενη σε ισχυρές βάσεις, τότε ο ρόλος του DPO και ο ρόλος του GDPR γενικότερα, δεν θα έχει καμία αξία και η εταιρεία θα είναι πλέον ιδιαίτερα ευάλωτη και εκτεθειμένη απέναντι σε ανεπιθύμητες ενέργειες και παραβιάσεις ή γραφειοκρατικούς κινδύνους.

Για την κινητοποίηση των εργαζομένων και τον ενστερνισμό μιας ενιαίας κουλτούρας, η ΒΙΑΝΕΞ δημιούργησε μια διεταιρική ομάδα 35 υψηλόβαθμων ατόμων από διάφορα τμήματα, των Πρεσβευτών (Ambassadors), τα οποία ενημερώνονται συνεχώς για τις εξελίξεις γύρω από το νέο Κανονισμό και αναλαμβάνουν την ενημέρωση σε όλα σχεδόν τα σημαντικά τμήματα της εταιρείας. Αυτό έχει σαν αποτέλεσμα να υπάρχει μεγάλη «ευαισθησία» και κινητικότητα μεταξύ των εργαζομένων για την εφαρμογή του GDPR και για τα προγράμματα ενημέρωσης σχετικά με αυτό.



***Εικόνα 7**: Χρονοδιάγραμμα 1ης φάσης GDPR στη ΒΙΑΝΕΞ*

2) Δεύτερη Φάση: Αξιολόγηση ετοιμότητας GDPR (Assessment)

Σε αυτή τη φάση, πραγματοποιείται μια σειρά ελέγχων και αξιολογήσεων, με σκοπό την καλύτερη δυνατή αποτύπωση της υφιστάμενης κατάστασης της επιχείρησης, των συστημάτων και των δεδομένων.

- **Διάγνωση 360°- Χαρτογράφηση (Data Mapping)**

Η διάγνωση και χαρτογράφηση των δεδομένων πραγματοποιείται μέσω συνεντεύξεων, ερωτηματολογίων και workshops με 1ης και 2ης βαθμίδας managers και αρμόδια στελέχη. Σκοπός αυτής της πρακτικής ήταν να διαπιστώσει η εταιρεία ποια προσωπικά δεδομένα διαθέτει και σε ποιους ανήκουν, πώς συλλέγονται τα δεδομένα, πού και πώς μεταφέρονται (εντός και εκτός εταιρείας και ΕΕ), πού αποθηκεύονται, με χρήση ποιων λογισμικών και μέσων αποθήκευσης, με ποιους τρόπους επεξεργάζονται και πόσος χρόνος χρειάζεται για τη διαγραφή τους.

Με την ολοκλήρωση της συγκέντρωσης όλων των παραπάνω στοιχείων, δημιουργείται ο χάρτης της ροής δεδομένων (Data flow mapping), η ανάλυση

ελλείψεων ως προς τον ΓΚΠΔ (Gap Analysis) και η εκτίμηση επιπτώσεων των προσωπικών δεδομένων (Privacy Impact Assessment-DPIA).

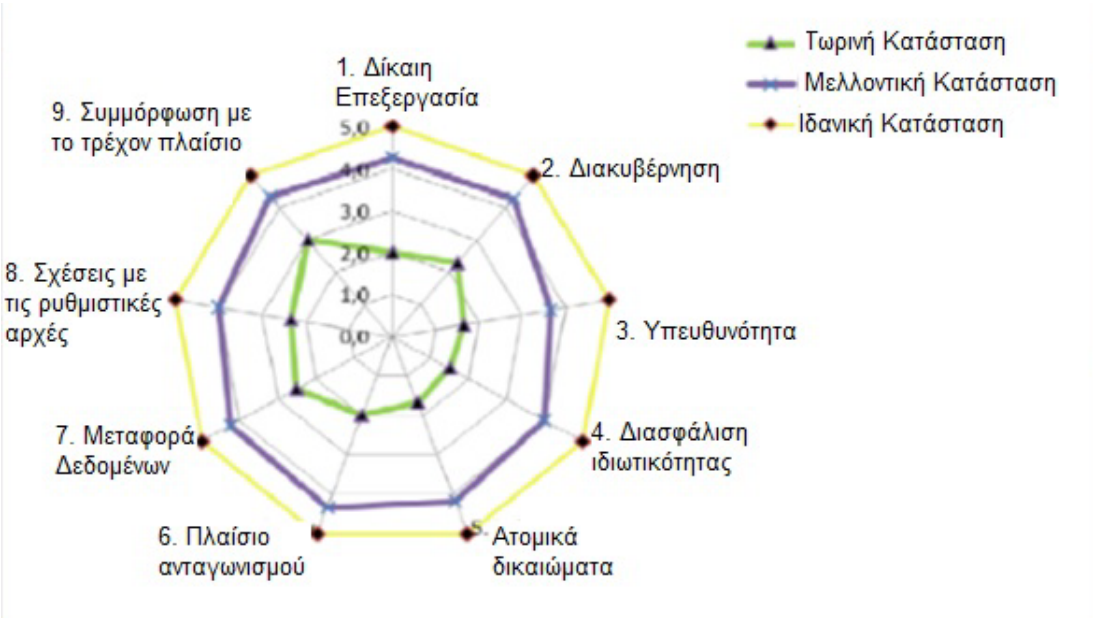
- **Αξιολόγηση Βαθμού ετοιμότητας (GDPR Readiness)**

Στη συνέχεια, αξιολογείται ο βαθμός ετοιμότητας της φαρμακοβιομηχανίας, δηλαδή με βάση συγκεκριμένα παραδείγματα συγκρίνεται η κατάσταση στην οποία βρίσκεται η εταιρεία τώρα με την ιδεατή κατάσταση που θέλει να πάει.

Η ΒΙΑΝΕΞ συγκεκριμένα δημιούργησε ένα προφίλ ετοιμότητας GDPR (GDPR Maturity Profiile), αξιολογώντας την ετοιμότητά της στις εξής, ίσης βαρύτητας διαστάσεις:

1. Δίκαιη Επεξεργασία (Fair Processing)
2. Διακυβέρνηση (Governance)
3. Υπευθυνότητα (Accountability)
4. Διασφάλιση ιδιωτικότητας (Security for Privacy)
5. Ατομικά δικαιώματα (Individual Rights)
6. Πλαίσιο Ανταγωνισμού (Competency Framework)
7. Μεταφορά δεδομένων (Transfers of data)
8. Σχέσεις με τις ρυθμιστικές αρχές (Relationship with regulators)
9. Συμμόρφωση με το τρέχον πλαίσιο (Compliance with current framework)

Το αποτέλεσμα φαίνεται στο παρακάτω σχήμα, όπου διαπιστώνεται ότι η παρούσα κατάσταση το Νοέμβριο του 2017 απέχει ακόμα πολύ από τη μελλοντική κατάσταση και ακόμα περισσότερο από την ιδεατή κατάσταση στην οποία στοχεύει η ΒΙΑΝΕΞ.



***Εικόνα 8**: GDRR Maturity Profile - Αξιολόγηση Βαθμού ετοιμότητας της ΒΙΑΝΕΞ (11/2017)*

- **<u>Ροή Δεδομένων-Πληροφοριών (Data/Information Flow)</u>**

Ακολούθως, κατηγοριοποιούνται τα δεδομένα και οι πληροφορίες που υπάρχουν, προσδιορίζοντας τα σημεία κλειδιά όπως:

- Στοιχεία δεδομένων (π.χ. ονόματα, e-mails, διευθύνσεις – δεδομένα υγείας και ποινικά δεδομένα – βιομετρικά δεδομένα θέσης)
- Μορφές δεδομένων (π.χ. σε χαρτί, σε ψηφιακή μορφή, σε βάσεις δεδομένων)
- Μέθοδοι μεταφοράς δεδομένων (π.χ. μέσω ταχυδρομείου, τηλεφώνου, μέσων κοινωνικής δικτύωσης – ενδοεταιρικά – εξωτερικά)
- Τοποθεσίες δεδομένων (π.χ σε γραφεία, σε σύννεφα (clouds), σε τρίτα μέρη (third parties)

Με αυτόν τον τρόπο η εταιρεία αποκτά μια πλήρη εικόνα σχετικά με τη «διαδρομή» των δεδομένων εντός και εκτός της εταιρείας.

- **<u>Ανάλυση Ελλείψεων (Gap Analysis) ως προς τον ΓΚΠΔ</u>**

Αφού συλλέξει όλα τα παραπάνω στοιχεία, εφαρμόζει την ανάλυση ελλείψεων για να διαπιστώσει από την παρούσα κατάσταση που βρίσκεται, τι ενέργειες απαιτούνται για να πετύχει την πρόκληση ή το στόχο που έχει θέσει.

