Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών
Κοινωνικά Πληροφοριακά Συστήματα

Μεταπτυχιακή Διατριβή

Κοινωνικά Πληροφοριακά Συστήματα και Συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (Social Information Systems and GDPR Compliance)

Καλλής Κάππελος

Επιβλέπουσα Καθηγήτρια
Αλεξάνδρα Μιχώτα

Μάιος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Κοινωνικά Πληροφοριακά Συστήματα

Μεταπτυχιακή Διατριβή

Κοινωνικά Πληροφοριακά Συστήματα και Συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (Social Information Systems and GDPR Compliance)

Καλλής Κάππελος

Επιβλέπουσα Καθηγήτρια
Αλεξάνδρα Μιχώτα

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στα Κοινωνικά Πληροφοριακά Συστήματα από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2019

Περίληψη

Ο σκοπός της παρούσας διπλωματικής εργασίας είναι η μοντελοποίηση των απαιτήσεων που εισάγει ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) [1] και ο καθορισμός τεχνικών προδιαγραφών που αφορούν την προστασία προσωπικών δεδομένων για τα Κοινωνικά Πληροφοριακά Συστήματα (ΚΠΣ). Στην εργασία αυτή παρουσιάζονται όλα τα βήματα που θα πρέπει οι κατασκευαστές των ΚΠΣ να ακολουθούν για σχεδίαση και ανάπτυξη συστημάτων εναρμονισμένων με τον Κανονισμό. Τα βήματα και οι προδιαγραφές που παρουσιάζονται και αναλύονται στην εργασία μπορούν να εφαρμοστούν τόσο σε νέα αλλά και υφιστάμενα ΚΠΣ, για τα οποία οι διαχειριστές των συστημάτων έχουν υποχρέωση για συμμόρφωση με τον ΓΚΠΔ.

Τα Κοινωνικά Πληροφοριακά Συστήματα είναι συστήματα πληροφοριών που βασίζονται σε κοινωνικές τεχνολογίες και ανοιχτή συνεργασία. Το κάθε ένα από μόνο του (είτε συνεργαζόμενα μεταξύ τους) είναι μια «κοινωνία» που έχει κουλτούρα, συνήθειες και κανόνες. Τα συστήματα αυτά έχουν αλλάξει τον τρόπο που οι άνθρωποι αλληλοεπιδρούν μέσω της χρήσης υπηρεσιών παγκόσμιου Ιστού. Σε όλη την έκταση της, η Διπλωματική εργασία, αναφέρεται στα ΚΠΣ με τρόπο τέτοιο, ώστε ο αναγνώστης να κατανοήσει τη δομή και τις λειτουργίες τους και να μπορέσει να αντιληφθεί τη σημαντικότητα της ορθής και αποτελεσματικής εναρμόνισης των συστημάτων αυτών με τον ΓΚΠΔ. Μέσω των ΚΠΣ συλλέγεται και τυγχάνει επεξεργασίας τεράστιος όγκος δεδομένων, αλλά πολλές φορές και ευαίσθητων προσωπικών δεδομένων και πληροφοριών, πράγμα το οποίο εγκυμονεί κινδύνους για την ασφάλεια και ιδιωτικότητα των προσωπικών στοιχείων των Υποκειμένων των Δεδομένων (χρηστών).

Η εργασία αυτή απαρτίζεται από 3 βασικά μέρη. Στο πρώτο μέρος (Κεφάλαιο 2) επισημαίνονται οι σημαντικές αλλαγές που επιφέρει ο ΓΚΠΔ, στο δεύτερο μέρος (Κεφάλαιο 3) καθορίζονται, παρουσιάζονται και αναλύονται τα βήματα τα οποία οι κατασκευαστές ΚΠΣ θα πρέπει να ακολουθούν ώστε τα συστήματα που αναπτύσσουν να συμμορφώνονται με τις απαιτήσεις του ΓΚΠΔ, και τέλος στο τρίτο μέρος (Κεφάλαια 4 και 5) παρουσιάζονται και αναλύονται τα ερωτηματολόγια που σχεδιάστηκαν και οι απαντήσεις που λήφθηκαν. Επίσης στο τρίτο μέρος της Διπλωματικής εργασίας γίνονται εισηγήσεις για επέκταση της εργασίας ενώ στο τέλος παρατίθενται και τα τελικά συμπεράσματα.

Summary

The purpose of this M.A. dissertation is to provide a prototype model for the requirements introduced by the General Data Protection Regulation (GDPR) [1] as well as technical specifications for the protection of personal data in Social Information Systems (SIS). This work presents all the steps that SIS developers should follow for the design and implementation of systems aligned with the GDPR. Moreover, the steps and specifications presented and analyzed in this M.A. dissertation can be applied to both new and existing SISs of which the system administrators are responsible for their compliance with all aspects of the GDPR.

Social Information Systems are based on social technologies and open collaboration. Each SIS independently (or in collaboration with others) is a "society" with culture, habits and rules. These systems have changed the way people interact with the use of web services. SISs are used not only to gather and process a huge amount of data (Big Data), but also sensitive data and information on a frequent basis, which may put the safety and privacy of the personal data of the Data Subjects (users) at high risk; so throughout its scope, this M.A. dissertation refers to SISs in such a way that the reader can understand their structure and functionalities as well as the importance of their proper and effective compliance with the GDPR.

This dissertation is divided into 3 main parts. The first part (Chapter 2) highlights significant changes introduced by the new Regulation, the second part (Chapter 3) defines, presents and analyzes all the steps that SIS developers should follow, in a way that the systems under development meet the requirements of the GDPR, and finally part three (Chapters 4 and 5) presents and analyzes our questionnaires and the received answers to them. Furthermore, the third part makes a few suggestions for future work and, at the end of Chapter 5, the final conclusions are presented.

Ευχαριστίες

Ευχαριστώ την Επιβλέπουσα Καθηγήτρια κα Αλεξάνδρα Μιχώτα για την επίβλεψη της παρούσας εργασίας. Επίσης θερμές ευχαριστίες στους κ.κ. Παπαδόπουλο και Ιωάννου για τον πολύτιμο χρόνο που είχαν αφιερώσει για την παραχώρηση συνέντευξης καθώς επίσης θα ήθελα να ευχαριστήσω τη Λειτουργό του γραφείου της Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα, Κύπρου, για το χρόνο που είχε αφιερώσει στη συμπλήρωση ερωτηματολογίου.

Θα ήταν παράλειψή μου να μην αναφερθώ στη μεγάλη βοήθεια που είχα από την οικογένειά μου, τη σύζυγό μου και τα τρία παιδιά μου, που με τον δικό τους τρόπο, καθ' όλη τη διάρκεια των μεταπτυχιακών σπουδών μου, μου έδιναν πάντοτε τη δύναμη που χρειαζόμουν για να φτάσω με επιτυχία μέχρι το τέλος. Τους ευχαριστώ από τα βάθη της καρδιάς μου και εύχομαι να έχουν και αυτοί παρόμοιες επιτυχίες στη ζωή τους.

Περιεχόμενα

Κεφάλαιο 1
Γενικά

1.1. Εισαγωγή

Η εξέλιξη της τεχνολογίας, η συνεχής χρήση του διαδικτύου καθώς επίσης η ροή του τεράστιου καθημερινού όγκου δεδομένων (Big Data[1]), που συνεχώς αποθηκεύεται και αναλύεται σε διάφορες μορφές, θέτουν την ιδιωτική ζωή και τα προσωπικά δεδομένα σε κίνδυνο κάνοντάς τα διαθέσιμα χωρίς περιορισμούς. Η απαίτηση της συμμόρφωσης, όλων όσων επεξεργάζονται δεδομένα, με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) είναι μία συνεχής διαδικασία που θα πρέπει όλοι να εναρμονιστούν και να ακολουθήσουν.

Η οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995 (εφεξής 95/46/ΕΚ), για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, «*επιδίωξε την εναρμόνιση της προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων όσον αφορά τις δραστηριότητες επεξεργασίας και τη διασφάλιση της ελεύθερης κυκλοφορίας δεδομένων προσωπικού χαρακτήρα μεταξύ κρατών μελών*», όπως αυτό αναφέρεται ρητά στην αιτιολογική σκέψη 3 του ΓΚΠΔ [1]. Σε μια προσπάθεια ενίσχυσης της προστασίας προσωπικών δεδομένων η οδηγία 95/46/ΕΚ καταργήθηκε και τον Μάιο του 2018 μπήκε σε εφαρμογή ο ΓΚΠΔ [1].

Η αιτιολογική σκέψη 10 (σελ. 2) της αιτιολογικής περιγραφής του ΓΚΠΔ, αναφέρει ότι ο νέος Κανονισμός αναθεωρεί σημαντικά τον τρόπο προστασίας των δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση (ΕΕ), αφού αποσκοπεί στη διασφάλιση συνεκτικής και υψηλού επιπέδου προστασίας των φυσικών προσώπων

[1] Big Data είναι ένας όρος που περιγράφει τον μεγάλο όγκο δεδομένων - δομημένων και μη δομημένων - που κατακλύζουν μια επιχείρηση σε καθημερινή βάση. Δεν είναι ο όγκος των δεδομένων που είναι σημαντικός αλλά αυτό που κάνουν οι οργανισμοί με τα δεδομένα. Μεγάλοι όγκοι δεδομένων μπορούν να αναλυθούν για ιδέες που οδηγούν σε καλύτερες αποφάσεις και επιχειρηματικές στρατηγικές κινήσεις. [20]

και στην άρση των εμποδίων στις ροές δεδομένων προσωπικού χαρακτήρα εντός και εκτός ΕΕ. «*Θα πρέπει να διασφαλίζεται συνεκτική και ομοιόμορφη εφαρμογή των κανόνων για την προστασία των θεμελιωδών δικαιωμάτων και των ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την Ένωση*». Με την εφαρμογή του ΓΚΠΔ, στις 25 Μαΐου 2018 αναμένεται ενίσχυση των δικαιωμάτων των υποκειμένων των δεδομένων (εφεξής ΥπΔε), παράλληλα της αύξησης των υποχρεώσεων του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία, οι οποίοι επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, ευρωπαίων πολιτών, εντός αλλά και εκτός της ΕΕ.

Οι νομικές υποχρεώσεις που εισάγονται με τον ΓΚΠΔ θα πρέπει να μεταφραστούν σε τεχνικές απαιτήσεις για όλα τα υφιστάμενα πληροφοριακά συστήματα αλλά και όσα νέα θα υλοποιηθούν, με στόχο να διασφαλίζονται τα δικαιώματα όλων των χρηστών που έχουν δώσει τη συγκατάθεσή τους για επεξεργασία των δεδομένων τους αλλά και αυτών που δεν αποδέχθηκαν τους όρους και δεν έχουν δώσει γραπτώς τη συγκατάθεσή τους. Για τη χρήση των Κοινωνικών Πληροφοριακών Συστημάτων (ΚΠΣ), η δημιουργία προφίλ με δήλωση προσωπικών δεδομένων του χρήστη είναι αναγκαία. Συνεπώς είναι εύκολα κατανοητό ότι η διαφύλαξη αυτών των δεδομένων, που ανά πάσα στιγμή μπορούν να χρησιμοποιηθούν για την ταυτοποίηση του χρήστη, κρίνεται απαραίτητη και από εδώ και στο εξής υποχρεωτική. Στην παρούσα εργασία παρουσιάζονται και αναλύονται οι γενικές προδιαγραφές τις οποίες θα πρέπει να ικανοποιεί κάθε ΚΠΣ, στις οποίες οι κατασκευαστές τέτοιων συστημάτων θα μπορούν να βασιστούν ώστε να αναπτύξουν συστήματα που ικανοποιούν τις απαιτήσεις που θέτει ο ΓΚΠΔ για την προστασία προσωπικών δεδομένων.

1.2. «Κοινωνικά Πληροφοριακά Συστήματα»

Τα Κοινωνικά Πληροφοριακά Συστήματα είναι συστήματα πληροφοριών που βασίζονται σε κοινωνικές τεχνολογίες και ανοιχτή συνεργασία [2]. Τα ΚΠΣ διαφέρουν από τα παραδοσιακά πληροφοριακά συστήματα αφού δεν αναπτύσσονται χρησιμοποιώντας απλά γλώσσες όπως PHP ή HTML, αλλά είναι μια «κοινωνία» που έχει κουλτούρα, συνήθειες και κανόνες. Τα συστήματα αυτά, τα τελευταία 15 χρόνια, έχουν εδραιωθεί στο χώρο του διαδικτύου και έχουν αλλάξει τον τρόπο που ο άνθρωπος αλληλεπιδρά με τα Πληροφοριακά Συστήματα (ΠΣ) αλλά κυρίως έχει αλλάξει ο τρόπος που οι άνθρωποι επικοινωνούν μεταξύ τους.

Η ανάπτυξη ενός ΚΠΣ γίνεται πάντα με βάση τον κύκλο ζωής ενός συστήματος αλλά αυτό που είναι σημαντικό για αυτά τα συστήματα είναι ότι όλα τα μέρη τους βασίζονται τόσο στην τεχνική πτυχή, που αφορά την υλοποίηση και τεχνική υποστήριξη ενός ΠΣ, όσο και στην κοινωνική πτυχή, που αφορά τη συνεχή ενεργή συμμετοχή και συνεισφορά των χρηστών μεταφέροντας γνώση και πληροφορία εντός του συστήματος, αναπτύσσοντάς το δυναμικά. Με άλλα λόγια, σήμερα οι κατασκευαστές ΚΠΣ, είναι πιθανό να οδηγηθούν σε αποτυχία αν προηγουμένως δεν καταφέρουν να κατανοήσουν, να αναλύσουν ή να αναπτύξουν τέτοια συστήματα χωρίς να τα προσεγγίσουν από κοινωνικο-τεχνικής άποψης. Τα συστήματα αυτά μεταθέτουν τη λειτουργία του πυρήνα τους από τη στατική υποστηρικτική εργασία στη δυναμική διαδικτυακή (online) κοινωνική αλληλεπίδραση και την ανοικτή συνεργασία (π.χ. το σύστημα επιτρέπει σχόλια, βαθμολογίες, "φιλίες" και μηχανισμούς ανατροφοδότησης και ο αριθμός των συμμετεχόντων ή αυτών που συνεισφέρουν ενεργά στο σύστημα δεν είναι προκαθορισμένος) [2].

Σήμερα όλο και περισσότεροι άνθρωποι χρησιμοποιούν τα ΚΠΣ για την καθημερινή τους ψυχαγωγία και δραστηριότητα στον παγκόσμιο ιστό. Όπως δείχνουν και οι τεράστιοι αριθμοί των πιο δημοφιλών ιστότοπων του πλανήτη[2], ο κοινωνικός ιστός έχει αποκτήσει παγκόσμια εμβέλεια αφού η χρήση των κοινωνικών μέσων έχει γίνει μια αγαπημένη δραστηριότητα ελεύθερου χρόνου και όχι μόνο, για τους χρήστες του Διαδικτύου. Παρατηρώντας την εξέλιξη αυτή που αναδείχθηκε με ραγδαίους ρυθμούς, εμφανίζονται διάφορες μορφές αυτόνομης συν-δημιουργίας, δηλαδή παρατηρείται η συμμετοχή όλο και περισσότερων χρηστών του Διαδικτύου οι οποίοι με τη **συνεισφορά** [3] τους αποτελούν ουσιαστικά την κυριότερη πηγή εισερχόμενης πληροφορίας για τα ΚΠΣ. Αυτό οδηγεί σε μια νέα ανεξάρτητη[4] μέθοδο παραγωγής και ανάπτυξης κοινωνικών ιστότοπων. Στο παρελθόν, δεν παρατηρήθηκε ποτέ ξανά παρόμοιου βαθμού ομαδική δραστηριότητα (συνεισφορά) με τόσο θετικό αντίκτυπο σε διάφορους τομείς. Εκτός από το Διαδίκτυο, σήμερα, παρατηρείται ότι η «συνεισφορά» αυτή αντανακλάται με θετικό τρόπο στις δραστηριότητες μεγάλων

[2] Βλ. https://www.alexa.com/topsites

[3] Η συνεισφορά σε ένα ΚΠΣ προέρχεται από ενεργούς κυρίως χρήστες οι οποίοι δραστηριοποιούνται πολύ συχνά στο σύστημα. Η εισαγωγή και η επεξεργασία πληροφορίας εντός του ΚΠΣ, είναι ροή δεδομένων που ενισχύουν και διατηρούν ενημερωμένο και ενεργό το σύστημα.

[4] Διαδικασία που δεν εξαρτάται στους κατασκευαστές των ΚΠΣ αλλά στη δραστηριότητα των χρηστών (π.χ. wikis)

επιχειρήσεων οι οποίες πλέον χρησιμοποιούν όλο και περισσότερο ανοικτές, κοινωνικές και συνεργατικές διαδικασίες για επικοινωνία μεταξύ πελατών και οργανισμού (εργαζομένων) με στόχο την ικανοποίηση των χρηστών αλλά φυσικά και την αύξηση των κερδών τους γενικότερα.

Για καλύτερη κατανόηση της έννοιας των Κοινωνικών Πληροφοριακών Συστημάτων, αξίζει εδώ να αναφερθούν αυτούσια τα γενικά χαρακτηριστικά και γενικές λειτουργίες των συστημάτων αυτών όπως έχουν μελετηθεί και καταγραφεί από τους Schlagwein, Schoder και Fischbach [2].

Κοινωνικότητα: Τα συστήματα κοινωνικής πληροφόρησης βασίζονται σε κοινωνικές αλληλεπιδράσεις. Οι δομές διακυβέρνησης (παγκόσμιος ιστός) βασίζονται συχνά σε κοινωνικούς και όχι νομικούς μηχανισμούς. Η διακυβέρνηση ακολουθεί τη λογική «από κάτω προς τα πάνω» και τη «λογική του κοινού» (απλού λαού). Ο έλεγχος υλοποιείται μέσω διαφάνειας και κοινωνικής ανάδρασης, όχι μέσω ιεραρχίας. Η απόφαση συμμετοχής ενός ατόμου θα επηρεαστεί από προηγούμενους κοινωνικούς δεσμούς με άλλους συμμετέχοντες.

Διαφάνεια: Τα ΚΠΣ συνήθως δεν έχουν προκαθορισμένο αριθμό συμμετεχόντων. Αντ' αυτού, το σύστημα είναι ανοικτό σε ένα ευρύ φάσμα συμμετεχόντων/συντελεστών. Συνήθως, η απόφαση συμμετοχής είναι εθελοντική.

Συνεισφορά: Οι συνεισφέροντες[5] και οι συμμετέχοντες στα ΚΠΣ είναι κοινότητες ατόμων, συχνά ανεξάρτητων χρηστών. Π.χ. οι εργαζόμενοι που αποφασίζουν να συμμετέχουν σε ΚΠΣ μπορούν να συνεισφέρουν εξίσου, για την ανάπτυξη των συστημάτων αυτών, όπως το κάνουν και μέσα από τις επίσημες οργανωτικές τους θέσεις, για λογαριασμό των επιχειρήσεων που εργάζονται.

[5] Ενεργοί χρήστες ενός ΚΠΣ είναι εκείνοι που δραστηριοποιούνται πολύ συχνά στο σύστημα. Η εισαγωγή και η επεξεργασία πληροφορίας εντός του ΚΠΣ, είναι ροή δεδομένων που ενισχύουν και διατηρούν ενημερωμένο και ενεργό το σύστημα.

Περιεχόμενο: Οι πληροφορίες που ρέουν μέσω ΚΠΣ παράγονται από το χρήστη. Το περιεχόμενο είναι προσβάσιμο σε όλους τους συμμετέχοντες. Το περιεχόμενο είναι δυναμικό, κοινόχρηστο και αυξάνεται με την πάροδο του χρόνου.

Τεχνολογία: Η τεχνολογία βασίζεται σε κοινωνικές τεχνολογίες όπως wikis, ιστότοποι κοινωνικής δικτύωσης, πλατφόρμες συνεργασίας, ιστολόγια και παρόμοια εργαλεία κοινωνικών μέσων. Αυτά τα εργαλεία είναι συνήθως εύχρηστα, εύκαμπτα σε δομή και μέγεθος και συχνά διατίθενται ως εργαλεία ανοιχτού κώδικα.

Τοποθεσία: Τα ΚΠΣ είναι ηλεκτρονικά συστήματα, βασισμένα στον Παγκόσμιο Ιστό (Web). Συνήθως φιλοξενούνται σε ένα διακομιστή Web και είναι προσβάσιμα μέσω ενός προγράμματος περιήγησης. Ως εκ τούτου, δεν υπάρχει τοπική εγκατάσταση στα συστήματα των χρηστών[6].

Μερικά παραδείγματα τέτοιων συστημάτων [3], που αρκετοί ήδη τα χρησιμοποιούν σε καθημερινή βάση είναι:

Wikipedia, λογισμικά ανοικτής πηγής (open source): Συνεργασία μεταξύ τελικών χρηστών. Συνεισφέρει ο καθένας σε παγκόσμιο επίπεδο.

Facebook και Twitter: Ιστότοποι κοινωνικών δικτύων - Κοινωνική αλληλεπίδραση. Επιτρέπει στους χρήστες να δημιουργούν δίκτυα φίλων και επαφών, διευκολύνοντας την ανταλλαγή περιεχομένου, κοινωνικοποίησης και οικοδόμησης κοινωνικών ομάδων (κοινότητες) όπως ποτέ δεν είχαν τέτοιο εύρος.

Φόρουμ: Συζητήσεις και αντιπαραθέσεις χρηστών με σχόλια και απόψεις. Χρησιμοποιείται για να συλλέγει τις σκέψεις και τις απόψεις των χρηστών σχετικά με προϊόντα, εστιατόρια, βιβλία, άρθρα ειδήσεων (π.χ. TripAdvisor, ιστοσελίδες ειδήσεων) που μπορούν να προωθήσουν τη συλλογική νοημοσύνη και την άτυπη μάθηση.

[6] Τα τελευταία χρόνια έχουν επεκταθεί και σε εφαρμογές φορητών συσκευών όπου εγκαθίστανται τοπικά στη συσκευή.

Μηχανή Αναζήτησης Google: Χρησιμοποιούνται οι έξυπνοι αλγόριθμοι της μηχανής αναζήτησης, για την οργάνωση και την ανάκτηση πληροφοριών και η συμπεριφορά των χρηστών καταγράφεται και χρησιμοποιείται με τέτοιο τρόπο ώστε να είναι αντικείμενα που συνεισφέρουν στη συλλογική νοημοσύνη του πλανήτη. Αυτή η συμπεριφορά είναι από τα «αγαπημένα» κομμάτια της ανάλυσης του Big Data που δε μένουν ανεκμετάλλευτα από τις μεγάλες ή/και μικρές επιχειρήσεις σε παγκόσμιο επίπεδο, για δικό τους όφελος (π.χ. διαφήμιση).

Τα ΚΠΣ διαδραματίζουν σημαντικό ρόλο στην καθημερινότητα του ανθρώπου αφού έχουν επηρεάσει τις σχέσεις του, τον τρόπο με τον οποίο επικοινωνεί, δουλεύει, μαθαίνει, διασκεδάζει.

1.3. Σκοπός της Μεταπτυχιακής Διατριβής

Σκοπός της εργασίας αυτής είναι ο καθορισμός, η παρουσίαση και η ανάλυση των βημάτων που θα πρέπει να ακολουθηθούν προκειμένου οι κατασκευαστές ΚΠΣ να συμμορφωθούν με τις απαιτήσεις του ΓΚΠΔ. Η μοντελοποίηση των απαιτήσεων που εισάγει ο ΓΚΠΔ και ο καθορισμός τεχνικών προδιαγραφών, που αφορούν την προστασία προσωπικών δεδομένων για τα ΚΠΣ, θα βοηθήσει τους εμπλεκόμενους στην ευκολότερη και ακριβέστερη εναρμόνιση των συστημάτων τους με τον Κανονισμό.

1.3.1. Αναγκαιότητα και σπουδαιότητα της έρευνας

Ο ΓΚΠΔ δεν αποτελεί επιλογή αλλά νομική υποχρέωση για τα κράτη-μέλη της Ευρωπαϊκής Ένωσης και για όσους διαχειρίζονται προσωπικά δεδομένα πολιτών της ΕΕ, από φυσικά πρόσωπα μέχρι επιχειρήσεις, οργανισμούς και κρατικές υπηρεσίες. Είναι άμεσα εφαρμοστέος από την 25η Μαΐου του 2018 και έχει εισαγάγει ένα νέο σύνολο κανόνων που αφορούν την προστασία των προσωπικών δεδομένων.

Το πρόστιμο μη συμμόρφωσης με τον ΓΚΠΔ είναι αρκετά υψηλό, έτσι η παραμετροποίηση και απλοποίηση των βημάτων για τη συμμόρφωση με τον Κανονισμό, όσον αφορά τα ΚΠΣ, κρίνεται επιτακτικά αναγκαίο ζήτημα και θα ήταν πολύ χρήσιμο να δημιουργηθεί ένα σχετικό μοντέλο προτυποποίησης για το σκοπό

αυτό. Επιχειρήσεις που θέλουν να διατηρούν το κύρος και την αξιοπιστία τους ψηλά στην εκτίμηση των πελατών τους, δε μπορούν να θέτουν σε κίνδυνο τη φήμη του ονόματός τους και να απειλούνται με πιθανή αποτυχία διαφύλαξης προσωπικών δεδομένων των πελατών/χρηστών τους. Για το λόγο αυτό επιβάλλεται η πλήρης συμμόρφωσή τους με τον ΓΚΠΔ. Προσδοκώμενα αποτελέσματα αυτής της εργασίας είναι η συγγραφή προτάσεων βελτίωσης των βημάτων υλοποίησης των ΚΠΣ, στοχεύοντας στη συμμόρφωση με τις απαιτήσεις που επιβάλλει ο ΓΚΠΔ μειώνοντας ταυτόχρονα το ρίσκο επιβολής ποινών από τις αρμόδιες αρχές.

Η καινοτομία αυτής της διατριβής εστιάζει στη μοντελοποίηση των απαιτήσεων που εισάγει ο ΓΚΠΔ που τέθηκε σε ισχύ τον Μάιο 2018 και τον καθορισμό συγκεκριμένων βημάτων που θα ακολουθούνται από τους κατασκευαστές των ΚΠΣ για την αποτελεσματική και πλήρη εναρμόνιση με τον ΓΚΠΔ προστατεύοντας τα προσωπικά δεδομένα στα Κοινωνικά Πληροφοριακά Συστήματα που θα καλεστούν να υλοποιήσουν.

Τα συνολικά 31 σημεία (τεχνικές προδιαγραφές για τους κατασκευαστές των ΚΠΣ) των «Πίνακας 1» και «Πίνακας 2» της παραγράφου 3.1.1.3, η εκτενής ανάλυση και των 31 σημείων στην παράγραφο 3.1.2 καθώς και τα 6 υποχρεωτικά βήματα της παραγράφου 3.1.1.2, αποτελούν τη μοντελοποίηση που αναφέρθηκε στην αμέσως προηγούμενη παράγραφο.

Ο ιδιοκτήτης (οργανισμός/επιχείρηση) ετοιμάζει τις δικές του τεχνικές απαιτήσεις, σύμφωνα με τις ανάγκες της οντότητάς του και ζητά από τον ανάδοχο να τις υλοποιήσει σε καινούριο ΚΠΣ (ισχύει και για υφιστάμενα ΚΠΣ). Ο ανάδοχος ακολουθεί όλα τα βήματα (βλ. προηγούμενη παράγραφο πιο πάνω) τα οποία καθορίζουν την υλοποίηση του έργου με συγκεκριμένο τρόπο και υποχρεώσεις, προς τον ιδιοκτήτη του ΚΠΣ. Όλες οι απαιτήσεις/προδιαγραφές του έργου θα πρέπει να είναι ξεκάθαρες και να ευθυγραμμίζονται άμεσα ή έμμεσα με τις πτυχές και απαιτήσεις του ΓΚΠΔ. Με τη βοήθεια των δύο πινάκων (παρ. 3.1.1.3) ο κατασκευαστής μπορεί να αποκωδικοποιήσει τα άρθρα του ΓΚΠΔ που αφορούν ειδικότερα τα ΚΠΣ και χωρίς ιδιαίτερη προσπάθεια και ανάγκη για ψάξιμο σε βάθος στον Κανονισμό, θα καταφέρει αποτελεσματικά την εναρμόνιση του ΚΠΣ με τις απαιτήσεις του ΓΚΠΔ.

Ο «Πίνακας 2» (παρ. 3.1.1.3) ο οποίος περιλαμβάνει σημεία που έχουν καταγραφεί από άλλες πηγές, πέραν του ΓΚΠΔ, τα οποία συμπληρώνουν τη μοντελοποίηση των προδιαγραφών συμμόρφωσης για τα ΚΠΣ είναι το σημείο στη Διπλωματική που κάνει την εργασία να ξεχωρίζει από άλλες που αναφέρονται στην εναρμόνιση πληροφοριακών συστημάτων με τον ΓΚΠΔ. Το κάθε σημείο του πίνακα αναλύεται στην παράγραφο 3.1.2 με αρκετή λεπτομέρεια για καλύτερη κατανόηση. Το σημαντικό για την εργασία είναι η εισήγηση που γίνεται προς τους κατασκευαστές ΚΠΣ να εφαρμόζουν όλα τα σημεία που αναγράφονται στους πίνακες, ενσωματώνοντάς τα στο ΚΠΣ με τέτοιο τρόπο ώστε **να δημιουργείται αυτόματη διαδικασία επεξεργασίας δεδομένων** ή το ίδιο το ΚΠΣ να συμβουλεύει άμεσα τους ΕτΕ [7] και τον ΥΕ [8] (βλ. εισηγήσεις υλοποίησης διαδικασιών για τα ΚΠΣ στην παράγραφο 3.1.2). Όταν και εφόσον υπάρχει αίτημα προς τους τελευταίους για ικανοποίηση των απαιτήσεων των ΥπΔε[9] που αντλούνται από τον ΓΚΠΔ, αυτό να γίνεται εύκολα, αποτελεσματικά και αυτόματα (ηλεκτρονικά) **χωρίς να ανατρέχουν συνεχώς στο κείμενο του ΓΚΠΔ**.

Δεν είναι λίγες οι φορές που έχει παρατηρηθεί ότι οι νομοθέτες τέτοιου μεγέθους Κανονισμών επανέρχονται με διορθώσεις και προσθέσεις στο αρχικό κείμενο. Τα σημεία του «Πίνακας 2» θα μπορούσαν να είναι επιπρόσθετα σημεία στις αιτιολογικές σκέψεις του ΓΚΠΔ. Μερικά σημεία του πίνακα μεταφέρουν την εμπειρία επαγγελματιών στον τομέα της προστασίας προσωπικών δεδομένων πράγμα χρήσιμο για την παρούσα εργασία, αφού θα βοηθήσει στην εξαγωγή χρήσιμων συμπερασμάτων.

1.4. Μεθοδολογία

Η μεθοδολογία που ακολουθήθηκε στην παρούσα εργασία παρουσιάζεται παρακάτω.

