Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Κοινωνικά Πληροφοριακά Συστήματα

Μεταπτυχιακή Διατριβή

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

Θωμάς Δελαβίνιας

Επιβλέπουσα Καθηγήτρια
Αλεξάνδρα Μιχώτα

Νοέμβριος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Κοινωνικά Πληροφοριακά Συστήματα

Μεταπτυχιακή Διατριβή

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

Θωμάς Δελαβίνιας

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.

Νοέμβριος 2019

Περίληψη

Ο νέος κανονισμός γενικής προστασίας δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης τέθηκε σε ισχύ στις 22 του Μαΐου 2018. Κάθε οργανισμός που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα των πολιτών της ΕΕ πρέπει να συμμορφώνεται με τον προαναφερθέντα κανονισμό. Στόχος της συγκεκριμένης πτυχιακής εργασίας είναι ο καθορισμός, παρουσίαση και ανάλυση των βημάτων που θα πρέπει να ακολουθήσουν οι δημιουργοί Κοινωνικών Πληροφοριακών Συστημάτων (ΚΠΣ) προκειμένου να συμμορφώνονται με τις απαιτήσεις του Ευρωπαϊκού Κανονισμού περί της προστασίας των προσωπικών δεδομένων (GDPR). Μετά από μία εκτενή βιβλιογραφική ανασκόπηση αναφορικά με τα βασικά δομικά στοιχεία των ΚΠΣ, όπως και της νομοθεσίας, επικεντρωνόμαστε σε συγκεκριμένα ερευνητικά ερωτήματα σχετικά με το πώς η νέα νομοθεσία του GDPR επηρεάζει τη ροή των δεδομένων σε ένα ΚΠΣ και ποιες είναι οι επιπτώσεις σχετικά με την προστασία των δεδομένων. Μελετούμε τις αποκλίσεις, και καταθέτουμε προτάσεις για την εναρμόνιση ενός ΚΠΣ με τις απαιτήσεις προστασίας των προσωπικών δεδομένων της νομοθεσίας.

Στην παρούσα μεταπτυχιακή διατριβή, η οποία εμπίπτει στον τομέα κοινωνικών πληροφοριακών συστημάτων μελετήθηκε το ερώτημα αν η νέα αυτή νομοθεσία καθορίζει με ακρίβεια το πλαίσιο προσαρμογής των λειτουργιών και των δεδομένων για την προστασία των προσωπικών δεδομένων ή αλλιώς την αποφυγή αποκλίσεων. “Μπορούν οι σχεδιαστές να αξιολογήσουν και να καθορίσουν σε ποιο λογικό επίπεδο πρέπει να αλλάξει το Πληροφοριακό Σύστημα για να ανταποκριθεί στις απαιτήσεις του GDPR;” “Έχει οριστεί κάποιο πρότυπο ή μοντέλο που μπορεί να καθοδηγήσει την προσαρμογή του ΚΠΣ σε όλους τους τομείς;”

Abstract

The new regulation of the European Union about Data Protection (GDPR) has been enforced since 22 May 2018. Any organization that processes personal data of EU citizens must comply with the Regulation. The objective of this thesis is to identify, present and analyze the steps that the designers of Social Information Systems (SIS) need to take in order to comply with the requirements of GDPR. After an exhaustive bibliographic review of the key SIS components as well as the compliance requirements of the regulation, we focused on identifying possible privacy risks in SIS processes and how these risks could be mitigated in an effective way. In this study, Recommendations on how GDPR compliant SIS can be developed are also provided.

The question of whether this new regulation precisely defines the framework for adapting functions and data for the protection of personal data or otherwise avoiding discrepancies has been addressed in this postgraduate thesis in the field of social information systems. “Can designers evaluate and determine at what level the Information System needs to change to meet GDPR requirements?” “Is there a template or model that can guide the adaptation of the CSF to all areas?”.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια μου κα Αλεξάνδρα Μιχώτα για την υπομονή της καθώς και την πολύτιμη βοήθεια της καθόλη την διάρκεια της εκπόνησης της μεταπτυχιακής μου διατριβής. Επίσης θα ήθελα να ευχαριστήσω τους γονείς μου που πίστεψαν σε μένα και στις δυνατότητές μου.

Πίνακας Περιεχομένων

Κεφάλαιο 1
Εισαγωγή

Ο νέος κανονισμός της Ευρωπαϊκής Ένωσης, ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), τέθηκε σε ισχύ στις 25 Μαΐου 2018. Κάθε οργανισμός που δραστηριοποιείται στην Ευρωπαϊκή Ένωση θα πρέπει ήδη να έχει προετοιμαστεί να καταστεί συμβατός με τον GDPR. Ο GDPR αυξάνει τα δικαιώματα των ατόμων (φυσικών προσώπων) να αναλάβουν τον έλεγχο των δικών τους δεδομένων. Η θεωρητική βάση του GDPR εισάγει έξι αρχές προστασίας της ιδιωτικής ζωής. Επιπλέον, τα δικαιώματα ενός φυσικού προσώπου έχουν απαριθμηθεί βάσει του νέου κανονισμού.