Τα ερωτήματα που τίθενται για να διαπιστωθούν τα σημεία που χρήζουν περαιτέρω προσοχής είναι αν:

- Επιτυγχάνονται οι βασικές αρχές προστασίας προσωπικών δεδομένων;
- Εξασφαλίζονται τα δικαιώματα των φυσικών προσώπων;
- Προβλέπεται η γνωστοποίηση παραβίασης προσωπικών δεδομένων;
- Είναι ασφαλής οι πληροφορίες;
- Είναι αποτελεσματική η οργανωτική δομή;
- Εφαρμόζονται οι πολιτικές και οι διαδικασίες όπως ορίστηκαν στο στρατηγικό πλάνο;
- Προβλέπονται συνεχείς επιθεωρήσεις και βελτιώσεις στην εφαρμογή του ΓΚΠΔ;

- **<u>Σχεδιασμός Προγράμματος Προστασίας Προσωπικών Δεδομένων (Compliance Plan) – Εξασφάλιση Δικαιωμάτων Φυσικών Προσώπων</u>**

Από την Ανάλυση Ελλείψεων (Gap Analysis) που πραγματοποίησε η ΒΙΑΝΕΞ και τις διαπιστώσεις που έκανε, διαμόρφωσε το πρόγραμμα συμμόρφωσης που περιλαμβάνει:

1) Την αλλαγή πρακτικών (π.χ. πληροφόρηση των πελατών, απαίτηση συναίνεσής τους στην επεξεργασία των δεδομένων τους, ελαχιστοποίηση του απαιτούμενου χρόνου διαγραφής των δεδομένων, ανωνυμοποίηση αυτών, αυστηρότεροι έλεγχοι πρόσβασης, σύναψη συμβάσεων με συνεργάτες και υπεύθυνους επεξεργασίας, θέσπιση αυστηρότερων πρακτικών ασφαλείας, κ.λπ.)
2) Τη θέσπιση νέων μηχανισμών (π.χ. για την εξασφάλιση των δικαιωμάτων των φυσικών προσώπων, για την αποτελεσματικότερη παρακολούθηση, βελτίωση και έλεγχο των προσωπικών δεδομένων, κ.λπ.),
3) Την αναβάθμιση των υποδομών ασφαλείας της,
4) Την αναθεώρηση σύνταξης των πολιτικών και των διαδικασιών της και
5) Την προσαρμογή της συνεχούς εκπαίδευσης του προσωπικού της.

- **<u>Απαιτούμενες Πολιτικές και Διαδικασίες Προστασίας Προσωπικών δεδομένων</u>**

Οι διαδικασίες που πρέπει να επαναπροσδιορίσουν ή αν δεν υπάρχουν να δημιουργήσουν εξαρχής για να υλοποιήσουν το στόχο, φαίνονται στην εικόνα που ακολουθεί:

Εικόνα 9: *Απαιτούμενες Πολιτικές και Διαδικασίες*

Οι βασικοί άξονες του οποίους επιδιώκει να συμπεριλάβει και να εντάξει στη στρατηγική της η ΒΙΑΝΕΞ είναι επιγραμματικά:

1) Η διαμόρφωση μιας πολιτικής αξιολόγησής της και συμμόρφωσής της με τον Κανονισμό, με την θέσπιση προτύπων συμμόρφωσης και διαδικασιών εσωτερικής αξιολόγησης.
2) Ο σχεδιασμός μιας πολιτικής για ορθολογικότερη και αποτελεσματικότερη διαχείριση των πληροφοριών, που περιλαμβάνουν τη συλλογή, χρήση και ανταλλαγή προσωπικών δεδομένων.

3) Η αναβάθμιση της πολιτικής ελέγχου των εγγράφων και των αρχείων προσωπικών δεδομένων της εταιρείας, εξασφαλίζοντας την ποιότητα, τη διατήρηση και τη διάθεση των δεδομένων.
4) Η δημιουργία μια πολιτικής δημόσιας εμπιστοσύνης, ώστε να διασφαλίζεται η πρόσβαση των υπευθύνων των δεδομένων, η έγκαιρη ενημέρωση και πληροφόρηση αυτών και η δυνατότητα διατύπωσης παραπόνων προς αυτούς.
5) Ο εκσυγχρονισμός της πολιτικής ασφαλείας των πληροφοριών μέσω στρατηγικών διαχείρισης κινδύνων και αναβάθμιση των διαδικασιών και των πολιτικών ελέγχου ασφαλείας.

- **<u>Συγγραφή Μελέτης Αντικτύπου Ιδιωτικότητας (DPIA)</u>**

Εφαρμόζοντας το άρθρο 35 του ΓΚΠΔ, η φαρμακευτική εταιρεία συντάσσει την μελέτη επίπτωσης προστασίας των προσωπικών δεδομένων, αξιολογώντας τους κινδύνους ανά κατηγορία προσωπικών δεδομένων ή ανά έργο/προϊόν και αναγνωρίζοντας τους κινδύνους ποσοτικά ή εκτιμώντας τις επιπτώσεις τους σχετικά με την προστασία δεδομένων.

Η συγκεκριμένη μελέτη είναι απαραίτητη σε περιπτώσεις που εμπλέκονται ευαίσθητα προσωπικά δεδομένα, κατηγοριοποίηση με βάση το προφίλ των υποκειμένων (profiling) ή κίνδυνοι νομικών επιπτώσεων από τη χρήση νέων τεχνολογιών.

Επιπλέον, αποτελεί μια ολοκληρωμένη αναφορά για τη Διοίκηση, τα ανώτατα στελέχη της εταιρείας και τον DPO, αφού επιτυγχάνεται ο προσδιορισμός των απαραίτητων ενεργειών και των οργανωτικών και τεχνικών μέτρων αποκατάστασης που θα πρέπει να εκτελεστούν.

Ωστόσο, η DPIA θα πρέπει να επαναλαμβάνεται τακτικά ώστε να επικαιροποιείται και να συσχετίζεται και με άλλες εκτιμήσεις κινδύνων

- **<u>Μηχανισμοί Διαβίβασης Δεδομένων σε Τρίτες Χώρες</u>**

Κατά τη σύνταξη της DPIA, θα πρέπει να συνυπολογίζονται και οι μηχανισμοί μεταφοράς δεδομένων σε τρίτες χώρες εκτός της ΕΕ.

Για τη διασφάλιση της μεταφοράς των δεδομένων σε τρίτους, η ΒΙΑΝΕΞ θέσπισε αυστηρότερες προϋποθέσεις και μηχανισμούς, όπως την ύπαρξη εταιρικών δεσμευτικών κανόνων (BCRs), πιστοποιήσεων και κωδικών ασφαλείας (π.χ. Privacy Shield), πρότυπων συμβατικών ρητρών (SCCs), ισοδύναμων αποφάσεων – εγγυήσεων και τις σχετικές αποφάσεις τρίτων χωρών.

***Εικόνα 10**: Χρονοδιάγραμμα Εξέλιξης 2ης Φάσης GDPR στη ΒΙΑΝΕΞ [23/11/2017]*

3) Τρίτη φάση: Υλοποίηση του GDPR

Στην τρίτη και τελευταία φάση, η ΒΙΑΝΕΞ έδωσε έμφαση στην υλοποίηση θεμάτων πληροφορικής, όπως εισάγοντας τη χρήση ψευδωνυμοποίησης, ανωνυμοποίησης ή κρυπτογράφησης των δεδομένων ώστε να διασφαλιστεί η προστασία όλων αυτών των δεδομένων.

- **Ο Οδικός Χάρτης (Roadmap) για την Υλοποίηση του GDPR**

Τα 25 Βήματα για την Υλοποίηση του GDPR φαίνονται στην παρακάτω εικόνα, που αποτελεί και τον βασικό οδηγό διαμόρφωσης, σχεδιασμού και υλοποίησης στρατηγικής για τη ΒΙΑΝΕΞ.

Επιγραμματικά, επιδιώκεται αρχικά η οικοδόμηση του έργου και της ομάδας που θα συμμετέχει σε αυτό με κατανομή των πόρων, προϋπολογισμό του χρόνου και του κόστους που θα απορροφήσει το έργο και κατανομή των ρόλων στους εργαζομένους, στους υπευθύνους και στον DPO.

Στη συνέχεια, γίνεται μια πρώτη εκτίμηση των κινδύνων μέσω της χαρτογράφησης και της απογραφής των δεδομένων και αναπτύσσονται πολιτικές και διαδικασίες ώστε να κινητοποιηθούν οι εργαζόμενοι στην αποτελεσματικότερη εφαρμογή τους.

Ακόμα, σχεδιάζονται και υλοποιούνται οι απαραίτητοι λειτουργικοί έλεγχοι για τη διασφάλιση των δικαιωμάτων των υποκειμένων και των προσωπικών τους δεδομένων και πραγματοποιούνται οι απαραίτητες ενέργειες για τη διαχείριση και την ενίσχυση των ελέγχων αυτών.

Τέλος, μέσω προσομοιώσεων και εκπαιδευτικών προγραμμάτων, ενισχύεται η διαρκής συμμόρφωση και η αξιολόγηση των ανθρωπίνων πόρων της εταιρείας ως προς την αποτελεσματικότητα και την ετοιμότητά τους για την ενσωμάτωση του ΓΚΠΔ.

Εικόνα 11: *Τα 25 βήματα του Οδικού Χάρτη Υλοποίησης του GDPR στη ΒΙΑΝΕΞ*

- **<u>IT Λύσεις Ιδιωτικότητας πληροφοριακών Συστημάτων</u>**

Για την αναβάθμιση και τον εκσυγχρονισμό των συστημάτων της, η ΒΙΑΝΕΞ έχει ενσωματώσει πληροφοριακά συστήματα και εφαρμογές για την κρυπτογράφηση και απόκρυψη των δεδομένων και των e-mail της, τον έλεγχο μεταφοράς των δεδομένων, τη χαρτογράφηση της ροής των δεδομένων και τη μελέτη των επιπτώσεων αυτών. Επίσης, έχει εξασφαλίσει την ασφαλή αναζήτηση, αποθήκευση και ταξινόμηση των δεδομένων, τη διαγραφή και φορητότητα αυτών, καθώς και την εξασφάλιση των δικαιωμάτων των πελατών της ως προς τα προσωπικά τους δεδομένα.