1.4.1. Βιβλιογραφική ανασκόπηση

Βιβλιογραφική ανασκόπηση έγινε με χρήση βιβλίων, άρθρων από συνέδρια και άρθρων δημοσιευμένων σε επιστημονικά περιοδικά. Στη βιβλιογραφία επίσης συμπεριλαμβάνεται το κείμενο του ΓΚΠΔ αλλά και μερικά παλαιότερα

[7] Βλ. σελ. 90, «Συντομογραφίες»
[8] Βλ. σελ. 90, «Συντομογραφίες»
[9] Βλ. σελ. 90, «Συντομογραφίες»

συμπληρωματικά κείμενα από Ομάδες εργασίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, για την προστασία των προσωπικών δεδομένων, τα οποία δεν έχουν καταργηθεί αλλά ισχύουν παράλληλα με τον ΓΚΠΔ.

Τα **ερευνητικά ερωτήματα**, τα οποία θα ακολουθήσει η έρευνα για να δώσει απαντήσεις αλλά παράλληλα θα βοηθήσουν στον καλύτερο σχεδιασμό της δομής της παρούσας Διατριβής, έχουν ως ακολούθως:

1. Τι είδους δεδομένα εισέρχονται στα ΚΠΣ[10];
2. Ποια άρθρα του ΓΚΠΔ θα πρέπει να λάβει σοβαρά υπόψη ο υπεύθυνος επεξεργασίας δεδομένων ενός Κοινωνικού Πληροφοριακού Συστήματος για τις καθημερινές του συναλλαγές/επικοινωνία με τους χρήστες[11];
3. Πόσο εύκολα μπορεί να εφαρμοστεί ο ΓΚΠΔ σε υφιστάμενα ΚΠΣ; Ποιες οι συνήθεις δυσκολίες[12];
4. Ποια είναι τα βήματα που πρέπει να ακολουθήσουν οι κατασκευαστές ΚΠΣ προκειμένου να πετύχουν συμμόρφωση με τις απαιτήσεις που εισάγει ο ΓΚΠΔ, σε υφιστάμενα και νέα συστήματα[13];
5. Πόσο προστατευμένοι πρέπει να νιώθουν οι χρήστες από τη μέχρι τώρα εναρμόνιση των ΚΠΣ με τον ΓΚΠΔ; (τι στοιχεία υπάρχουν που δείχνουν το ποσοστό ενσωμάτωσης του ΓΚΠΔ σε ΚΠΣ;) Οι πολιτικές απορρήτου των κοινωνικών πληροφοριακών συστημάτων συμμορφώνονται με τον ΓΚΠΔ[14];
6. Σε τι βαθμό μπορεί να ανταποκριθεί ο Επίτροπος Προστασίας Προσωπικών Δεδομένων (Εποπτική Αρχή) για συχνό έλεγχο επίτευξης της συμμόρφωσης των διεργασιών που εκτελούνται μέσω των ΚΠΣ με τον ΓΚΠΔ;

1.4.2. Άλλες πηγές εισαγωγής στοιχείων και πληροφοριών (Data collection)

Επιπρόσθετα της βιβλιογραφίας, έχουν χρησιμοποιηθεί και άλλες μέθοδοι για την εισαγωγή χρήσιμων στοιχείων και πληροφοριών σχετικά με τη συμμόρφωση των ΚΠΣ

[10] Βλ. παράγραφο 2.4.1

[11] Για το ερευνητικό ερώτημα αυτό ο ΥΕ θα πρέπει να λάβει υπόψη όλα τα άρθρα που αντιστοιχούν στα σημεία του Πίνακα 1 που αναφέρονται άμεσα ή έμμεσα σε διάδραση του ΥπΔε με το ΚΠΣ (δηλ. τα σημεία 2, 3, 5, 6, 7, 8, 9, 10, 12,13, 14, 15, 16, 17, 18 και 19) ενώ στον Πίνακα 2, τα σημεία 2 και 5 δίνουν απάντηση στο ερώτημα αυτό αφού αναφέρονται ρητά στη διάδραση με τους χρήστες των ΚΠΣ.

[12] Βλ. Κεφάλαιο 3 και συνέντευξη στο Κεφάλαιο 4

[13] Βλ. Κεφάλαιο 3

[14] Για ερευνητικά ερωτήματα 5 και 6, βλ. Κεφάλαιο 4, απαντήσεις ερωτηματολογίου από Εποπτική Αρχή

με τις πρόνοιες του ΓΚΠΔ. Ακολούθως φαίνονται οι δύο μέθοδοι συλλογής δεδομένων που χρησιμοποιήθηκαν στην προσπάθεια να προσεγγιστούν κάποια από τα ερευνητικά ερωτήματα με τη διαδικασία της ποιοτικής έρευνας.

- Σχεδιασμός και αποστολή ερωτηματολογίου βασισμένο σε ερωτήσεις με σχετικό εύρος.
- Διενέργεια συνεντεύξεων με επαγγελματίες συμβούλους Υπεύθυνους Προσωπικών Δεδομένων (ΥΠΔ) που εξειδικεύονται σε Πληροφοριακά Συστήματα.

Τη συλλογή των πληροφοριών από τις απαντήσεις που συλλέγηκαν μέσω του ερωτηματολογίου και τις συνεντεύξεις, ακολούθησε ανάλυση δεδομένων μέσω ανάλυσης κειμένων (απαντήσεων) και εξαγωγή σημαντικών στοιχείων τα οποία καταγράφονται με λεπτομέρεια στο Κεφάλαιο 4 της παρούσας Διατριβής. Επίσης κάποια στοιχεία που θεωρήθηκαν πολύ σημαντικά και αφού δεν αναφέρονται στα άρθρα του ΓΚΠΔ αλλά ούτε περιλαμβάνονται στις αιτιολογικές σκέψεις του Κανονισμού, συμπεριλήφθηκαν στον «Πίνακας 2» ως επιπρόσθετες τεχνικές προδιαγραφές για τα ΚΠΣ. Τα σημεία αυτά αναλύονται περαιτέρω στην παράγραφο 3.1.2, της Διατριβής.

1.4.3. Επιλογή δείγματος

Παρόλο που το δείγμα που χρησιμοποιήθηκε είναι μικρό είναι αντιπροσωπευτικό καθώς οι ρόλοι των ατόμων που επιλέξαμε για το ερωτηματολόγιο και τις συνεντεύξεις που διενεργήθηκαν είναι ιδιαίτερα σημαντικοί στον τομέα προστασίας προσωπικών δεδομένων**.**

Πιο συγκεκριμένα:

- **Γραφείο της Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα της Κύπρου**.

  Η σημαντικότητα των απαντήσεων του ερωτηματολογίου έγκειται στο γεγονός ότι οι απαντήσεις αυτές έχουν ληφθεί από άτομα που εμπλέκονται άμεσα σε ζητήματα που αφορούν στη συμμόρφωση με τον ΓΚΠΔ. Τα άτομα του Γραφείου της Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα της Κύπρου, που έχουν εμπλακεί για τις απαντήσεις του ερωτηματολογίου, έχουν αποκτήσει την εμπειρία τους, στη συμμόρφωση με τον ΓΚΠΔ των διαφόρων οντοτήτων, μέσω της επαφής που είχαν και συνεχίζουν να έχουν καθημερινά με ιδιώτες Υπεύθυνους Προστασίας Δεδομένων, με Διευθυντικά στελέχη, διακεκριμένα άτομα

επιχειρήσεων/οργανισμών που εξειδικεύονται σε δύσκολα επαγγέλματα (Γιατροί, Δημοσιογράφοι, Αρχιτέκτονες, Πολιτικοί Μηχανικοί, Ακαδημαϊκοί κ.α.) αλλά και υπάλληλους που υποχρεούνται να δίνουν υπηρεσίες ορθής επεξεργασίας προσωπικών δεδομένων, όπως απαιτεί ο ΓΚΠΔ.

- **Επαγγελματίες σύμβουλοι (ΥΠΔ):**

  Οι δύο επαγγελματίες σύμβουλοι που επιλέχθηκαν και τους ζητήθηκε να δώσουν συνέντευξη, εξειδικεύονται στη συμμόρφωση των οργανισμών/επιχειρήσεων με τον ΓΚΠΔ. Οι σύμβουλοι, πέραν των γνώσεων τους για τις πρόνοιες του ΓΚΠΔ, έχουν ειδίκευση σε Πληροφοριακά Συστήματα που χρησιμοποιούνται σε μεγάλους οργανισμούς και επιχειρήσεις στην Κύπρο αλλά και στο εξωτερικό. Είναι πιστοποιημένοι Σύμβουλοι Προστασίας Δεδομένων από την πρώτη μέρα εφαρμογής του Κανονισμού και δέχονται έλεγχο από τον Καναδικό Φορέα Πιστοποίησης PECB με τον οποίο είναι και συνεργάτες. Κατέχουν πιστοποίηση για παροχή εκπαίδευσης για DPO, ISO27000 family και ISO29100 family. Έχουν εμπλακεί στη διαδικασία παροχής συμβουλευτικών υπηρεσιών για την πλήρη συμμόρφωση με τον ΓΚΠΔ για περισσότερες από 20 οντότητες. Ακόμα παρέχουν εκπαιδευτικές υπηρεσίες σε περισσότερες από 50 οντότητες. Οι συμβουλευτικές τους υπηρεσίες καλύπτουν υφιστάμενα αλλά και καινούρια Πληροφοριακά Συστήματα (συμπεριλαμβανομένων των ΚΠΣ) και, όπως μας έχουν πει χαρακτηριστικά, καθιστούν με σαφήνεια στην κάθε οντότητα που θα χρησιμοποιήσει κάποιο ΠΣ/ΚΠΣ (υφιστάμενο ή νέο) να μεριμνήσει ώστε τα συστήματα αυτά να είναι εναρμονισμένα με όλες τις πρόνοιες του Κανονισμού σε διαφορετική περίπτωση να μην προχωρούν στη χρήση τους. Σε τοπικό επίπεδο οι δύο αυτοί σύμβουλοι είναι ίσως οι μοναδικοί αυτή τη στιγμή στο είδος τους που δραστηριοποιούνται στον τομέα αυτό καλύπτοντας τα ΠΣ (συμπεριλαμβανομένων των ΚΠΣ) που χρησιμοποιούνται στην τοπική αγορά αλλά και την ευρύτερη περιοχή.

1.5. Δομή της Μεταπτυχιακής Διατριβής

Η εργασία αποτελείται από 3 βασικές ενότητες.

1. Στην **πρώτη ενότητα (Κεφάλαιο 2)** επισημαίνονται οι αλλαγές που επιφέρει ο νέος Κανονισμός και γίνεται σύγκριση με την 95/46/ΕΚ (εστιάζοντας κυρίως στα σημεία που αφορούν τα ΚΠΣ). Γίνεται εκτενής αναφορά στην αρχή της «Ιδιωτικότητα», αρχή για την οποία γίνεται έντονη

προσπάθεια να διαφυλαχθεί, μέσω της επίτευξης της συμμόρφωσης των διεργασιών που εκτελούνται μέσω των ΚΠΣ με τον ΓΚΠΔ. Επιπρόσθετα, παρουσιάζονται οι τύποι των δεδομένων και πληροφοριών που εισέρχονται σε ένα ΚΠΣ καθώς επίσης και οι ρόλοι και τα δικαιώματα που έχουν οι εμπλεκόμενοι σε ένα τέτοιο σύστημα.

2. Η **δεύτερη ενότητα (Κεφάλαιο 3)**, που είναι και το κύριο μέρος της παρούσας εργασίας, δίνει έμφαση στον καθορισμό, την παρουσίαση και την ανάλυση των βημάτων που θα πρέπει να ακολουθηθούν προκειμένου οι κατασκευαστές ΚΠΣ να συμμορφωθούν με τις απαιτήσεις του ΓΚΠΔ. Επισημαίνονται και παρουσιάζονται τα άρθρα του ΓΚΠΔ τα οποία πρέπει να λαμβάνουν υπόψη τους οι κατασκευαστές ΚΠΣ κατά το σχεδιασμό και την ανάπτυξη νέων συστημάτων ή εφαρμογής αλλαγών σε υφιστάμενα. Επίσης, είναι αυτά τα άρθρα που θα πρέπει να συμβουλεύονται οι υπεύθυνοι επεξεργασίας δεδομένων και οι εκτελούντες την επεξεργασία σε ΚΠΣ, ώστε να αποφεύγεται οποιαδήποτε παράνομη ενέργεια που σχετίζεται με την επεξεργασία/χρήση προσωπικών δεδομένων από τρίτους.
3. Στην **τρίτη ενότητα (Κεφάλαια 4 και 5)** παρουσιάζονται, οι απαντήσεις που συλλέχθηκαν μέσω της συνέντευξης με επαγγελματίες συμβούλους που εξειδικεύονται στο θέμα της συμμόρφωσης των επιχειρήσεων με το ΓΚΠΔ καθώς επίσης και το ερωτηματολόγιο που απαντήθηκε από Λειτουργό της Αρμόδιας Αρχής. Στη δεύτερη περίπτωση, μεταξύ άλλων, ζητήθηκαν πληροφορίες που αφορούν το ποσοστό ενσωμάτωσης του ΓΚΠΔ στα ΚΠΣ των οργανισμών (ιδιωτικών ή δημόσιων) τα οποία παρατίθενται και αναλύονται στο Κεφάλαιο 4, στην παράγραφο 4.1.2. Στο Κεφάλαιο 5 γίνεται αναφορά στην επέκταση της παρούσας εργασίας. Η εργασία ολοκληρώνεται με τα τελικά συμπεράσματα.

Κεφάλαιο 2

ΓΚΠΔ και προσωπικά δεδομένα σε ΚΠΣ

2.1. Εισαγωγή

Στον ΓΚΠΔ διαπιστώνεται ότι ο νομοθέτης προσπάθησε[15] να καλύψει όλες τις περιπτώσεις που αφορούν την προστασία των ΥπΔε, πολιτών της Ευρωπαϊκής Ένωσης. Για τους σκοπούς της παρούσας εργασίας, παρατίθενται και αναλύονται ορισμοί και σημεία τα οποία επηρεάζουν γενικά τα πληροφοριακά συστήματα (ΠΣ) όπου κατ' επέκταση επηρεάζουν και τα ΚΠΣ. Στη συνέχεια, δίνεται έμφαση στους ορισμούς και τα σημεία του Κανονισμού τα οποία αφορούν ειδικά τα ΚΠΣ. Η μελέτη αυτή εστιάζει σε ΚΠΣ και δε σημαίνει ότι οι οδηγίες που θα παρουσιαστούν θα βρουν εφαρμογή σε όλα τα ΠΣ, εκτός εάν κάποιες από τις διαδικασίες συλλογής, φύλαξης και επεξεργασίας των δεδομένων συμπίπτουν με αυτές των ΚΠΣ (πχ. δημιουργία προφίλ του χρήστη).

Προς καλύτερη κατανόηση των «υποχρεωτικών» προδιαγραφών που απορρέουν από την απαίτηση εναρμόνισης με τον ΓΚΠΔ, είναι σημαντικό να καταγραφούν οι αλλαγές που έχει επιφέρει ο ΓΚΠΔ με την κατάργηση της 95/46/ΕΚ. Στην παράγραφο 2.2.1 που ακολουθεί γίνεται σύγκριση των νέων πτυχών με τις προηγούμενες της 95/46/ΕΚ. Τα σημεία αυτά θα αναλυθούν περεταίρω, ενσωματώνοντάς τα στην ανάλυση των προδιαγραφών που ακολουθεί στην παράγραφο 3.1.2 της παρούσας Μεταπτυχιακής Διατριβής.

[15] Ο ΓΚΠΔ είναι ένα μεγάλο σε έκταση κείμενο το οποίο είναι γραμμένο με μεγάλη λεπτομέρεια και δείχνει να καλύπτει σε αρκετά μεγάλο βαθμό όλες τις πτυχές που αφορούν την προστασία προσωπικών δεδομένων κατά τη και μετά από τη συλλογή και επεξεργασία τους.

2.2. Αλλαγές και επεκτάσεις του ΓΚΠΔ σε σχέση με την οδηγία 95/46/ΕΚ

Είναι υποχρέωση του κάθε οργανισμού/επιχείρησης να ορίζει για κάθε έργο ή για κάθε σημείο αποθήκευσης προσωπικών δεδομένων υπεύθυνο επεξεργασίας (ΥΕ) των αντίστοιχων δεδομένων (συνήθως αυτός είναι ο Εκτελεστικός Διευθυντής ή αντιπρόσωπός του). Ο ΥΕ είναι υπεύθυνος να ορίζει άτομα υπεύθυνα για την εκτέλεση της οποιασδήποτε επεξεργασίας προσωπικών δεδομένων και αυτός ονομάζεται εκτελών την επεξεργασία (ΕτΕ), καθώς και Υπεύθυνο Προστασίας Δεδομένων[16] (ΥΠΔ) για κάθε έργο που ενδέχεται να επεξεργάζεται δεδομένα. Την αύξηση των υποχρεώσεων και των ευθυνών των υπεύθυνων επεξεργασίας και εκτελούντων την επεξεργασία, οι οποίοι επεξεργάζονται προσωπικά δεδομένα, εντός ή εκτός της ΕΕ και αφορούν πολίτες της ΕΕ, ακολουθούν αυστηρότατες διοικητικές κυρώσεις σε περίπτωση παραβίασης του ΓΚΠΔ.

Στον ΓΚΠΔ διαπιστώνονται σημαντικές και ουσιαστικές αλλαγές στους όρους χρήσης των προσωπικών δεδομένων, από τους ΥΕ και ΕτΕ οπουδήποτε κι αν βρίσκονται αυτοί (εντός ή εκτός ΕΕ). Οι επιχειρήσεις και οργανισμοί είναι πλέον υποχρεωμένοι να ζητούν τακτικότερα (με κάθε αλλαγή) τη συγκατάθεση του ΥπΔε για τη συλλογή και επεξεργασία προσωπικών στοιχείων. Η μέχρι πρότινος διαδικασία της συγκατάθεσης με την υποχρεωτική αποδοχή της πολιτικής του απορρήτου χωρίς το δικαίωμα της άρνησης μέρους ή ολόκληρου του κειμένου, θα αλλάξει υποχρεωτικά για όλους και θα δίνουν το δικαίωμα της επιλογής στο χρήστη, σε απλή γλώσσα και κατανοητή ορολογία.

Ο κάθε Ευρωπαίος πολίτης θα έχει το δικαίωμα της πρόσβασης σε όλα τα δεδομένα που αναφέρονται σε αυτόν, οπουδήποτε βρίσκονται ανά την υφήλιο. Το GoogleTakeout[17] είναι ένα εργαλείο της Google το οποίο επιτρέπει σε κάθε χρήστη των υπηρεσιών της Google να ζητά και να «κατεβάζει» ηλεκτρονικά τα προσωπικά του δεδομένα σε κατανοητό κείμενο.

[16] Ο κάθε οργανισμός/επιχείρηση διορίζει μόνο ένα ΥΠΔ για όλες τις περιπτώσεις επεξεργασίας προσωπικών δεδομένων

[17] https://en.wikipedia.org/wiki/Google_Takeout

Η υποχρεωτική εφαρμογή του νέου Κανονισμού θα αλλάξει τον μέχρι σήμερα τρόπο που οι επιχειρήσεις προσέγγιζαν τα analytics[18] αλλά και τη διαφήμιση. Οι συνεργάτες μιας ιστοσελίδας που διαφημίζει τρίτους είναι άγνωστοι στα ΥπΔε, αλλά μέχρι σήμερα χρησιμοποιούσε τα δεδομένα του ΥπΔε χωρίς να ενημερώνει τον τελευταίο, αλλά το κυριότερο δεν είχε καν τη συγκατάθεσή του. Ο νέος Κανονισμός όμως είναι ξεκάθαρος και υποχρεώνει ρητά όλους τους οργανισμούς/επιχειρήσεις να χειρίζονται τα προσωπικά δεδομένα με διαφάνεια και να ενημερώνουν τα ΥπΔε για το που πιθανόν να καταλήξουν τα προσωπικά τους στοιχεία.

Όπως έχει ήδη αναφερθεί στην παράγραφος 1.1, ο νέος Κανονισμός δεν είναι κάτι το καινούριο αλλά τα περισσότερα άρθρα του βασίζονται στην 95/46/ΕΚ. Υπάρχουν αρκετές νέες ορολογίες, διατάξεις και αρχές για τις οποίες ακολουθεί αναφορά και επεξήγησή τους. Για όλα αυτά, η εργασία βασίστηκε στο σύγγραμμα των Tikkinen-Piri, Rohunen και Markkula [4], στον οδηγό για επιχειρήσεις της εταιρείας A&L Goodbody [5] και στο επίσημο κείμενο του ΓΚΠΔ όπως έχει δημοσιευτεί στην επίσημη εφημερίδα της Ευρωπαϊκής Ένωσης [1].

2.2.1. Σύγκριση άρθρων ΓΚΠΔ με τα αντίστοιχα της 95/46/ΕΚ

I. <u>Γενικές διατάξεις και αρχές</u>

Τα πρώτα 11 άρθρα του ΓΚΠΔ βασίζονται στα άρθρα 2, 4, 6, 7, και 8 της 95/46/ΕΚ με τις εξής σημαντικές αλλαγές:

- **Οι ΥΕ και ΕτΕ, ανεξάρτητα από το χώρο (εντός ή εκτός ΕΕ)** στον οποίο γίνεται η επεξεργασία των προσωπικών δεδομένων οποιουδήποτε Ευρωπαίου πολίτη, έχουν υποχρέωση να συμμορφώνονται με τον ΓΚΠΔ.
- **Νέες ορολογίες**: ψευδωνυμοποίηση (άρθρο 4 – Ορισμοί), ελαχιστοποίηση των δεδομένων (άρθρο 5), ευαίσθητους τύπους προσωπικών δεδομένων (γενετικά δεδομένα, βιομετρικά δεδομένα, δεδομένα σχετικά με την υγεία) [5](σελ. 8), δεσμευτικοί εταιρικοί κανόνες (διαβίβαση προσωπικών δεδομένων σε τρίτες χώρες για επεξεργασία και χρήση, πέραν της νόμιμης και δίκαιης επεξεργασίας που επιβάλλεται από την 95/46/ΕΚ), παραβίαση των

[18] https://en.wikipedia.org/wiki/Google_Analytics

προσωπικών δεδομένων, προϋποθέσεις συναίνεσης[19] και νόμιμη επεξεργασία δεδομένων (άρθρο 7).

- **Νέες διατάξεις και αρχές**: διαφάνεια στην επεξεργασία δεδομένων (δηλ. επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο διαφανή σε σχέση με το ΥπΔε), λογοδοσία (δηλ. ο ΥΕ υποχρεούται να αποδεικνύει τη συμμόρφωσή του με τις διαδικασίες επεξεργασίας του νέου Κανονισμού) και επεξεργασία που δεν επιβάλλει ταυτοποίηση (δηλ. να μπορεί να γίνει επεξεργασία με τέτοιο τρόπο όπου οι ΥΕ και ΕτΕ αποφεύγουν να ζητούν συμπληρωματικές πληροφορίες) (άρθρο 11).
- Προστιθέμενες προϋποθέσεις σχετικά με τη **συγκατάθεση του παιδιού** σε σχέση με τις υπηρεσίες της κοινωνίας της πληροφορίας: επιβάλλεται συγκατάθεση ή εξουσιοδότηση από τον γονέα ή τον κηδεμόνα του παιδιού εάν το παιδί είναι μικρότερο από 16 ετών (κάθε κράτος μέλος της ΕΕ έχει το δικαίωμα να ορίζει μικρότερη ηλικία, με ελάχιστη την ηλικία των 13 ετών).

II. <u>Διαφάνεια</u>

Το άρθρο 12 βασίζεται στο αντίστοιχο άρθρο 12 της 95/46/ΕΚ με τις εξής σημαντικές αλλαγές:

- Ο ΓΚΠΔ υποχρεώνει τον ΥΕ να παρέχει στο ΥπΔε οποιαδήποτε πληροφορία και επικοινωνία σχετικά με την επεξεργασία των προσωπικών δεδομένων σε κατανοητή μορφή. Η 95/46/ΕΚ το ζητούσε, αλλά δεν ανέφερε συγκεκριμένες απαιτήσεις για τη μορφή των πληροφοριών. Ο ΓΚΠΔ ορίζει ότι πρέπει να χρησιμοποιείται σαφής και απλή γλώσσα, προσαρμοσμένη σε κατανοητή μορφή. Αυτό είναι ιδιαίτερα σημαντικό όταν οι πληροφορίες απευθύνονται σε παιδιά. Ο ΓΚΠΔ επεκτείνει το δικαίωμα του ΥπΔε να λαμβάνει πληροφορίες σχετικά με την επεξεργασία των προσωπικών του δεδομένων, μετά από αίτημα. Εάν τα δεδομένα προσωπικού χαρακτήρα επεξεργάζονται με αυτοματοποιημένο τρόπο (ηλεκτρονικά), ο ελεγκτής πρέπει να παράσχει τα μέσα για την υποβολή αιτήσεων, ηλεκτρονικά. Σύμφωνα με τον ΓΚΠΔ, ο υπεύθυνος επεξεργασίας πρέπει να απαντήσει στο ΥπΔε και να παράσχει τις

[19] Η 95/46/ΕΚ προέβλεπε τη σαφή συγκατάθεση του ΥπΔε, ενώ ο ΓΚΠΔ επιβάλλει να παρέχεται ελεύθερα η συναίνεση του ΥπΔε και να αποτελεί συγκεκριμένη, ενημερωμένη και ρητή ένδειξη των επιθυμιών του. Σύμφωνα με το ΓΚΠΔ, ο ΥΕ φέρει το βάρος της απόδειξης της συγκατάθεσης του ΥπΔε για την επεξεργασία των προσωπικών του δεδομένων. Το ΥπΔε έχει επίσης το δικαίωμα να αποσύρει τη συναίνεσή του ανά πάσα στιγμή. Ωστόσο, η απόσυρση δεν επηρεάζει τη νομιμότητα της επεξεργασίας βάσει της συγκατάθεσης πριν από την απόσυρσή της.

ζητούμενες πληροφορίες εντός ενός μηνός από την υποβολή της αίτησης, ενώ η 95/46/ΕΚ απαιτούσε μόνο την επαναφορά «χωρίς υπερβολική καθυστέρηση».

III. <u>Πληροφόρηση προς το ΥπΔε και απαίτηση πρόσβασης στα προσωπικά του δεδομένα με δικαίωμα διόρθωσης ή διαγραφής τους</u>

Τα άρθρα 13-22 βασίζονται στα αντίστοιχα άρθρα 10, 11, 12, 14 και15 της 95/46/ΕΚ με τις εξής σημαντικές αλλαγές:

- Στα σημεία αυτά παρατηρούνται αξιόλογες αλλαγές που αφορούν τις υποχρεώσεις του ΥΕ να συμμορφώνεται με τον νέο Κανονισμό όσων αφορά τις πληροφορίες που θα πρέπει να παρέχει στο ΥπΔε όταν ο τελευταίος τις ζητήσεις και όποτε το θελήσει αυτό. Οι πληροφορίες αυτές αφορούν,
  - τα στοιχεία επικοινωνίας του ΥΕ, του εκπροσώπου του ελεγκτή (ΕτΕ εάν υπάρχει) και του υπεύθυνου προσωπικών δεδομένων,
  - τη νομιμότητα της επεξεργασίας των δεδομένων,
  - τη νομική βάση στην οποία ο ΥΕ ή τρίτος προς αυτόν νομιμοποιούνται για την επεξεργασία αυτή,
  - πληροφορίες σχετικά με την πηγή των προσωπικών δεδομένων (εάν δεν συλλέγονται από το ΥπΔε) και εάν προέρχονται από πηγές που είναι κοινά προσβάσιμες,
  - την περίοδο για την οποία αποθηκεύονται τα προσωπικά δεδομένα.
- Επιπλέον, ο υπεύθυνος επεξεργασίας υποχρεούται να ενημερώσει το ΥπΔε σχετικά με τα δικαιώματα του τελευταίου όσον αφορά:
  - το δικαίωμα διόρθωσης ή/και διαγραφής20 των προσωπικών δεδομένων,
  - τους περιορισμούς της επεξεργασίας (προς όφελος του ΥπΔε),
  - το αντικείμενο/λόγο της επεξεργασίας,
  - τη δυνατότητα μεταφοράς δεδομένων (προώθηση),
  - την υποβολή καταγγελίας στην Εποπτική Αρχή προστασίας προσωπικών δεδομένων,
  - το δικαίωμα του να αποσύρει, οποιαδήποτε στιγμή, τη συγκατάθεσή του,
  - το δικαίωμα του ΥπΔε να αντιτάσσεται στην επεξεργασία των προσωπικών του στοιχείων (άρθρο 21),

[20] Ο ΓΚΠΔ προβλέπει το δικαίωμα στη λήθη (διαγραφή για πάντα όλων/μέρος των δεδομένων) χωρίς τους λόγους που απαιτούνται από την 95/46/ΕΚ

- τη μεταφορά δεδομένων σε τρίτη χώρα ή σε διεθνή οργανισμό,
- την ύπαρξη, τη λογική και τις προβλεπόμενες συνέπειες της αυτοματοποιημένης λήψης αποφάσεων (συμπεριλαμβανομένης της προώθησης) [6].

- Εάν ο ΥΕ προτίθεται να επεξεργαστεί τα προσωπικά δεδομένα για σκοπό διαφορετικό από τον αρχικό, πρέπει να παρέχει στο πρόσωπο στο οποίο αναφέρονται τα δεδομένα πληροφορίες σχετικά με αυτό το νέο σκοπό πριν από την επεξεργασία.

IV. <u>Γενικές υποχρεώσεις (Άρθρα 24-31)</u>

Τα άρθρα 24-31 βασίζονται στα αντίστοιχα άρθρα 16, 17, 18 και19 της 95/46/ΕΚ με τις εξής σημαντικές αλλαγές:

- Προστασία των δεδομένων ήδη **από το σχεδιασμό** και **εξ ορισμού** (by design and by default) (Άρθρο 25)
  - Τόσο κατά τον καθορισμό των μέσων επεξεργασίας (**από το σχεδιασμό**) όσο και κατά την επεξεργασία, ο ΥΕ εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα, π.χ. η ψευδωνυμοποίηση, η ελαχιστοποίηση των δεδομένων, η ασφάλεια δικτύου καθώς και τα κατάλληλα άτομα με τις αντίστοιχες υποχρεώσεις που αναλογούν στον καθένα.
  - **Εξ ορισμού**, διασφαλίζεται από τον ΥΕ ότι μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα υπόκεινται σε επεξεργασία και δεν καθίστανται προσβάσιμα χωρίς την έγκριση του ΥπΔε σε αόριστο αριθμό φυσικών προσώπων.
- Αρχεία των δραστηριοτήτων επεξεργασίας (Άρθρο 30)
  - Υποχρέωση των ΥΕ και ΕτΕ να τηρούν αρχείο όλων των κατηγοριών δραστηριοτήτων επεξεργασίας, γραπτώς, τουλάχιστο σε ηλεκτρονική μορφή.
  - Η υποχρέωση αναφέρεται σε οργανισμούς που εργοδοτούνται όχι λιγότερα των 250 ατόμων, ή αν η επεξεργασία των προσωπικών δεδομένων θεωρείται υψηλού κινδύνου.
- Λογοδοσία (Άρθρα 24 και 5)
  - Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει (άρθρο 5.2) τη συμμόρφωση με την παράγραφο 1 του άρθρου 5 η οποία αναφέρει τα ακόλουθα:

- Τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία με νομιμότητα, αντικειμενικότητα και διαφάνεια.
- Συλλέγονται μόνο τα αναγκαία δεδομένα για καθορισμένους, ρητούς και νόμιμους σκοπούς.
- Πρέπει να διέπονται από ακρίβεια και να διαγράφονται ή διορθώνονται όσα δεδομένα προσωπικού χαρακτήρα είναι ανακριβή.
- Η αποθήκευσή τους να περιορίζεται στο ελάχιστο και όσο χρόνο επιβάλλεται για την επεξεργασία τους.
- Προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια.

o Σύμφωνα με το άρθρο 24 ο υπεύθυνος επεξεργασίας υποχρεούται να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό.