Το κείμενο του GDPR είναι πολύπλοκο και εισάγει αρκετές προκλήσεις για όσους θέλουν να οργανώσουν κοινωνικές έρευνες ή εργασίες (πχ ανάπτυξη λογισμικού ανοιχτού κώδικα) ή ανάλυση δεδομένων από κοινωνικά μέσα μέσω ενός πληροφοριακού συστήματος. Στρατηγικές συμμόρφωσης με τον GDPR πρέπει να παρουσιαστούν στο τρόπο σχεδίασης και λειτουργίας των Κοινωνικών Πληροφοριακών Συστημάτων (ΚΠΣ) και πολλές από αυτές θα είναι δύσκολο να ερμηνευτούν χωρίς γνώση ενός συγκεκριμένου τομέα. Ως εκ τούτου, οι ίδιες οι κοινότητες- χρήστες ενός ΚΠΣ θα πρέπει να γνωρίζουν τις συνέπειες του GDPR και να το αντικατοπτρίζουν.

Στόχος της συγκεκριμένης πτυχιακής εργασίας είναι ο καθορισμός, παρουσίαση και ανάλυση των βημάτων που θα πρέπει να ακολουθήσουν οι δημιουργοί Κοινωνικών Πληροφοριακών Συστημάτων (ΚΠΣ) προκειμένου να συμμορφώνονται με τις απαιτήσεις του Ευρωπαϊκού Κανονισμού περί της προστασίας του απορρήτου των

προσωπικών δεδομένων (GDPR). Βασικά ερευνητικά ερωτήματα που καλείται η εργασία να απαντήσει και να παραθέσει μια λεπτομερή προσέγγιση είναι τα εξής:

- Καταγραφή της ροής των δεδομένων που εισέρχονται στα Κοινωνικά Πληροφοριακά Συστήματα
- Εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων
- Ανάλυση των αποκλίσεων
- Διατύπωση προτάσεων για την εναρμόνιση τους με τις απαιτήσεις προστασίας των προσωπικών δεδομένων βάσει GDPR.

1.1 Ορισμοί

1.2 Σκοπός και Στόχοι Έρευνας

Ο βασικός σκοπός της παρούσας διατριβής είναι να διερευνηθεί ο καθορισμός, η παρουσίαση και ανάλυση των βημάτων που θα πρέπει να ακολουθήσουν οι κατασκευαστές Κοινωνικών Πληροφοριακών Συστημάτων (ΚΠΣ) προκειμένου να συμμορφώνονται με τις απαιτήσεις του Ευρωπαϊκού Κανονισμού περί της προστασίας της ιδιωτικότητας, Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR).

Σε αυτήν την διατριβή μελετάται αν υπάρχει κάποιο πρότυπο ή μοντέλο που να καθοδηγεί:

(α) τη χαρτογράφηση των προσωπικών δεδομένων και τις επιπτώσεις στη ροή των δεδομένων μέσω του συστήματος

(β) τη συσχέτιση των νέων πολιτικών πρόσβασης που πρέπει να οριστούν σε σχέση με τους υφιστάμενους και νέους ρόλους που πρέπει να δημιουργηθούν σε ένα ΚΠΣ

(γ) τα GDPR χαρακτηριστικά του Πληροφοριακού Συστήματος

(δ) την ενσωμάτωση της νομοθεσίας στις λειτουργίες και τα δεδομένα του Συστήματος

(ε) την παρακολούθηση των αλλαγών, των επιπτώσεων και των αποκλίσεων

1.3 Δομή της Διατριβής

Στο Κεφάλαιο 2 γίνεται ανασκόπηση βιβλιογραφίας όσο αναφορά τα βασικά στοιχεία των ΚΠΣ, τις βασικές κατηγορίες και λειτουργείες τους, τον σχεδιασμό τους και την προστασία των προσωπικών δεδομένων μέσα σε αυτά. Επίσης αναλύεται η Ευρωπαική Νομοθεσία προστασίας των προσωπικών δεδομένων και πραγματοποιείται καταγραφή της ροής των δεδομένων που εισέρχονται στα Κοινωνικά Πληροφοριακά Συστήματα σε σχέση με τον GDPR.