- **<u>GDPR Stress Testing</u>**

Πραγματοποιείται στην τελευταία φάση του έργου και αφορά κάποια σενάρια «προσομοίωσης» για τον έλεγχο της ετοιμότητας της εταιρίας σε κάθε ένα από τα βασικά σημεία που απαιτούν προσοχή.

Περιλαμβάνει 3 διαφορετικές περιπτώσεις:

- Επίσκεψη της Αρχής Προστασίας Δεδομένων (Data protection authority visit)
- Αντικείμενο: Προσομοίωση επίσκεψης της Αρχής για τον καθορισμό της ελαστικότητας στην εφαρμογή των μέτρων και των κανόνων συμμόρφωσης με τον Κανονισμό.
- Βήματα: Αρχικά πραγματοποιείται η έρευνα όπως ορίζεται από την προσομοίωση, καταγράφονται τα πρώτα ευρήματα και κατατίθενται οι απόψεις και οι παρατηρήσεις των εμπλεκομένων στην προσομοίωση γύρω από αυτά. Έπειτα, μέσω των συζητήσεων καταγράφονται τα καθοριστικά ευρήματα της έρευνας και πραγματοποιείται ανάλυση του αντικτύπου από τη δημοσίευση αυτών, καθώς και των επιπτώσεων από την εφαρμογή του νέου Κανονισμού.
- Αποτέλεσμα: Μία έκθεση που περιέχει τα ευρήματα της έρευνας, την ανάλυση του δημόσιου αντικτύπου και την ανάλυση των μέτρων εφαρμογής.

- Προσομοίωση παραβίασης δεδομένων (Data breach simulation)
- Αντικείμενο: Προσομοίωση και παρακολούθηση παραβίασης προσωπικών δεδομένων με σκοπό τον προσδιορισμό της κατάστασης της τρέχουσας διαδικασίας.
- Βήματα: Αρχικά προσομοιώνεται η κατάσταση παραβίασης των προσωπικών δεδομένων και ενεργοποιούνται οι μηχανισμοί ειδοποίησης στο εσωτερικό της εταιρείας. Στη συνέχεια εξετάζεται η αποτελεσματικότητα της συνεχούς παρακολούθησης τέτοιων περιστατικών από την εταιρεία, αναλύονται τα ευρήματα της ετοιμότητας και των χειρισμών του προσωπικού και υποβάλλεται η τελική έκθεση.
- Αποτέλεσμα: Μία έκθεση που περιέχει τα ευρήματα της έρευνας και ταυτόχρονα εκπαίδευση των υπαλλήλων για το χειρισμό παραβιάσεων προσωπικών δεδομένων.

- Δημόσια δράση (Public action)
- Αντικείμενο: Προσομοίωση επίσκεψης της Αρχής για τον καθορισμό της ελαστικότητας στην εφαρμογή των μέτρων και των κανόνων συμμόρφωσης με τον Κανονισμό.
- Βήματα: Σε πρώτο στάδιο προσομοιώνεται ο τρόπος άσκησης των δικαιωμάτων των υποκειμένων και ελέγχεται η πρόσβαση στα προσωπικά τους δεδομένα, η δυνατότητα διόρθωσης, διαγραφής και ο αποκλεισμός από αυτά.

Έπειτα, πραγματοποιείται η προσομοίωση δημόσιων συμβάντων με σκοπό τον έλεγχο ετοιμότητας και επίγνωσης των διαδικασιών που ακολουθούνται από τους εργαζομένους και τους υπευθύνους της εταιρείας.

- Αποτέλεσμα: Μία έκθεση που περιέχει τα ευρήματα της έρευνας, την ανάλυση του δημόσιου αντικτύπου και την ανάλυση των μέτρων εφαρμογής.

- **Διαμόρφωση Κώδικα Επιχειρηματικής Συμπεριφοράς για προσωπικά δεδομένα**

Τελευταίο και σημαντικότερο στη φάση υλοποίησης της στρατηγικής της ΒΙΑΝΕΞ είναι η δημιουργία και η διαμόρφωση ενός εταιρικού κώδικα δεοντολογίας, πέρα από τις πιστοποιήσεις και τα ISO που αποκτά.

Η συγκεκριμένη εταιρεία ακολουθεί και προσαρμόζει κατά βάση στην κουλτούρα και την οργάνωσή της εταιρικούς και κλαδικούς κώδικες δεοντολογίας και επιχειρηματικής συμπεριφοράς, όπως για παράδειγμα των Κώδικα EFPIA για τα προσωπικά δεδομένα, που αποτελεί παράρτημα του Κώδικα των Συνδέσμων Φαρμακευτικών Εταιρειών Ελλάδας (ΣΦΕΕ).,

Ο Κώδικας Δεοντολογίας του ΣΦΕΕ, περιλαμβάνει τις ουσιαστικές ρυθμίσεις για την προώθηση των συνταγογραφημένων φαρμάκων, τη δημοσιοποίηση των παροχών από φαρμακευτικές επιχειρήσεις προς Επαγγελματίες Υγείας και Επιστημονικούς Υγειονομικούς Φορείς, τη Διαδικασία Ελέγχου Εφαρμογής, τον ενδεικτικό υπολογισμό της αμοιβής των επαγγελματιών υγείας για παρεχόμενες υπηρεσίες σε φαρμακευτικές επιχειρήσεις και το μητρώο κλινικών μη παρεκβατικών μελετών.

- **Συνεχής Επιθεώρηση και Παρακολούθηση του Προγράμματος (Auditing and Monitoring)**

Σε όλη τη διάρκεια του σχεδιασμού τη στρατηγικής, της αξιολόγησης και της υλοποίησης της, υπάρχει μια συνεχής ανάδραση και παρακολούθηση των βημάτων και της προετοιμασίας συμμόρφωσης με τον ΓΚΠΔ, ώστε να μπορούν να βελτιώνονται, να αλλάζουν ή να τροποποιούνται διαδικασίες που κρίνονται απαραίτητες για την εκπλήρωση του τελικού στόχου.

- **<u>Χρονοδιάγραμμα Υλοποίησης Έργου του GDPR</u>**

Με την εφαρμογή όλων των παραπάνω μέτρων και διαδικασιών, η ΒΙΑΝΕΞ επιδιώκει την ασφαλέστερη και ομαλότερη μετάβαση της στα νέα δεδομένα.

Εικόνα 12: *Χρονοδιάγραμμα Υλοποίησης GDPR στη ΒΙΑΝΕΞ [4/2017 – 5/2018]*

Στην εικόνα, παρουσιάζεται το τελικό χρονοδιάγραμμα υλοποίησης του έργου της με τα βήματα που ακολουθεί και που περιγράφηκαν αναλυτικότερα προηγουμένως, από την έναρξη των διαδικασιών προσαρμογής της τον Απρίλιο του 2017 μέχρι και τον Μάιο του 2018 που θα πρέπει να είναι έτοιμη να συμμορφωθεί πλήρως με το νέο Κανονισμό.

6.4 Σύνοψη

Στο παρόν κεφάλαιο, έγινε μια αναφορά της επιρροής του GDPR στις φαρμακοβιομηχανίες και στα προβλήματα που θα αντιμετωπίσουν στη επεξεργασία των δεδομένων με την εισαγωγή του νέου Κανονισμού. Επιπλέον, επιδιώχθηκε να παρουσιαστεί η εφαρμογή της μεθοδολογίας συμμόρφωσης με τον GDPR όπως τη σχεδίασε η ελληνική φαρμακευτική εταιρεία ΒΙΑΝΕΞ και να συσχετιστεί η θεωρία με την πράξη.

Διαπιστώθηκε ότι τα κύρια σημεία υλοποίησης της στρατηγικής συμμόρφωσης με τον Κανονισμό παραμένουν κατά πλειοψηφία ίδια, τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο, ενώ ο βασικός πυρήνας για την πραγματοποίηση του μέχρι το τελικό στάδιο, είναι η διαμόρφωση μιας ενιαίας αντίληψης και κουλτούρας του προσωπικού μέσα στην επιχείρηση.

7. ΣΥΜΠΕΡΑΣΜΑΤΑ

7.1 Εισαγωγή

Ο σκοπός της παρούσας μεταπτυχιακής εργασίας, είναι η παρουσίαση του Νέου Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων, των αλλαγών και των προκλήσεων που θα επιφέρει στους πολίτες και στις επιχειρήσεις, καθώς και η μελέτη και αξιοποίηση όλων των στρατηγικών και εργαλείων που υπάρχουν μέχρι στιγμής διαθέσιμα, για το σχεδιασμό και την υποβολή προτάσεων στρατηγικής, που θα βοηθήσουν τις επιχειρήσεις να ενσωματώσουν το νέο Κανονισμό στις εσωτερικές τους διαδικασίες.

Για τους λόγους αυτούς, έγινε μια πλήρης αναφορά στην αναγκαιότητα προστασίας των προσωπικών δεδομένων, όπως επίσης και στις συνθήκες που οδήγησαν τα κράτη, ήδη από πολύ παλιά, στη θέσπιση κανόνων και ρυθμιστικών πλαισίων για την προστασία και διασφάλιση των προσωπικών δεδομένων. Ωστόσο, παρά τις συνεχείς τροποποιήσεις και προσαρμογές των νομικών πλαισίων στα νέα δεδομένα, οι συνεχείς και ραγδαίες εξελίξεις της τεχνολογίας και της παγκοσμιοποίησης, κατέστησαν αναγκαία τη θέσπιση για μία ακόμα φορά, ενός νέου ευρύτερου και πιο εκσυγχρονισμένου ρυθμιστικού πλαισίου, το οποίο θα εφαρμόζει αυστηρότερα μέτρα διασφάλισης και κατοχύρωσης των προσωπικών δεδομένων.