V. <u>Ασφάλεια δεδομένων προσωπικού χαρακτήρα (Άρθρα 32-34)</u>

Τα άρθρα 31-34 βασίζονται στα αντίστοιχα άρθρα 17, 4 της 95/46/ΕΚ με τις εξής σημαντικές αλλαγές:

- Μέτρα ασφαλείας (Άρθρο 32)
  - o Ο ΥΕ και ο ΕτΕ εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα τέτοια ώστε να εξασφαλίζεται κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, όπως:
    - Ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων.
    - Διασφάλιση του απορρήτου, ακεραιότητα, διαθεσιμότητα και αξιοπιστία των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση.
    - Άμεση αποκατάσταση της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε περίπτωση φυσικού ή τεχνικού συμβάντος.
    - Τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών για την απόδειξη της ασφάλειας της επεξεργασίας.
  - o Εκτιμώντας το κατάλληλο επίπεδο ασφάλειας λαμβάνονται υπόψη οι κίνδυνοι της επεξεργασίας, κυρίως από τυχαία ή αθέμιτη καταστροφή, απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση σε προσωπικά

δεδομένα που μεταφέρονται, αποθηκεύονται ή υποβάλλονται σε επεξεργασία μη ενδεδειγμένη.

- Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην Εποπτική Αρχή (Άρθρο 33)
  - Ο ΕτΕ έχει την υποχρέωση να ενημερώσει τον ΥΕ αντιληφθεί παραβίαση δεδομένων προσωπικού χαρακτήρα και ο ΥΕ, με τη σειρά του, έχει την υποχρέωση να ενημερώνει άμεσα και έγκαιρα, εντός 72 ωρών, την Εποπτεύουσα Αρχή, για την παραβίαση αυτή.
- Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο ΥπΔε (Άρθρο 34)
  - Ανακοινώνεται άμεσα στο ΥπΔε, όταν η παραβίαση είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες του.
  - Δεν επιβάλλεται ανακοίνωση υπό προϋποθέσεις (βλ. Άρθρο 34, παρ. 3)

VI. <u>Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων</u>

Τα άρθρα 35, 36 βασίζονται στο αντίστοιχο άρθρο 20 της 95/46/ΕΚ με τις εξής σημαντικές αλλαγές:

Με το άρθρο 35 του ΓΚΠΔ εισάγεται η καινούρια έννοια της Εκτίμησης Αντικτύπου σχετικά με την Προστασία Δεδομένων (ΕΑΠΔ) (Data Protection Impact Assessment - DPIA).

- Η ΕΑΠΔ περιλαμβάνει υποχρεωτικά τα ακόλουθα:
  - Για λογαριασμό του οργανισμού που εκπροσωπεί και του έννομου συμφέροντος που είναι εντεταλμένος να υποστηρίξει, ο ΥΕ εκτελεί συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας,
  - Διενεργείται εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,
  - Γίνεται εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των ΥπΔε που αναφέρονται στην παράγραφο 1 του Άρθρου 35 του ΓΚΠΔ και
  - Έχοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των ΥπΔε λαμβάνονται τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων

προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό.

- Η εκτίμηση αποτελεί σημαντικό εργαλείο στη διάθεση των ΥΕ αφού τους βοηθά να λογοδοτήσουν αποτελεσματικά ακολουθώντας τις απαιτήσεις του ΓΚΠΔ. Επίσης με τον τρόπο αυτό συλλέγουν ακριβή στοιχεία για να αποδείξουν ότι έχουν ληφθεί τα κατάλληλα μέτρα για να διασφαλιστεί η συμμόρφωση με τον κανονισμό.
- Η μη συμμόρφωση με τις απαιτήσεις της ΕΑΠΔ μπορεί να οδηγήσει σε πρόστιμα, σε παγκόσμιο επίπεδο, έως €10εκ. ή έως 2% επί του συνολικού ετήσιου κύκλου εργασιών κατά το προηγούμενο οικονομικό έτος (όποιο από τα δύο είναι υψηλότερο) και αυτά επιβάλλονται από την Εποπτική Αρχή (Επίτροπος Προστασίας Προσωπικών Δεδομένων).
- Ως μη συμμόρφωση θεωρείται τόσο η εκτέλεση ΕΑΠΔ με εσφαλμένο τρόπο (Άρθρο 35, παρ. 2-7 και Άρθρο 36, παρ. 3ε), όσο και η μη εκτέλεση ΕΑΠΔ όταν η επεξεργασία υπόκειται σε εκτίμηση αντικτύπου (Άρθρο 35, παρ. 1,3-4).
- Ο ΥΕ θα πρέπει να είναι ιδιαίτερα προσεκτικός και πολύ συγκεκριμένος με τα αποτελέσματα της διαδικασίας αυτής αφού ο ΓΚΠΔ είναι πολύ σαφής και ξεκάθαρος. Αν η ΕΑΠΔ έχει σαν αποτέλεσμα ότι η οποιαδήποτε επεξεργασία προσωπικών δεδομένων ενδέχεται να οδηγούν σε υψηλό κίνδυνο που ο ΥΕ δεν μπορεί να ακολουθήσει ή να ελέγξει χρησιμοποιώντας κατάλληλο εξοπλισμό (μηχανογραφικό ή άλλως πως) ή το κόστος υλοποίησης της εφαρμογής είναι εκτός των δυνατοτήτων του οργανισμού, τότε ο ΥΕ υποχρεούται να διαβουλεύεται με την Εποπτική Αρχή πριν προχωρήσει στην επεξεργασία (αιτιολογική σκέψη 84, ΓΚΠΔ) [1].
- Ο ΓΚΔΠ καθορίζει ρητά την εμπλοκή του ΥΠΔ στη εκτέλεση ΕΑΠΔ ως εξής:
    - «*Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων*» (άρθρο 35 παρ. 2),
    - Ο ΓΚΠΔ, ανάμεσα στα καθήκοντα του ΥΠΔ, ορίζει ρητά ότι, «*παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35*» (άρθρο 39, παρ. 1γ).

VII. Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ ή DPO)

Τα άρθρα 37, 38 και 39 βασίζονται στο αντίστοιχο άρθρο 18 της 95/46/ΕΚ με τις εξής σημαντικές αλλαγές:

Όλοι οι δημόσιοι/ιδιωτικοί οργανισμοί και επιχειρήσεις για τους οποίους συγκαταλέγεται στις δραστηριότητές τους η επεξεργασία προσωπικών δεδομένων, συστηματικά και σε μεγάλη κλίμακα, υποχρεούνται να ορίσουν Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ - Data Protection Officer - DPO).

Η οποιαδήποτε παραβίαση του ΓΚΠΔ δεν βαραίνει τον ΥΠΔ ο οποίος κυρίως ενεργεί συμβουλευτικά προς τους ΥΕ και ΕτΕ. Ελέγχει και εξασφαλίζει ότι οι ΥΕ και ΕτΕ είναι σε θέση να αποδεικνύουν σε κάθε περίπτωση ότι η επεξεργασία των δεδομένων πραγματοποιείται σύμφωνα με τις διατάξεις του ΓΚΠΔ (βλ. Άρθρο 24, παρ. 1). Η συμμόρφωση της προστασίας δεδομένων αποτελεί ευθύνη του ΥΕ ή του ΕτΕ.

Δεν είναι αρκετός από μόνος του ο διορισμός του ΥΠΔ, αλλά για την αποτελεσματική εκτέλεση των καθηκόντων του πρέπει να του παρέχεται επαρκής αυτονομία και πόροι, τέτοια που να είναι απρόσκοπτος και συνεχής ο συμβουλευτικός του χαρακτήρας, να εκτελεί ορθά την παρακολούθηση της συμμόρφωσης με τον κανονισμό και να ενεργεί ως σημείο επαφής με την Εποπτεύουσα Αρχή.

2.3. Ιδιωτικότητα στα ΚΠΣ

Στο βιβλίο του, The Information: A History. A Theory. A Flood, ο δημοσιογράφος James Gleick [7], υποστηρίζει ότι οι πληροφορίες είναι «*το αίμα και το καύσιμο, η ζωτική αρχή της ζωής μας*». Ο Gleick, στον πρόλογο του βιβλίου, κάνει μια αναδρομή στην εξέλιξη της διακίνησης της πληροφορίας του τελευταίου αιώνα, αφ' ότου άρχισε η προσπάθεια του ανθρώπου να μαζέψει την πληροφορία στην παλάμη του ενός χεριού του. Ο καθένας πλέον έχει στο χέρι του ένα κινητό τηλέφωνο όπου, στην ουσία, με αυτό το μέσο επικοινωνίας μπορεί να έχει όση πληροφορία υπάρχει. Όντως έτσι είναι τα δεδομένα σήμερα; Ο Gleick αναφέρει στο βιβλίο του «*Είναι τελικά φυσικό - ακόμα και αναπόφευκτο - να τίθεται το ερώτημα, πόση πληροφορία υπάρχει στο σύμπαν;*».

2.3.1. Η μηχανή αναζήτησης της Google, το DeepWeb και το DarkNet

Η Google έχει σήμερα πρόσβαση (indexing) μόνο στο 0.004% [8] της παγκόσμιας πληροφορίας αλλά ταυτόχρονα έχει και το 91%[21] του μεριδίου της παγκόσμιας επισκεψιμότητας/χρήσης προς αναζήτηση του Κυβερνοχώρου. Κυβερνοχώρος όμως δεν είναι μόνο αυτό που «ξέρει» το Google search. Το υπόλοιπο 99.996%, είναι καλά κρυμμένο από το ευρύ κοινό του Ιστοχώρου. Το DeepWeb είναι μια διαδικτυακή κοινωνία συλλογής και διακίνησης δεδομένων στους οποίους υπάρχει ελεγχόμενη πρόσβαση. Στο DeepWeb συμπεριλαμβάνονται και οι πληροφορίες όλων των επιχειρήσεων σε παγκόσμιο επίπεδο, δεδομένα τα οποία είναι επιθυμητό, από τους ιδιοκτήτες, να είναι πάντα ασφαλή. Είναι ιστοσελίδες ή χώροι αποθήκευσης (cloudstorage), περιορισμένης πρόσβασης, στις οποίες μια μηχανή αναζήτησης σταματά μέχρι το σημείο που είναι ανοικτό στο ευρύ κοινό. Από την άλλη όμως το DarkNet, αν και συμπεριλαμβάνεται στο DeepWeb, εντούτοις είναι ορατό μόνο από λίγους. Οι πράξεις που διενεργούνται στο DarkNet είναι ανώνυμες και μη ανιχνεύσιμες. Γενικά θεωρείται παράδεισος για παράνομη δραστηριότητα όπου διακινούνται τεράστια χρηματικά ποσά για οικονομικές πράξεις, χωρίς τη διαμεσολάβηση των γνωστών σε όλους Τραπεζών.

Ενδεικτικά αναφέρονται μερικά παραδείγματα δοσοληψιών, στο DarkaNet, τα οποία έχουν να κάνουν με τεράστιους αριθμούς προσωπικών δεδομένων που έχουν διακινηθεί ή καλύτερα πωληθεί στο δίκτυο αυτό, σύμφωνα με δημοσίευμα του έγκυρου περιοδικού «Network Security» της εταιρείας Elsevier Ltd [9].

Χαρακτηριστικό είναι το γεγονός ότι μετά τη διαρροή 117 εκατομμυρίων λογαριασμών του κοινωνικού δικτύου LinkedIn, το 2012, που περιλάμβαναν διευθύνσεις ηλεκτρονικού ταχυδρομείου και «αδύνατους»[22] κωδικούς πρόσβασης, αφότου το LinkedIn αδυνατούσε να χρησιμοποιήσει την κρυπτογράφηση «salt»[23] (ένα σημείο όπου οι κατασκευαστές των ΚΠΣ θα πρέπει να έχουν σοβαρά υπόψη), το

[21] https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/

[22] «SHA-1 hashed password» χωρίς τη χρήση της κρυπτογράφηση «salt» όπου το τελευταίο ενισχύει το συνδυασμό του μυστικού κωδικού (βλ. https://www.thesslstore.com/blog/difference-encryption-hashing-salting/)

[23] Στην κρυπτογράφηση, το «salt» είναι μέθοδος που χρησιμοποιείται ως πρόσθετη λειτουργία μονής κατεύθυνσης η οποία σε συνδυασμό με τη μέθοδο κρυπτογράφησης «hashing» (hashing: μετατρέπει οποιαδήποτε μορφή δεδομένων σε μια μοναδική σειρά χαρακτήρων), σε δεδομένα ή σε κωδικούς πρόσβασης, κάνει την κωδικοποίηση ασφαλέστερη. Η μέθοδος «salt» χρησιμοποιείται για την προστασία των κωδικών πρόσβασης όταν οι κωδικοί αυτοί αποθηκεύονται.

κοινωνικό αυτό δίκτυο προχώρησε σε συμφωνία για πώλησή του στην Microsoft. Άρα είναι πολύ σημαντικό για έναν οργανισμό να διατηρεί ακέραια τα ηλεκτρονικά κυρίως δεδομένα των ΚΠΣ του, διότι αυτή η προσπάθεια είναι μόνο προς όφελός του αφού μεγαλώνει την αξία του οργανισμού. Σε διαφορετική περίπτωση μια επιχείρηση καταλήγει σαν την LinkedIn να εξαγοραστεί σε πολύ χαμηλότερη τιμή.

Αν ο πιο πάνω αριθμός των 117 εκατομμυρίων ακούγεται μικρός, αξίζει να αναφερθεί ότι άλλα 360 εκατομμύρια λογαριασμοί του κοινωνικού δικτύου MySpace έχουν συλλεχθεί και προσφερθεί προς πώληση στο DarkNet από τον ίδιο «hacker» με το ψευδώνυμο «Peace», πριν τον Ιούνιο του 2013, μήνας κατά τον οποίο η εταιρεία είχε αλλάξει ριζικά την πλατφόρμα της, σύμφωνα πάντα με το ίδιο περιοδικό [9]. Μέχρι τότε όμως τίποτα δεν είχε ανακοινώσει στο κοινό η MySpace (κατά τον ΓΚΠΔ έπρεπε να δηλωθεί σε 72 ώρες) και φυσικά δεν είχε παραδεχτεί ευθέως τη διαρροή προσωπικών δεδομένων. Για πολλά άλλα κοινωνικά δίκτυα έχει αναφερθεί διαρροή δεδομένων (κλοπή καλύτερα) και πώλησή τους στο DarkNet, μεταξύ των οποίων το Tumblr της Yahoo (το έτος 2013 και δεν είχε αναφερθεί τίποτα από την ιδιοκτήτρια μέχρι το Μάιο του 2016), το iMesh (51 εκ. λογαριασμοί το έτος 2013), το «dating site» Fling (μερικά εκατομμύρια IDs το έτος 2011), το Twitter (33 εκ. λογαριασμοί) και το TeamViewer. Χαρακτηριστικό είναι ότι όλες οι πιο πάνω επιχειρήσεις είχαν αποκρύψει ή δεν έχουν ποτέ παραδεχτεί τη διαρροή των εκατομμυρίων προσωπικών λογαριασμών, πράγμα που το καθιστά πολύ επικίνδυνο για το χρήστη.

2.3.2. Υποχρεωτική και όχι προαιρετική η συμμόρφωση με τον ΓΚΠΔ

Όλων των τύπων τα Κοινωνικά Πληροφοριακά Συστήματα όπως οι ηλεκτρονικές πλατφόρμες, τα κοινωνικά δίκτυα και οι εφαρμογές για κινητά (π.χ. το LinkedIn, το Facebook, το Google) πρέπει να προσαρμόσουν τις πολιτικές τους σχετικά με τη χρήση και τη διακίνηση προσωπικών δεδομένων, ώστε να συμμορφωθούν με τον ΓΚΠΔ.

Οι μηχανισμοί αποδοχής χρήσης από τους χρήστες σχετικά με τη συλλογή, την αποθήκευση, την κοινή χρήση και τη διακίνηση των δεδομένων τους, πρέπει να τροποποιηθούν (αν αυτό δεν έχει ακόμα γίνει) έτσι ώστε να μην προεπιλέγονται οι ρυθμίσεις απορρήτου, αλλά θα πρέπει να είναι μια συνειδητή, πλήρως υπεύθυνη συγκατάθεση του χρήστη. Επομένως, καλό είναι οι χρήστες να μη γίνονται «θύματα» της αυτόματης εγγραφής στην αγορά (market) του ηλεκτρονικού ταχυδρομείου, της

αυτόματης ανταλλαγής δεδομένων μεταξύ διαφορετικών ΚΠΣ (ή και άλλων ΠΣ) ή γενικά των καλά κρυμμένων προεπιλογών χωρίς τη ρητή συγκατάθεσή τους. Ο ορισμός της συγκατάθεσης, όπως αυτό καταγράφεται ξεκάθαρα στον ΓΚΠΔ, δεν είναι πλέον αντικείμενο που επιδέχεται περεταίρω ερμηνεία αλλά το ΥπΔε πρέπει να ενημερωθεί σχετικά με τις ακόλουθες πληροφορίες: τον τύπο των δεδομένων που συλλέγει το ΚΠΣ, τον τρόπο με τον οποίο τα δεδομένα θα χρησιμοποιηθούν, με ποιους (ποια άλλα ΠΣ) τα δεδομένα θα μοιραστούν/διαδοθούν και το σημαντικότερο, για πόσο καιρό θα διατηρηθούν αποθηκευμένα στη βάση δεδομένων του κάθε ΚΠΣ [10].

Ήδη, επιχειρήσεις κολοσσοί φαίνεται να έχουν αρχίσει να συμμορφώνονται με τις πιο πάνω πρόνοιες του ΓΚΠΔ, αναφέρουν στο άρθρο τους οι Spataru-Negura και Lazar [10]. Η PayPal, μια από τις μεγαλύτερες πλατφόρμες ηλεκτρονικών τραπεζικών συναλλαγών, στις αρχές του έτους 2018, αποκάλυψε μια λίστα συνεργατών στους οποίους η πλατφόρμα μοιράζεται τα προσωπικά δεδομένα των χρηστών (π.χ. πλήρες όνομα, τραπεζικό λογαριασμό, στοιχεία επιχείρησης, στοιχεία επικοινωνίας, λεπτομέρειες συναλλαγών), πράγμα το οποίο δε γνώριζαν οι χρήστες προηγουμένως. Φυσικά η PayPal θα πρέπει να κάνει πολλά περισσότερα ώστε να συμμορφωθεί πλήρως με τον ΓΚΠΔ ώστε να μην έχει την ίδια κατάληξη όπως την εταιρεία Google στην οποία Γαλλικό δικαστήριο έχει επιβάλει πρόστιμο 50 εκ. ευρώ[24] για τη μη ξεκάθαρη πολιτική απορρήτου για την οποία ανάγκαζε τον χρήστη να δώσει τη συγκατάθεσή του χωρίς να του δίνει το δικαίωμα της επιλογής.

Επιπλέον της ενημέρωσης, σχετικά με τα δεδομένα του ΥπΔε που το κάθε ΚΠΣ θα επεξεργαστεί και με ποιον τρόπο, από τη στιγμή που θα δημιουργηθεί ένας λογαριασμός χρήστη σε ένα ΚΠΣ, οι χρήστες θα μπορούν να ζητούν από τους ΥΕ την πρόσβαση σε όλα τα προσωπικά δεδομένα που έχουν αποθηκευτεί. Επίσης όλα τα ΚΠΣ (συμπεριλαμβανομένων και όλων των κοινωνικών δικτύων) είναι υποχρεωμένα να δώσουν πρόσβαση σε όλα τα δεδομένα τα οποία έχουν συλλεχθεί πριν τις 25 Μαΐου 2018, αφότου μπήκε σε εφαρμογή τον ΓΚΠΔ. Με τον όρο πρόσβαση συνεπάγεται το δικαίωμα της επεξεργασίας (συμπεριλαμβανομένης και της πλήρους διαγραφής) [10]. Αξίζει να σημειωθεί η υπόθεση (2015) του Αυστριακού φοιτητή της νομικής Μαξ Σρεμς όπου σε ένα τετραετή δικαστικό αγώνα με τη FB κατάφερε να πετύχει τη

[24] https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-gdpr-fine-eu-data-privacy-cnil-amazon-apple-a8740191.html

διαγραφή όλων των δεδομένων που βρίσκονταν σε όλα τα σημεία αποθήκευσης δεδομένων (servers) της κοινωνικής πλατφόρμας παρά τις αρχικές αντιρρήσεις της FB. Ο δικαστικός αυτός αγώνας κράτησε 4 χρόνια αφού είχε λάβει χώρα πολύ πριν την εφαρμογή του ΓΚΠΔ (Μάιος 2018). Τώρα φαίνεται ότι αυτού του είδους οι υποθέσεις δεν θα είναι τόσο χρονοβόρες αφού ο ΓΚΠΔ είναι πολύ ξεκάθαρος.

Σε πρόσφατη υπόθεση εκδίκασης (αρχές 2018) από Βελγικό δικαστήριο, το Facebook (FB) απειλείται με πρόστιμο μέχρι και 100 εκ. ευρώ αν εξακολουθεί να παρακολουθεί την ηλεκτρονική συμπεριφορά Βέλγων χρηστών του FB (ή και μη χρηστών του FB), μέσω τεχνολογίας cookies[25] και καλά κρυμμένων στιγμάτων (pixels, π.χ. κουμπί like στο FB) σε ιστοσελίδες τρίτων. Το Βελγικό δικαστήριο απαίτησε τη διαγραφή όλων των δεδομένων που αφορούσαν την πιο πάνω δραστηριότητα. [11]

Δεν είναι οι μόνες περιπτώσεις που η FB ήρθε αντιμέτωπη με τη δικαιοσύνη. Το 2017, ένα ισπανικό δικαστήριο του επέβαλε πρόστιμο 1,2 εκ. ευρώ, αφού η εθνική υπηρεσία προστασίας δεδομένων της χώρας, απέδειξε ότι το Facebook συγκέντρωσε και χρησιμοποίησε προσωπικά δεδομένα για διαφημιστικούς σκοπούς. Η πλατφόρμα συγκέντρωνε στοιχεία σχετικά με το σεξουαλικό προσανατολισμό των ανθρώπων και τις θρησκευτικές πεποιθήσεις τόσο από την πλατφόρμα του κοινωνικού δικτύου όσο και από τρίτες πλατφόρμες, χωρίς τη συναίνεση του ΥπΔε. [12]

2.3.3. Αποκλεισμός χρήστη από τη χρήση ενός ΚΠΣ

Δεν είναι λίγοι εκείνοι οι χρήστες που αποδέχονται τυφλά τη χρήση ενός ΚΠΣ, χωρίς να παρατηρούν εξ αρχής τί ζητά το σύστημα αυτό από εκείνους ώστε να τους επιτρέψει τη χρήση του. Στην έμμεση «απειλή» για τον αποκλεισμό στο δικαίωμα της χρήσης ενός ΚΠΣ, ο χρήστης εξαναγκάζεται να αποδεχτεί «χωρίς (δεύτερη) ανάγνωση» όλους τους όρους και περιορισμούς του συστήματος (Πολιτική Απορρήτου - Privacy Policy) πριν προχωρήσει στη χρήση του. Αν όμως δινόταν στους χρήστες ένα πιο απλό και κατανοητό κείμενο το οποίο θα μπορούσαν να διαβάσουν

[25] Τα cookies είναι μικρά αρχεία που αποθηκεύονται στον υπολογιστή ενός χρήστη. Έχουν σχεδιαστεί για να συλλέγουν δεδομένων ειδικά για ένα συγκεκριμένο πελάτη και ένα ιστότοπο. Αυτά στέλνονται και αποθηκεύονται σε κάποιον εξυπηρετητή (server). Αυτό επιτρέπει στον διακομιστή (webserver) να παραδώσει μια σελίδα προσαρμοσμένη σε ένα συγκεκριμένο χρήστη ή η ίδια η σελίδα μπορεί να περιέχει κάποιο σενάριο που γνωρίζει τα δεδομένα στο cookie και έτσι μπορεί να μεταφέρει πληροφορίες από μίαν επίσκεψη σε έναν ιστότοπο, στον επόμενο ιστότοπο που επισκέπτεται ο χρήστης.
Επίσης βλ. ιστοσελίδα Γραφείου Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα, Κύπρου
http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/71B32C48C08B5AC1C22582780040F80E?OpenDocument&highlight=cookies

εύκολα με την πρώτη ματιά [13] [14], τότε θα μπορούσαν ελεύθερα να επιλέξουν εάν επιθυμούν να δώσουν τη συγκατάθεσή τους ή όχι για χρήση των προσωπικών τους δεδομένων.
Αν ο χρήστης είχε το δικαίωμα να δεχτεί ή να απορρίψει κάποιους από τους κανόνες ή/και περιορισμούς του πληροφοριακού συστήματος αντί του εξαναγκασμού της ολικής αποδοχής, τότε θα γινόταν η παραδοχή ότι ο κατασκευαστής εφάρμοσε τις πρόνοιες του ΓΚΠΔ, όσον αφορά το θέμα της συγκατάθεσης.

Ένα ιδιαίτερα αξιοσημείωτο παράδειγμα της μεγάλης υποχώρησης που κάνει πάντοτε ο τελικός χρήστης, στο βωμό της τεχνολογικής ανάπτυξης, είναι να θυσιάζει την ιδιωτικότητά του έναντι της ασφάλειάς του (Knobel & Bowker, 2011). Αυτό συμβαίνει πολύ συχνά όταν ο χρήστης είναι συνεχώς συνδεδεμένος, μέσω κάποιου λογαριασμού του στον Παγκόσμιο Ιστό (πχ. Google account). Επίσης συμβαίνει και σε μεγάλο βαθμό με τα λογισμικά των «έξυπνων τηλεφώνων» (smartphones), όπου ανιχνεύουν την κίνηση, την τοποθεσία και τις επιθυμίες του χρήστη. Με απλά λόγια η κάθε του ενέργεια καταγράφεται και δυστυχώς ποτέ δεν του δίνεται εύκολα το δικαίωμα της διαγραφής. Ίσως τώρα με την εφαρμογή του ΓΚΠΔ να γίνουν σχετικές βελτιώσεις.

2.3.4. Κοινωνικές αξίες και Ιδιωτικότητα στα ΚΠΣ

Σήμερα, όσο ποτέ άλλοτε, ο χρήστης επιζητεί την ευκολία του μέσω των εκατοντάδων εφαρμογών που έχει εγκατεστημένες στον υπολογιστή του ή το κινητό του τηλέφωνο, όμως είναι καιρός να απαιτεί τη διασφάλιση της ιδιωτικότητας χωρίς να την απεμπολεί, έτσι απλά για χάριν και μόνο της χρήσης μιας νέας τεχνολογίας ή ενός καινούριου ΚΠΣ. Οι Knobel & Bowker [13], για την ύπαρξη και προβολή των κατάλληλων **κοινωνικών αξιών** σε ένα σύστημα, αναφέρουν σαν κύρια πρόκληση πως οι κοινωνικές αξίες διαφέρουν από άτομο σε άτομο και είναι πολύ δύσκολο, ο άνθρωπος (κατασκευαστής ΚΠΣ), να εντοπίσει ή να αποφασίσει με ποιες αξίες θα σχεδιάσει μια νέα τεχνολογία. Τα πληροφοριακά συστήματα συνήθως αποκαλύπτουν τις κοινωνικές αρχές και αξίες των δημιουργών τους, έτσι τις πλείστες φορές οι σχεδιαστές των συστημάτων δεν εστιάζουν σε αυτές αλλά κυρίως στην κερδοφορία, παραβιάζοντας σε μεγάλο βαθμό και την ιδιωτική ζωή των χρηστών. Καλύτερα πληροφοριακά προϊόντα θα αναπτύσσονταν εάν σχεδιάζονταν συλλογικά και με περισσότερη εστίαση στις κοινωνικές αξίες και τα δικαιώματα του χρήστη, αναφέρουν στο άρθρο τους οι Knobel & Bowker [13]. Σήμερα είναι ξεκάθαρο πως ο

σχεδιασμός και η υλοποίηση ενός ΚΠΣ θα πρέπει να συμμορφώνονται με όλα τα άρθρα του ΓΚΠΔ, πριν αυτό είναι διαθέσιμο για κοινή χρήση.

2.3.5. Ο άνθρωπος ως χρήστης και «συνεργάτης[26]» για τα ΚΠΣ

Ο ανθρώπινος παράγοντας είναι **η μεγαλύτερη ανάγκη για την ύπαρξη των ΚΠΣ**. **Η ενεργή συμμετοχή** των χρηστών στην Κοινωνία ενός Πληροφοριακού Συστήματος, κρατάει το ΚΠΣ ζωντανό αλλά ταυτόχρονα το βοηθάει να αναπτύσσεται και να εξελίσσεται παράλληλα όπως η τεχνολογία προχωράει με γοργούς ρυθμούς. Με τη συμμετοχή του ανθρώπου σε ένα οποιοδήποτε ΚΠΣ εξυπακούεται και η δημιουργία λογαριασμού (personal account), όπου καλείται να δηλώσει πολλά προσωπικά του στοιχεία. Αυτά τα στοιχεία, μαζί με τη δραστηριότητα του κάθε χρήστη, είναι το «καύσιμο» σε πολύ μεγάλο βαθμό για τις πράξεις οικονομικού οφέλους που εφαρμόζονται στον Ιστό, σήμερα. Είναι το μέρος της αποθηκευμένης πληροφορίας που οι περισσότεροι θα ήθελαν να έχουν στη κατοχή τους, με απώτερο στόχο το οικονομικό όφελος, από την επεξεργασία και χρήση της. Είναι αυτά τα στοιχεία που χρησιμοποιούνται για να εντοπίζουν το «στόχο» τους οι διαφημιστές και να δημιουργούν τα δίκτυα διαφημίσεων τους. Η διαφήμιση είναι η κύρια πηγή εσόδων για τους περισσότερους κατασκευαστές εφαρμογών για κινητά τηλέφωνα και ως αντάλλαγμα αυτές οι εφαρμογές να δίνονται «δωρεάν» στον τελικό χρήστη. [15]

2.4. Ρόλοι και Τύποι Δεδομένων/Πληροφοριών στα ΚΠΣ

Στη μοντελοποίηση των προδιαγραφών υλοποίησης ΚΠΣ με γνώμονα τα άρθρα του ΓΚΠΔ, σημαντικό ρόλο θα παίξουν τα δεδομένα που εισάγονται, επεξεργάζονται και εξάγονται από τα ΚΠΣ καθώς και οι ρόλοι που αντιστοιχούν σε κάθε άτομο που εμπλέκεται σε όλη τη διαδικασία σχεδίασης/καταγραφής απαιτήσεων, υλοποίησης και λειτουργίας ενός τέτοιου συστήματος.

2.4.1. Τύποι δεδομένων που εισάγονται στα ΚΠΣ

Με την αναφορά όλων των πιο πάνω γεγονότων και πληροφοριών, αλλά έχοντας υπόψη και τα άρθρα καθώς και την αιτιολογική περιγραφή που αναφέρονται στον

[26] Βλ. «συνεισφορά», παράγραφος 1.2, παρούσας εργασίας

ΓΚΠΔ, έγινε κατάληξη στην καταγραφή των **τύπων δεδομένων** που εισάγονται στα ΚΠΣ.