Στο Κεφάλαιο 3 γίνεται αναφορά στην προστασία των δεδομένων, στην χαρτογράφηση των προσωπικών δεδομένων, ποιος έχει πρόσβαση στα δεδομένα, και αναφέρεται μια διαδικασία κοινοποίησης πιθανής παραβίασης δεδομένων. Στην συνέχεια παρουσιάζονται προτάσεις για την μελλοντική εναρμόνιση των ΚΠΣ με τις απαιτήσεις του GDPR.

Τέλος στο κεφάλαιο 4 παρουσιάζονται τα τελικά συμπεράσματα.

Κεφάλαιο 2
Ανασκόπηση της βιβλιογραφίας

Η αποτελεσματική μελέτη των ΚΠΣ βασίζεται σε ένα ευρύ φάσμα τεχνολογιών και των επιστημών, συμπεριλαμβανομένης της επιστήμης των υπολογιστών, της οικονομίας, της ψυχολογίας και της κοινωνιολογίας. Η κοινωνική πληροφορική αναφέρεται σε συστήματα ανθρώπων και ηλεκτρονικών υπολογιστών που συνδέονται ηλεκτρονικά, με υπολογισμούς που πραγματοποιούνται μέσω κοινωνικών όσο και αλγοριθμικών μηχανισμών. Ουσιαστικά, η έννοια του υπολογισμού αναφέρεται στην ανάγκη οι Η/Υ να συμπεριλαμβάνουν και τα προϊόντα των ανθρώπινων διαδικασιών και αλληλεπίδρασης.

2.1 Βασικά στοιχεία των Κοινωνικών Πληροφοριακών Συστημάτων

Τα περισσότερα ΚΠΣ είναι παρόμοια όσον αφορά τις βασικές δομές και τα στοιχεία τους, παρά το γεγονός ότι χρησιμοποιούνται για πολλούς διαφορετικούς σκοπούς. Συνήθως, τα βασικά στοιχεία είναι: χρήστες, προφίλ, δίκτυο (γράφημα) κοινωνικών σχέσεων, πόροι και υπηρεσίες.

Οι χρήστες είναι η βασική οντότητα στα ΚΠΣ, που εκπροσωπούν άτομα και συλλογικές κοινωνικές μονάδες. Οι χρήστες μπορούν να παράσχουν πληροφορίες

σχετικά με τον εαυτό τους, που αποτελούν το προφίλ του χρήστη. Το προφίλ ενός χρήστη δείχνει την ταυτότητα του καθώς περιλαμβάνει προσωπικές πληροφορίες, όπως: όνομα, ηλικία, φύλο και ημερομηνία γέννησης. Η δημιουργία προφίλ πραγματοποιείται αμέσως μετά την εγγραφή από το χρήστη σε κάποια ΚΠΣ, γεγονός που τον καθιστά άμεσα συνδεδεμένο και ορατό με τους άλλους χρήστες. Οι Tapiador και Carrera (2012) μελέτησαν 16 διαφορετικά ΚΠΣ (Facebook, LiveJournal, MySpace, Orkut, Twitter, XING, LinkedIn, Flickr, Badoo, deviantART, StumbleUpon,Taringa!, Tagged, SoundCloud, Viadeo), και κατέληξαν ότι τα πιο δημοφιλή στοιχεία σε ένα προφίλ είναι:

- Avatar: εικόνα που αντιπροσωπεύει τον χρήστη
- Λίστα επαφών (ονομάζεται επίσης ως λίστα φίλων): περιλαμβάνει όλες τις επαφές του χρήστη
- Ημερολόγιο ενεργειών: μια σύνοψη των πρόσφατων ενεργειών που σχετίζονται με το χρήστη.
- «Τοίχος»: επιτρέπει στο χρήστη και σε άλλους να δημοσιεύουν δραστηριότητες, να προσθέτουν ή να δημιουργούν οποιοδήποτε τύπο περιεχομένου εντός του ΚΠΣ.

Το δίκτυο (γράφημα) κοινωνικών σχέσεων δημιουργείται από τις κοινωνικές σχέσεις των χρηστών εντός του ΚΠΣ. Οι σχέσεις στο γράφημα μπορεί να είναι συμμετρικές ή ασύμμετρες (Tapiador και Carrera, 2012). Για τη δημιουργία συμμετρικών (επίσης αποκαλούμενων αμφίδρομων) σχέσεων, ένας χρήστης στέλνει ένα "αίτημα φιλίας" σε ένα άλλο μέλος και εφόσον γίνεται αποδεκτό, δημιουργείται μια σύνδεση όπου κάποιος μπορεί να δημοσιεύσει στον τοίχο του φίλου και αντίστροφα.