Δεδομένου ότι ο GDPR αποτελεί έναν νέο, ευρύτερο και άμεσης εφαρμογής Κανονισμό από τις 25 Μαΐου 2018, περιγράφηκαν πλήρως το περιεχόμενο, οι ορισμοί και τα νέα δεδομένα που εισάγει, καθώς και οι προκλήσεις τις οποίες καλούνται να αντιμετωπίσουν πολίτες και επιχειρήσεις κατά την εφαρμογή του.

Μέσα από την περιγραφή αυτή, παρουσιάστηκαν οι νέες αλλαγές, όπως η υποχρέωση γνωστοποίησης στις αρμόδιες Αρχές σε περίπτωση παραβίασης προσωπικών δεδομένων, η μελέτη της εκτίμησης αντικτύπου της παραβίασης, η εισαγωγή του ρόλου του Υπευθύνου Προστασίας Δεδομένων, οι νέοι κανόνες για την προστασία των παιδιών, αλλά και οι κυρώσεις και τα πρόστιμα με τα οποία έρχονται αντιμέτωπες οι επιχειρήσεις σε περίπτωση που δεν συμμορφωθούν με τον GDPR.

Για την καλύτερη κατανόηση όλων των παραπάνω, αναπτύχθηκαν τα βήματα προετοιμασίας και η γενική μεθοδολογία που μπορούν να ακολουθήσουν οι επιχειρήσεις και οι οργανισμοί, για να εναρμονιστούν με το νέο πλαίσιο του Κανονισμού. Σε αυτή τη φάση, επισημάνθηκε ιδιαίτερα ο κρίσιμος ρόλος του DPO και οι προκλήσεις που καλείται να αντιμετωπίσει κατά την εφαρμογή της μεθοδολογίας ενσωμάτωσης του GDPR στην εσωτερική δομή της επιχείρησης, ενώ έγινε αναφορά στα ζητήματα και τους προβληματισμούς που αντιμετωπίζουν οι επιχειρήσεις κατά την επιλογή και το διορισμό του. Επιπλέον, διαπιστώθηκε η σημαντικότητα ύπαρξης ενός πλάνου εκπαίδευσης για το προσωπικό του οργανισμού και η συνεχής επικαιροποίηση και επανάληψη αυτού.

Στη υποστήριξη και την καλύτερη εφαρμογή της μεθοδολογίας, μπορούν να συμβάλλουν τα διαθέσιμα λογισμικά και πληροφοριακά συστήματα της αγοράς ή και η συνεργασία με εξωτερικές εταιρείες παροχής υπηρεσιών και συμβούλων. Γι’ αυτό το λόγο, αναλύθηκαν μερικά από τα χαρακτηριστικά των συστημάτων και λογισμικών υποστήριξης κορυφαίων εταιρειών στο χώρο της πληροφορικής, αλλά και οι παρεχόμενες υπηρεσίες που μπορούν να προσφέρουν στην επιχείρηση, εξειδικευμένες εταιρείες πιστοποιημένων συμβούλων σε αυτό τον τομέα.

Τέλος, με το συνδυασμό όλων των παραπάνω κανόνων, γνώσεων, προτάσεων και εφαρμογών, πραγματοποιήθηκε η πρακτική εφαρμογή της μεθοδολογίας που μπορούν να ακολουθήσουν οι επιχειρήσεις. Πιο συγκεκριμένα, διαπιστώθηκε η επίδραση του νέου Κανονισμού στην προστασία των προσωπικών δεδομένων για τις φαρμακοβιομηχανίες και περιγράφηκε ο σχεδιασμός και η υλοποίηση του στρατηγικού πλάνου της ελληνικής φαρμακευτικής εταιρείας ΒΙΑΝΕΞ, με σκοπό την εφαρμογή του GDPR στις εσωτερικές λειτουργίες της εταιρείας. Έτσι, δόθηκε η ευκαιρία για την τελική διατύπωση ορισμένων προτάσεων και την εξαγωγή των κυριότερων συμπερασμάτων από την ολοκλήρωση της εργασίας, τα οποία διατυπώνονται στη συνέχεια.

7.2 Κύρια Συμπεράσματα

Η προστασία των προσωπικών δεδομένων, ήταν ανέκαθεν ένα από τα κύρια ζητήματα που απασχολούσαν τόσο τα φυσικά πρόσωπα και τις επιχειρήσεις, όσο και τα ίδια τα κράτη, ήδη από τα παλιότερα χρόνια που η τεχνολογία δεν ήταν τόσο εξελιγμένη. Με την εισαγωγή του νέου Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων, που θα τεθεί σε ισχύ στις 25.5.2018, η ασφάλεια των δεδομένων καθίσταται πλέον αναγκαία και επιτακτική, με τα μέτρα για την εφαρμογή της να γίνονται αυστηρότερα και να συμπεριλαμβάνουν όλο και περισσότερους τομείς εφαρμογών.

Τα κύρια συμπεράσματα αυτής της εργασίας από την ανάλυση της εισαγωγής και εφαρμογής του GDPR, μπορούν να συνοψισθούν ως εξής:

1. Ο GDPR αποτελεί το βασικό νομοθέτημα για την προστασία προσωπικών δεδομένων σε επίπεδο Ευρωπαϊκών Κοινοτήτων, καταργώντας την Οδηγία 95/46/ΕΚ. Έχει σχεδιαστεί κατά τέτοιο τρόπο ώστε να δώσει στους πολίτες μεγαλύτερο έλεγχο των προσωπικών τους στοιχείων στα πλαίσια του νέου, ψηφιακού κόσμου αλλά και να απλοποιήσει το ρυθμιστικό περιβάλλον για τις διεθνείς επιχειρήσεις με την ενοποίηση του Κανονισμού εντός της ΕΕ.

2. Ο GDPR αφορά όλες τις επιχειρήσεις, (ιδιωτικού και δημόσιου τομέα) που με οποιοδήποτε τρόπο διαχειρίζονται προσωπικά δεδομένα τα οποία αφορούν σε άτομα (εργαζομένους, συνεργάτες, πελάτες, ή άλλα φυσικά πρόσωπα) εντός της Ευρωπαϊκής Ένωσης. Δηλαδή αφορά σχεδόν το σύνολο των επιχειρήσεων, ανεξαρτήτως του κλάδου που δραστηριοποιούνται. Ωστόσο κάποιες, λόγω της φύσης των δραστηριοτήτων τους, θα επηρεαστούν σε μεγαλύτερο βαθμό, όπως:
    - οι υπηρεσίες υγείας,
    - οι χρηματοοικονομικές υπηρεσίες,
    - οι υπηρεσίες ανθρώπινου δυναμικού,
    - οι υπηρεσίες φιλοξενίας και μετακινήσεων,
    - οι υπηρεσίες διαδικτυακών και προσωποποιημένων πωλήσεων,
    - η παροχή τηλεπικοινωνιακών υπηρεσιών,
    - η παροχή υπηρεσιών ενέργειας και

- οι υπηρεσίες του κρατικού τομέα.

Σε κάθε οργανισμό, οποιαδήποτε λειτουργία στην οποία χρησιμοποιούνται προσωπικά δεδομένα, σε οποιαδήποτε μορφή, θα επηρεαστούν εξίσου ή και σε μεγαλύτερο βαθμό, συνεπώς ο νέος Κανονισμός είναι ένα ζήτημα που δεν αφορά αποκλειστικά τη Διεύθυνση Πληροφοριακών Συστημάτων μιας εταιρείας αλλά το σύνολο του οργανισμού.

3. Οι βασικές αλλαγές που προκύπτουν από την εφαρμογή του νέου Κανονισμού για τις επιχειρήσεις είναι:
    - Συνολική υποχρέωση εναρμόνισης και συμμόρφωσης των οργανισμών με τον GDPR.
    - Αυξημένη διαφάνεια εσωτερικών διαδικασιών και ανάγκη ύπαρξης εσωτερικού μητρώου δεδομένων.
    - Εισαγωγή του ρόλου του Υπευθύνου Προστασίας Δεδομένων (DPO).
    - Υποχρέωση αναφοράς και γνωστοποίησης περιστατικών παραβίασης προστασίας δεδομένων.
    - Σαφής και ακριβής συγκατάθεση εκ μέρους των ατόμων κατά την επεξεργασία των προσωπικών δεδομένων τους.
    - Αυξημένα δικαιώματα σε κάθε άτομο για διαγραφή και μεταβολή των προσωπικών του δεδομένων.
    - Περιορισμός της πρόσβασης στα δεδομένα όταν πραγματοποιείται η επεξεργασία τους.
    - Εκτέλεση εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων (DPIA)
    - Συνεχής παρακολούθηση των κινδύνων προστασίας - προσωπικών δεδομένων σε ολόκληρο τον οργανισμό
    - Επιβολή Υψηλών Προστίμων (4% παγκόσμιου τζίρου ή 20 εκατομμύρια ευρώ – όποιο είναι μεγαλύτερο).

4. Οι ενέργειες που οφείλουν να ακολουθούν οι εταιρείες και οι οργανισμοί είναι:

- Να προστατεύουν τα προσωπικά δεδομένα λαμβάνοντας κατάλληλα μέτρα ασφαλείας.
- Να γνωστοποιούν στις εποπτικές αρχές τις παραβιάσεις προσωπικών δεδομένων εντός 72 ωρών.
- Να λαμβάνουν συγκατάθεση για τη συλλογή και την επεξεργασία προσωπικών δεδομένων.
- Να τηρούν αρχεία που θα παρέχουν αναλυτικές πληροφορίες για τις δραστηριότητες επεξεργασίας δεδομένων.
- Να παρέχουν σαφή γνωστοποίηση για τη συλλογή δεδομένων.
- Να περιγράφουν το λόγο και τις περιπτώσεις επεξεργασίας των προσωπικών δεδομένων.
- Να ορίζουν πολιτικές διατήρησης και διαγραφής δεδομένων.