- **Ευαίσθητα δεδομένα**

  Τα προσωπικά στοιχεία που συμπληρώνουν τους πιο κάτω τύπους δεδομένων ή/και η δραστηριότητα (επιγραμμικό αναγνωριστικό ταυτότητας) του κάθε χρήστη (ΥπΔε) είναι αυτό που ορίζεται ως «δεδομένα προσωπικού χαρακτήρα» (Άρθρο 4, παρ. 1) [1]. Ταυτόχρονα, μέρος των δεδομένων αυτών ονομάζονται «ευαίσθητα δεδομένα» για τα οποία ο ΓΚΠΔ αναφέρεται στο άρθρο 9 και απαγορεύεται ρητά (εκτός σε πολύ ειδικές περιπτώσεις) «*η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη 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 τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό»* (Άρθρο 9, παράγραφος 1) [1]. Σε γενικές γραμμές απαγορεύεται η επεξεργασία δεδομένων, για τα οποία ένα άτομο μπορεί να ταυτοποιηθεί, χωρίς τη ρητή του συγκατάθεση εκτός εάν το ΥπΔε έχει ήδη προχωρήσει από μόνος του στη δημοσιοποίηση των δεδομένων αυτών. Επίσης, για τα ευαίσθητα δεδομένα ο ΓΚΠΔ αναφέρει ότι «*Τα κράτη μέλη μπορούν να διατηρούν ή* να *θεσπίζουν περαιτέρω όρους, μεταξύ άλλων και περιορισμούς, όσον αφορά την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν την υγεία*» (Άρθρο 9, παράγραφος 4).

  Στα ΚΠΣ (ειδικά τα κοινωνικά δίκτυα), όσον αφορά τους ΥΕ και ΕτΕ, δεν επιτρέπεται ο έλεγχος και η επεξεργασία οποιωνδήποτε ευαίσθητων δεδομένων που αναφέρονται σε εγγεγραμμένους χρήστες ή μη χρήστες των δικτύων αυτών (**μη χρήστες** βλ. δικαστική υπόθεση Βελγικού δικαστηρίου εναντίον του FB [11]), χωρίς τη ρητή συγκατάθεσή τους. Εάν κάποιο ΚΠΣ, μέσω ηλεκτρονικής φόρμας εγγραφής για τη δημιουργία προφίλ, έχει πρόθεση να συλλέξει ευαίσθητα δεδομένα χρηστών με τη χρήση ερωτήσεων, θα πρέπει το σύστημα να διευκρινίσει από την αρχή ότι οι απαντήσεις στις ερωτήσεις αυτές είναι εθελοντικές.

- **Στοιχεία που ταυτοποιούν (ή κάνουν ταυτοποιήσιμο – έμμεση ταυτοποίηση) ένα χρήστη στην πραγματική ζωή**
  - Όνομα
  - Επίθετο
  - Κρατικά έγγραφα (Πολιτική ταυτότητα, Διαβατήριο κ.α.)
  - Αριθμός τηλεφώνου, Διεύθυνση
  - Καταγωγή
  - Κοινωνική τάξη
  - IBAN
- **Στοιχεία μέσω έξυπνων τηλεφώνων (smartphones)**
  - Άμεσα μηνύματα, τηλεφωνικές κλήσης, βιντεοκλήσεις, μηνύματα φωνοκιβωτίου
  - Φωτογραφικό άλμπουμ
  - Τοποθεσία (location)
  - Επαφές (contacts)
  - Μοναδικός αριθμός συσκευής και αναγνωριστικό πελάτη (π.χ. IMEI13, IMSI14, UDID15 και αριθμός τηλεφώνου)
  - Πιστωτική κάρτα και δεδομένα πληρωμών
  - Ιστορικό διαδικτυακής πλοήγησης (Browsing history)
  - Πληροφορίες για τα ΚΠΣ (σε ποια είναι μέλος)
  - Κωδικοί πρόσβασης
  - Βιομετρικά στοιχεία (π.χ. facial recognition and fingerprint templates)
- **Ηλεκτρονικά στοιχεία**
  - Όνομα λογαριασμού χρήστη
  - Ηλεκτρονική διεύθυνση (email)
  - Διεύθυνση μηχανής (IP address)
  - Τοποθεσία σύνδεσης (συντεταγμένες GPS – tracking)
  - Σύνδεση σε διακομιστή
- **Δραστηριότητα Χρήστη στα ΚΠΣ**
  - Ιστορικό συνδέσεων
  - Χρόνος που παραμένει στο σύστημα
  - Από ποιες μηχανές συνδέθηκε (laptop, smartphone, PC)
  - Σελίδες που επισκέφτηκε
  - Ομάδες άλλων χρηστών που συνδέεται περισσότερο ή συχνότερα

- Επαφές (contacts)
- Θέματα που τον ενδιαφέρουν περισσότερο
- Κωδικοί πρόσβασης
- Μηνύματα και βιντεοκλήσεις

- **Ενεργά και μη ενεργά δεδομένα**

  Δεδομένα που έχει αναρτήσει ο χρήστης (ΥπΔε) για τα οποία τα ενεργά δεδομένα διαχωρίζονται από τα διαγραμμένα δεδομένα (μη ενεργά) αλλά όλα βρίσκονται αποθηκευμένα στους εξυπηρετητές του ΚΠΣ (σχόλια, φωτογραφίες, βίντεο κ.α.). Η πλήρης διαγραφή των δεδομένων αυτών γίνεται μόνο μετά από αίτημα του χρήστη προς τον ΥΕ του ΚΠΣ.

2.4.2. Ρόλοι στα ΚΠΣ (κατά τη σχεδίαση, υλοποίηση και λειτουργία των συστημάτων)

Το ΥπΔε θα πρέπει να γνωρίζει τα υποκείμενα (χειριστές) που θα μπορεί να επικοινωνεί μαζί τους σε περίπτωση που χρειαστεί. Επίσης, η Εποπτική Αρχή του κάθε αντίστοιχου κράτους μέλους της ΕΕ, έχει το δικαίωμα της επίβλεψης και ελέγχου των συστημάτων αυτών επικοινωνώντας με τον ορισθέντα ΥΠΔ, με βάση τα δικαιώματα που πηγάζουν από τον ΓΚΠΔ αλλά και βάσει εθνικού νόμου (ανά κράτος ξεχωριστά) που υποχρεώθηκαν τα εθνικά κοινοβούλια να προωθήσουν προς ψήφιση. Άρα ο ΥΕ δηλώνει στην Εποπτική Αρχή τα στοιχεία του ΥΠΔ του κάθε έργου για το οποίο ενδέχεται να επεξεργάζεται δεδομένα, όταν αυτό εκτελεστεί και τα πληροφοριακά συστήματα τεθούν σε λειτουργία (δηλ. να τεθεί σε εφαρμογή και χρήση από το κοινό).

Για τη δημιουργία (κατασκευή) και τη σωστή λειτουργία των ΚΠΣ, καταγράφονται οι ρόλοι των υποκειμένων που εμπλέκονται σε αυτά.

- **Υπεύθυνος Προσωπικών Δεδομένων (ΥΠΔ)**

  Ο ΥΠΔ ενεργεί συμβουλευτικά και ελέγχει τον ΥΕ αλλά και τον κατασκευαστή καθ' όλη τη διάρκεια της σχεδίασης και υλοποίησης ενός ΚΠΣ. Το τελικό αποτέλεσμα θα πρέπει να συμμορφώνεται με τις απαιτήσεις του ΓΚΠΔ. Σε διαφορετική περίπτωση ο ΥΠΔ καταγγέλλει στην Εποπτική Αρχή τους ΥΕ και κατασκευαστή του ΚΠΣ ως υπεύθυνους της μη τήρησης του Κανονισμού. Γενικά, ο ΥΠΔ είναι το σημείο επαφής του οργανισμού με τον Επίτροπος Προστασίας Προσωπικών Δεδομένων, όταν αυτό κριθεί αναγκαίο.

- **Κατασκευαστής**
  - Υπάλληλος οργανισμού/επιχείρησης ή
  - Εξωτερικός συνεργάτης ή Προμηθευτής

Ο κατασκευαστής έχει την ευθύνη να σχεδιάσει και να αναπτύξει το ΚΠΣ σύμφωνα με τις πρόνοιες του ΓΚΠΔ και να παραδώσει ένα σύστημα πλήρως συμμορφωμένο με τον Κανονισμό.

Στο πλαίσιο της παρούσας μεταπτυχιακής εργασίας διενεργήθηκε συνέντευξη για την εξαγωγή συμπερασμάτων που αφορούν στην ανταπόκριση των επιχειρήσεων σχετικά με την επίτευξη της συμμόρφωσης των διεργασιών που εκτελούνται μέσω των ΚΠΣ με τον ΓΚΠΔ. Μερικές από τις απαντήσεις που παραχωρήθηκαν από τους συμμετέχοντες κ.κ. Παπαδόπουλος και Ιωάννου παρουσιάζονται παρακάτω.

1. *Οι κατασκευαστές ΚΠΣ δεν πρέπει να αγνοούν καμία πρόνοια του ΓΚΠΔ και να τις διαχωρίζουν σε λιγότερο ή περισσότερο σημαντικές. Αυτοί φέρουν την μεγαλύτερη ευθύνη για την ενσωμάτωση όλων των απαιτούμενων προνοιών του Κανονισμού (οι οποίες αντιστοιχούν στο εκάστοτε ΚΠΣ).*
2. *Στην εν μέρη ενσωμάτωση των υποχρεωτικών σημείων του Κανονισμού, κατά την υλοποίηση εναρμόνισης υφιστάμενου συστήματος με το ΓΚΠΔ ή την υλοποίηση ενός νέου, ο κατασκευαστής (και οι συνεργάτες του, αν υπάρχουν) έχει την απόλυτη ευθύνη αφού θα πρέπει να μεριμνήσει για την εφαρμογή των αρχών προστασίας δεδομένων που υπογραμμίζονται στο ΓΚΠΔ, από την αρχή της λειτουργίας του συστήματος. Θα πρέπει να καλύψει όλα τα βήματα εναρμόνισης πριν παραδώσει το προϊόν στον πελάτη. Επίσης ο κατασκευαστής/προμηθευτής θα πρέπει να απαιτήσει να τηρηθούν όλες οι απαιτούμενες πρόνοιες του κανονισμού για το περιβάλλον εργασίας που θα τοποθετηθεί και θα τεθεί σε λειτουργία το νέο σύστημα. Αυτό ισχύει και για όλα τα υφιστάμενα συστήματα για τα οποία ο οργανισμός θα πρέπει να μεριμνήσει για πιθανές αλλαγές που χρειάζονται ώστε να επιτευχθεί η εναρμόνισή τους με τη συμβολή του κατασκευαστή/προμηθευτή.*
3. *Αν κατά τον έλεγχο, από την Εποπτική Αρχή, σε κάποιο νέο ΚΠΣ διαφανούν κενά τα οποία πηγάζουν από υλοποίηση συστήματος που δεν πληροί τις απαιτήσεις για ασφάλεια προσωπικών δεδομένων των χρηστών, την ευθύνη*

φέρει ο κατασκευαστής/προμηθευτής αλλά εάν οι ελλείψεις αφορούν πρόνοιες που δε ζητήθηκαν, την ευθύνη φέρει ο οργανισμός που όφειλε να τις ζητήσει. Επίσης, την ευθύνη φέρει ο ίδιος ο οργανισμός, αν ο οργανισμός δεν τηρεί τις διαδικασίες που ορίστηκαν από τον κατασκευαστή/προμηθευτή.

- **Διαχειριστής ΚΠΣ (Υπεύθυνος Επεξεργασίας)**
  - Εκτελεστικός Διευθυντής οργανισμού ή
  - Ιδιοκτήτης/Διευθυντής επιχείρησης.

Και οι δύο αυτές επαγγελματικές θέσεις έχουν το ρόλο του ΥΕ των ΚΠΣ του οργανισμού/επιχείρησης και έχουν το δικαίωμα να διορίζουν ένα ΥΠΔ για τον οργανισμό και πολλούς ΕτΕ για κάθε έργο, για το οποίο ο ΥΕ ενδέχεται να επεξεργάζεται δεδομένα. Επίσης, έχουν τη μεγαλύτερη ευθύνη [27] για τη συμμόρφωση με τον ΓΚΠΔ. Όλες οι οδηγίες για κάθε επεξεργασία δεδομένων ξεκινούν από αυτούς ή αντιπροσώπους τους. Δεν παύουν ποτέ να ευθύνονται για οποιαδήποτε λάθη συμβούν στην επεξεργασία δεδομένων ακόμα κι αν αυτά δεν έχουν γίνει απευθείας από αυτούς.

- **Εκτελών την Επεξεργασία**
  - Υπάλληλος οργανισμού/επιχείρησης
  - Εξωτερικοί συνεργάτες (Οποιοσδήποτε Τρίτος)

Και στις δύο περιπτώσεις είναι άτομα διορισμένοι από τον ΥΕ για να εκτελέσουν επεξεργασία προσωπικών δεδομένων (κατά την κατασκευή του συστήματος ή κατά την εργασία σε υφιστάμενο ΚΠΣ). Οι οδηγίες που παίρνουν είναι συγκεκριμένες και δε μπορούν να παρεκκλίνουν από αυτές.

Ο ΥΕ έχει την ευθύνη της επιλογής του ΕτΕ. Ο ΕτΕ, για να μπορεί να προχωρήσει στην επεξεργασία προσωπικών δεδομένων, υποχρεούται να συνάψει σύμβαση με τον ΥΕ (γραπτώς - εντύπως ή ηλεκτρονικώς), με τρόπο ξεκάθαρο και με συγκεκριμένο περιεχόμενο (άρθρο 14, ΓΚΠΔ) [1].

[27] Ο ΥΕ έχει και νομική ευθύνη. Είναι αυτός που θα πρέπει να εμφανιστεί σε δικαστήριο αν μετά από καταγγελία η υπόθεση καταλήξει να δικάζεται στο δικαστήριο.

Τα ΥπΔε έχουν το δικαίωμα να προσφύγουν με καταγγελία, στον ΥΠΔ ή στην Εποπτική Αρχή, τόσο κατά του ΥΕ είτε κατά του ΕτΕ (εφόσον ο τελευταίος δεν ανταποκρίθηκε στις υποχρεώσεις του παρόντος κανονισμού ή ενήργησαν αντίθετα προς τις νόμιμες εντολές του ΥΕ) και να ζητήσουν αποζημίωση και αποκατάσταση της ζημιάς που υπέστησαν («*Κάθε πρόσωπο το οποίο υπέστη υλική ή μη υλική ζημία ως αποτέλεσμα παραβίασης του παρόντος κανονισμού δικαιούται αποζημίωση από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία για τη ζημία που υπέστη*» - άρθρο 82, ΓΚΠΔ).

Ο Εκτελών μετατρέπεται σε ΥΕ, εφόσον ο πρώτος χρησιμοποιήσει τα δεδομένα για δικούς του σκοπούς, έτσι θα φέρει πλέον ακεραία την ευθύνη, να συμμορφώνεται με το ΓΚΔΠ, ως ΥΕ.

- **Συντηρητές συστημάτων**
  - Υπάλληλος οργανισμού/επιχείρησης
  - Εξωτερικοί συνεργάτες (Οποιοσδήποτε Τρίτος)

Και στις δύο περιπτώσεις είναι άτομα διορισμένοι από τον ΥΕ ως Εκτελούντες την Επεξεργασία (ΕτΕ). Οι οδηγίες είναι συγκεκριμένες και δεν μπορεί ο ΕτΕ να παρεκκλίνει από αυτές.

Η συντήρηση των ΚΠΣ αφορά επεκτάσεις ή διορθώσεις/αλλαγές του συστήματος, μεταφορά/αποθήκευση δεδομένων που έχουν κριθεί απαρχαιωμένα, αναβαθμίσεις του υλικού (διακομιστές), εργασίες σε άλλα συστήματα που συνδέεται/συγχρονίζεται το ΚΠΣ (π.χ. στην περίπτωση ενός Πανεπιστημίου η βάση δεδομένων των φοιτητών θα πρέπει να είναι κεντρικά εγκατεστημένη και δεν πρέπει να μεταφέρονται δεδομένα σε άλλα συστήματα. Τα συνδεδεμένα, με τη βάση δεδομένων, συστήματα «ζητούν» να συγχρονίζονται με τη βάση για να διαβάσουν δεδομένα ενός χρήστη. Εδώ εφαρμόζεται ψευδωνυμοποίηση μέσω ενός Πανεπιστημιακού αριθμού, μοναδικού για τον κάθε φοιτητή. Αυτός ο αριθμός είναι το μόνο στοιχείο που παίρνει το ΚΠΣ, σχετικά με τα προσωπικά στοιχεία του φοιτητή, που φυλάσσονται στην κεντρική βάση δεδομένων).

- **Χρήστης (ΥπΔε)**
  - Εσωτερικοί
  - Εξωτερικοί

  Εσωτερικοί χρήστες είναι οι υπάλληλοι του οργανισμού/επιχείρησης (πιθανόν να οριστούν και ΕτΕ αν αυτό κριθεί αναγκαίο).

  Εξωτερικοί χρήστες ονομάζονται αυτοί που χρησιμοποιούν το σύστημα απλά και μόνο για να έρθουν σε επαφή με τις υπηρεσίες του οργανισμού ή να επικοινωνήσουν με άλλους χρήστες.

  Και στις δύο περιπτώσεις οι πιο πάνω χρήστες προστατεύονται ρητά από τον ΓΚΠΔ. Τα προσωπικά τους δεδομένα υπόκεινται σε επεξεργασία μόνο με τη ρητή τους συγκατάθεση και ενημερώνονται για οποιαδήποτε αλλαγή γίνει σε σχέση με αυτά.

2.4.3. Εξαγωγή στοιχείων και πληροφοριών από τα ΚΠΣ

Τα ΚΠΣ έχουν τη δυνατότητα να εξάγουν στοιχεία, μεμονωμένα (παρουσίαση στην οθόνη) ή μέσα από αναφορές (reports), τα οποία μπορούν να ταυτοποίησουν ή να κάνουν ένα ΥπΔε ταυτοποιήσιμο. Η εξαγωγή και διάθεση των οποιονδήποτε στοιχείων υπόκειται κάτω από τον ΓΚΠΔ, έτσι υποχρεωτικά πριν τη δραστηριότητα αυτή θα πρέπει να προηγείται η κατάλληλη συναίνεση του ΥπΔε. Οι πιο κάτω ενέργειες θεωρούνται εξαγωγή στοιχείων από ένα ΚΠΣ.

- **Ηλεκτρονικές ή έντυπες αναφορές**

  Αναφορές τις οποίες θα μπορούσε να προβάλει στην οθόνη του ο διαχειριστής του συστήματος, να τις εκτυπώσει σε έντυπη μορφή ή ακόμα να τις καταγράψει ηλεκτρονικά σε αρχείο και να τις καταχωρήσει/αποθηκεύσει σε αποθηκευτική συσκευή.
- **Στατιστικά στοιχεία συστήματος**

  Μέσα από τα στατιστικά στοιχεία που θα μπορούσε ο Διαχειριστής (ΥΕ ή ΕτΕ) να ζητήσει από το σύστημα, υπάρχει η δυνατότητα το ΥπΔε να γίνει ταυτοποιήσιμο (στήλες οι οποίες καταγράφουν γένος, ηλικία, επάγγελμα, τόπο καταγωγής κ.α. - π.χ. «Άντρες ηλικίας 70 χρόνων και άνω, Κρεοπώλες, από το Γέρι». Αν το

αποτέλεσμα είναι ένας άντρας υπάρχει μεγάλη πιθανότητα να έχει ήδη ταυτοποιηθεί βάσει των πιο πάνω στοιχείων (το ΥπΔε είναι ταυτοποιήσιμο)).

- **Ιστορικό δραστηριότητας χρήστη**

  Το ιστορικό της κίνησης ενός χρήστη σε ένα ΚΠΣ καταγράφεται αλλά αυτό δε θα πρέπει να κρατείται πέραν του χρονικού διαστήματος, για το οποίο έχει παρθεί η συγκατάθεση του ΥπΔε. Κατά τη διάρκεια αυτή δε, δίνεται το δικαίωμα να παρακολουθείται ή να καταγράφεται σε αναφορές η δραστηριότητα του χρήστη, εκτός αν γνωστοποιείται κάθε φορά η πρόθεση και ο σκοπός της επεξεργασίας αυτής στο ΥπΔε, αφού κάθε φορά τα στοιχεία του είναι διαφορετικά (π.χ. ημερομηνία, ώρα, τόπος σύνδεσης, συσκευή σύνδεσης, χρόνος που παρέμεινε στο σύστημα, σελίδες που επισκέφτηκε κ.α.).

- **Log files**

  Η καταγραφή εισόδου/εξόδου/περιήγηση, κυρίως, του διαχειριστή (ΥΕ ή ΕτΕ) στο ΚΠΣ είναι στοιχεία που δείχνουν δραστηριότητα. Η ανάγκη της παρατήρησης αυτής θα πρέπει να γίνεται μόνο αν αυτό κριθεί αναγκαίο, μόνο για την εύρυθμη λειτουργία του συστήματος. Θα πρέπει να προστατεύονται οι ενέργειες (κινήσεις μέσα στο σύστημα) του διαχειριστή για την καλύτερη άσκηση των καθηκόντων του.

- **Μεταφορά στοιχείων των ΥπΔε σε τρίτους**

  Η χρήση προσωπικών στοιχείων του ΥπΔε για εξαγωγή αναλύσεων (π.χ. Google Analytics) ή για Διαφημιστικούς σκοπούς δεν επιτρέπεται χωρίς τη ρητή συγκατάθεση του ΥπΔε. Στην περίπτωση που η μεταφορά δεδομένων γίνεται σε χώρα εκτός της ΕΕ τότε κρίνεται αναγκαία η άδεια εκτέλεσης της πράξης αυτής, από την Εποπτική Αρχή.

Κεφάλαιο 3

ΚΠΣ και Συμμόρφωση με ΓΚΠΔ

3.1. Προδιαγραφές για το Σχεδιασμό, Υλοποίηση και Λειτουργία των ΚΠΣ

Ένα ΚΠΣ κατατάσσεται στο γενικό πλαίσιο των Πληροφοριακών Συστημάτων και ακολούθως διαφοροποιείται και εντάσσεται στην ειδική κατηγορία των πληροφοριακών συστημάτων. Η λειτουργία των ΚΠΣ βασίζεται και σε ξεχωριστούς παράγοντες, άλλους από αυτούς των γενικών ΠΣ, άρα ό,τι ισχύει για ένα ΠΣ αυτό ισχύει και εφαρμόζεται σε οποιοδήποτε ΚΠΣ.

Όπως έχει ήδη αναφερθεί, ο σκοπός της διατριβής αυτής είναι η μοντελοποίηση των νομικών απαιτήσεων που εισάγει ο ΓΚΠΔ και η «μετάφρασή» τους σε τεχνικές προδιαγραφές για τα ΚΠΣ, πράγμα το οποίο θα βοηθήσει τους εμπλεκόμενους να επιτύχουν συμμόρφωση των συστημάτων τους με τον ΓΚΠΔ.

Έχουν καταγραφεί όλα τα βήματα που θα πρέπει να ακολουθήσει ένας κατασκευαστής ώστε να παραδώσει στον ΥΕ του οργανισμού/επιχείρησης ένα ΚΠΣ το οποίο θα πληροί όλες τις απαιτήσεις του ΓΚΠΔ. Με τον τρόπο αυτό η ευθύνη μετατίθεται στον ΥΕ ο οποίος υποχρεούται πλέον να διενεργεί την επεξεργασία των προσωπικών δεδομένων ως ορίζει ο ΓΚΠΔ.

3.1.1. Προδιαγραφές ΚΠΣ οι οποίες υπόκεινται στον ΓΚΠΔ

Ακολούθως παρατίθενται όλες οι απαιτούμενες προδιαγραφές για συμμόρφωση ενός ΚΠΣ κατά το στάδιο του σχεδιασμού και ανάπτυξής του. Οι συλλογή και παρουσίαση των προδιαγραφών που παρουσιάζονται βασίζονται σε όλη τη βιβλιογραφία της παρούσας εργασίας (επιστημονικά άρθρα, βιβλία, περιοδικά, ιστοσελίδες κ.α.) και στις πληροφορίες που συλλέγηκαν μέσα από τη συνέντευξη και το ερωτηματολόγιο που έχουν διενεργηθεί. Το κάθε χαρακτηριστικό που αναφέρεται πιο κάτω, αναλύεται και

περιγράφεται κατάλληλα ώστε να γίνει περισσότερο κατανοητό στον αναγνώστη, ανεξαρτήτως του γνωστικού του αντικειμένου.

3.1.1.1. Ορισμοί[28]

«*Έργο*»: Η κατασκευή ενός ΚΠΣ. Επίσης καλύπτει και την περίπτωση ανάθεσης εργασιών για αναβάθμιση (για συμμόρφωση με το ΓΚΠΔ) υφιστάμενων ΚΠΣ. Ακόμα αναφέρεται και στην περίπτωση που ένα ΚΠΣ δεν κατασκευάζεται με τη συμμετοχή του φορέα αλλά ο φορέας προμηθεύεται προκατασκευασμένο σύστημα και το προσαρμόζει στα δικά του κριτήρια ή το χρησιμοποιεί αυτούσιο.

«*Φορέας*»: Ο οργανισμός που θα εκτελέσει το έργο (ΚΠΣ)

«*Τρίτος*»: Εταιρεία ή άτομο, εξωτερικός συνεργάτης του φορέα, διορισμένος από τον φορέα.

«*ΕΠΔ*»: Επεξεργασία προσωπικών δεδομένων

«*Σύμβαση ΕΠΔ*» : Ετοιμάζεται από τον ΥΕ και αφορά ρητή δέσμευση του ΕτΕ για πρόσβαση και επεξεργασία προσωπικών δεδομένων από τον ΕτΕ.

«*Ανάδοχος*»: Η εταιρία/κατασκευαστής του ΚΠΣ (υφιστάμενα ή καινούρια).

«*Σύμβαση υλοποίησης έργου*»: Όροι διεξαγωγής του έργου με τις αρχικές απαιτήσεις του φορέα, για εγγυήσεις προστασίας δεδομένων κατά την επεξεργασία και χρήση τους καθ' όλη τη διάρκεια του έργου. Η σύμβαση αυτή υπογράφεται μεταξύ του φορέα και του ανάδοχου του έργου.

3.1.1.2. Βήματα πριν την έναρξη του έργου

Πριν την έναρξη του έργου ακολουθούνται τα πιο κάτω **υποχρεωτικά βήματα** ώστε να διαπιστωθεί από τον φορέα (ΥΕ ο οποίος ονομάζεται και διαχειριστής του έργου), ότι η όλη διαδικασία, μέχρι και την ολοκλήρωση του έργου αλλά και αργότερα κατά

[28] Οι ορισμοί στην παράγραφο αυτή έχουν αποκλειστική χρήση στην παρούσα εργασία (δηλ. δεν έχουν καμία σχέση με το κείμενο του ΓΚΠΔ)

τη διάρκεια που το ΚΠΣ θα τεθεί σε λειτουργία, θα συμμορφώνεται με τις απαιτήσεις του ΓΚΠΔ. Αυτό μειώνει την πιθανότητα διαρροής δεδομένων, εξαιτίας οποιασδήποτε κακής επεξεργασίας αυτών. Όλα τα παρακάτω βήματα μπορούν να εφαρμοστούν τόσο σε καινούρια όσο και σε υφιστάμενα ΚΠΣ, εκτός από το βήμα 6 που αφορά μόνο τα υφιστάμενα ΚΠΣ.

- Βήμα 1ο

  Ο ΥΕ διεξάγει Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων (ΕΑΠΔ), για να διαπιστώσει ότι δεν υπάρχει κίνδυνος κατά την υλοποίηση του έργου και η οποιαδήποτε επεξεργασία προσωπικών δεδομένων να οδηγήσει σε διαρροή δεδομένων, την οποία ο ΥΕ δε θα μπορεί να ακολουθήσει ή να ελέγξει χρησιμοποιώντας κατάλληλους μηχανισμούς αντιμετώπισης ή το κόστος υλοποίησης της εφαρμογής να είναι εκτός των δυνατοτήτων του φορέα. Εάν η ΕΑΠΔ εμφανίσει υψηλά επίπεδα κινδύνου που θα οδηγήσει στη μη συμμόρφωσης με το ΓΚΠΔ, το έργο προσωρινά διακόπτεται και ο ΥΕ συμβουλεύεται την Εποπτική Αρχή ώστε με τις κατάλληλες οδηγίες του Επιτρόπου Προστασίας Προσωπικών Δεδομένων να αποφασιστεί η πορεία του έργου.

  Όταν αποφασιστεί να προχωρήσει το έργο, ο ΥΕ διορίζει ΥΠΔ ο οποίος θα είναι ο σύμβουλος του έργου μέχρι και την παράδοσή του αλλά και στη συνέχεια, κατά τη λειτουργία του ΚΠΣ και όποτε χρειαστεί να επέμβει ο ΥΠΔ μπορεί να το κάνει.

- Βήμα 2ο

  Ζητείται έκθεση αποτίμησης αποκλίσεων (IT Gap Analysis) από τους διαχειριστές του δικτύου (network) του φορέα, ότι:

  - το δίκτυο ικανοποιεί όλες τις απαιτήσεις για την ασφάλεια των συστημάτων από οποιαδήποτε κακόβουλη πρόσβαση από εντός ή/και εκτός του δικτύου
  - υπάρχουν δικλείδες ασφαλείας και περιορισμοί στη μεταφορά δεδομένων από το δίκτυο εντός του οργανισμού προς άλλο εξωτερικό δίκτυο[29]

[29] Θα μπορούσε να είναι το Διαδίκτυο ή ένα δίκτυο άλλου οργανισμού που έχει κάνει διμερή συμφωνία με τον φορέα

- ο φορέας διαθέτει σύστημα εντοπισμού και έγκαιρης ειδοποίησης (Intrusions Detection System) [30] από ενδεχόμενη «διαδικτυακή επίθεση» προς το δίκτυο του οργανισμού
- το δίκτυο διαθέτει πρωτόκολλο SSH[31] το οποίο παρέχει ένα ασφαλές κανάλι επικοινωνίας του δικτύου του φορέα με άλλα δίκτυα μέσω αρχιτεκτονικής χρήστη και διακομιστή (client-server)-(στην περίπτωση αυτή, χρήστης θα μπορούσε να είναι και ένας άλλος διακομιστής εκτός του δικτύου του φορέα)
- εφαρμογή του πρωτοκόλλου HTTPS[32] για ασφάλεια στην επικοινωνία του δικτύου του φορέα με το διαδίκτυο. Το πρωτόκολλο αυτό, μέσω του επιπέδου δικτύου TLS (Transport Layer Security) [33] , χρησιμοποιεί κρυπτογράφηση στην επικοινωνία του δικτύου του οργανισμού με το διαδίκτυο και με παράλληλη χρήση του πρωτοκόλλου IPsec [34] , διασφαλίζεται και η ασφαλής μετάδοση πακέτων στον παγκόσμιο Ιστό, μέσω αυθεντικοποίησης (authentication) και κρυπτογράφησης (encryption).