5. Από την άλλη μεριά, τα φυσικά πρόσωπα ή υποκείμενα των δεδομένων, αποκτούν μια σειρά από δικαιώματα, όπως:
    - Το δικαίωμα ενημέρωσης για τον τρόπο με τον οποίο χρησιμοποιούνται τα προσωπικά τους δεδομένα από του οργανισμούς.
    - Το δικαίωμα πρόσβασης ώστε να γνωρίζουν επακριβώς ποιες πληροφορίες υφίστανται επεξεργασία, πώς και για ποιο σκοπό.
    - Το δικαίωμα διόρθωσης που τους επιτρέπει να ζητήσουν διόρθωση των προσωπικών τους δεδομένων αν αυτά είναι ανακριβή ή ελλιπή.
    - Το δικαίωμα διαγραφής ή αλλιώς «το δικαίωμα λήθης», με το οποίο μπορούν να ζητήσουν διαγραφή ή κατάργηση των προσωπικών τους δεδομένων χωρίς να χρειάζεται κάποιος συγκεκριμένος λόγος.
    - Το δικαίωμα περιορισμού της επεξεργασίας ώστε να μπορούν να αποκλείουν ή να καταστέλλουν την επεξεργασία των προσωπικών τους δεδομένων.
    - Το δικαίωμα μεταφοράς δεδομένων που τους επιτρέπει να διατηρούν και να επαναχρησιμοποιούν τα προσωπικά τους δεδομένα για δικό τους σκοπό.
    - Το δικαίωμα αντικρούσεως, με το οποίο μπορούν να αντιταχθούν στην χρήση των προσωπικών τους δεδομένων.
    - Το δικαίωμα (μη) αυτοματοποιημένης λήψης αποφάσεων και διαμόρφωσης προφίλ, με το οποίο μπορούν να μην αποτελέσουν

αντικείμενο αυτοματοποιημένης απόφασης αν αυτή έχει έννομες συνέπειες.

6. Σύμφωνα με έρευνες που έχουν πραγματοποιηθεί, οι περισσότερες επιχειρήσεις δεν είναι ακόμα έτοιμες να υποδεχθούν και να συμμορφωθούν με τον GDPR, είτε λόγω αντίδρασής του στο νέο Κανονισμό, είτε λόγω μη επαρκούς ενημέρωσής τους για τον τρόπο εφαρμογής του. Για το λόγο αυτό, προτάθηκαν τα βασικά βήματα προετοιμασίας και οι μεθοδολογίες που μπορούν να βοηθήσουν μια επιχείρηση στην ομαλότερη μετάβαση στον GDPR. Αυτά σχετίζονται με: την κατανόηση του Κανονισμού και την αναγνώριση του είδους των προσωπικών δεδομένων που έχει στην κατοχή της η επιχείρηση, την ανίχνευση και την αξιολόγηση των συστημάτων και των δικλείδων ασφαλείας που παρέχει στους πελάτες της για την προστασία των δεδομένων τους, τον ορισμό του DPO, την αναδιοργάνωση των εσωτερικών της λειτουργιών και πληροφοριακών υποδομών της, τη συνεχή εκπαίδευση του προσωπικού της και το σχεδιασμό και την υλοποίηση μιας ολοκληρωμένης στρατηγικής που θα οδηγήσει στη συμμόρφωση με τον GDPR.

7. Ο ρόλος του DPO αποδεικνύεται ότι είναι κρίσιμης σημασίας στην εναρμόνιση της εταιρείας με τον GDPR, αφού καθίσταται υπεύθυνος για τη συνεχή παρακολούθηση των εργασιών μετάβασης στα νέα δεδομένα αλλά και αρμόδιος για τον έλεγχο τόσο των ενεργειών του υπευθύνου και του εκτελούντος την επεξεργασία των δεδομένων, όσο και για τη συμβουλευτική υποστήριξη και εκπαίδευση του προσωπικού. Οφείλει να έχει όλα τα απαραίτητα προσόντα που θα τον κάνουν αποτελεσματικότερο στην εκπλήρωση των στόχων του οργανισμού και τα οποία θα μπορούν να δικαιολογούν και την ανάλογη αμοιβή του. Ωστόσο, βρίσκεται στη διάθεση της επιχείρησης η επιλογή του αν ο DPO θα είναι εσωτερικός ή εξωτερικός συνεργάτης, αφού πρέπει να λαμβάνεται υπόψιν τόσο η αμεροληψία και οι ικανότητές του, όσο και το κόστος του για την επιχείρηση σε κάθε περίπτωση.

8. Το προσωπικό από την, άλλη οφείλει να ενημερώνεται και να εκπαιδεύεται διαρκώς σχετικά με τον συγκεκριμένο Κανονισμό, ώστε να μπορεί να ανταπεξέρχεται και να βρίσκεται σε συνεχή ετοιμότητα για τυχόν μελλοντικές

παραβιάσεις ή έκτακτες καταστάσεις που μπορεί να προκύψουν. Η επικαραιποίηση της εκπαίδευσής του, μπορεί να προέλθει από την παρακολούθηση ειδικών σεμιναρίων, workshops ή συνεδρίων σχετικών με το GDPR, ώστε να έχει γνώση των τελευταίων εξελίξεων γύρω από το θέμα.

9. Με την αναφορά που έγινε στα λογισμικά υποστήριξης που έχουν αναπτύξει ή προσαρμόσει μερικές από τις γνωστότερες εταιρείες πληροφορικής στο χώρο, προκύπτει ότι υπάρχει ένα μεγάλο εύρος προϊόντων στην αγορά, ανάλογα με τις ανάγκες, τη χρήση και τον τύπο δεδομένων της κάθε επιχείρησης. Ωστόσο, διαπιστώνεται, ότι εταιρείες όπως η ORACLE, που να διαθέτουν ολοκληρωμένα και ειδικά διαμορφωμένα συστήματα για την ενσωμάτωση του GDPR, είναι ελάχιστες. Οι περισσότερες επιλέγουν την ενσωμάτωση νέων λειτουργιών στα ήδη υπάρχοντα συστήματα τους, ώστε να συμβαδίζουν με τον ήδη υπάρχοντα εξοπλισμό της επιχείρησης, και δεν επιλέγουν τόσο την εξ' αρχής ανάπτυξη νέων λογισμικών ειδικά για τον GDPR, λόγω μεγαλύτερου κόστους και χρόνου υλοποίησης.

10. Στη διάθεση των επιχειρήσεων για την εναρμόνισή τους με το νέο Κανονισμό, βρίσκονται και διάφορες εταιρείες παροχής συμβουλευτικών και εκπαιδευτικών υπηρεσιών, οι οποίες διαθέτουν το κατάλληλα εξειδικευμένο προσωπικό για να βοηθήσει την επιχείρηση να ανταπεξέλθει γρηγορότερα στη μετάβαση των όρων του νέου Κανονισμού. Οι εταιρείες αυτές, παρέχουν ολοκληρωμένες λύσεις για το σχεδιασμό και την υλοποίηση της στρατηγικής συμμόρφωσης της εταιρείας, από το πρώτο βήμα μέχρι το τελευταίο, ενώ ταυτόχρονα βρίσκονται δίπλα στην επιχείρηση καθ' όλη τη διάρκεια ισχύς του Κανονισμού.

11. Με την εφαρμογή της προτεινόμενης μεθοδολογίας στο σχεδιασμό συμμόρφωσης με τον GDPR της ΒΙΑΝΕΞ, διαπιστώθηκε ότι το θεωρητικό υπόβαθρο συγκλίνει με την πρακτική εφαρμογή του Κανονισμού. Η γενική ιδέα της προετοιμασίας και ανίχνευσης των δεδομένων, της αξιολόγησης και εκτίμησης αυτών και της υλοποίησης της στρατηγικής παραμένουν ίδια, ενώ μεγάλο αντίκτυπο για την πραγματοποίηση όλων αυτών έχει η διαμόρφωση μιας ενιαίας κουλτούρας στις εσωτερικές λειτουργίες της επιχείρησης. Χαρακτηριστικά, η μεθοδολογία συμμόρφωσης της ΒΙΑΝΕΞ περιλαμβάνει συνοπτικά τα εξής βήματα:

- Δημιουργία Ομάδας Έργου και DPO
- Κατανομή ρόλων και αρμοδιοτήτων στην Ομάδα Έργου GDPR
- Αλλαγή Κουλτούρας
- Διάγνωση 360°- Χαρτογράφηση (Data Mapping)
- Αξιολόγηση Βαθμού ετοιμότητας (GDPR Readiness)
- Ροή Δεδομένων-Πληροφοριών (Data/Information Flow)
- Ανάλυση Ελλείψεων (Gap Analysis) ως προς τον GDPR
- Σχεδιασμό Προγράμματος Προστασίας Προσωπικών Δεδομένων (Compliance Plan) και Εξασφάλιση Δικαιωμάτων Φυσικών Προσώπων
- Απαιτούμενες Πολιτικές και Διαδικασίες Προστασίας Προσωπικών δεδομένων
- Συγγραφή Μελέτης Αντικτύπου Ιδιωτικότητας (DPIA)
- Μηχανισμούς Διαβίβασης Δεδομένων σε Τρίτες Χώρες
- Οδικό Χάρτη (Roadmap) για την Υλοποίηση του GDPR
- IT Λύσεις Ιδιωτικότητας πληροφοριακών συστημάτων
- GDPR Stress Testing
- Διαμόρφωση Κώδικα Επιχειρηματικής Συμπεριφοράς για προσωπικά δεδομένα
- Συνεχής Επιθεώρηση και Παρακολούθηση του Προγράμματος (Auditing and Monitoring)

12. Ωστόσο, παρατηρείται ότι είναι νωρίς ακόμα για την εξαγωγή ασφαλών συμπερασμάτων σχετικά με την πρακτική εφαρμογή του νέου Κανονισμού, καθώς όσες επιχειρήσεις προσαρμόζουν τα συστήματά τους για να συμμορφωθούν με τον GDPR, βασίζονται στη θεωρητική πλευρά της μεθοδολογίας του Κανονισμού, αφού η πραγματικότητα της εφαρμογής όλων αυτών των αλλαγών θα φανεί με την έναρξη ισχύος του Κανονισμού στις 25.5.2018.