- Βήμα 3ο

  Διασφαλίζεται ότι ο φορέας εφαρμόζει ικανοποιητικό επίπεδο στη χρήση συνθηματικών για πρόσβαση στα πληροφοριακά του συστήματα, πράγμα που θα εφαρμοστεί και σε οποιοδήποτε ΚΠΣ που θα κατασκευαστεί στον οργανισμό ή θα προμηθευτεί προκατασκευασμένο σύστημα. Επιπρόσθετα το βήμα αυτό θα μπορούσε να υποστηριχθεί με συγγραφή σχετικής πολιτικής συνθηματικού (password policy).

- Βήμα 4ο

  Διορισμός ΕτΕ εντός και εκτός του φορέα οι οποίοι θα εργαστούν για τον σχεδιασμό, καταγραφή απαιτήσεων, υλοποίηση και επίβλεψη του έργου.

[30] Βλ. https://en.wikipedia.org/wiki/Intrusion_detection_system
[31] Βλ. https://en.wikipedia.org/wiki/Secure_Shell
[32] Βλ. https://en.wikipedia.org/wiki/HTTPS
[33] Βλ. https://en.wikipedia.org/wiki/Transport_Layer_Security
[34] Βλ. https://en.wikipedia.org/wiki/IPsec

Οι ΕτΕ υποχρεούνται να υπογράψουν «Σύμβαση ΕΠΔ» που θα τηρήσουν για όσο χρόνο χρειαστεί μέχρι την ολοκλήρωση της κατασκευής ή προμήθειας του έργου.

- Βήμα 5ο

  Προσδιορισμός δεδομένων («Data classification»)
  Αρχικά γίνεται ο προσδιορισμός των δεδομένων (βλ. παρ. 2.4.1 - τύποι δεδομένων) που θα εισάγονται στο σύστημα.

  Στο βήμα αυτό, για κάθε συλλογή δεδομένων, που θα ακολουθήσει στα στάδια που φαίνονται στον Πίνακα 1, πρέπει να λαμβάνονται υπόψη τα ακόλουθα:

  - Ποια είναι η πηγή των δεδομένων;
  - Για ποιό σκοπό συλλέγονται;

  Στο μέρος 3.1.2 (Ανάλυση σημείων Πίνακας 1, σημείο 1) που ακολουθεί θα προσδιοριστεί η ροή των δεδομένων και μαζί με το 5ο βήμα που αναλύεται εδώ, θα ολοκληρωθεί η διαδικασία χαρτογράφησης δεδομένων (data mapping). Τα δεδομένα δηλώνονται από το ίδιο το ΥπΔε ή εισάγονται από άλλο σύστημα μετά από συναίνεση του ΥπΔε που επηρεάζεται από τη μεταφορά αυτή.

  - Τι δεδομένα συλλέγονται;
  - Πως γίνεται η εισαγωγή/εξαγωγή τους στο ΚΠΣ;
  - Ποια είναι η χρήση τους;
  - Ποιοι έχουν πρόσβαση σε αυτά και τι δικαιώματα έχουν (ποιοι τα βλέπουν, τα επεξεργάζονται, σε ποιους κοινοποιούνται κλπ.);

  Όπως έχει ήδη αναφερθεί σε αρκετά σημεία στην παρούσα εργασία, προτείνεται να ακολουθούνται οι παραπάνω ενέργειες προσδιορισμού δεδομένων, ώστε η επεξεργασία των προσωπικών δεδομένων που ακολουθείται να μην παρεκκλίνει έστω και το ελάχιστο από το ΓΚΠΔ. Τα μέτρα ασφαλείας (ως τεχνικά μέτρα) που θα πρέπει να σχεδιάζονται και εφαρμόζονται είναι υποχρέωση του ΥΕ και των ΕτΕ με ρητές και γραπτές οδηγίες προς τους τελευταίους.

- Βήμα 6ο

  Στην περίπτωση που το έργο αφορά υφιστάμενα ΚΠΣ, εφαρμόζεται ανάλυση αποκλίσεων ή αλλιώς έκθεση αποτίμησης αποκλίσεων (Gap analysis)

  - Με την αποτίμηση των αποκλίσεων επιτυγχάνεται η έγκαιρη αναγνώριση των βασικών κενών και περιοχών προς βελτίωση στην υποδομή του οργανισμού, λαμβάνοντας πάντα υπόψη τις απαιτήσεις του ΓΚΠΔ
  - Ο οργανισμός αποκτά μια καλύτερη εικόνα για τις λειτουργίες και διαδικασίες του ΚΠΣ που θα χρειασθεί ο ΥΕ να εισηγηθεί βελτιώσεις προς συμμόρφωση με τον Κανονισμό
  - Κάθε απόκλιση που καταγράφεται, είναι θεμιτό να συνοδεύεται από μια σύντομη και κατανοητή περιγραφή ώστε το άτομο που θα αναλάβει τις διορθώσεις να είναι σε θέση να τις υλοποιήσει σωστά και χωρίς χρονοτριβή.

3.1.1.3. Πίνακες Προδιαγραφών για την κατασκευή ΚΠΣ

Ένα ΚΠΣ κατασκευάζεται εντός του οργανισμού από τον ίδιο τον οργανισμό και τους ειδικούς για την εργασία αυτή ή το έργο ανατίθεται σε «ανάδοχη» εταιρεία. Οι ΕτΕ (συνήθως υπάλληλοι του οργανισμού) αναλαμβάνουν να προσδιορίσουν τις τεχνικές προδιαγραφές (γενικές ή ειδικές προδιαγραφές) του έργου. Οι προδιαγραφές που θα προσδιοριστούν και θα ακολουθηθούν από τον «ανάδοχο» θα καθορίσουν την υλοποίηση του έργου με συγκεκριμένο τρόπο και υποχρεώσεις, προς τον φορέα και ιδιοκτήτη του ΚΠΣ. Όλες οι απαιτήσεις/προδιαγραφές (υποχρεωτικές ή/και προαιρετικές) του έργου θα πρέπει να είναι ξεκάθαρες και να ευθυγραμμίζονται άμεσα ή έμμεσα με τις πτυχές και απαιτήσεις του ΓΚΠΔ.

Η μοντελοποίηση των απαιτήσεων του ΓΚΠΔ που καταγράφονται πιο κάτω, ως προδιαγραφές υλοποίησης του έργου, μπορούν να εφαρμοστούν τόσο σε καινούρια όσο και σε υφιστάμενα ΚΠΣ. Οι τεχνικές προδιαγραφές για την υλοποίηση του έργου, ετοιμάζονται από τους ΕτΕ και μπορούν να ακολουθούν τις οδηγίες που παρουσιάζονται στους παρακάτω πίνακες ώστε με σιγουριά να επιτευχθεί κάλυψη όλων των υποχρεώσεων του φορέα έναντι του ΓΚΠΔ. Το κάθε σημείο μπορεί να αφορά από μία ή περισσότερες τεχνικές προδιαγραφές του έργου (κατά τον σχεδιασμό). Ο ανάδοχος, ενδείκνυται να λαμβάνει σοβαρά υπόψη τον οδηγό αυτό ώστε χωρίς ιδιαίτερη αναζήτηση να προσαρμόσει το ΚΠΣ με τις απαιτήσεις του ΓΚΠΔ.

Το κάθε σημείο του πίνακα αναλύεται στη συνέχεια με αρκετή λεπτομέρεια για καλύτερη κατανόηση. Όπως έχει αναφερθεί και στην εισαγωγή της εργασίας, το σημαντικό στο στάδιο αυτό είναι η εισήγηση που γίνεται προς τους κατασκευαστές ΚΠΣ να εφαρμόζουν, όλα τα σημεία που αναγράφονται στους πίνακες, ενσωματώνοντάς τα στο ΚΠΣ με τέτοιο τρόπο ώστε να δημιουργείται αυτόματη διαδικασία επεξεργασίας δεδομένων ή το ίδιο το ΚΠΣ να συμβουλεύει άμεσα τους ΕτΕ και τον ΥΕ.

Α/Α	Πεδία προδιαγραφών για ΚΠΣ	Στάδιο	Άρθρα ΓΚΠΔ
1	Προσδιορισμός δεδομένων - ροή δεδομένων («Data mapping»)	Σχεδιασμός, Υλοποίηση, Λειτουργία	Άρθρα 5, 6, 9, 13, 14, 16, 17, 18, 20, 25, 30, ΚΕΦΑΛΑΙΟ V (όλα τα άρθρα), 85, 88 (Αιτιολογικές σκέψεις 34, 35, 39, 57, 58, 59, 60, 61, 62, 65, 68, 75, 89)
2	Διαφάνεια	Υλοποίηση, Λειτουργία	Άρθρο 12 (Αιτιολογικές σκέψεις 39, 57, 58, 59, 60)
3	Συγκατάθεση	Σχεδιασμός, Υλοποίηση, Λειτουργία	Άρθρα 6,7,8 (Αιτιολογικές σκέψεις 32)
4	Αρχή του περιορισμού του σκοπού	Υλοποίηση, Λειτουργία	Άρθρο 5(1)β
5	Γνωστοποίηση και ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα	Υλοποίηση, Λειτουργία	Άρθρα 33, 34 (Αιτιολογική σκέψη 85)
6	Καθορισμός δικαιωμάτων πρόσβασης (permissions)	Σχεδιασμός, Υλοποίηση, Λειτουργία	(Αιτιολογική σκέψη 49, 64)
7	Ελαχιστοποίηση της επεξεργασίας των δεδομένων	Υλοποίηση, Λειτουργία	Άρθρο 5(1)γ
8	Λογοδοσία	Λειτουργία	Άρθρα 5, 24
9	Πρόσβαση εξ αποστάσεως	Υλοποίηση, Λειτουργία	(Αιτιολογικές σκέψεις 59, 63)
10	Δεδομένα τα οποία μεταφέρονται εκτός ΕΕ. Η πράξη αυτή γνωστοποιείται στη Εποπτική Αρχή(υπό προϋποθέσεις)	Υλοποίηση, Λειτουργία	Άρθρο 45(1)
11	Ψευδωνυμοποίηση	Υλοποίηση, Λειτουργία	Άρθρο 32 (Αιτιολογικές σκέψεις 28, 29)

12	Δημιουργία προφίλ	Λειτουργία	Άρθρο 22 (Αιτιολογικές σκέψεις 24, 70, 71, 72, 73, 75)
13	Προστασία των δεδομένων ήδη **από το σχεδιασμό** και **εξ ορισμού** (by design and by default)	Σχεδιασμός, Υλοποίηση, Λειτουργία	(Άρθρο 25) (Αιτιολογική σκέψη 78)
14	Ασφαλή μετάδοση δεδομένων και κρυπτογραφημένη αποθήκευση τους	Σχεδιασμός, Υλοποίηση, Λειτουργία	ΚΕΦΑΛΑΙΟ V (όλα τα άρθρα)
15	Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων, όποτε το επιθυμεί	Λειτουργία	Άρθρο 15
16	Ανάπτυξη διαλειτουργικών μορφότυπων που επιτρέπουν τη φορητότητα των δεδομένων	Υλοποίηση, Λειτουργία	Άρθρο 20 (Αιτιολογική σκέψη 68)
17	Περίοδος διατήρησης δεδομένων (Retention period)	Υλοποίηση, Λειτουργία	Άρθρα 5(1)ε, 23(2)στ, (Αιτιολογικές σκέψεις 39, 65)
18	Αναγνώριση φυσικών προσώπων μέσω επιγραμμικών αναγνωριστικών στοιχείων ταυτότητας (π.χ. Διεύθυνση δικτύου IP, προφίλ κ.α.)	Υλοποίηση, Λειτουργία	Αιτιολογικές σκέψεις 30, 70, 71
19	Πρόνοια χρήσης του ΚΠΣ από παιδιά	Λειτουργία	(Αιτιολογική σκέψη 38)
20	Αρχείο δραστηριοτήτων	Λειτουργία	(Άρθρο 30) (Αιτιολογικές σκέψεις 13, 82)
21	Απευθείας επικοινωνία των ΥπΔε με τον ΥΠΔ	Υλοποίηση, Λειτουργία	Άρθρο 38(4)
22	Μέτρα ασφαλείας στον εξυπηρετητή (server)	Σχεδιασμός, Υλοποίηση, Λειτουργία	(Αιτιολογικές σκέψεις 49, 64, 78)

Πίνακας 1. Μοντελοποίηση των απαιτήσεων του ΓΚΠΔ για τα ΚΠΣ

Ακολούθως παρατίθεται ο «Πίνακας 2» ο οποίος περιλαμβάνει σημεία που έχουν καταγραφεί από άλλες πηγές, πέραν του ΓΚΠΔ, τα οποία συμπληρώνουν τη μοντελοποίηση των προδιαγραφών συμμόρφωσης για τα ΚΠΣ. Τα πιο κάτω σημεία θα μπορούσαν να είναι επιπρόσθετα σημεία στις αιτιολογικές σκέψεις του ΓΚΠΔ. Μερικά από αυτά μεταφέρουν την εμπειρία επαγγελματιών ΥΠΔ, πράγμα που έχει βοηθήσει στην εξαγωγή χρήσιμων συμπερασμάτων.

Α/Α	Πεδία προδιαγραφών για ΚΠΣ	Στάδιο	Άλλες πηγές
1	Ανάθεση εργασίας από Κατασκευαστή/φορέα σε Τρίτο ως ο ΕτΕ	Υλοποίηση	WP202 [16]
2	Μείωση του διαμοιρασμού των προσωπικών δεδομένων	Υλοποίηση, Λειτουργία	WP202 [16] (σελ. 5)
3	Έλεγχος και διαχείριση των «αρχείων κίνησης και δραστηριότητας των διαχειριστών» του εξυπηρετητή («Log files»)	Υλοποίηση, Λειτουργία	Συνέντευξη Παπαδόπουλου και Ιωάννου, ερώτημα 4
4	Συνεχής ενημέρωση και εκπαίδευση των υπαλλήλων του οργανισμού που χειρίζονται το σύστημα (ΕτΕ)	Λειτουργία	Συνέντευξη Παπαδόπουλου και Ιωάννου, ερώτημα 4
5	Καταγραφή των διαδικασιών σε εύκολα κατανοητά εγχειρίδια, διαθέσιμα σε όλους τους χρήστες	Λειτουργία	Συνέντευξη Παπαδόπουλου και Ιωάννου, ερώτημα 6(i)
6	Ευθύνη του κατασκευαστή (ΕτΕ) η διασφάλιση της συμμόρφωσης με όλες τις απαιτήσεις που ορίζονται στον ΓΚΠΔ	Υλοποίηση	Συνέντευξη Παπαδόπουλου και Ιωάννου, ερώτημα 7
7	Μη χρησιμοποίηση του Διαδικτύου κατά τη διάρκεια της υλοποίησης (όπου είναι εφικτό)	Υλοποίηση	Webinar [17]
8	Μέθοδος Κρυπτογράφησης «salt»	Υλοποίηση	Network Security [9]
9	Λίστα ελέγχου συμμόρφωσης	Υλοποίηση, Λειτουργία	

Πίνακας 2. Μοντελοποίηση απαιτήσεων για προστασία δεδομένων πέραν του ΓΚΠΔ

3.1.2. Ανάλυση προδιαγραφών

Οι τεχνικές προδιαγραφές υλοποίησης του έργου θα πρέπει να είναι ξεκάθαρες και όσο περισσότερο αναλυτικές γίνεται ώστε ο κατασκευαστής να μπορεί εύκολα να τις ακολουθήσει και να βασιστεί σε αυτές και να είναι σίγουρος ότι μπορεί να επιτύχει πλήρη συμμόρφωση με όλες τις απαιτήσεις του ΓΚΠΔ. Ακολουθεί ανάλυση όλων των σημείων που αναφέρθηκαν στον Πίνακα 1 και Πίνακα 2, πιο πάνω.

Ανάλυση σημείων Πίνακα 1

1. Προσδιορισμός δεδομένων - ροή δεδομένων («Data mapping»)

   Κανένα Πληροφοριακό Σύστημα (ΠΣ) δε μπορεί να λειτουργήσει χωρίς την ύπαρξη δεδομένων. Τα δεδομένα είναι αυτό το στοιχείο του συστήματος για

τα οποία υπάρχει η επιθυμία να διασφαλιστεί η ακεραιότητά τους έναντι όλων των κινδύνων που έχουν αναφερθεί, σε πολλά σημεία της παρούσας εργασίας. Έχουν ήδη προσδιοριστεί οι τύποι δεδομένων στο σημείο 2.4.1, με τους οποίους μπορούν οι κατασκευαστές ΚΠΣ να εργαστούν στο παρόν σημείο του Πίνακα 1 και με βάσει αυτούς τους τύπους να συλλεχθούν μόνο τα απαραίτητα δεδομένα εκείνα που θα κάνουν το ΚΠΣ λειτουργικό και ευέλικτο κατά τη επεξεργασία τους. Ο κάθε ΥΕ ή ΕτΕ, που θα εργαστεί για τον προσδιορισμό των δεδομένων, συστήνεται όπως δημιουργήσει πίνακα καταγραφής όλων των δεδομένων και να τα διαχωρίσει σε κάθε τύπο ξεχωριστά για καλύτερο σχεδιασμό και υλοποίηση του έργου.

2. <u>Διαφάνεια</u>

Οι κατασκευαστές ΚΠΣ θα ήταν καλό[35] να ενσωματώσουν στα συστήματα αυτόματες λειτουργίες διαφάνειας ώστε να παρέχονται αναλυτικές πληροφορίες στα ΥπΔε σχετικά με τον τρόπο που οι ΥΕ και ΕτΕ επεξεργάζονται τα προσωπικά δεδομένα των χρηστών. Η ενημέρωση των ΥπΔε για την επεξεργασία των δεδομένων του, θα πρέπει να είναι συνοπτική, διαφανής, κατανοητή και σε εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη σε παιδιά (Άρθρο 12(1)). Είναι γεγονός ότι, αυτές είναι καινούριες λειτουργίες που θα πρέπει να ενσωματωθούν στα Κοινωνικά Πληροφοριακά Συστήματα και θα χρειαστεί μεγαλύτερη προσπάθεια αλλά και επιπλέον κόστος για τους οργανισμούς/επιχειρήσεις που θα θελήσουν να τις υλοποιήσουν ως αυτόματες λειτουργίες των συστημάτων αυτών.

Οι πληροφορίες μπορούν να παρέχονται σε συνδυασμό με τυποποιημένα εικονίδια, προκειμένου να δίδεται με ευδιάκριτο τρόπο μια ουσιαστική επισκόπηση της προβλεπόμενης επεξεργασίας (Άρθρο 12(7)).

«*Ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων πληροφορίες για την ενέργεια που πραγματοποιείται κατόπιν αιτήματος δυνάμει των άρθρων 15 έως 22* ***χωρίς καθυστέρηση και σε κάθε περίπτωση εντός μηνός από την παραλαβή του αιτήματος****. Η εν λόγω*

[35] Είναι επιλογή του φορέα αν θέλει να δίνει με αυτόματο τρόπο ή χειροκίνητα αυτές τις λειτουργίες.

προθεσμία μπορεί να παραταθεί κατά δύο ακόμη μήνες, εφόσον απαιτείται, λαμβανομένων υπόψη της πολυπλοκότητας του αιτήματος και του αριθμού των αιτημάτων» (Άρθρο 12(3)).

3. Συγκατάθεση

Η έλλειψη διαφάνειας συνδέεται στενά με την έλλειψη ελεύθερης και ενημερωμένης συναίνεσης (συγκατάθεσης). «*Η συγκατάθεση θα πρέπει να παρέχεται με σαφή θετική ενέργεια η οποία να συνιστά ελεύθερη, συγκεκριμένη, ρητή και εν πλήρη επίγνωση της συμφωνίας του υποκειμένου των δεδομένων υπέρ της επεξεργασίας των δεδομένων που το αφορούν*». «*Η σιωπή, τα προ-συμπληρωμένα τετραγωνίδια ή η αδράνεια δεν θα πρέπει να εκλαμβάνονται ως συγκατάθεση*». Μέχρι σήμερα παρατηρείται, η «συγκατάθεση» να περιορίζεται συχνά σε ένα τετραγωνίδιο που υποδείκνυε ότι ο τελικός χρήστης αποδέχεται τους όρους και τις προϋποθέσεις. Ο χρήστης δεν είχε το δικαίωμα της επιλογής «να μη συναινέσει» με τους όρους χρήσης. Από τη στιγμή που αρνείτο να συναινέσει, σταματούσε εκεί η χρήση του συστήματος. Σύμφωνα με μια μελέτη της GSMA από το Σεπτέμβριο του 2011, το 92% των χρηστών των εφαρμογών σε κινητά επιθυμούσαν να έχουν μια ευρύτερη επιλογή για την τελική τους συναίνεση και επίσης να έχουν την επιλογή να αρνηθούν. «*Εάν η συγκατάθεση του υποκειμένου των δεδομένων πρόκειται να δοθεί κατόπιν αιτήματος με ηλεκτρονικά μέσα, το αίτημα πρέπει να είναι σαφές, περιεκτικό και* ***να μη διαταράσσει αδικαιολόγητα τη χρήση της υπηρεσίας για την οποία παρέχεται***» (Αιτιολογική σκέψη 32).

Η απαίτηση συγκατάθεσης του άρθρου 5 παράγραφος 3 ισχύει για οποιεσδήποτε πληροφορίες, ανεξάρτητα από τη φύση των δεδομένων που αποθηκεύονται ή έχουν πρόσβαση σε αυτά.

«*Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή*» (Άρθρο 7(3)). Στις περιπτώσεις που είχε δοθεί συγκατάθεση από το ΥπΔε για δημοσιοποίηση δεδομένων (π.χ. φωτογραφίες, βίντεο ή άλλα δεδομένα που ταυτοποιούν το ΥπΔε) και αυτά έχουν δημοσιοποιηθεί και το ΥπΔε ανακαλέσει τη συγκατάθεσή του, η ανάκληση

αυτή δεν εφαρμόζεται στα ήδη δημοσιοποιημένα στοιχεία αλλά σε οτιδήποτε αφορούσε επεξεργασία που θα γινόταν από τη μέρα της ανάκλησης και μετά.

4. <u>Αρχή του περιορισμού του σκοπού</u>

(Άρθρο 5(1β))

«*Τα δεδομένα προσωπικού χαρακτήρα, συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς*».

(Αιτιολογική σκέψη 29)

«*Κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σύννομη και δίκαιη. Θα πρέπει να είναι σαφές για τα φυσικά πρόσωπα ότι δεδομένα προσωπικού χαρακτήρα που τα αφορούν συλλέγονται, χρησιμοποιούνται, λαμβάνονται υπόψη ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία, καθώς και σε ποιο βαθμό τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται ή θα υποβληθούν σε επεξεργασία*».

Η παραβίαση (λόγω άγνοιας ή πρόθεσης) της αρχής του περιορισμού του σκοπού, η οποία επιβάλλει τη συλλογή και επεξεργασία προσωπικών δεδομένων μόνο για συγκεκριμένους και νόμιμους σκοπούς, πρέπει να διασφαλίζεται όπως αναφέρεται ρητά στα πιο πάνω σημεία του Κανονισμού (Άρθρο 5(1β)) και (Αιτιολογική σκέψη 29). Τα προσωπικά δεδομένα που συλλέγονται από εφαρμογές μπορούν να διανεμηθούν ευρέως σε τρίτους για αόριστους σκοπούς ή με στόχο την κερδοφορία, όπως η «έρευνα αγοράς» και η διαφήμιση. Η ίδια ανησυχητική παραβίαση φαίνεται να συμβαίνει και για την αρχή της ελαχιστοποίησης των δεδομένων που αναφέρεται πιο κάτω. Πρόσφατες έρευνες έδειξαν ότι πολλές εφαρμογές συλλέγουν άφθονα δεδομένα από «έξυπνα τηλέφωνα» (smartphones), χωρίς καμία ουσιαστική σχέση με την εμφανή λειτουργεία της εφαρμογής. Θα πρέπει να διασφαλιστεί πλέον ότι αυτό δεν πρέπει να γίνεται μέσα από τα ΚΠΣ που διαχειρίζεται ο οποιοσδήποτε οργανισμός/επιχείρηση.

5. <u>Γνωστοποίηση και ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα</u>

Ο κατασκευαστής ενθαρρύνεται να αυτοματοποιεί τη διαδικασία ενημέρωσης σε περίπτωση διαρροής δεδομένων και ταυτόχρονα με την αυτοματοποίηση δημιουργίας του αρχείου δραστηριοτήτων (βλ. σημείο 21 πιο κάτω) να είναι σε θέση, εντός χρονικού πλαισίου 72 ωρών, να ενημερώνει έγκαιρα την Εποπτική Αρχή για την απώλεια προσωπικών δεδομένων. Ο ΥΕ είναι υποχρεωμένος να ενημερώνει τόσο την Εποπτική Αρχή όσο και το επηρεαζόμενο ΥπΔε (εκτός σε εξαιρετικές περιπτώσεις δεν χρειάζεται να ενημερώνει το ΥπΔε) για την ολότητα της απώλειας των δεδομένων του τελευταίου.

Στην περίπτωση πολύ μεγάλου αριθμού χαμένων λογαριασμών χρηστών το σύστημα (με ενέργειες του ΥΕ) μπορεί να ενημερώνει τους επηρεαζόμενους χρήστες, ηλεκτρονικά.

Επιπρόσθετα ο κατασκευαστής μπορεί να ανατρέξει στα άρθρα 33 και 34 τα οποία περιγράφουν με λεπτομέρεια όλες τις ενέργειες που πρέπει να τηρήσει ο ΥΕ και ΕτΕ αμέσως μετά την ενδεχόμενη απώλεια προσωπικών δεδομένων. Όπως ήδη έχει αναφερθεί, μέρος αυτών συστήνεται όπως γίνονται αυτόματα και ηλεκτρονικά μέσω του συστήματος.

6. <u>Καθορισμός δικαιωμάτων πρόσβασης (permissions)</u>

Από τα πρώτα και πιο σημαντικά σημεία που θα πρέπει να διασφαλιστεί ότι το ΚΠΣ διατηρεί σε πολύ ψηλά επίπεδα ασφάλειας είναι η υποχρεωτική χρήση κωδικών πρόσβασης αλλά και δικαιώματα/περιορισμούς χρήσης στις λειτουργίες του συστήματος τα οποία είναι κρίσιμα σημεία που πρέπει να απαιτηθεί να υλοποιηθούν από τον κατασκευαστή. Σε περίπτωση απώλειας δεδομένων, αν αυτό το σημείο δεν εφαρμόστηκε σωστά, φέρει ακεραία την ευθύνη ο ΥΕ που δεν είχε απαιτήσει από τον κατασκευαστή να το υλοποιήσει κατάλληλα σύμφωνα με την κρισιμότητα που κουβαλά η απαίτηση αυτή.

Ο καθορισμός δικαιωμάτων πρόσβασης μπορεί να γίνεται αναλόγως του συστήματος, σε διάφορα επίπεδα δικαιωμάτων π.χ. δικαιώματα διαχειριστή και δικαιώματα απλών χρηστών. Δηλαδή, στον ΕτΕ δίνονται δικαιώματα που περιορίζονται σε τέτοιο σημείο ώστε να μπορεί να κάνει την επεξεργασία των

δεδομένων που του ανατίθεται, ενώ τα δικαιώματα και περιορισμοί πρόσβασης του απλού χρήστη περιορίζονται στα πιο βασικά που επιτρέπει το σύστημα. Οι χρήστες μπορεί να πετυχαίνουν ευρύτερη πρόσβαση αν το ΚΠΣ προσφέρει περισσότερες από μια κατηγορίες χρηστών, δηλ. δωρεάν χρήστες, εγγεγραμμένοι χρήστες με χαμηλού κόστους συνδρομή και άλλους με ψηλότερο κόστος συνδρομής.

7. <u>Ελαχιστοποίηση της επεξεργασίας των δεδομένων</u>

Άρθρο 5(1γ)

«*Τα δεδομένα προσωπικού χαρακτήρα είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία*».

Είναι ευθύνη του ΥΕ να δώσει τις κατάλληλες οδηγίες στον κατασκευαστή για τον διαχωρισμό των δεδομένων, ώστε κατά την υλοποίηση του έργου να δημιουργηθούν οι απαραίτητες λειτουργίες στο σύστημα ώστε να μπορεί εύκολα να προσδιορίζεται και να επεξεργάζεται ο ελάχιστος δυνατός όγκος προσωπικών δεδομένων των ΥπΔε.

Η ξεχωριστή ομαδοποίηση των δεδομένων εντός του ΚΠΣ και η διατήρηση των συμπληρωματικών δεδομένων ξεχωριστά (Αιτιολογική σκέψη 29), είναι ένα αποτελεσματικό μέτρο ώστε οι ΕτΕ να επεξεργάζονται μόνο τα δεδομένα που πρέπει και σύμφωνα με τα δικαιώματα που έχει ο καθένας (αναλόγως του ρόλου του) εντός του συστήματος. Με τον τρόπο αυτό θα μπορεί να διασφαλιστεί η προστασία των δεδομένων των ΥπΔε, αφού το σύστημα, θα δίνει τη δυνατότητα περιορισμού της πρόσβασης σε μη εξουσιοδοτημένα άτομα έστω και αν αυτά καταφέρουν να έχουν «παράνομη» πρόσβαση στο σύστημα. Συνεπώς, ο στόχος του περιορισμού του ρίσκου της απώλειας/διαρροής δεδομένων επιτυγχάνεται με την ελαχιστοποίηση των δεδομένων (αλλά πάντα με τον συνδυασμό και άλλων τεχνικών όπως είναι η ψευδωνυμοποίηση και η κρυπτογράφηση), αφού αν υπάρξει απώλεια δεδομένων θα πρέπει να διασφαλιστεί ότι ο μη εξουσιοδοτημένος κάτοχος των δεδομένων αυτών δεν θα έχει τη δυνατότητα να τα επεξεργαστεί.

8. <u>Λογοδοσία:</u>

Υποχρέωση του ΥΕ να αναλαμβάνει την ευθύνη για τον τρόπο με τον οποίο διαχειρίζεται τα δεδομένα και για τα μέτρα ασφαλείας που πρέπει να πάρει ώστε να συμμορφώνεται με τις αρχές προστασίας των δεδομένων.

Το σύστημα, μέσω διάδρασης χρήστη-υπολογιστή, θα πρέπει να είναι ικανό να ενημερώνει ορθά τα ΥπΔε για τα δικαιώματά τους (με ευθύνη του ΥΕ). Στην παράγραφο 2.2.1(IV), της παρούσας εργασίας, έχουν αναφερθεί οι υποχρεωτικές πρόνοιες του ΓΚΠΔ που θα πρέπει να τηρούνται από το ίδιο το σύστημα, με άμεσα υπεύθυνο τον ΥΕ.

9. <u>Πρόσβαση εξ αποστάσεως</u>

Παραχώρηση του δικαιώματος πρόσβασης στο ΥπΔε, προκειμένου να έχει επίγνωση και να επαληθεύει τη νομιμότητα της επεξεργασίας.