13. Τέλος, από την βιβλιογραφική έρευνα που πραγματοποιήθηκε, διαπιστώθηκε ότι οι διαδικασίες εφαρμογής του νέου Κανονισμού στο δημόσιο τομέα, είναι σχεδόν ανύπαρκτες, ενώ αντίθετα στον ιδιωτικό τομέα, παρά τις δυσκολίες που

αντιμετωπίζουν οι επιχειρήσεις στην προσαρμογή στον Κανονισμό, οι προσπάθειες που γίνονται είναι μεγαλύτερες και με γρηγορότερους ρυθμούς.

7.3 Εκπλήρωση των στόχων της εργασίας

Κατά τη διάρκεια αυτής της εργασίας εκπληρώθηκαν όλοι οι στόχοι που τέθηκαν στο υποκεφάλαιο 1.3 και συγκεκριμένα :

- ✓ Έγινε μια γενική παρουσίαση των προσωπικών δεδομένων και της ιστορικής εξέλιξης τους, καθώς και της επιτακτικής ανάγκης που υπάρχει για τη διασφάλιση και προστασία αυτών.
- ✓ Παρουσιάστηκαν και αναλύθηκαν όλα τα ευρωπαϊκά και εθνικά νομικά ρυθμιστικά πλαίσια για την εξασφάλιση της προστασίας των προσωπικών δεδομένων.
- ✓ Παρουσιάστηκαν όλα τα σημαντικά νέα δεδομένα, οι αλλαγές και οι νέες ρυθμίσεις που επιφέρει ο Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων, τόσο στον ιδιωτικό τομέα όσο και στον δημόσιο.
- ✓ Παρουσιάστηκαν τα δικαιώματα που αποκτούν τα φυσικά πρόσωπα με την εφαρμογή του νέου Κανονισμού, καθώς και οι περιορισμοί και οι κυρώσεις που αντιμετωπίζουν οι επιχειρήσεις από τη μη συμμόρφωση με τον Κανονισμό.
- ✓ Αναλύθηκαν η γενική μεθοδολογία και τα βήματα προετοιμασίας που μπορούν να ακολουθήσουν οι επιχειρήσεις για την ένταξη και τη συμμόρφωσή τους με τον GDPR.
- ✓ Διαπιστώθηκε ο κρίσιμος ρόλος του Υπευθύνου Προστασίας Δεδομένων (DPO) στην εφαρμογή της μεθοδολογίας για τον GDPR.
- ✓ Παρουσιάσθηκαν και αναπτύχθηκαν προτάσεις και μεθοδολογίες που αφορούν στη συμμόρφωση με τον GDPR και οι οποίες χρησιμοποιήθηκαν για την πρακτική εφαρμογή τους στην υλοποίηση της στρατηγικής συμμόρφωσης με τον GDPR σε μια ελληνική φαρμακευτική εταιρεία.

7.4 Σύνοψη

Στο τελευταίο κεφάλαιο της παρούσας μεταπτυχιακής εργασίας παρουσιάστηκαν τα συμπεράσματα που προέκυψαν από τη συνολική μελέτη της εφαρμογής του νέου

Γενικού Κανονισμού για την προστασία των προσωπικών δεδομένων και των μεθόδων που μπορούν να ακολουθήσουν οι επιχειρήσεις και ο οργανισμοί για τη συμμόρφωσή τους με αυτόν. Η αποτελεσματική αξιοποίηση όλων των παρεχόμενων εργαλείων και υπηρεσιών σε συνδυασμό με τις προτεινόμενες μεθόδους προετοιμασίας των επιχειρήσεων για τη μετάβαση στα νέα δεδομένα, μπορούν να αποτελέσουν απαραίτητα στοιχεία στη δημιουργία κατευθυντήριων γραμμών για την εναρμόνιση με το νέο Κανονισμό, τόσο στον ιδιωτικό όσο και στο δημόσιο τομέα.

8. ΑΝΑΦΟΡΕΣ

ΠΑΡΟΥΣΙΑΣΕΙΣ – ΔΙΑΦΑΝΕΙΕΣ – ΕΝΗΜΕΡΩΤΙΚΑ ΔΕΛΤΙΑ

ALGOSYSTEMS, Διαφάνειες: “GDPR Presentation”, [1/2018]

ALGOSYSTEMS, Φυλλάδιο “GDPR: WILL YOU BE READY? Algosystems Meets Your GDPR Challenge”, [1/2018]

ALTIMA Business Integrator, “GDPR in SAP”, [9/2017]

Asnot B., Solution SE Benelux, “General Data Protection Regulation Using Symantec Technology to Support the Data Privacy Lifecycle”, [11/2017]

Axl & Trax, The security company for SAP environments, “GDPR & SAP ACCESS MANAGEMENT”, [10/2017]

Balaganski A., “Leadership Compass Database Security”, KuppingerCole Report No 70970, [11/2017]

Chantzos I., EMEA & APJ, Παρουσίαση: “How to understand and comply with GDPR”, [12/2017]

De Jong M., Oracle EMEA, “The EU General Data Protection Regulation: How Oracle Systems and Storage Capabilities Can Help”, [10/2017]

Deloitte Risk Advisory, “General Data Protection Regulation (GDPR): Deloitte NWE Privacy Services–Vision and Approach”, [12/2017]

Derek E. Brink, Aberdeen Group, “Countdown to GDPR Enforcement: Is your organization technology ready?”, [6/2017]

Dr. Ntouskas T., «ΓΚΠΔ: Μεθοδολογία Πρακτικής Εναρμόνισης», 3ο Παγκόσμιο Συνέδριο ICT Security, Αθήνα, [6/2017]

Jourová V., «Μεταρρύθμιση της προστασίας των δεδομένων στην ΕΕ: Ποια είναι τα οφέλη για τις επιχειρήσεις στην Ευρώπη», Ενημερωτικό δελτίο, [1/2016]

Microsoft, Παρουσίαση: “Beginning your General Data Protection Regulation (GDPR) Journey-Accelerate GDPR compliance with the Microsoft Cloud” [11/2017]

Miller L., CISSP, “Database protection for dummies-A Wiley Brand”, Oracle Special Edition, [11/2017]

Pouliou A., Παρουσίαση: “Pseudonymization Best Practice: The Value of Data and De-ID Examples”, Αθήνα, [27/6/2017]

Priority Business Intelligence, Διαφάνειες: «GDPR: μία νέα πραγματικότητα για τις επιχειρήσεις και πώς η PRIORITY μπορεί να σας βοηθήσει», [1/2018]

Priority Business Intelligence, Διαφάνειες: «GDPR η πρόκληση και η ολοκληρωμένη προσέγγιση», [1/2018]

Rajasekharan D., “Accelerate Your Response to the EU General Data Protection Regulation (GDPR) Using Oracle Database Security Products”, Oracle white paper, [1/2017]

SAP, “Data Protection and Privacy at SAP – Getting ready for May 25, 2018 – Part 2: Product and Services Compliance”, Version: 2.0-Public, [3/7/2017]

Symantec, Solution Brief, “Why you need an Information Centric Security model for the GDPR”, [11/2017]

Symantec, Διαφάνειες: “GDPR: Are you compliance-ready? Countdown to GDPR”. [11/2017]

Symantec, Φυλλάδιο: “Control Compliance Suite and GDPR”, [11/2017]

Theodoropoulos D., Παρουσίαση: “The EU General Data Protection Regulation and how Oracle can help”, Oracle, 2015

Vordos I., Intracom Telecom, Παρουσίαση: «Preparing for Compliance with GDPR-Background and Solutions», [12/2017]

Zarsky T., «Incompatible: The GDPR in the Age of Big Data», [8/8/2017]

ΑΠΔΠΧ, Φυλλάδιο: «Ο νέος Κανονισμός για την προστασία των προσωπικών δεδομένων» [10/2017]

ΑΠΔΠΧ, Φυλλάδιο: «Προσωπικά Δεδομένα και διαδίκτυο», [11/2017]

Ευαγγελίδης Α., Διαφάνειες Παρουσίασης: «Η Υλοποίηση του GDPR σε μια Ελληνική Φαρμακευτική Εταιρεία, VIANEX & VIAN S.A, [11/2017]

Ζωγραφόπουλος Δ., «Η υποχρέωση διενέργειας εκτίμησης αντικτύπου (Data protection impact assessment - DPIA) στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR)», ΣΥΝήΓΟΡΟΣ, τεύχος 120/2017, [12/2017]