Η πρόσβαση εξ αποστάσεως είναι μια λειτουργία που βοηθά στη γρήγορη διεκπεραίωση πολλών διαδικασιών που αφορούν τις υποχρεώσεις του ΥΕ έναντι των ΥπΔε. Η απρόσκοπτη και συνεχής πρόσβαση του χρήστη στο ΚΠΣ δίνει την ευκαιρία στο ΥπΔε να ενημερώνεται όποτε επιθυμεί και να επεξεργάζεται τα δεδομένα από όποιο σημείο του Πλανήτη κι αν βρίσκεται. Επίσης όλες αυτές οι διαδικασίες θα μπορούν να γίνονται οποιαδήποτε ώρα και μέρα θελήσει το ΥπΔε και δεν θα εξαρτάται από τους περιορισμούς του ωραρίου εργασίας του ΥΕ. Οι αιτιολογικές σκέψεις 59 και 63 (βλ. πιο κάτω) ενθαρρύνουν τους κατασκευαστές να δημιουργούν συστήματα για ηλεκτρονική επικοινωνία του ΥΕ και του ΥπΔε, πάντοτε σε ένα ασφαλές ηλεκτρονικό περιβάλλον.

(Αιτιολογική σκέψη 59)

«…*Ο υπεύθυνος επεξεργασίας θα πρέπει επίσης να παρέχει τα μέσα για ηλεκτρονική υποβολή των αιτημάτων, ιδίως όταν δεδομένα προσωπικού χαρακτήρα υφίστανται* ***επεξεργασία με ηλεκτρονικά μέσα***.»

(Αιτιολογική σκέψη 63)

«…***Ο υπεύθυνος επεξεργασίας θα πρέπει να δύναται να παρέχει πρόσβαση εξ αποστάσεως σε ασφαλές σύστημα*** *μέσω του οποίου το*

υποκείμενο των δεδομένων αποκτά άμεση πρόσβαση στα δεδομένα που το αφορούν. Το δικαίωμα αυτό δεν θα πρέπει να επηρεάζει αρνητικά τα δικαιώματα ή τις ελευθερίες άλλων, όπως το επαγγελματικό απόρρητο ή το δικαίωμα διανοητικής ιδιοκτησίας και, ειδικότερα, το δικαίωμα δημιουργού που προστατεύει το λογισμικό…»

10. <u>Δεδομένα τα οποία μεταφέρονται εκτός ΕΕ</u>

Η πράξη αυτή δεν επιβάλλει γνωστοποίηση στην Εποπτική Αρχή αν τηρούνται οι πρόνοιες και οδηγίες των άρθρων 45 και 46, του ΓΚΠΔ.

Αυτόματα και χωρίς επίπονες και χειροκίνητες διαδικασίες από τον ΥΕ, το ΚΠΣ θα πρέπει να «γνωρίζει», να καταγράφει καθώς και να ενημερώνει τον ΥΕ, μέσω της κατάλληλης υλοποίησης από τον κατασκευαστή, πότε και πού, οποιαδήποτε προσωπικά δεδομένα διαβιβάζονται σε Τρίτη χώρα. Με τη σημερινή εξέλιξη της τεχνολογίας και με απλό κώδικα δεν είναι δύσκολο να ενσωματωθεί ένας τέτοιος έλεγχος εντός οποιουδήποτε ΚΠΣ, αφού όλοι πλέον κατέχουν τις συντεταγμένες του κάθε σημείου πάνω στη Γη και σε συνδυασμό με την ενημέρωση που θα παίρνει αυτόματα (ηλεκτρονικά) από την Επιτροπή (Ευρωπαϊκή Επιτροπή για τον ΓΚΠΔ – όπως ονομάζεται και στα έγγραφο του Κανονισμού) θα μπορεί το ΚΠΣ να αποφασίζει αν χρειάζεται ειδική άδεια από την Εποπτική Αρχή ή αν θα υπάρχει ευχέρεια να προχωρά η μεταβίβαση δεδομένων χωρίς επιπρόσθετες συμφωνίες με την Τρίτη χώρα, η οποία ζητεί να μεταβιβαστούν προσωπικά δεδομένα.

11. <u>Ψευδωνυμοποίηση</u>

(Αιτιολογική σκέψη 28)

«*Η χρήση της ψευδωνυμοποίησης στα δεδομένα προσωπικού χαρακτήρα μπορεί να μειώσει τους κινδύνους για τα υποκείμενα των δεδομένων και να διευκολύνει τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία να τηρήσουν τις οικείες υποχρεώσεις περί προστασίας των δεδομένων.*»

(Αιτιολογική σκέψη 29)

«*Για να δημιουργηθούν κίνητρα για την ψευδωνυμοποίηση κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, θα πρέπει να είναι δυνατή η λήψη μέτρων ψευδωνυμοποίησης*».

Όπως αναφέρεται και στις αιτιολογικές σκέψεις 28 και 29 αλλά και στο άρθρο 32(1)α, είναι υποχρεωτική η χρήση ψευδωνυμοποίησης. Άρα είναι υποχρέωση του ΥΕ (φορέας) να μεριμνήσει για την εφαρμογή της ψευδωνυμοποίησης στα ΚΠΣ, έτσι ο κατασκευαστής, από την αρχή, θα πρέπει να παίρνει ρητές οδηγίες για την απαίτηση αυτή και να την υλοποιεί χωρίς επιπρόσθετες διευκρινήσεις.

Όπως έχει ήδη αναφερθεί και στην παράγραφο 3.1.2 σημείο 7 (ελαχιστοποίηση της επεξεργασίας των δεδομένων), η ψευδωνυμοποίησης εφαρμόζεται με τέτοιο τρόπο ώστε να βοηθά στην απαίτηση της ελαχιστοποίησης των δεδομένων καθώς και στη διασφάλιση της απόκρυψης της ταυτότητας του ΥπΔε ακόμα κι αν τα δεδομένα υποστούν απώλεια. Η ψευδωνυμοποίηση δεν υλοποιείται από μόνη της αλλά πάντα σε συνδυασμό με άλλες τεχνικές («*Η ρητή εισαγωγή της «ψευδωνυμοποίησης» του παρόντος κανονισμού δεν προορίζεται να αποκλείσει κάθε άλλο μέτρο προστασίας των δεδομένων*»). (Αιτιολογική σκέψη 28)

12. <u>Δημιουργία προφίλ</u>

(Άρθρο 4 παράγραφος 4)

«Ο*ποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου*».

Για τη δημιουργία προφίλ στον ΓΚΠΔ θα πρέπει να συνυπάρχουν οι τρεις πιο κάτω προϋποθέσεις:

- αυτοματοποιημένη μορφή επεξεργασίας

- διεξάγεται σε δεδομένα προσωπικού χαρακτήρα
- ο στόχος είναι η παρατήρηση των προσωπικών χαρακτηριστικών του ΥπΔε.

Επομένως, η ταξινόμηση των ατόμων με βάση χαρακτηριστικά όπως το φύλο, το ύψος και η ηλικία τους θα μπορούσε να οδηγήσει σε δημιουργία προφίλ.
Τα τρία διακριτά στάδια του προφίλ:

- συλλογή δεδομένων
- αυτοματοποιημένη ανάλυση για τον προσδιορισμό των συσχετισμών (ενός ατόμου με άλλα άτομα ή καταστάσεις)
- εφαρμογή της συσχέτισης με ένα άτομο για τον προσδιορισμό των χαρακτηριστικών της παρούσας ή της μελλοντικής συμπεριφοράς

Στον ΓΚΠΔ αναφέρεται η «Αυτοματοποιημένη λήψη αποφάσεων» και αυτό ερμηνεύεται ως ικανότητα λήψης αποφάσεων με τεχνολογικά μέσα χωρίς ανθρώπινη συμμετοχή. Αυτό υλοποιείται και εφαρμόζεται από πολλά ΠΣ, αλλά με την εφαρμογή του ΓΚΠΔ, αυτό πλέον θα πρέπει να εφαρμόζεται μόνο με τη ρητή συναίνεση του ΥπΔε.

Το ΥπΔε θα **μπορεί να αντιτίθεται** στην οποιαδήποτε επεξεργασία των δεδομένων του **για σκοπούς εμπορικής προώθησης**.

Οι υπεύθυνοι επεξεργασίας που επιδιώκουν να βασίζονται στη συγκατάθεση ως βάση για τη διαμόρφωση του προφίλ πρέπει να αποδείξουν ότι τα υποκείμενα των δεδομένων κατανοούν ακριβώς σε τι συμφωνούν. Σε όλες τις περιπτώσεις, τα υποκείμενα των δεδομένων θα πρέπει να διαθέτουν αρκετές σχετικές πληροφορίες αναφορικά με την προβλεπόμενη χρήση και τις συνέπειες της επεξεργασίας, ώστε να διασφαλίζεται ότι η συναίνεση που παρέχουν αποτελεί μια ενημερωμένη επιλογή, όπως αναφέρεται στο Άρθρο 6 παράγραφος 1.

Όταν το υποκείμενο των δεδομένων δεν έχει άλλη επιλογή, όπως για παράδειγμα, σε περιπτώσεις όπου η συγκατάθεση για τη δημιουργία προφίλ είναι προϋπόθεση για την πρόσβαση στις υπηρεσίες του ΥΕ ή όταν υπάρχει

ανισορροπία ισχύος, όπως σε σχέση εργοδότη-εργαζομένου, η συγκατάθεση δεν αποτελεί κατάλληλη βάση για τη επεξεργασία.

13. Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (by design and by default)

Όπως έχει αναφερθεί και στο σημείο 2.2.1(IV) της παρούσας εργασίας, ο ΥΕ εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα (**από το σχεδιασμό**) καθώς και να διασφαλίζεται από τον ΥΕ ότι μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα υπόκεινται σε επεξεργασία (**Εξ ορισμού)** (άρθρο 25).

Αρκετές από τις τεχνικές που εφαρμόζονται για την ικανοποίηση της απαίτησης αυτής έχουν καταγραφεί σε αυτή την ενότητα και θεωρούνται πολύ σημαντικές. Αυτές είναι η ψευδωνυμοποίηση, η ελαχιστοποίηση των δεδομένων, η κρυπτογράφηση, η δημιουργία προφίλ, ο καθορισμός δικαιωμάτων πρόσβασης, η μείωση του βαθμού διαμοιρασμού [16] των προσωπικών δεδομένων.

Ένας σημαντικός αριθμός ΚΠΣ που χρησιμοποιούνται σήμερα εφαρμόζονται σε κινητές συσκευές, ειδικά σε έξυπνα κινητά τηλέφωνα. Οι κατασκευαστές, λαμβάνοντας υπόψη την ορθή εφαρμογή κατάλληλων τεχνικών μέτρων θα πρέπει να μεριμνήσουν ώστε οι εφαρμογές για κινητά να εκτελούνται σε συγκεκριμένες τοποθεσίες εντός της μνήμης των συσκευών (sandboxes[36]), προκειμένου να μειωθούν οι συνέπειες που είναι πιθανόν να προκύψουν μέσα από κακόβουλα προγράμματα/εφαρμογές. Σε στενή συνεργασία με τον κατασκευαστή λειτουργικών συστημάτων και/ή κατάστημα εφαρμογών (app store), οι κατασκευαστές εφαρμογών πρέπει να χρησιμοποιούν διαθέσιμους μηχανισμούς που επιτρέπουν στους χρήστες να βλέπουν ποια δεδομένα επεξεργάζονται από τις εφαρμογές και να έχουν τη δυνατότητα να ενεργοποιούν ή να απενεργοποιούν επιλεκτικά τα δικαιώματα. **Δεν πρέπει να επιτρέπεται η χρήση κρυφών λειτουργιών**.

14. Ασφαλή μετάδοση δεδομένων και κρυπτογραφημένη αποθήκευσή τους

[36] Το sandbox είναι ένας μηχανισμός ασφαλείας για τον διαχωρισμό των προγραμμάτων που εκτελούνται

Πιο κάτω αναφέρεται ενδεικτικά η κρυπτογράφηση «salt» η οποία είναι μια καλή μέθοδος κρυπτογράφησης. Συνεχώς εμφανίζονται διάφορες μέθοδοι όπου μπορούν να εφαρμόζονται συνδυασμοί αυτών για να επιτυγχάνεται ασφαλέστερη μετάδοση ή αποθήκευση δεδομένων. Σε περίπτωση απώλειας δεδομένων, ο ΥΕ, θα πρέπει να αποδείξει (στην Εποπτική Αρχή) ότι έχει εφαρμόσει τέτοιες τεχνικές κρυπτογράφησης ώστε τα δεδομένα να θεωρούνται ασφαλή έστω κι αν γίνουν προσβάσιμα από μη εξουσιοδοτημένα άτομα. Τα κρυπτογραφημένα δεδομένα βοηθούν σε περίπτωση διαρροής δεδομένων, ώστε να μην είναι δυνατή η επεξεργασία τους έξω από το ΚΠΣ από το οποίο είχαν διαρρεύσει.

15. <u>Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων, όποτε το επιθυμεί</u>

Σε συνάρτηση με την πρόσβαση εξ αποστάσεως το ΥπΔε θα πρέπει να μπορεί να έχει τη δυνατότητα πρόσβασης στα δεδομένα του, όποτε αυτός επιθυμεί, χωρίς περιορισμούς. Αυτό είναι ένα από τα βασικά δικαιώματα που του εκχωρεί ο Κανονισμός (διόρθωση, διαγραφή, δικαίωμα στη λήθη αλλά και επιπλέον δικαιώματα όπως αναφέρονται στην παράγραφο 2.2.1(ΙΙΙ), της παρούσας εργασίας και στο άρθρο 15 του ΓΚΠΔ).

Το σύστημα ενδείκνυται να έχει τη δυνατότητα να προβάλλει στο ΥπΔε τα δεδομένα που υποβάλλονται σε επεξεργασία όπως αναφέρεται ρητά και στην παράγραφο 3 του άρθρου 15 του ΓΚΠΔ.
«*Ο υπεύθυνος επεξεργασίας παρέχει αντίγραφο των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία*».

16. <u>Ανάπτυξη διαλειτουργικών μορφότυπων που επιτρέπουν τη φορητότητα των δεδομένων</u>

Οι υπεύθυνοι επεξεργασίας των δεδομένων (με τη βοήθεια του κατασκευαστή) θα πρέπει να ενθαρρύνονται να αναπτύσσουν διαλειτουργικούς μορφότυπους (αναγνώσιμοι από μηχανήματα/ηλ. υπολογιστές) που επιτρέπουν τη φορητότητα των δεδομένων (άρθρο 20, ΓΚΠΔ). Η αιτιολογική σκέψη 68 αναφέρει χρήσιμα στοιχεία για τις παραμέτρους αυτής της πτυχής του ΓΚΠΔ και μεταξύ άλλων αναφέρει τα ακόλουθα που αξίζει να ληφθούν υπόψη στο πλαίσιο συγγραφής αυτής της εργασίας: «*Για να ενισχυθεί*

περαιτέρω ο έλεγχος επί των δεδομένων του προσωπικού χαρακτήρα, όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα διενεργείται με αυτοματοποιημένα μέσα, το υποκείμενο των δεδομένων θα πρέπει να έχει επίσης τη δυνατότητα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν και που έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα διαλειτουργικό μορφότυπο, και να τα διαβιβάζει σε άλλον υπεύθυνο επεξεργασίας».

Είναι προς όφελος του φορέα να ζητήσει από τον κατασκευαστή ΚΠΣ να λάβει υπόψη κατά την υλοποίηση κάθε έργου την απαίτηση αυτή αφού θα αποφορτίζονται οι ΥΕ/ΕτΕ να εκτελούν χειροκίνητα τέτοιου είδους αιτήματα που είναι πιθανό να λάβουν από τα ΥπΔε.

17. <u>Περίοδος διατήρησης δεδομένων (Retention period)</u>

(Αιτιολογική σκέψη 39)

«… *το διάστημα αποθήκευσης των δεδομένων προσωπικού χαρακτήρα να περιορίζεται στο ελάχιστο δυνατό. Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υποβάλλονται σε επεξεργασία μόνο εάν ο σκοπός της επεξεργασίας δεν μπορεί να επιτευχθεί με άλλα μέσα. Για να διασφαλιστεί ότι τα δεδομένα προσωπικού χαρακτήρα δεν διατηρούνται περισσότερο από όσο είναι αναγκαίο, ο υπεύθυνος επεξεργασίας θα πρέπει να ορίζει προθεσμίες για τη διαγραφή τους ή για την περιοδική επανεξέτασή τους. Θα πρέπει να λαμβάνεται κάθε εύλογο μέτρο, ώστε να διασφαλίζεται ότι τα δεδομένα προσωπικού χαρακτήρα που δεν είναι ακριβή διορθώνονται ή διαγράφονται*…»

Είναι αναγκαίο να υπάρχει αυτόματος μηχανισμός του συστήματος ο οποίος να διαχειρίζεται την πληροφορία αυτή ώστε ο ΥΕ να μην παρεκκλίνει ποτέ της υποχρέωσης της συμμόρφωσης με τον όρο αυτό.

Το ΥπΔε έχει το δικαίωμα να γνωρίζει «*το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα*», όπως αναφέρει ρητά ο ΓΚΠΔ στην παράγραφο 1δ του άρθρου 15. Το δικαίωμα αυτό είναι συγκεκριμένο και πρέπει να τηρείται χωρίς να επιτρέπεται η οποιαδήποτε

παρέκκλιση (εκτός σε ειδικές περιπτώσεις, βλ. άρθρο 5 παράγραφος 1ε) και ο ΥΕ να ενημερώνει το ΥπΔε για τις ενέργειες που έχουν γίνει όταν η περίοδος αυτή έχει εξαντληθεί (αρχή της διαφάνειας) ή αν θα πρέπει να επεκταθεί για συγκεκριμένους λόγους (βλ. αιτιολογική σκέψη 65).

18. <u>Αναγνώριση φυσικών προσώπων μέσω επιγραμμικών αναγνωριστικών στοιχείων ταυτότητας (π.χ. Διεύθυνση δικτύου IP, προφίλ κ.α.)</u>

Στη συνέχεια ακολουθούν αυτούσια μερικά κομμάτια αιτιολογικών σκέψεων που αφορούν το θέμα αυτό. Ο τρόπος που παρουσιάζονται στον Κανονισμό είναι πολύ απλός και κατανοητός. Η πιθανή δημιουργία προφίλ μέσα από την επεξεργασία τέτοιων δεδομένων απαγορεύεται και πρέπει να προλαμβάνεται μέσω ενεργειών του κατασκευαστή των ΚΠΣ. Συστήνεται όπως οι κατασκευαστές ενσωματώσουν δικλίδες ασφαλείας τέτοιες ώστε, όπου είναι δυνατό, να μην αποκαλύπτονται σε τρίτους επιγραμμικά αναγνωριστικά στοιχεία ταυτότητας (όπως αναφέρονται στην αιτιολογική σκέψη 30), τα οποία στη συνέχεια μπορεί να υφίστανται επεξεργασία για διαφημιστικούς κυρίως σκοπούς.

(Αιτιολογική σκέψη 30)

«*Τα φυσικά πρόσωπα μπορεί να συνδέονται με επιγραμμικά αναγνωριστικά στοιχεία ταυτότητας, τα οποία παρέχονται από τις συσκευές, τις εφαρμογές, τα εργαλεία και τα πρωτόκολλά τους, όπως διευθύνσεις διαδικτυακού πρωτοκόλλου, αναγνωριστικά cookies ή άλλα αναγνωριστικά στοιχεία όπως ετικέτες αναγνώρισης μέσω ραδιοσυχνοτήτων. Αυτά μπορεί να αφήνουν ίχνη τα οποία, ιδίως όταν συνδυαστούν με μοναδικά αναγνωριστικά στοιχεία ταυτότητας και άλλες πληροφορίες που λαμβάνουν οι εξυπηρετητές, μπορούν να χρησιμοποιηθούν για να δημιουργηθεί το προφίλ των φυσικών προσώπων και να αναγνωριστεί η ταυτότητά τους.*»

(Αιτιολογική σκέψη 70)

«*Όταν δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία* ***για σκοπούς της απευθείας εμπορικής προώθησης****, το υποκείμενο των δεδομένων θα πρέπει να* ***έχει το δικαίωμα να αντιτεθεί στην εν λόγω***

***επεξεργασία**, συμπεριλαμβανομένης της κατάρτισης προφίλ στον βαθμό που αυτή συνδέεται με την εν λόγω απευθείας εμπορική προώθηση…*»

(Αιτιολογική σκέψη 71)

«*Το υποκείμενο των δεδομένων θα πρέπει να έχει το δικαίωμα να μην υπόκειται σε απόφαση, η οποία μπορεί να περιλαμβάνει κάποιο μέτρο, με την οποία αξιολογούνται **προσωπικές πτυχές που το αφορούν** … ιδίως την ανάλυση ή την πρόβλεψη πτυχών που αφορούν τις επιδόσεις στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή κινήσεις του υποκειμένου των δεδομένων, στον βαθμό που παράγει νομικά αποτελέσματα έναντι του προσώπου αυτού ή το επηρεάζει σημαντικά κατά ανάλογο τρόπο…*»

19. <u>Πρόνοια χρήσης των ΚΠΣ από παιδιά</u>

(Αιτιολογική σκέψη 38)

«***Τα παιδιά απαιτούν ειδική προστασία όσον αφορά τα δεδομένα τους προσωπικού χαρακτήρα**, καθώς τα παιδιά μπορεί να έχουν μικρότερη επίγνωση των σχετικών κινδύνων, συνεπειών και εγγυήσεων και των δικαιωμάτων τους σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα…*»

Η επεξεργασία των δεδομένων ενός παιδιού θα πρέπει να διέπεται από όλα όσα αναφέρονται σε αυτή την εργασία με στόχο την προστασία του παιδιού, πολύ πιο έντονα και ισχυρές δικλείδες ασφαλείας να τεθούν σε ισχύ. Θα πρέπει να αποφεύγεται ιδιαίτερα η δημιουργία προφίλ για ένα παιδί ή/και η προώθηση διαφημίσεων σε αυτό. Για όλες τις ενέργειες προς επεξεργασία των προσωπικών δεδομένων παιδιών θα πρέπει να συνοδεύεται πάντοτε με τη συγκατάθεση του γονέα ή κηδεμόνα. «*Η συγκατάθεση του γονέα ή κηδεμόνα δεν θα πρέπει να είναι απαραίτητη σε συνάρτηση με υπηρεσίες πρόληψης ή παροχής συμβουλών που προσφέρονται άμεσα σε ένα παιδί*» (Αιτιολογική σκέψη 38).

Όσον αφορά τις εφαρμογές που απευθύνονται σε παιδιά θα πρέπει να δίνεται **προσοχή στο όριο ηλικίας που ορίζει, για τα παιδιά ή τους ανηλίκους, η**

εθνική νομοθεσία. Επίσης θα πρέπει να επιλέγεται πιο περιοριστική προσέγγιση επεξεργασίας δεδομένων με πλήρη σεβασμό των αρχών της ελαχιστοποίησης των δεδομένων και του περιορισμού του σκοπού.

20. <u>Αρχείο δραστηριοτήτων</u>

Κάθε ΥΕ και/ή ΕτΕ και κατά περίπτωση οι εκπρόσωποί τους θα πρέπει να τηρούν αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνοι. Το εν λόγω αρχείο περιλαμβάνει πληροφορίες και στοιχεία που καταγράφονται με κατανοητή και ευανάγνωστη γλώσσα στο άρθρο 30 του ΓΚΠΔ.

Τα αρχεία αυτά ετοιμάζονται γραπτώς και είναι υποχρέωση του ΥΕ να διατηρεί και ηλεκτρονικό αντίγραφο, αν αυτό το πρωτότυπο είναι γραπτό κείμενο σε φυσική μορφή. Με ευθύνη του ΥΕ ή του ΕτΕ, το αρχείο αυτό τίθεται στη διάθεση της Εποπτική Αρχής, κατόπιν αιτήματος. Η απαίτηση αυτή, του ΓΚΠΔ, εφαρμόζεται για οργανισμούς που εργοδοτούν πέραν των 250 υπαλλήλων ή το όριο αυτό δεν ισχύει στην περίπτωση που η επεξεργασία αφορά δεδομένα υψηλού κινδύνου.

Η διαδικασία αυτή μπορεί να αυτοματοποιηθεί όπου το επιτρέπει το κόστος κατασκευής της. Σε διαφορετική περίπτωση θα πρέπει ο ΥΕ ή ΕτΕ να διατηρεί αρχείο δραστηριοτήτων καθ' όλη τη διάρκεια επεξεργασίας (μέχρι και την πλήρη διαγραφή) αφού **σε περίπτωση διαρροής δεδομένων το αρχείο αυτό θα αποτελέσει σημείο συμμόρφωσης με τον ΓΚΠΔ**.

21. <u>Απευθείας επικοινωνία των ΥπΔε με τον ΥΠΔ</u>

Άρθρο 38(4)

«*Τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν με τον υπεύθυνο προστασίας δεδομένων για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και με την άσκηση των δικαιωμάτων τους δυνάμει του παρόντος κανονισμού*».

Τα ΥπΔε έχουν κάθε δικαίωμα να έρχονται σε επικοινωνία με τον ΥΠΔ χωρίς τη μεσολάβηση οποιουδήποτε άλλου ατόμου (ΥΕ ή ΕτΕ) του φορέα. Ο

καταλληλότερος τρόπος, ώστε η διαδικασία αυτή να είναι εύκολη, διαφανής και χωρίς χρονοτριβή, είναι η υλοποίηση διαδραστικής επικοινωνίας μεταξύ των δύο μερών, η οποία μπορεί να παρέχεται μέσω του ΚΠΣ. Άρα δε χρειάζεται κάθε φορά το ΥπΔε να ανατρέχει σε άλλες πηγές πληροφόρησης για να μάθει τα στοιχεία του ΥΠΔ αλλά ο οργανισμός /επιχείρηση θα μεριμνά ώστε πάντα το σύστημα να είναι ενημερωμένο με τα επικαιροποιημένα στοιχεία του ΥΠΔ.

22. Μέτρα ασφαλείας στον εξυπηρετητή (server)

    Ένα πολύ σημαντικό σημείο για το οποίο οι κατασκευαστές θα πρέπει να είναι ιδιαίτερα προσεκτικοί είναι η εγκατάσταση και διαμόρφωση [18] του εξυπηρετητή που θα φιλοξενεί όλα τα δεδομένα του ΚΠΣ. Ο κατασκευαστής υποχρεούται να πάρει όλα τα ενδεδειγμένα μέτρα ώστε η ασφάλεια του εξυπηρετητή να μη γίνει ποτέ η αιτία για διαρροή δεδομένων. Επίσης θα πρέπει να διασφαλίζεται η ελεγχόμενη πρόσβαση με καθορισμένους ρόλους και δικαιώματα. Συστήνεται, ο κατασκευαστής να συμβουλεύονται το πρότυπο ISO27001, μέρος του οποίου αναλύεται εύστοχα στον οδηγό του Frank Simorjay, της εταιρείας Microsoft [18]. Ο οδηγός αυτός περιγράφει την εφαρμογή αποτελεσματικών μέτρων ασφαλείας σε συστήματα απομακρυσμένης πρόσβασης και αποθήκευσης δεδομένων (cloud), μέθοδοι οι οποίες συστήνονται γενικά για την ασφάλεια των πληροφοριακών συστημάτων.

Ανάλυση σημείων Πίνακα 2

1. Ανάθεση εργασίας από Κατασκευαστή/φορέα σε Τρίτο ως ο ΕτΕ

   Στο βαθμό που ένας κατασκευαστής ΚΠΣ έχει αναθέσει σε τρίτο, μέρος ή το σύνολο της επεξεργασίας δεδομένων και ο τρίτος αναλαμβάνει το ρόλο ενός ΕτΕ, τότε ο κατασκευαστής ενεργεί ως ΥΕ και πρέπει να συμμορφώνεται με όλες τις υποχρεώσεις που σχετίζονται με το διορισμό ενός ΕτΕ (π.χ υπογραφή σύμβασης μεταξύ ΥΕ και ΕτΕ). Αυτό ισχύει και στην περίπτωση που ο φορέας αποφασίσει να δώσει υπηρεσίες σε τρίτους, παράλληλα με τη λειτουργία ενός ΚΠΣ.

   Στην περίπτωση που ο φορέας προχωρεί σε συμφωνίες για εμπορικούς ή τεχνικούς σκοπούς με τρίτους, η ευθύνη κάθε μέρους θα πρέπει να καθορίζεται

κατά περίπτωση, λαμβάνοντας υπόψη τις ειδικές συνθήκες της επεξεργασίας, σύμφωνα πάντα με την ικανοποίηση όλων των επηρεαζόμενων πτυχών του ΓΚΠΔ.

2. Μείωση του διαμοιρασμού των προσωπικών δεδομένων

   Ένας υψηλός κίνδυνος για την προστασία των δεδομένων πηγάζει επίσης από τον βαθμό διαμοιρασμού μεταξύ των πολλών παραγόντων στο τοπίο ανάπτυξης εφαρμογών για ΚΠΣ. Επειδή ενδέχεται να υπάρχουν διαφορετικοί τύποι συμφωνιών - εμπορικών και τεχνικών - μεταξύ προγραμματιστών εφαρμογών και τρίτων (αναλυτές δεδομένων ή διαφημιστές), η ευθύνη κάθε μέρους θα πρέπει να καθορίζεται κατά περίπτωση, λαμβάνοντας υπόψη τις ειδικές συνθήκες της επεξεργασίας. [16]

   Ένας προγραμματιστής εφαρμογών μπορεί να χρησιμοποιεί βιβλιοθήκες τρίτων με λογισμικό που παρέχει κοινές λειτουργίες, όπως για παράδειγμα μια βιβλιοθήκη για μια κοινωνική πλατφόρμα παιχνιδιών. Ο προγραμματιστής της εφαρμογής πρέπει να διασφαλίσει ότι οι χρήστες γνωρίζουν οποιαδήποτε επεξεργασία δεδομένων πραγματοποιείται από τρίτους. Εάν συμβαίνει αυτό θα πρέπει η επεξεργασία των προσωπικών δεδομένων των χρηστών να συμμορφώνεται με τον ΓΚΠΔ και οποιαδήποτε επεξεργασία θα γίνεται δεδομένου ότι έχει δοθεί η συναίνεση του χρήστη. Επομένως, οι προγραμματιστές εφαρμογών θα πρέπει να εμποδίζουν τη χρήση λειτουργιών που αποκρύπτονται από το χρήστη και να τον ενημερώνουν για αυτές.

3. Έλεγχος και διαχείριση των «αρχείων κίνησης και δραστηριότητας των διαχειριστών» του εξυπηρετητή («Log files»)

   Στο σημείο 2.4.3, πιο πάνω, αναφέρεται επιγραμματικά η έννοια του όρου «Log files» αλλά και ο τρόπος χρήσης τους, διαφυλάσσοντας τα προσωπικά δεδομένα των διαχειριστών των ΚΠΣ. **Τα στοιχεία αυτά είναι ιδιαίτερα σημαντικά όταν υπάρχει ανάγκη για έλεγχο της παραβίασης δεδομένων σε δεκάδες ή/και εκατοντάδες εξυπηρετητές ταυτόχρονα και εντός χρονικού πλαισίου 72 ωρών**[37]. Η καταγραφή της κίνησης των διαχειριστών στους εξυπηρετητές φυλάσσεται σε ένα συγκεκριμένο σημείο του λειτουργικού, έτσι ώστε ο έλεγχος να γίνεται γρηγορότερα και

[37] Βλ. Άρθρο 33, παράγραφος 1 του ΓΚΠΔ

αποτελεσματικότερα. Οι κατασκευαστές θα πρέπει να γνωρίζουν αυτές τις τεχνικές σωστής χρήσης και διαχείρισης των «log files» ώστε να μπορούν να τα χρησιμοποιήσουν στην περίπτωση απώλειας δεδομένων, αφού ο χρόνος που έχουν οι ΥΕ για να ενεργήσουν για τη γνωστοποίηση των απολεσθέντων δεδομένων με συγκεκριμένα και ακριβή στοιχεία, δεν είναι πολύ μεγάλος.

4. <u>Συνεχής ενημέρωση και εκπαίδευση των υπαλλήλων του οργανισμού που χειρίζονται το σύστημα (ΕτΕ)</u>

   Είναι υποχρέωση των ΥΕ να μεριμνούν για την εκπαίδευση όλων των εμπλεκομένων μερών που επεξεργάζονται δεδομένα σε κάθε ΚΠΣ. Εκτός από τη γενική εκπαίδευση που είναι υποχρεωμένος ο οργανισμός να κάνει σε όλους τους υπαλλήλους ή όσους έρχονται σε επαφή με προσωπικά δεδομένα (ακόμα και στις καθαρίστριες[38]) το ΚΠΣ θα ήταν καλό να διαθέτει διαδικασία (κατά τακτά χρονικά διαστήματα) υποχρεωτικής εκπαίδευσης του προσωπικού που έχει οδηγίες για την επεξεργασία δεδομένων του συστήματος. Πχ. E-learning πλατφόρμα που να αξιολογεί το επίπεδο γνώσεων των εργαζομένων όσον αφορά την προστασία προσωπικών δεδομένων.

5. <u>Καταγραφή των διαδικασιών σε εύκολα κατανοητά εγχειρίδια, διαθέσιμα σε όλους τους χρήστες</u>

   Κατά τη συνέντευξη που διενεργήθηκε με τους κ.κ. Παπαδόπουλο και Ιωάννου, αναφέρθηκε ότι η ετοιμασία εγχειριδίων της χρήσης και λειτουργίας του ΚΠΣ βοηθά το χρήστη να μάθει τα δικαιώματα και υποχρεώσεις του. Κατά τη χρήση οποιασδήποτε διαδικασίας του συστήματος συστήνεται όπως το σύστημα διαθέτει επεξηγήσεις για όλες τις αντίστοιχες λειτουργίες ώστε να μπορεί να αποφασίζει ευκολότερα ο χρήστης αν θα πρέπει να προχωρήσει με αυτή ή να την απορρίψει (πχ, βοηθητικές λειτουργίες). Παράλληλα με τη χρήση του ΚΠΣ, εκτός από τις βοηθητικές οδηγίες χρήσης που θα εμφανίζονται αυτόματα εσωτερικά του συστήματος (τουλάχιστο την πρώτη φορά χρήσης), το σύστημα θα πρέπει να διαθέτει και εξωτερικό ολοκληρωμένο οδηγό με όλες τις λεπτομέρειες χρήσης του συστήματος.

[38] Οι καθαρίστριες μπορεί να έρθουν σε επαφή με δεδομένα που είναι εκτεθειμένα πάνω σε ένα γραφείο ή ακόμα και μέσα στον κάλαθο.

6. Ευθύνη του κατασκευαστή (ΕτΕ) η διασφάλιση της συμμόρφωσης με όλες τις απαιτήσεις που ορίζονται στον ΓΚΠΔ

   Ακόμα ένα πολύ σημαντικό στοιχείο που αναφέρθηκε στη συνέντευξη Παπαδόπουλου-Ιωάννου, το οποίο δε διαφαίνεται καθαρά μέσα από τα άρθρα του κειμένου του ΓΚΠΔ είναι ότι ο φορέας προσδιορίζει, από τη φάση του σχεδιασμού, πως ο κατασκευαστής φέρει πλήρως την ευθύνη της επίτευξη της συμμόρφωσης των διεργασιών που εκτελούνται μέσω των ΚΠΣ με τον ΓΚΠΔ, μέχρι τη στιγμή που αυτό παραδοθεί προς χρήση (και ίσως αργότερα σε ορισμένες περιπτώσεις).

   Ο κατασκευαστής είναι υποχρεωμένος να εφαρμόσει τις υποχρεωτικές διατάξεις του Κανονισμού και ό,τι άλλο του έχει υποδείξει ο φορέας.

7. Μη χρησιμοποίηση του Διαδικτύου κατά τη διάρκεια της υλοποίησης (όπου είναι εφικτό)

   Τεχνικές που εφαρμόζονται στην υλοποίηση συστημάτων με κρίσιμα δεδομένα απαιτούν τη μη χρησιμοποίηση του διαδικτύου μέχρι ο κατασκευαστής να κρίνει ότι το σύστημα είναι απολύτως έτοιμο να δοθεί online. Κατά τη διάρκεια της υλοποίησης, ένα ημιτελές ΚΠΣ συνήθως έχει ευάλωτα σημεία (τρύπες), όπου διάφορα εργαλεία «διάνοιξης» διαδρόμων (paths) μπορούν να δώσουν πληροφορίες σε χάκερς και με διάφορες άλλες τεχνικές να υποκλέψουν δεδομένα τα οποία εάν θεωρηθούν χρήσιμα θα μπορούσαν να τα χρησιμοποιήσουν για ίδιον όφελος με στόχο το οικονομικό κέρδος (π.χ. ο χάκερ Peace, βλ. παράγραφο 2.3.1).

8. Μέθοδος Κρυπτογράφησης «salt»

   Όπως έχει αναφερθεί παραπάνω, στο σημείο 2.3.1, εάν στα απολεσθέντα δεδομένα της εταιρείας LinkedIn (117 εκατομμύρια accounts) εφαρμοζόταν η κρυπτογράφηση «salt» (ενδεικτική μέθοδος κρυπτογράφησης) στους κωδικούς πρόσβασης των λογαριασμών, δε θα υπήρχε λόγος ανησυχίας διαρροής δεδομένων αφού θα κρινόταν ότι εφαρμόστηκαν τα ενδεδειγμένα τεχνικά μέτρα που θα καθιστούσαν μη αναγνώσιμα τα δεδομένα προσωπικού χαρακτήρα σε όσους δε θα διέθεταν άδεια εξουσιοδοτημένης πρόσβασης σε αυτά (βλ. άρθρο 34(3)α).

Η Google απαιτεί κατ' ελάχιστον κρυπτογράφηση κατακερματισμού SHA256 και συνιστά ιδιαίτερα τη χρήση κρυπτογράφησης «salt», με τουλάχιστον 8 χαρακτήρες[39]. Αυτό δείχνει ότι ο μεγαλύτερος κολοσσός τεχνολογίας του διαδικτύου χρησιμοποιεί τεχνικές πέραν των συνηθισμένων τεχνικών που χρησιμοποιούνταν μέχρι πρόσφατα, ώστε να διασφαλίζει την ακεραιότητα των κωδικών πρόσβασης στα συστήματά της αλλά και κατά τη μεταφορά δεδομένων να υπάρχει η μεγαλύτερη δυνατή ασφάλεια. Οι κατασκευαστές των ΚΠΣ θα πρέπει να εφαρμόζουν τέτοιες τεχνικές αλλά και να ενημερώνονται παράλληλα και για όλες τις νέες τεχνικές που αντικαθιστούν τις παλιές ώστε να επανέρχονται με ενημερώσεις λογισμικού.

9. Λίστα ελέγχου συμμόρφωσης

Με τους ανωτέρω πίνακες υπάρχει η πεποίθηση ότι έχουν συγκεντρωθεί όλα εκείνα τα στοιχεία που θα μπορούσαν να αποτελέσουν μια ενδεικτική **Λίστα ελέγχου** συμμόρφωσης[40] στην οποία θα μπορούσαν να βασιστούν οι κατασκευαστές ΚΠΣ για την επιτυχή επίτευξη της συμμόρφωσης των διεργασιών που εκτελούνται μέσω των ΚΠΣ με τον ΓΚΠΔ. Τα αποτελέσματα του ελέγχου μέσω της λίστας αυτής είναι δυναμικά και επιδέχονται συνεχείς προσαρμογές για διατήρηση της συμμόρφωσης με τον ΓΚΠΔ. Δηλαδή, καθ' όλη τη διάρκεια της λειτουργίας και ζωής του συστήματος, θα πρέπει να εφαρμόζεται η λίστα ελέγχου για να διαπιστώνεται συνεχής συμμόρφωση με τον ΓΚΠΔ. Τα αποτελέσματα αυτά μπορούν να αλλάζουν και να προσαρμόζονται με τα νέα δεδομένα που ίσως να προκύπτουν κατά τακτά χρονικά διαστήματα (π.χ. συγκατάθεση, ροή δεδομένων, διαφάνεια, ενημέρωση και δικαίωμα στην αλλαγή/διαγραφή δεδομένων του ΥπΔε, μετάδοση δεδομένων, ελαχιστοποίηση των δεδομένων, αρχείο δραστηριοτήτων κ.α.).

[39] https://support.google.com/analytics/answer/6366371?hl=el

[40] Υπάρχουν πολλές «λίστες ελέγχου» στο διαδίκτυο που αφορούν τη συμμόρφωση ενός οργανισμού/επιχείρηση με το ΓΚΠΔ, αλλά η λίστα αυτή είναι εξειδικευμένη και καλύπτει τα ΚΠΣ. Μια έτοιμη λίστα ελέγχου δεν καλύπτει ποτέ όλα τα ΚΠΣ ή ΠΣ γενικά, αλλά θα πρέπει να ετοιμάζεται από τον κατασκευαστή, διαφορετική κάθε φορά που αυτός υλοποιεί ένα ΚΠΣ. Ο όρος «λίστα ελέγχου» αναφέρεται και στην ιστοσελίδα της Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα της Κύπρου, http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/1957A162BCC48279C225824A0037F7AE?OpenDocument

Κεφάλαιο 4
Συνεντεύξεις

4.1. Τί είπαν οι επαγγελματίες στο χώρο της αγοράς και η Επίτροπος Δεδομένων Προσωπικού Χαρακτήρα της Κύπρου

Έχει πραγματοποιηθεί συνέντευξη με επαγγελματίες συμβούλους που εξειδικεύονται σε όλα τα είδη Πληροφοριακών Συστημάτων που χρησιμοποιούνται σε οργανισμούς/επιχειρήσεις και τη συμμόρφωσή των φορέων αυτών με τον ΓΚΠΔ. Επίσης στάλθηκε ερωτηματολόγιο σε εκπρόσωπο του γραφείου της «Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα» της Κύπρου. Ακολούθως αναλύονται οι απαντήσεις που πάρθηκαν και στις δύο περιπτώσεις και παρατίθενται οι παρατηρήσεις επί τούτων.

4.1.1. Συνέντευξη με επαγγελματίες συμβούλους που εξειδικεύονται στο θέμα της συμμόρφωσης των οργανισμών/επιχειρήσεων με τον ΓΚΠΔ

Ακολούθως γίνεται ανάλυση των απαντήσεων που πάρθηκαν κατά τη συνέντευξη. Όλες οι ερωτήσεις της συνέντευξης παρουσιάζονται στο Παράτημα Α.

Στόχος αυτής της συνάντησης ήταν η συλλογή πληροφοριών μέσα από την εξειδικευμένη εμπειρία επαγγελματιών στα ΚΠ (συμπερλαμβανομένων και των ΚΠΣ) ώστε να γίνει εξαγωγή καλύτερων συμπερασμάτων σχετικά με την ανταπόκριση των επιχειρήσεων για την υποχρεωτική εναρμόνιση με τον ΓΚΠΔ. Έγινε προσπάθεια καταγραφής του βαθμού αντίληψης από τους Ιδιοκτήτες/Διευθυντές για τις δικές τους υποχρεώσεις αλλά και τις ευθύνες τους έναντι όλων των προσώπων που συνεργάζεται ο οργανισμός/επιχείρησή τους και παράλληλα εκτελείται επεξεργασία προσωπικών δεδομένων για όλους αυτούς.

Ένας ΥΠΔ, που διορίζεται από τον ΥΕ μιας οντότητας θα πρέπει να συμμετέχει σε όλη τη διαδικασία της συμμόρφωσης με τον ΓΚΠΔ, από την απλή ενημέρωση μέχρι την τελική πιστοποίηση των ατόμων, προϊόντων και των συστημάτων διαχείρισης. Μερικά παραδείγματα διαδικασιών που ακολουθούν οι οργανισμοί/επιχειρήσεις είναι η «έκθεση ανάλυσης ελλείψεων» (GAP analysis), η «χαρτογράφηση της ροής δεδομένων και πληροφοριών» (Data Mapping), η εφαρμογή κυρίως του άρθρου 25 «Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού» (Data protection by design and by default), η εκπαίδευση όλων των χρηστών (υπαλλήλων του οργανισμού) πάνω σε ετήσια βάση και γενικά γίνεται προσπάθεια για πρόληψη και αντίδραση (proactive and forensic). Ένα σημείο που θεωρείται ιδιαίτερα σημαντικό το οποίο αναφέρθηκε στα σημεία της μοντελοποίησης (βλ. Πίνακας 2, σημείο 3) είναι η παρατήρηση και η διαφύλαξη της ακεραιότητας αλλά και του απορρήτου των Log files του λειτουργικού συστήματος που αναφέρεται στο κάθε ΚΠΣ. Μεταφέρονται αυτούσια τα λόγια του κ. Παπαδόπουλου: «*Κάτι που δεν κάνουν πολλοί αλλά εμείς το εφαρμόζουμε είναι το logfile management (centralized management όταν έχουμε πολλούς servers). Διαχείριση (επεξεργασία και διαφύλαξη ακεραιότητας) των logfiles. Τα αρχεία αυτά είναι πολύ σημαντικά για να παίρνουμε πληροφορίες για τις λειτουργίες ενός συστήματος έτσι μπορεί να αποκαλύψει πληροφορίες για τους χρήστες (κυρίως για τις ενέργειες του διαχειριστή), πράγμα που επιβάλλεται να διαφυλαχθεί στα πλαίσια του ΓΚΠΔ*».

Ο ρόλος του ΥΠΔ είναι πολύ σημαντικός και μετά το τέλος της διαδικασίας συμμόρφωσης αφού αυτή θα πρέπει να διατηρείται για πάντα. Έτσι και οι Παπαδόπουλος-Ιωάννου είπαν ότι γίνεται, εκ μέρους τους, συνεχής καθημερινή εμπλοκή σε όλο το φάσμα των ενεργειών της οντότητας (πχ. συμβουλή για κοινοποίηση δεδομένων σε τρίτο, συμμετοχή σε συνεδρίες του οργανισμού, συνεχείς συνεργασία με νομικούς συμβούλους). Επίσης παρέχουν συμβουλές για συντήρηση και συνεχή βελτίωση του συστήματος ελέγχου προσωπικών δεδομένων (αναβάθμιση hardware και software).

Αν και λέχθηκε ότι όλα τα άρθρα είναι σημαντικά και οι κατασκευαστές ΚΠΣ δεν πρέπει να αγνοούν καμία πρόνοια του ΓΚΠΔ και να τις διαχωρίζουν σε λιγότερο ή περισσότερο σημαντικές, εντούτοις, από τους δύο οικοδεσπότες, αναφέρθηκαν ως

πολύ κρίσιμα τα άρθρα που αφορούν την «*κρυπτογράφηση*», την «*ψευδωνυμοποίηση*», την «*Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού*», την «*εκπλήρωση όλων των αιτημάτων του υποκειμένου των δεδομένων*» (βλ. 2.2.1(ΙΙΙ), πιο πάνω), την «*αλλαγή ή απόσυρση της συγκατάθεσης των ΥπΔε*» και την «*καταγραφή όλων των διαδικασιών σε εύκολα κατανοητά εγχειρίδια, διαθέσιμα σε όλους τους χρήστες*». Όλα τα σημεία αυτά έχουν καταγραφεί και αναλυθεί στις προδιαγραφές για την κατασκευή των ΚΠΣ (βλ. παράγραφος 3.1.2, παρούσας εργασίας).

Ο κατασκευαστής ΚΠΣ (και οι συνεργάτες του, αν υπάρχουν) φέρει εξ ολοκλήρου την ευθύνη αφού θα πρέπει να μεριμνήσει για την εφαρμογή του ΓΚΠΔ, με τη λειτουργία του συστήματος. Θα πρέπει να καλύψει όλα τα βήματα εναρμόνισης πριν παραδώσει το προϊόν στον πελάτη. Επίσης ο κατασκευαστής/προμηθευτής [41] θα πρέπει να απαιτήσει να τηρηθούν όλες οι απαιτούμενες πρόνοιες του κανονισμού για το περιβάλλον που θα τοποθετηθεί και θα τεθεί σε λειτουργία το νέο σύστημα. Αυτό ισχύει και για όλα τα υφιστάμενα συστήματα για τα οποία ο οργανισμός θα πρέπει να μεριμνήσει για την εναρμόνισή τους με ή χωρίς την εμπλοκή του κατασκευαστή/προμηθευτή. Στην περίπτωση όμως που υπάρχουν ελλείψεις και αυτές αφορούν πρόνοιες που δεν ζητήθηκαν (π.χ. συγχρονισμός ΚΠΣ με διαδικασίες άλλων συστημάτων κ.α.), την ευθύνη φέρει ο Οργανισμός που όφειλε να τις ζητήσει και να πληρώσει το επιπλέον κόστος γι' αυτά. Επίσης αν ο οργανισμός, μετά τη λειτουργία του ΚΠΣ, δεν τηρεί τις διαδικασίες που ορίστηκαν από τον κατασκευαστή/προμηθευτή τότε ο τελευταίος δεν φέρει καμία ευθύνη. Δεν υπάρχει περίοδος χάριτος για κανένα λόγο, μετά την παράδοση του συστήματος προς χρήση.

Κατά τη διαδικασία εναρμόνισης κάθε Κοινωνικού Πληροφοριακού Συστήματος συναντώνται προβλήματα τα οποία εύκολα ή δύσκολα ξεπερνιούνται με την επιμονή κυρίως των συμβούλων. Μερικά όμως σημεία, που καλούνται οι ΥΠΔ να υλοποιήσουν για τη συμμόρφωση ενός οργανισμού με τον ΓΚΠΔ, τους προκαλούν μεγάλο βραχνά αφού σε κάποιες περιπτώσεις αναγκάζονται να διακόψουν τη διαδικασία εναρμόνισης. Αυτές οι λεγόμενες «τρύπες» που προκαλούν πρόβλημα είναι η «*συγκατάθεση*», «*το infrastructure που συνήθως δεν είναι εναρμονισμένο*», «*η*

[41] Αυτό αφορά προκατασκευασμένα συστήματα και υπάρχει μεσάζον (πωλητής) ο οποίος πρέπει να μεριμνά για την εναρμόνιση του ΚΠΣ με τον ΓΚΠΔ.

νοοτροπία των υπαλλήλων που δεν θέλουν να αλλάξουν τον τρόπο που δουλεύουν» και «*η άρνηση της Διεύθυνσης για πραγματική δέσμευση*».

Για να επιτευχθεί η εναρμόνιση των ΚΠΣ ενός οργανισμού με τον ΓΚΠΔ δεν απαιτείται η ύπαρξη άλλων προτύπων ασφαλείας (π.χ. ISO). Αν υπάρχουν όμως υφιστάμενα συστήματα διαχείρισης, όταν η διαδικασία εναρμόνισης ολοκληρωθεί, αυτά θα πρέπει να εναρμονίζονται μεταξύ τους και κατ' επέκταση με τον ΓΚΠΔ. Η εναρμόνιση όλων των προτύπων ασφαλείας μαζί και πρωτίστως με τον ΓΚΠΔ, διευκολύνει την αποδοτικότητα ενός οργανισμού και ενισχύει τη θέση του οργανισμού στην αγορά (μεγαλύτερη οικονομική αξία της επιχείρησης). Επίσης η συμμόρφωση με τον ΓΚΠΔ είναι πιο ομαλή αφού πολλές πρόνοιες του ΓΚΠΔ είναι ήδη εφαρμοσμένες.

Ακόμα ένα σημαντικό στοιχείο που εξήχθη από τη συνέντευξη είναι πως βρίσκεται σε διαδικασία δρομολόγησης, για γνωμοδότηση (consultation) από την ανεξάρτητη Ευρωπαϊκή Αρχή «European Data Protection Supervisor» (EDPS), η έκδοση πιστοποίησης συμβατότητας των Λογισμικών ΚΠΣ με τον ΓΚΠΔ, από εγκεκριμένους οργανισμούς. Όχι πολύ μακριά αλλά στο άμεσο μέλλον θα μπορεί ένας οργανισμός να ζητήσει πιστοποίηση με τον ΓΚΠΔ, αποκλειστικά και μόνο για ένα νέο λογισμικό του.

Με τις απαντήσεις των κ.κ. Παπαδόπουλου και Ιωάννου διαπιστώνεται πως η εναρμόνιση με τον ΓΚΠΔ δεν είναι καθόλου εύκολη υπόθεση. Λίγες είναι οι επιχειρήσεις και οργανισμοί που έχουν αντιληφθεί ότι η υποχρέωση της συμμόρφωσής τους έχει αρχίσει από τις 25 Μαΐου 2018 και είναι συνεχής. Πολλές ακόμα επιχειρήσεις και οργανισμοί δεν προχώρησαν με ουσιαστικό τρόπο στην ολοκλήρωση τις εναρμόνισης με τον ΓΚΠΔ, πράγμα που εγκυμονεί μεγάλο ρίσκο απώλειας δεδομένων αλλά και επιβολής μεγάλων προστίμων.

Καμία επιχείρηση και για κανένα λόγο (εκτός σε πολύ ειδικές περιπτώσεις οι οποίες αναφέρονται στην ανάλυση των προδιαγραφών του Κεφαλαίου 3) δεν μπορεί να παρεκκλίνει το ελάχιστο από τα άρθρα του Κανονισμού.

4.1.2. Παρατηρήσεις στο ερωτηματολόγιο που έχει σταλεί σε αντιπρόσωπο του γραφείου της «Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα» της Κύπρου

Στάλθηκε ερωτηματολόγιο, στο γραφείο της Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα, μέσω ηλεκτρονικού ταχυδρομείου και λήφθηκαν απαντήσεις σε όλα τα ερωτήματα, με το ίδιο μέσο επικοινωνίας.

Με το ερωτηματολόγιο αυτό τέθηκε ο στόχο να ληφθεί η εμπειρία της Εποπτική Αρχής για τους τελευταίους έντεκα μήνες, αφότου μπήκε σε εφαρμογή ο ΓΚΠΔ. Μέσω των απαντήσεων λήφθηκε μια καλή εικόνα για τις ενέργειες που κάνει κάθε φορά η Εποπτική Αρχή όταν έχει να κάνει έλεγχο σε πληροφοριακά συστήματα.

Φάνηκε ότι δεν διαχωρίζονται τα ΚΠΣ από τα ΠΣ πράγμα που καθιστά τον έλεγχο συμμόρφωσης λιγότερο αποτελεσματικό για τα ΚΠΣ. Όπως αναφέρθηκε και νωρίτερα στην παρούσα εργασία, ο χρήστης ενός ΚΠΣ εκφράζει άποψη για τα δρόμενα στην κοινωνία ενός ΚΠΣ, συνεργάζεται και συνδιαλέγεται με άλλους χρήστες (γνωστούς ή άγνωστους, φίλους ή απλούς ακόλουθους), συνεισφέρει στην ανάπτυξη του συστήματος αλλά και άλλες ενέργειες που καθιστά ένα άτομο ταυτοποιήσιμο. Με την επεξεργασία των δεδομένων αυτών, ενδιαφερόμενοι τρίτοι παράγοντες, έχουν τη δυνατότητα να διενεργούν εκτενείς αναλύσεις στα δεδομένα αυτά (κείμενα αλλά και την «κίνηση» που κάνει ο κάθε χρήστης εντός του ΚΠΣ). Ο τρόπος αυτός βοηθά στην εξαγωγή συμπερασμάτων για συμπεριφορές χρηστών οι οποίες συνδυάζονται με άλλους χρήστες από το στενό τους περιβάλλον (συνάδελφοι στον ίδιο οργανισμό, φίλοι ή ακολουθούμενοι από άλλους σε ένα Κοινωνικό Δίκτυο, συμφοιτητές, άτομα που διαμένουν στην ίδια περιοχή[42]), με στόχο να δημιουργήσουν διαφημιστικές ομάδες ανθρώπων που ίσως να ενδιαφέρονται περισσότερο για προϊόντα και υπηρεσίες Α, από άλλους χρήστες που ενδιαφέρονται για προϊόντα και υπηρεσίες Β.

Μέσα από τις απαντήσεις που λήφθηκαν, εστιάστηκε η προσοχή σε κάποια στοιχεία που θεωρήθηκε σημαντικό να αναφερθούν ως γενικές ενέργειες που επηρεάζουν και

[42] π.χ ανοίγει ένα κατάστημα σε μια γεωγραφική περιοχή και παρατηρείται προηγούμενη συμπεριφορά χρηστών που διαμένουν στην περιοχή εκείνη.

τα ΚΠΣ. Ακολούθως παρουσιάζονται τα σημεία αυτά και παρατηρήσεις επί τούτων. Το ερωτηματολόγιο παρουσιάζεται στο Παράτημα Β.

- Η Εποπτική Αρχή δεν έχει ακόμα προχωρήσει σε παρουσιάσεις εξειδικευμένες για ΠΣ ή ΚΠΣ. Αυτό θα πρέπει να εξεταστεί άμεσα από την Επίτροπο, αφού η ζωή πολλών πολιτών έχει ταυτιστεί πλέον με την εικονική ζωή που προσφέρουν πολλά ΚΠΣ. Όλα τα σημεία, τα οποία έχουν αναφερθεί στην αμέσως προηγούμενη παράγραφο αλλά και στις παραγράφους 1.2 και 2.3 της παρούσας εργασίας, μπορούν να επηρεάσουν την ιδιωτικότητα ενός ατόμου σε τέτοιο βαθμό ώστε να επηρεάζεται η ζωή του στον πραγματικό κόσμο ή ακόμα να κινδυνεύει ακόμα και η ίδια του η ζωή (βλ. παρ. 2.3 – παράνομες διακινήσεις δεδομένων και πληροφοριών στο Dark Web). Η πολιτεία οφείλει μέσω Αρμόδιων Σωμάτων της (π.χ. το γραφείο Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα) να ενημερώνει τα ΥπΔε για τους κινδύνους που διατρέχουν τα προσωπικά τους δεδομένα αν αυτοί οι ίδιοι δεν χρησιμοποιούν σωστά ένα ΚΠΣ ή αν δεν απαιτούν κάποιες λειτουργίες των ΚΠΣ να εναρμονίζονται με τον ΓΚΠΔ (λειτουργίες στις οποίες ίσως ακόμα να μην δίνεται η απαιτούμενη σημασία για έλεγχο από την Εποπτική Αρχή) (απαντήσεις στα ερωτήματα 1, 2, 7, 8, 9, 10, 11, του ερωτηματολογίου).
- Πολύ θετικό στοιχείο είναι το γεγονός ότι οι επαγγελματίες στο χώρο (ιδιοκτήτες/διευθυντές επιχειρήσεων ή εκτελεστικοί διευθυντές οργανισμών) δείχνουν να είναι πάντα πρόθυμοι να συνεργαστούν με την Εποπτική Αρχή. Αυτό δείχνει ότι έχουν αποδεχτεί την ύπαρξη και σοβαρότητα του ΓΚΠΔ πράγμα που ενισχύει την προσπάθεια της συμμόρφωσης όλων όσων επεξεργάζονται δεδομένα με όλες τις πτυχές του Κανονισμού. Αν και είναι δύσκολο να υπολογιστεί το ποσοστό συμμόρφωσης στο παρόν στάδιο αφού δεν έχει ακόμη διενεργηθεί ικανοποιητικός αριθμός ελέγχων, εντούτοις φαίνεται ότι η προσπάθεια αυτή θα φέρει σύντομα αποτελέσματα αφού η ενημέρωση για τη σοβαρότητα του θέματος (εναρμόνιση με τον ΓΚΠΔ) μεταδίδεται με γοργούς ρυθμούς μέσω της ιστοσελίδας του γραφείου της Εποπτική Αρχής αλλά και μεταξύ των επηρεαζόμενων επαγγελματιών που δέχτηκαν ελέγχους, αλλά προς το παρών υποβάλλονται συστάσεις, αντί προστίμων (απαντήσεις στα ερωτήματα 3, 4, 5, 6, του ερωτηματολογίου).

- Στο ερώτημα 8 λήφθηκε μια πολύ συγκεκριμένη και σημαντική απάντηση η οποία δείχνει την ανησυχία των πολιτών για την έκθεσή τους κυρίως στον παγκόσμιο Ιστό (Διαδίκτυο και δίκτυο διαφημίσεων προϊόντων). Η άγνοια για τα δικαιώματά τους που πηγάζουν από τον ΓΚΠΔ και σε συνάρτηση με την αγωνία που έχουν για τους μεγάλους κίνδυνους που διατρέχουν οι χρήστες που δραστηριοποιούνται καθημερινά στο διαδίκτυο (ειδικότερα τα παιδιά), αυτό μετατρέπεται σε ανασφάλεια, πράγμα που φαίνεται από τα παράπονα που παίρνει το γραφείο της Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα (Κύπρου), σε καθημερινή βάση.
- Η απάντηση στο ερώτημα 9, του ερωτηματολογίου, δείχνει ότι τα Κράτη μέλη της ΕΕ άρχισαν δειλά δειλά να βλέπουν με περισσότερη σοβαρότητα την επεξεργασία του μεγάλου όγκου δεδομένων (Big data) που διακινείται, μέσω των μεγάλων κυρίως κοινωνικών δικτύων, αφού αυτό επηρεάζει μεγάλο αριθμό πολιτών της ΕΕ (μερικές εκατοντάδες εκατομμύρια, καθημερινά). Αυτή η κίνηση ίσως να γίνει η αρχή της προσπάθειας ελέγχου, εναρμόνισης, σε μεγαλύτερο βάθος στα ΚΠΣ.

Κεφάλαιο 5

Εισηγήσεις και τελικά συμπεράσματα

5.1. Εισηγήσεις για επέκταση της εργασίας

Όπως έχει ήδη αναφερθεί στη συνέντευξη με τους κ.κ. Παπαδόπουλο και Ιωάννου, η πιστοποίηση με τον ΓΚΠΔ ήδη βρίσκεται σε διαδικασία δρομολόγησης για γνωμοδότηση (consultation) από την ανεξάρτητη Ευρωπαϊκή Αρχή «European Data Protection Supervisor» (EDPS). Η πιστοποίηση αυτή θα παρέχεται σε οργανισμούς στους οποίους έπειτα από σειρά ελέγχων θα έχει διαπιστωθεί ότι τόσο το τεχνικό κομμάτι των διαδικασιών (διεργασίες που τρέχουν στα πληροφορικά του συστήματα) όσο και το κομμάτι των εσωτερικών πολιτικών και διαδικασιών αποβλέπει στην προστασία των δεδομένων προσωπικού χαρακτήρα [19]. Με βάση την παρούσα μελέτη και με γνώμονα την πιο πάνω πληροφόρηση θα μπορούσε να διερευνηθεί αν η έρευνα αυτή μπορεί να συνεχιστεί και να οδηγήσει σε συγγραφή βέλτιστων πρακτικών για πιστοποίηση με τον ΓΚΠΔ.

Στη συνέχεια αναφέρονται άλλες πιθανές επεκτάσεις της εργασίας αυτής.