Μήτρου Λ., Διαφάνειες: «Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (2016/679) - Νέο Δίκαιο, Νέες Προκλήσεις, Νέες απαιτήσεις», [10/2017]

Μήτρου Λ., Διαφάνειες: «Η ιστορία της προστασίας προσωπικών δεδομένων», [10/2017]

Περιοδικό netweek, "A Practical Guide to GDPR", Ετήσια Έκδοση 2017, [11/2017]

Σταθοπούλου Λ., Priority Business Intelligence, Παρουσίαση: «GDPR Εμπειρίες και διδάγματα από τα πρώτα ολοκληρωμένα έργα», [1/2018]

Τσόλιας Γ., «Υποχρεώσεις συμμόρφωσης στον Γενικό Κανονισμό Προσωπικών Δεδομένων (GDPR) και ο ρόλος του Υπευθύνου Προστασίας Δεδομένων (DPO)», [1/2018]

ΠΗΓΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Biscoe C., "3 tips for successful GDPR staff training", https://www.itgovernance.co.uk/blog/3-tips-for-successful-gdpr-staff-training/, [Πρόσβαση: 12/2017]

Business News, «Wind: Ολοκλήρωσε έργο EU GDPR με τεχνολογίες Oracle», http://www.businessnews.gr/article/91283/wind-oloklirose-ergo-eu-gdpr-me-tehnologies-oracle, [Πρόσβαση: 12/2017]

Chen D., «Outsourcing your organization's DPO duties? Consider this», https://iapp.org/news/a/outsourcing-your-organizations-dpo-duties-consider-this/, [Πρόσβαση: 12/2017]

Cyber Insurance Greece, «480 ημέρες έχουν απομείνει για την εφαρμογή του Γενκού Κανονισμού Προστασίας Δεδομένων (GDPR), εσείς πότε θα είστε έτοιμοι?», http://www.cyberinsurancegreece.com/news/a480-imeres-echoyn-apomeinei-gia-tin-efarmogi-toy-genkoy-kanonismoy-prostasias-dedomenon-gdpr-eseis-pote-tha-eiste-etoimoi/, [Πρόσβαση: 10/2017]

Cyber Insurance Greece, «Η εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων και ο ορισμός DPO θα εξασφαλίσει την ασφαλισιμότητα των εταιριών και θα βοηθήσει στην ανάπτυξη της αγοράς ασφάλισης Cyber Insurance», http://www.cyberinsurancegreece.com/news/i-efarmogi-toy-genikoy-kanonismoy-prostasias-dedomenon-kai-o-orismos-dpo-tha-exasfalisei-tin-asfalisimotita-ton-etairion-kai-tha-voithisei-stin-anaptyxi-tis-agoras-asfalisis-cyber-insurance/, [Πρόσβαση: 10/2017]

Cyber Insurance Quote.gr, «10 Βήματα προετοιμασίας για την εφαρμογή του νέου Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων», http://www.cyberinsurancequote.gr/news/a10-vimata-proetoimasias-gia-tin-efarmogi-toy-neoy-genikoy-kanonismoy-gia-tin-prostasia-ton-prosopikon-dedomenon/, [Πρόσβαση: 12/2017]

ESNC Enterprise Security and Compliance, “GDPR and SAP – Three Things To Do Now To Prevent Major Data Breaches and Fines”, https://www.esnc.de/blog/gdpr-sap/index.html, [Πρόσβαση: 1/2018]

ESNC Enterprise Security and Compliance,«GDPR and SAP – Three Things To Do Now To Prevent Major Data Breaches and Fines», https://www.esnc.de/blog/gdpr-sap/index.html, [Πρόσβαση: 12/2017]

Euro2day, «Επιχειρήσεις: Τα 5 βήματα για προστασία των προσωπικών δεδομένων», http://www.euro2day.gr/news/enterprises/article/1578362/epiheirhseis-ta-5-vhmata-gia-prostasia-ton-prosopi.html, [Πρόσβαση: 12/2017]

Hunton & Williams, “CNIL Publishes Six Step Methodology and Tools to Prepare for GDPR”, https://www.huntonprivacyblog.com/2017/03/17/cnil-publishes-six-step-methodology-tools-prepare-gdpr/, [Πρόσβαση: 10/2017]

IBM, «Η IBM προτείνει το πλαίσιο προσαρμογής των εταιρειών στον επικείμενο Γενικό Κανονισμό της ΕΕ για την προστασία Δεδομένων Προσωπικού Χαρακτήρα», http://www.ictplus.gr/default.asp?pid=30&rID=50348&ct=2&la=1, 2017, Πρόσβαση: 12/2017]

Lawspot.gr, «Η επιβολή διοικητικών προστίμων με βάση τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR)», https://www.lawspot.gr/nomika-nea/i-epivoli-

dioikitikon-prostimon-me-vasi-ton-geniko-kanonismo-gia-tin-prostasia-dedomenon, [Πρόσβαση: 11/2017]

Lawspot.gr, «Η επιβολή διοικητικών προστίμων με βάση τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR)», https://www.lawspot.gr/nomika-nea/i-epivoli-dioikitikon-prostimon-me-vasi-ton-geniko-kanonismo-gia-tin-prostasia-dedomenon, [Πρόσβαση: 1/2018]

Lawspot.gr, «Οδηγίες για τη γνωστοποίηση παραβίασης προσωπικών δεδομένων σύμφωνα με τον Γενικό Κανονισμό (GDPR)», https://www.lawspot.gr/nomika-nea/odigies-gia-ti-gnostopoiisi-paraviasis-prosopikon-dedomenon-symfona-me-ton-geniko, [Πρόσβαση: 1/2018]

Mancier C., "GDPR: Top 5 Tips for Staff Training", https://www.gorvins.com/news-media/blog/top-5-tips-gdpr/, [Πρόσβαση: 10/2017]

Miseta E., «Pharma "Not Prepared" For New EU Data Protection Regulation», https://www.clinicalleader.com/doc/pharma-not-prepared-for-new-eu-data-protection-regulation-0001, [Πρόσβαση: 11/2017]

Nextdeal newsroom, «Forrester: Το 80% των επιχειρήσεων θα αποτύχουν να συμμορφωθούν με το νόμο GDPR το 2018», https://www.nextdeal.gr/%CE%B5%CE%B9%CE%B4%CE%AE%CF%83%CE%B5%CE%B9%CF%82/%CF%84%CE%B5%CF%87%CE%BD%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%B1/forrester-to-80-twn-epicheirhsewn-tha-apotychoyn-na-symmorfwthoyn-me-to-nomo-gdpr-to-2018, [Πρόσβαση: 11/2017]

Palmer D., «What is GDPR? Everything you need to know about the new general data protection regulations», http://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/, [Πρόσβαση: 10/2017]

Pendergast T., "The GDPR is Coming: 3 Things for DPOs to Consider About Privacy Awareness", http://www.trustarc.com/blog/2017/05/31/gdpr-coming-3-things-dpos-consider-privacy-awareness/, [Πρόσβαση: 12/2017]

SAS Insights, «Όχι απλά πολύς θόρυβος για το τίποτα», https://www.sas.com/el_gr/insights/articles/data-management/local/eu-data-protection-gdpr.html, [Πρόσβαση: 10/2017]

Seb Joseph, «The GDPR Impact: The state of the ad industry's preparations for the GDPR, in 4 charts», https://digiday.com/marketing/state-ad-industrys-preparations-gdpr-4-charts/, [Πρόσβαση: 1/2018]

SYNTAX, «GDPR Guidance», http://syntax.gr/wp/general-data-protection-regulation/, [Πρόσβαση: 1/2018]

UKISUG Blog, «How can SAP users prepare for GDPR?», https://www.sapusers.org/news/407/how-can-sap-users-prepare-for-gdpr, [Πρόσβαση: 12/2017]

Voria.gr, «ΕΕΔΕ: Workshop από το Ελληνικό Ινστιτούτο Πληροφορικής», http://www.voria.gr/article/eede-workshop-apo-to-elliniko-institouto-pliroforikis---epikinonion, [Πρόσβαση: 1/2018]

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, «10 Ερωτήσεις-απαντήσεις για τα προσωπικά δεδομένα», http://www.dpa.gr/portal/page?_pageid=33,18990&_dad=portal&_schema=PORTAL, [Πρόσβαση: 11/2017]

Βασιλόπουλος Β., «Η ενιαία ψηφιακή αγορά της Ε.Ε. και ο GDPR», http://www.huffingtonpost.gr/vasilis-vasilopoulos/-gdpr_b_17302766.html, [Πρόσβαση: 11/2017]

Βασιλόπουλος Β., «Η Ενιαία ψηφιακή αγορά, οι κανονισμοί και οι παρεκκλίσεις», http://www.euractiv.gr/section/oikonomia/opinion/i-eniea-psifiaki-agora-i-kanonismi-ke-i-parekklisis/, [Πρόσβαση: 12/2017]

Δοξαράς Γ., «Οι αλλαγές του GDPR στο marketing», http://www.marketingweek.gr/default.asp?pid=9&la=1&arId=64985, [Πρόσβαση: 10/2017]

Ελληνικό Κέντρο Ασφαλούς Διαδικτύου, «Προστασία των παιδιών βάση του νέου κανονισμού για τα προσωπικά δεδομένα», https://saferinternet4kids.gr/nea/advisory-board-meeting/, [Πρόσβαση: 1/2018]

Ζέρβα Χ., «Ο νέος Ευρωπαϊκός Κανονισμός για την προστασία προσωπικών δεδομένων», http://www.voria.gr/article/o-neos-evropaikos-kanonismos-gia-tin-prostasia-prosopikon-dedomenon, [Πρόσβαση: 11/2017]