1. Να κατασκευαστεί ιστοσελίδα (ίσως και app για έξυπνες συσκευές), με στόχο την ενημέρωση και ηλεκτρονική επικοινωνία παρέχοντας συμβουλές σε εμπλεκόμενους με την κατασκευή ΚΠΣ αλλά και σε απλούς χρήστες που θέλουν να ενημερωθούν για τα δικαιώματα και τις υποχρεώσεις τους στα ΚΠΣ (ειδικότερα στα κοινωνικά δίκτυα που δραστηριοποιούνται καθημερινά).
2. Να επιχειρηθεί η υλοποίηση εφαρμογής για αυτοματοποιημένη συγγραφή Πολιτικής απορρήτου η οποία θα χρησιμοποιείται για τη λήψη της συγκατάθεση του ΥπΔε από το σύστημα. Για τον κατασκευαστή ΚΠΣ, προκειμένου να δημιουργήσει εύκολα και αποτελεσματικά το κατάλληλο κείμενο, **θα είναι μία διαδικασία παραμετροποίησης και προσαρμογής (customization)** όπου θα του δίνει την επιλογή της προσθήκης και αφαίρεσης μερών του κείμενου. Όσον

αφορά το ΥπΔε θα έχει την ευχέρεια της επιλογής με την εμφάνιση διάφορων παραθύρων ή/και πεδίων που θα μπορεί να συμφωνεί με όλο το κείμενο ή μέρος αυτού.

3. Επέκταση της εργασίας για την εξέταση σε βάθος, όλων των πτυχών που αφορούν τα ΚΠΣ για **τα οποία συνδέονται άμεσα με κινητές συσκευές**. Περιορισμοί και δικαιώματα στους κατασκευαστές ΚΠΣ ή σε τρίτους (που ενδεχομένως να μπορέσουν να πάρουν δεδομένα από κάποιο ΚΠΣ) μέσω του Λειτουργικού Συστήματος (π.χ. Android, iOS), αλλά και υποχρεώσεις των κατασκευαστών για τη μη απόκρυψη λειτουργιών, έναντι του (ευάλωτου/ανυποψίαστου) χρήστη, είναι κρίσιμα θέματα που θα μπορούσαν να εξετασθούν.
4. Με βάση την υπάρχουσα βιβλιογραφία, η παρούσα Διπλωματική εργασία παρουσιάζει όλα τα βασικά σημεία που πρέπει να ληφθούν υπόψη κατά την κατασκευή ενός ΚΠΣ (ή υφιστάμενων ΚΠΣ). Εντούτοις γίνεται εισήγηση για την προσπάθεια εντοπισμού εκείνων των σημείων που επιδέχονται συμπλήρωση ή και εντοπισμού στοιχείων που δεν έχουν αναφερθεί στις προδιαγραφές των πινάκων της παραγράφου 3.1.1.3.

   Μία καλή πρακτική εντοπισμού τέτοιων παραλήψεων ή/και αποκλίσεων είναι η μελέτη περίπτωσης. **Προτείνεται όπως γίνει μελέτη περίπτωσης** για υφιστάμενα ΚΠΣ μεγάλου οργανισμού (real case scenario), στην οποία θα πραγματοποιηθεί καταγραφή των απαιτήσεων σε περίπτωση κατασκευής ενός νέου ΚΠΣ ή αξιολόγηση λειτουργιών και διαδικασιών υφιστάμενου ΚΠΣ, ως προς την προστασία προσωπικών δεδομένων.

5.2. Τελικά συμπεράσματα

Τα Κοινωνικά Πληροφοριακά Συστήματα είναι μια «κοινωνία» που έχει κουλτούρα, συνήθειες και κανόνες. Τα συστήματα αυτά πλέον έχουν εδραιωθεί και έχουν αλλάξει τον τρόπο που οι άνθρωποι επικοινωνούν και αλληλοεπιδρούν μεταξύ τους. Η καθημερινή δραστηριότητα του ανθρώπου σήμερα επηρεάζεται σε μεγάλο βαθμό, από τη χρήση των ΚΠΣ και ακολούθως από την ανταλλαγή ψηφιακής πληροφορίας. Κρίνεται λοιπόν απαραίτητο και πλέον λόγ ω της αυστηρότερης νομοθεσίας που αφορά την προστασία προσωπικών δεδομένων να προσφέρονται υπηρεσίες που εναρμονίζονται με τον ΓΚΠΔ ώστε οι οργανισμοί/επιχειρήσεις να μπορούν να επεξεργάζονται προσωπικά δεδομένα χωρίς μεγάλο ρίσκο διαρροής τους.

Ο ΓΚΠΔ έχει εισάγει αυστηρές αρχές για την προστασία δεδομένων και επιβάλλει την πλήρη συμμόρφωση όλων όσων διαχειρίζονται προσωπικά δεδομένα. Από το Μάιο του 2018 όπου ο ΓΚΠΔ είναι σε ισχύ, όλοι οι οργανισμοί, εταιρείες και άλλοι φορείς που επεξεργάζονται προσωπικά δεδομένα θα πρέπει να συμμορφώνονται πλήρως με τις απαιτήσεις του ΓΚΠΔ. Η μερική και ερασιτεχνική προσέγγιση της συμμόρφωσης δεν ενδείκνυται ενώ ιδιαίτερη βάση θα πρέπει να δίνεται στη **διατήρηση της συμμόρφωσης με τον ΓΚΠΔ**. Σε αντίθετη περίπτωση, όποιος παρεκκλίνει στο ελάχιστο θα κινδυνεύει να υποστεί τις συνέπειες των αυστηρών προστίμων που προβλέπονται από τον Κανονισμό. Αξίζει να αναφερθεί η πρόσφατη επιβολή προστίμου 50 εκ. ευρώ στην εταιρεία Google από Γαλλικό Δικαστήριο[43] (Γενάρης 2019).

Είναι λοιπόν πολύ σημαντικό για έναν οργανισμό να διατηρεί ακέραια τα δεδομένα που εισέρχονται και διατηρούνται στα ΚΠΣ του, διότι αυτή η προσπάθεια είναι μόνο προς όφελός του αφού **έχει σαν αποτέλεσμα την καλή φήμη του οργανισμού αυξάνοντας ταυτόχρονα την αξιοπιστία του**.

Για επίτευξη της συμμόρφωσης των διεργασιών που εκτελούνται μέσω των ΚΠΣ με το ΓΚΠΔ, **θα πρέπει οι κατασκευαστές ΚΠΣ να συμβουλεύονται ειδικούς** που γνωρίζουν το αντικείμενο της ασφάλειας και ιδιωτικότητας των πληροφοριών ή

[43] https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-gdpr-fine-eu-data-privacy-cnil-amazon-apple-a8740191.html

τουλάχιστον να έχουν αρκετά χρόνια εμπειρίας στην ασφάλεια και διαχείριση πληροφοριακών συστημάτων, **ώστε να μπορούν να κατανοήσουν και ακολούθως να αποκωδικοποιήσουν τις απαιτήσεις του ΓΚΠΔ**. Αυτό επιβεβαιώθηκε και από τις απαντήσεις που συλλέγηκαν στη συνέντευξη με τους κ.κ. Παπαδόπουλο και Ιωάννου. Στην ίδια συνέντευξη, ιδιαίτερη έμφαση δόθηκε στα ζητήματα που ακολουθούν:

i. *Σωστή διαχείριση των log files (που αποτελούν ένα από τα βασικά αποδεικτικά στοιχεία σε περίπτωση ελέγχων)*
ii. *Εφαρμογή της πρόληψης και αντίδρασης ειδικά όταν υπάρχει η ανάγκη για τη διαχείριση εκατοντάδων servers*
iii. *Συχνός έλεγχος συμβατότητας και συμμόρφωσης με τον ΓΚΠΔ του hardware και software του οργανισμού και όπου είναι αναγκαίο εφαρμόζονται συχνές αναβαθμίσεις*
iv. *Όλες οι διαδικασίες πρέπει να καταγράφονται σε σχετικά εγχειρίδια τα οποία να είναι εύκολα προσβάσιμα για ενημέρωση των εμπλεκομένων*

Στην ίδια συνέντευξη επισημάνθηκε ότι **ο κατασκευαστής ΚΠΣ πρέπει να ακολουθήσει/εφαρμόσει πλήρως όλα τα άρθρα του ΓΚΠΔ, που αναφέρονται στον Πίνακα 1 (παρ. 3.1.1.3) πριν παραδώσει στον εντολέα του (οργανισμός/επιχείρηση) το «έργο**» και παραχωρήσει προσβάσεις στο σύστημα για το ευρύ κοινό. Για εναρμόνιση με τον ΓΚΠΔ, δεν είναι αρκετή μόνο η συμμόρφωση των ατόμων η οποία μπορεί να επιτευχθεί με αλλαγή του τρόπου που εργάζονται και ένα ΚΠΣ που προσφέρει διεργασίες εναρμονισμένες με τις απαιτήσεις του κανονισμού αυτού. Αντ' αυτού, όλα τα υπόλοιπα ψηφιακά συστήματα που χρησιμοποιούνται εντός και εκτός του οργανισμού ως υποστηρικτικά για τη λειτουργία των ΚΠΣ, αλλά και ο εξοπλισμός (hardware) του οργανισμού, θα πρέπει να πληρούν τις τεχνικές προδιαγραφές που παρουσιάστηκαν σε αυτή την εργασία. **Άρα η συμμόρφωση δεν περιορίζεται μόνο στο πλαίσιο της λειτουργίας ενός ΚΠΣ αλλά εξαρτάται και από εξωγενείς παράγοντες που πρέπει να λαμβάνονται σοβαρά υπόψη πριν δοθεί ένα ΚΠΣ σε λειτουργία**.

Ένα σημαντικό συμπέρασμα που βγήκε από τις απαντήσεις που λήφθηκαν από το γραφείο της Εποπτικής Αρχής είναι ότι τα ΚΠΣ δεν διαχωρίζονται από τα Πληροφοριακά Συστήματα πράγμα που καθιστά τον έλεγχο συμμόρφωσης λιγότερο αποτελεσματικό για τα ΚΠΣ. Συστήνεται όπως οι Εποπτικές Αρχές λάβουν σοβαρά

υπόψη αυτό το κενό αφού σήμερα με τη μεγάλη δραστηριότητα των ΥπΔε στο Διαδίκτυο και κυρίως στα Κοινωνικά Δίκτυα, ο κίνδυνος λανθασμένης επεξεργασίας των προσωπικών δεδομένων των ΥπΔε είναι όσο ποτέ άλλοτε υψηλού ρίσκου.

Ο ΓΚΠΔ κάνει πολύ συχνά αναφορά στα «**ευαίσθητα προσωπικά δεδομένα**». Πρόκειται για ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που λαμβάνουν ειδική προστασία σύμφωνα με τον ΓΚΠΔ. Γενικός κανόνας είναι ότι η επεξεργασία δεδομένων των ανωτέρω κατηγοριών απαγορεύεται. Ωστόσο, υπάρχουν ορισμένες εξαιρέσεις βάσει των οποίων μια εταιρεία ή ένας οργανισμός μπορεί ενδεχομένως να επεξεργάζεται ευαίσθητα δεδομένα προσωπικού χαρακτήρα, όταν το ΥπΔε παραχωρήσει τη **ρητή συγκατάθεση του ή εάν το υποκείμενο των δεδομένων έχει κάνει τα δεδομένα προφανώς δημόσια** (άρθρο 9, παράγραφος 2ε) [1].

Μεταξύ άλλων, ένας υψηλός κίνδυνος για την προστασία των δεδομένων των ΥπΔε πηγάζει από τον βαθμό διαμοιρασμού των προσωπικών δεδομένων μεταξύ των πολλών παραγόντων στο τοπίο ανάπτυξης ΚΠΣ[44] για το οποίο θα πρέπει ο καθένας να είναι πολύ καλά ενημερωμένος για το βαθμό που αυτό συμβαίνει ώστε να μην ξεφεύγει από τη σφαίρα του ελέγχου του [16](σελ. 5).

Σημαντικό ρόλο πλέον στην προστασία προσωπικών δεδομένων παίζει ο ΥΠΔ ο οποίος θα πρέπει να ορίζεται από κάθε εταιρία/οργανισμό και να δηλώνεται στην Εποπτική Αρχή.

Στο ΓΚΠΔ γίνεται επίσης λόγος για τα cookies τα οποία χρησιμοποιούνται κυρίως για εμπορικούς και διαφημιστικούς σκοπούς προς όφελος του πωλητή/διαφημιστή. Ο τρόπος που λειτουργούν αυτά προς όφελος τρίτων, είναι η επεξεργασία δεδομένων με τέτοιο τρόπο, που αυξάνει την πιθανότητα δημιουργίας προφίλ, πράγμα που απαγορεύεται[45] (Αιτιολογική σκέψη 30). Ο κατασκευαστής των ΚΠΣ θα πρέπει μέσω κατάλληλων ενεργειών να προλαμβάνει τέτοιες καταστάσεις και να μειώνει τον κίνδυνο έκθεσης των χρηστών, στη σφαίρα των διαφημιστών για ανεξέλεγκτη διαφήμιση, χωρίς τη συγκατάθεση του ΥπΔε.

[44] βλ. παράγραφο 3.1.2, «Ανάλυση σημείων Πίνακα 1», σημείο 13 και «Ανάλυση σημείων Πίνακα 2», σημείο 2.
[45] βλ. παράγραφο 3.1.2, «Ανάλυση σημείων Πίνακα 1», σημείο 18

Αισίως έχει περάσει το πρώτο έτος από την ημέρα που έχει εφαρμοστεί ο ΓΚΠΔ, αλλά φαίνεται οι Αρμόδιες Αρχές να μην είναι τόσο αυστηρές, όπως απαιτεί ο Κανονισμός, πράγμα το οποίο βεβαιώθηκε και από το Γραφείο της Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα της Κύπρου, αφού για την ώρα υποβάλλονται μόνο συστάσεις. Κάθε ΥπΔε, δε θα πρέπει να βασίζεται μόνο στις ενέργειες που γίνονται από την Αρμόδια Αρχή αλλά και ο ίδιος/-α να μεριμνά για την προστασία των προσωπικών του δεδομένων διαβάζοντας τον Κανονισμό και γνωρίζοντας τα δικαιώματα που έχει όταν παρέχει τα προσωπικά του δεδομένα σε κάθε είδους ψηφιακό σύστημα. Οι οργανισμοί και οι επιχειρήσεις μπορούν να συνεισφέρουν στην προσπάθεια ενημέρωσης των ΥπΔε παρουσιάζοντας στο χρήστη πολιτικές απορρήτου εύκολα κατανοητές από όλους και για όλες τις ηλικίες.

Παράρτημα Α

Συνέντευξη με επαγγελματίες συμβούλους

Α.1 Ερωτήσεις και απαντήσεις συνέντευξης

Παρατίθεται πιο κάτω αυτούσιο το ερωτηματολόγιο όπως δόθηκε στους κ.κ. Παπαδόπουλο και Ιωάννου. Να σημειωθεί ότι έχει δοθεί η συναίνεσή τους για τη χρήση των επαγγελματικών τους στοιχείων στην εργασία αυτή.

Συνέντευξη με επαγγελματίες συμβούλους που εξειδικεύονται στο θέμα της συμμόρφωσης των οργανισμών/επιχειρήσεων με το ΓΚΠΔ

Στα πλαίσια της Μεταπτυχιακής Διατριβής «Κοινωνικά Πληροφοριακά Συστήματα και Συμμόρφωση με το Γενικό Κανονισμό Προστασίας Δεδομένων», υποβάλλονται τα παρακάτω ερωτήματα σε ιδιώτες επαγγελματίες Συμβούλους Προστασίας Δεδομένων (εφεξής, Σύμβουλοι) οργανισμών/επιχειρήσεων. Σκοπός των συνεντεύξεων είναι η εξαγωγή συμπερασμάτων που αφορούν στην ανταπόκριση των επιχειρήσεων σχετικά με την υποχρεωτική εναρμόνιση των ΚΠΣ με τον ΓΚΠΔ.

Δημογραφικά στοιχεία Συμβούλου

Ονοματεπώνυμο ----------

Υπηκοότητα (Εθνικότητα) ----------

Οργανισμός/Επιχείρηση ----------

Είδος Οργανισμού ----------

Θέση μέσα στον Οργανισμό/Επιχείρηση ----------

Συμμόρφωση Οργανισμού ή Επιχείρησης με το ΓΚΠΔ ή και με άλλα πρότυπα περί προστασίας προσωπικών δεδομένων

Ερωτήσεις προς τους Συμβούλους

1. Είστε πιστοποιημένος Σύμβουλος Προστασίας Δεδομένων; Από ποιον δέχεστε έλεγχο γι' αυτή σας την επαγγελματική ιδιότητα;

2. Με πόσους οργανισμούς/εταιρείες έχετε εμπλακεί στη διαδικασία αυτή;

3. Σας καλούν για συμβουλές (ως εξωτερικό συνεργάτη) σε υφιστάμενα ΠΣ ή/και υλοποίηση νέων;

4. Συμμετέχετε σε όλη τη διαδικασία; (GAP analysis , εκπαίδευση υπαλλήλων κ.α.)

5. Ποιος είναι ο ρόλος σας μετά την ολοκλήρωση της διαδικασίας εναρμόνισης;

6. Βάσει της εμπειρίας σας μέχρι σήμερα:
   i. Ποια σημεία/άρθρα στον ΓΚΠΔ θεωρούνται πιο σημαντικά για τη σωστή εφαρμογή του Κανονισμού στα ΚΠΣ;
   ii. Έχουν όλα την ίδια βαρύτητα;
   iii. Μπορεί κάποιος κατασκευαστής ΚΠΣ να αγνοήσει κάποιες πτυχές του Κανονισμού ως λιγότερο σημαντικές;

7. Ποια η ευθύνη του κατασκευαστή ΚΠΣ στην εν μέρη ενσωμάτωση των υποχρεωτικών σημείων του Κανονισμού, κατά την υλοποίηση εναρμόνισης υφιστάμενου συστήματος με τον ΓΚΠΔ ή την υλοποίηση ενός νέου;

8. Έλεγχος από την αρμόδια Αρχή:

i. Αν κατά τον έλεγχο, από την αρμόδια Αρχή, σε κάποιο νέο ΚΠΣ διαφανούν κενά τα οποία πηγάζουν από υλοποίηση συστήματος που δεν πληροί τις απαιτήσεις για ασφάλεια προσωπικών δεδομένων των χρηστών, ποιος φέρει την ευθύνη;
ii. Υπάρχει «περίοδος χάριτος» για τη λειτουργία ενός νέου ΚΠΣ;

---

9. Δυσκολίες κατά τη διαδικασία της εφαρμογής του ΓΚΠΔ στα ΚΠΣ:
   i. Ποια είναι τα συχνότερα προβλήματα («τρύπες») που συναντάτε στα ΚΠΣ;
   ii. Ποια τα κυριότερα προβλήματα που συναντάτε με τους υπαλλήλους (χρήστες) που εκπαιδεύετε και ποια με τους ιδιοκτήτες επιχειρήσεων ή τους διαχειριστές ή τους υπεύθυνους έργων ή ακόμα τους Γενικούς Διευθυντές μεγάλων οργανισμών;

---

10. Κατά τη διαδικασία της εφαρμογής του ΓΚΠΔ στα ΚΠΣ, παρατηρείτε αν ο οργανισμός/επιχείρηση συμμορφώνεται με κάποιο πρότυπο ασφάλειας προσωπικών δεδομένων και ελέγχετε εάν υπάρχει σχετική πιστοποίηση;
    Αν ναι, πως αυτό διευκολύνει τη συμμόρφωση με το ΓΚΠΔ;

---

11. Από τη μέχρι σήμερα εμπειρία σας πιστεύετε ή γνωρίζετε αν υπάρχει σκέψη στο μέλλον για έκδοση πιστοποίησης συμβατότητας των Λογισμικών των ΚΠΣ με το ΓΚΠΔ, από εγκεκριμένους οργανισμούς;

Συναίνεση Συμβούλου

Στα πλαίσια της παρούσας Μεταπτυχιακής Διατριβής, συναινείτε στη δημοσίευση των πιο πάνω δημογραφικών στοιχείων που έχουν συλλεχθεί;

Υπογραφή Συμβούλου ---

Παράρτημα Β

Ερωτηματολόγιο στην «Επίτροπο Δεδομένων Προσωπικού Χαρακτήρα» της Κύπρου

Β.1 Ερωτήσεις και απαντήσεις ερωτηματολογίου

Παρατίθεται πιο κάτω αυτούσιο το ερωτηματολόγιο όπως είχε σταλεί στο γραφείου της Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα. Το ερωτηματολόγιο στάλθηκε μέσω ηλεκτρονικού ταχυδρομείου. Οι απαντήσεις λήφθηκαν με το ίδιο μέσο.

Ερωτήσεις προς αντιπρόσωπο του γραφείου της «Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα»

Υποβλήθηκαν τα παρακάτω ερωτήματα σε αντιπρόσωπο του γραφείου της Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα και στόχος του ερωτηματολογίου ήταν ο σχηματισμός της κατάλληλης εικόνας σχετικά με ποια σημεία του ΓΚΠΔ, η Εποπτική Αρχή, δίνει περισσότερη βαρύτητα όσον αφορά το μηχανογραφικό μέρος που διαχειρίζεται προσωπικά δεδομένα (για οργανισμούς, επιχειρήσεις κ.α.). Αναπόφευκτα, αυτό καλύπτει και όλα τα Πληροφοριακά Συστήματα (ΠΣ) και ειδικότερα τα Κοινωνικά Πληροφοριακά Συστήματα (ΚΠΣ).

Εξασφαλίστηκε, μέσω ηλεκτρονικού ταχυδρομείου, η συναίνεση του γραφείου της Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα, για να δημοσιοποιηθεί το περιεχόμενο του ερωτηματολογίου, αν χρειαστεί.

Ερωτήσεις προς το άτομο που θα αντιπροσωπεύσει το γραφείο της «Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα»

Στα πλαίσια της Μεταπτυχιακής Διατριβής «Κοινωνικά Πληροφοριακά Συστήματα και Συμμόρφωση με το Γενικό Κανονισμό Προστασίας Δεδομένων» (Μεταπτυχιακό Πρόγραμμα Σπουδών ΑΠΚΥ), υποβάλλονται τα παρακάτω ερωτήματα στην Επίτροπο Δεδομένων Προσωπικού Χαρακτήρα ή Αντιπρόσωπό της (εφεξής, Επίτροπος ή Αντιπρόσωπος, ανάλογα). Στόχος της συνάντησης αυτής είναι ο σχηματισμός της κατάλληλης εικόνας σχετικά με ποια σημεία του ΓΚΠΔ, η αρμόδια αρχή, δίνει περισσότερη βαρύτητα όσον αφορά το μηχανογραφικό μέρος που διαχειρίζεται προσωπικά δεδομένα (για οργανισμούς, επιχειρήσεις κ.α.). Αναπόφευκτα, αυτό καλύπτει και όλα τα Πληροφοριακά Συστήματα (ΠΣ) και ειδικότερα τα Κοινωνικά Πληροφοριακά Συστήματα (ΚΠΣ).

<u>Επαγγελματικά Στοιχεία</u>

Ονοματεπώνυμο ----------

Θέση μέσα στον Οργανισμό ----------

Σχετική Ειδικότητα ----------

Συναίνεση

Στα πλαίσια της παρούσας Μεταπτυχιακής Διατριβής, συναινείτε στη δημοσίευση των πιο πάνω επαγγελματικών στοιχείων που έχουν συλλεχθεί;

Υπογραφές: ---------- ----------

Ερωτήσεις προς την Επίτροπο ή Αντιπρόσωπο

1. Έχουν γίνει παρουσιάσεις που αφορούν ειδικά τα ΠΣ (μηχανογράφηση οργανισμών/επιχειρήσεων);

2. Επιστήνετε την προσοχή σας σε κάποια σημεία του Γενικού κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) σημαντικότερα από άλλα ή θεωρείτε όλα τα σημεία του Κανονισμού ίδιας σημασίας και βαρύτητας;

3. Οι επαγγελματίες είναι πρόθυμοι να συνεργαστούν όταν γίνεται έλεγχος;

4. Γίνεται έλεγχος για το αν έχει γίνει η κατάλληλη εκπαίδευση των υπαλλήλων και ειδικότερα αυτών που ορίζονται ως Εκτελούντες την Επεξεργασία;

5. Υπάρχουν στατιστικά στοιχεία που δείχνουν το ποσοστό συμμόρφωσης γενικά αλλά και ειδικότερα στα ΚΠΣ (αν υπάρχουν στοιχεία). Αυτά δίνονται στη δημοσιότητα;

6. Έχουν επιβληθεί τιμωρίες μέχρι τώρα που να έχουν σχέση με αποκλίσεις της μηχανογράφησης οργανισμών/επιχειρήσεων, με τον ΓΚΠΔ;

7. Ποια είναι τα πιο συνηθισμένα προβλήματα (τρύπες) που αντιμετωπίζουν οι οργανισμοί/επιχειρήσεις σχετικά με τη μηχανογράφησή τους; Αυτά τα στοιχεία δίνονται στη δημοσιότητα ώστε να ενημερώνονται οι ενδιαφερόμενοι για να μην κάνουν παρόμοια λάθη;

8. Έχετε διερευνήσει κατά πόσο οι χρήστες των ΚΠΣ νιώθουν να προστατεύονται ικανοποιητικά από τη μέχρι τώρα εναρμόνιση των ΚΠΣ με το ΓΚΠΔ;

---

9. Τι στοιχεία υπάρχουν που δείχνουν το ποσοστό ενσωμάτωσης του ΓΚΠΔ στα ΚΠΣ;

---

10. Οι πολιτικές απορρήτου (συγκατάθεση) των ΚΠΣ συμμορφώνονται με τον ΓΚΠΔ;

---

11. Σε ποιο βαθμό μπορεί να ανταποκριθεί η αρμόδια υπηρεσία του Κράτους για συχνό έλεγχο συμμόρφωσης των ΚΠΣ με το ΓΚΠΔ;

Συντομογραφίες

ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
95/46/ΕΚ	Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995
ΕΕ	Ευρωπαϊκή Ένωση
ΥπΔε	Υποκείμενο των δεδομένων (χρήστης ΚΠΣ)
ΠΣ	Πληροφοριακό Σύστημα
ΚΠΣ	Κοινωνικό Πληροφοριακό Σύστημα
Web	Παγκόσμιος Ιστός
Εποπτική Αρχή	Επίτροπος Προστασίας Προσωπικών Δεδομένων ή Επίτροπος Δεδομένων Προσωπικού Χαρακτήρα (Κύπρου)
ΥΕ	Υπεύθυνος Επεξεργασίας (δεδομένων)
ΕτΕ	Εκτελών την Επεξεργασία (δεδομένων)
ΥΠΔ	Υπεύθυνος [19] Προστασίας Δεδομένων
ΕΑΠΔ	Εκτίμηση Αντικτύπου Προσωπικών Δεδομένων (DPIA)
Σύμβαση ΕΠΔ	Σύμβαση επεξεργασίας προσωπικών δεδομένων
Επιτροπή	Ευρωπαϊκή Επιτροπή για τον ΓΚΠΔ

Βιβλιογραφία

[1] Ευρωπαϊκό Κοινοβούλιο, *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και (...),* Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 2016.

[2] D. Schlagwein, D. Schoder και K. Fischbach, «Social information systems: Review, framework, and research agenda,» σε *Thirty Second International Conference on Informati on Systems* , Shanghai, 2011.

[3] J. Otterbacher, *Ανοικτό Πανεπιστήμιο Κύπρου, Διαφάνειες Θεματικής Ενότητας ΚΠΣ514: Πληροφορίες σε κοινωνικά συστήματα,* Otterbacher Jahna, 2017.

[4] C. Tikkinen-Piri, A. Rohunen και J. Markkula, «EU General Data Protection Regulation: Changes and implications for personal data collecting companies,» *Computer Law & Security Review 34(1),* pp. 134-153, February 2018.

[5] A. Goodbody, «THE GDPR: A Guide for Businesses,» A&L Goodbody, New York, 2016.

[6] Ε. Κ. κ. τ. Σ. WP248 - Ομάδα εργασίας για την προστασία δεδομένων του άρθρου 29, *Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679,* Brussels: Επίσημη Εφημερίδα ΕΕ, 2017.

[7] J. Gleick, «Prologue,» σε *The Information: A History. A Theory. A Flood*, London, Fourth Estate, Great Britain and Pantheon, United States, 2012, pp. 3-12.

[8] T. Dominguez, «Seeker,» Group Nine Media, Inc., 9 February 2015. [Ηλεκτρονικό]. Available: https://www.seeker.com/how-much-of-the-internet-is-hidden-1792697912.html.

[9] S. Mansfield-Devine, «Network Security, Millions of user credentials for popular sites sold on dark markets,» Elsevier Ltd, June 2016. [Ηλεκτρονικό]. Available: http://www.networksecuritynewsletter.com.

[10] L.-C. Spataru-Negura και C. Lazar, «LIFTING THE VEIL OF THE GDPR TO DATA SUBJECTS,» σε *Challenges of the Knowledge Society: 658-667*, Bucharest, 2018.

[11] A. Smith και D. Holmes, «Articles,» Thomson Reuters, 16 February 2018. [Ηλεκτρονικό]. Available: https://www.reuters.com/article/us-facebook-belgium/facebook-loses-belgian-privacy-case-faces-fine-of-up-to-125-million-idUSKCN1G01LG.

[12] J. G. Cabañas, «GroundAI,» 14 February 2018. [Ηλεκτρονικό]. Available: https://www.groundai.com/project/facebook-use-of-sensitive-data-for-advertising-in-europe.

[13] C. Knobel και G. C. Bowker, «Values in Design,» *Communications of the ACM,* pp. 26-26, July 2011.

[14] A. Michota και S. Katsikas, «Designing a seamless privacy policy for social networks,» σε *Proceedings of the 19th Panhellenic Conference on Informatics, PCI15*, Athens, Greece, 2015.

[15] A. 2. D. P. W. PARTY, *Opinion 02/2013 on apps on smart devices,* Brussels: Official Journal Europian Union, 2013.

[16] Ε. Κ. κ. τ. Σ. WP 202 - Ομάδα εργασίας για την προστασία δεδομένων του άρθρου 29, *Opinion 02/2013 on apps on smart devices,* Brussels: Επίσημη Εφημερίδα ΕΕ, 2013.

[17] P. Tsiavos, «Webinar on Open Science and Personal Data: applying the General Data Protection Regulation in today's digital science,» OpenAIRE, 8 April 2019. [Ηλεκτρονικό]. Available: https://www.youtube.com/watch?v=WueqqxiiNFU&feature=youtu.be.

[18] F. Simorjay, «13 Effective Security Controls for ISO 27001 Compliance,» Microsoft, January 2016. [Ηλεκτρονικό]. Available: http://download.microsoft.com/download/1/2/9/12943B91-BBE8-415C-

9E0A-4844407E4377/13%20Effective%20Security%20Controls%20for%20ISO%2027001%20Compliance.pdf.

[19] E. U. A. f. N. a. I. S. (ENISA), «ENISA report: Concepts and recommendations on European Data Protection Certification mechanisms,» ENISA, 27 11 2017. [Ηλεκτρονικό]. Available: https://www.enisa.europa.eu/news/enisa-news/enisa-report-concepts-and-recommendations-on-european-data-protection-certification-mechanisms.

[20] T. H. Davenport, «Big Data,» 2013. [Ηλεκτρονικό]. Available: https://www.sas.com/en_us/insights/big-data/what-is-big-data.html.

[21] karfitsa.gr, «Δικαστική απόφαση-σταθμός κατά του Facebook!,» karfitsa.gr, 6 October 2015. [Ηλεκτρονικό]. Available: https://www.karfitsa.gr/dikastiki-apofasi-stathmos-kata-toy-facebook.