ΚΟΙΝΗ ΓΝΩΜΗ.gr ,«Προστασία των παιδιών βάσει του κανονισμού για τα προσωπικά δεδομένα», http://www.koinignomi.gr/news/koinonia/2017/10/23/prostasia-ton-paidion-vasei-toy-kanonismoy-gia-ta-prosopika-dedomena.html, [Πρόσβαση: 12/2017]

Κοσμάτου Λ., «KPMG: Ερωτήσεις και απαντήσεις για την προστασία των προσωπικών δεδομένων», https://www.nextdeal.gr/%CE%B5%CE%B9%CE%B4%CE%AE%CF%83%CE%B5%CE%B9%CF%82/%CF%84%CE%B5%CF%87%CE%BD%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%B1/kpmg-erwthseis-kai-apanthseis-gia-thn-prostasia-twn-proswpikwn-dedomenwn, [Πρόσβαση: 12/2017]

Μαλλάς Δ., «GDPR: Ο νέος κανονισμός της ΕΕ με τον οποίο πρέπει να συμμορφωθούν όλες οι επιχειρήσεις», http://www.cnn.gr/tech/story/109708/gdpr-o-neos-kanonismos-tis-ee-me-ton-opoio-prepei-na-symmorfothoyn-oles-oi-epixeiriseis, [Πρόσβαση: 1/2018]

Μιχαλοπούλου Ι., «Το νέο πλαίσιο συμμόρφωσης και ο κομβικός ρόλος του υπεύθυνου προστασίας δεδομένων», http://www.capital.gr/technology/3213046/to-neo-plaisio-summorfosis-kai-o-kombikos-rolos-tou-upeuthunou-prostasias-dedomenon, [Πρόσβαση: 12/2017]

Νούσιας Α., Ομάδα Εργασίας για τα Ανοιχτά Δεδομένα, «Καλώς ήρθατε στο Web 3.0.! Ο Γενικός Κανονισμός Προστασίας Δεδομένων και ο Ρόλος του Υπευθύνου Επεξεργασίας Δεδομένων», https://opendata.ellak.gr/2017/01/25/kalos-irthate-sto-web-3-0-o-genikos-kanonismos-prostasias-dedomenon-ke-o-rolos-tou-ipefthinou-epexergasias-dedomenon/, [Πρόσβαση: 11/2017]

Χριστοφίδης Γ., «Προστασία Προσωπικών Δεδομένων: Νέα τάξη πραγμάτων», http://www.sigmalive.com/news/opinions_sigmalive/451294/prostasia-prosopikon-dedomenon-nea-taksi-pragmaton, [Πρόσβαση: 10/2017]

Максим, «GDPR for SAP: How to restrict personal data processing?», https://sapbazar.com/articles/item/347-gdpr-for-sap-how-to-restrict-personal-data-processing, [Πρόσβαση: 10/2017]

9. ΒΙΒΛΙΟΓΡΑΦΙΑ

Αλεξανδροπούλου- Αιγυπτιάδου Ε., (2007), *Προσωπικά Δεδομένα - Η νομική ρύθμιση της ηλεκτρονικής επεξεργασίας τους*, Εκδόσεις: Αντ. Ν. Σάκκουλα. 2007.

Αρμαμέντος Π., Σωτηρόπουλος Β., (2005), *Προσωπικά Δεδομένα: ερμηνεία Ν.2472/1997*, Αθήνα – Θεσσαλονίκη, Εκδόσεις: Αντ. Ν. Σάκκουλα.

Γέροντας, Α., (2002), *Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων* , Αθήνα – Κομοτηνή, Εκδόσεις: Αντ. Ν. Σάκκουλα.

Γεωργόπουλος, Ν., Κοπανάκη, Ε., Πανταζή, Μ., Νικολαράκος, Χ. και Βαγγελάτος, Ι. (2013), *Ηλεκτρονικό Επιχειρείν*, 2η εκδ. Αθήνα: Εκδόσεις Ευγ. Μπένου.

Δελούκα-Ιγγλέση, Κ. (2015), *Νομικά Θέματα Ηλεκτρονικού Εμπορίου*, 2η εκδ. Αθήνα – Θεσσαλονίκη, Εκδόσεις: Αντ. Ν. Σάκκουλα.

Ιγγλεζάκης Ι., (2003), *Ευαίσθητα προσωπικά δεδομένα*, Αθήνα – Θεσσαλονίκη, Εκδ. Αντ. Ν. Σάκκουλα.

Καμπούρης, Α. (2015), *Εκτίμηση των Επιπτώσεων Σχετικά με την Προστασία των Δεδομένων*, Μεταπτυχιακή Διπλωματική Εργασία στο πλαίσιο του Διαπανεπιστημιακού Προγράμματος Μεταπτυχιακών Σπουδών: «Τεχνο –οικονομικά συστήματα», ΕΜΠ-Πανεπιστήμιο Πειραιώς.

Οικονόμου, Γ. και Γεωργόπουλος, Ν. (2004), *Πληροφοριακά Συστήματα για τη Διοίκηση Επιχειρήσεων,* 3η εκδ. Αθήνα, Εκδόσεις: Ευγ. Μπένου.

Σιασιάκος Κ., Αναστασίου Σ. και Τούντας Κ. (2016), Paper: *Εκτίμηση των Επιπτώσεων σχετικά με την Προστασία Δεδομένων σε έργα Ηλεκτρονικής Διακυβέρνησης*.

ΚΑΝΟΝΙΣΜΟΙ – ΟΔΗΓΙΕΣ - ΣΥΣΤΑΣΕΙΣ

Κανονισμός 2016/679/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων), Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης αριθ. L 119/1 της 4/5/2016. Διαθέσιμη στο Διαδίκτυο στη διεύθυνση: http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679

Οδηγία 1/2005 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για την ασφαλή καταστροφή των δεδομένων. Διαθέσιμη στο Διαδίκτυο στη διεύθυνση: http://www.dpa.gr/

Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες), Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης αριθ. L 207 της 31/07/2002. Διαθέσιμη στο Διαδίκτυο στη διεύθυνση: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:el:PDF

Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2006 για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών και τροποποίηση της Οδηγίας 2002/58/ΕΚ. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης αριθ. L 105 της 13/04/2006. Διαθέσιμη στο Διαδίκτυο στη διεύθυνση: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/RELATIVELAW/%CE%9F%CE%94%CE%97%CE%93%CE%8A%CE%912006-24-%CE%95%CE%9A.PDF

Οδηγία 2009/136/ΕΚ, του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2009, για τροποποίηση της Οδηγίας 2002/22/ΕΚ για την καθολική

υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών. Διαθέσιμη στο Διαδίκτυο στη διεύθυνση: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:El:PDF

Οδηγία 2016/680/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της της 27ης Απριλίου 2016, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης Διαθέσιμη στο Διαδίκτυο στη διεύθυνση: http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016L0680

Οδηγία 2016/681/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Διαθέσιμη στο Διαδίκτυο στη διεύθυνση: https://publications.europa.eu/el/publication-detail/-/publication/2ba036c2-11bd-11e6-ba9a-01aa75ed71a1/language-el

Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης αριθ. L 281 της 23/11/1995. Διαθέσιμη στο Διαδίκτυο στη διεύθυνση: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:el:HTML

Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων, «Guidelines on Data Protection Officers (‘DPOs’)», [5/4/2017]

Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων, «Guidelines on the right to data portability», [5/4/2017]

Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων, «Γνώμη 06/2014 σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας, σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ», [9/4/2014]

Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων, “Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679”, [3/10/2017]

Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων, Δεσμευτικοί Εταιρικοί Κανόνες, “Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules”, [7/12/2017]

Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων, Εκτίμηση Επιπτώσεων, “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679”, [4/4/2017]

Ομάδα Εργασίας του άρθρου 29, γνωμοδότηση για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στο εργασιακό πλαίσιο δεδομένων, «Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης», [10 Απριλίου 2014]

Οργανισμός Ηνωμένων Εθνών (ΟΗΕ) (1948) Οικουμενική διακήρυξη για τα Ανθρώπινα Δικαιώματα, 9/2016, Διαθέσιμη στην ιστοσελίδα: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/grk.pdf

ΝΟΜΟΙ

Νόμος 2472/1997 (ΦΕΚ Α’ 50/10.4.1997), Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα με ενσωματωμένες τις τροποποιήσεις.

Νόμος 3471/2006 (ΦΕΚ Α’ 133/28-06-2006) Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997.

Νόμος 3917/2011 (ΦΕΚ Α’ 22/21-02-2011) Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.

Νόμος 4070/2012 (ΦΕΚ Α’ 82/10-04-2012) Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις.

10. ΠΗΓΕΣ ΕΙΚΟΝΩΝ

Εικόνα 1: http://www.taseism.gr/trehonta-anoihta-seminaria/epimorfotiko-seminario-o-genikos-kanonismos-gia-tin-prostasia-dedomenon

Εικόνα 2: http://www.crowesol.gr/wp-content/uploads/2018/01/Diagram2.png

Εικόνα 3: http://www.taseism.gr/trehonta-anoihta-seminaria/epimorfotiko-seminario-o-genikos-kanonismos-gia-tin-prostasia-dedomenon

Εικόνες 4 – 12: Διαφάνειες Παρουσίασης Κου Ευαγγελίδη Αντώνη: «Η Υλοποίηση του GDPR σε μια ελληνική φαρμακευτική εταιρεία», ΒΙΑΝΕΞ Α.Ε. [11/2017]