Για να δημιουργηθούν ασύμμετρες (επίσης αποκαλούμενες μονοκατευθυντικές) σχέσεις, οι χρήστες δεν χρειάζονται "αιτήματα φιλίας" που πρέπει να επιβεβαιωθούν και ένας χρήστης "ακολουθεί" (π.χ. Twitter) έναν άλλο χρήστη. Συνήθως, ένα κοινωνικό δίκτυο μπορεί να έχει εκατοντάδες άμεσες και έμμεσες συνδέσεις με φίλους, οικογένειες, γνωστούς και συναδέλφους. Επί του παρόντος, τα

πιο γνωστά ΚΠΣ παρέχουν επίσης αρκετούς τρόπους για να βοηθήσουν τους χρήστες να δημιουργήσουν το δικό τους κοινωνικό γράφημα (δηλαδή προτάσεις φιλίας ή συλλογή από βιβλία διευθύνσεων και άλλες λίστες επαφών).

Οι πόροι είναι περιεχόμενο που αντιπροσωπεύουν τα περιουσιακά στοιχεία των χρηστών. Ένα στοιχείο για έναν χρήστη είναι μια συλλογή σχετικών κομματιών περιεχομένου, που μοιράζονται με ή από τον χρήστη. Οι χρήστες μπορούν να μεταφορτώσουν, να προσθέσουν ή να δημιουργήσουν περιεχόμενο στο διαδικτυακό τους χώρο που είναι γενικά προσωπικά και μερικές φορές ευαίσθητα δεδομένα. Παραδείγματα αυτών των περιεχομένων είναι: τα προφίλ, το κοινωνικό τους δίκτυο, τα μηνύματα, οι εικόνες, τα βίντεο, μεταξύ άλλων.

Τα περισσότερα από τα τρέχοντα ΚΠΣ έχουν μια πληθώρα εσωτερικών υπηρεσιών, όπως ειδήσεις, παιχνίδια, εφαρμογές και ετικέτες. Για να ενεργοποιηθεί η επικοινωνία μεταξύ χρηστών, οι υπηρεσίες των ΚΠΣ συνήθως αφορούν κοινές υπηρεσίες μηνυμάτων, όπως μηνύματα ηλεκτρονικού ταχυδρομείου, συνομιλίες, μηνύματα κειμένου, blogging και υπηρεσίες τηλεφωνίας μέσω Διαδικτύου. Ένας άλλος τύπος σχετικής υπηρεσίας είναι η ανταλλαγή περιεχομένου (π.χ. χρησιμοποιώντας κουμπιά "like", "share", "follow" ή "send"), τα οποία μπορούν να αποκαλύψουν απόψεις για ένα συγκεκριμένο θέμα.

Πολλές εφαρμογές τρίτου μέρους που αλληλεπιδρούν με τις πλατφόρμες ΚΠΣ, αλλά βασίζονται σε εξωτερικούς διακομιστές παρέχουν επιπρόσθετες υπηρεσίες. Δύο σημαντικά παραδείγματα είναι το API (Application Programming Interface) του Facebook, το οποίο επιτρέπει στα μέλη να έχουν πρόσβαση σε πολλές εφαρμογές εκτός του Facebook (2007) και το Open Social της Google, το οποίο παρέχει πρόσβαση σε εφαρμογές στο κοινωνικό δίκτυο, καθώς και υπηρεσία ανταλλαγής μηνυμάτων και ροές δεδομένων (Google, 2007). Το μεγαλύτερο πλεονέκτημα του API Open Social API της Google είναι η διαλειτουργικότητα με άλλα ΚΠΣ.

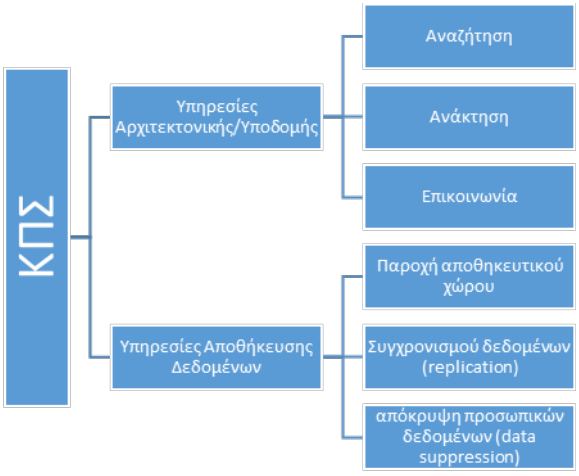
Αυτά τα κοινά βασικά στοιχεία επιτρέπουν στους χρήστες να παρουσιάζονται και να αλληλεπιδρούν με αποτελεσματικό τρόπο μέσα στο ΚΠΣ. Ως εκ τούτου, οι χρήστες μπορούν να λάβουν τα οφέλη που συνδέονται με διαφορετικούς τύπους

ΚΠΣ όπως η (κοινωνική) εργασία, οι οικογενειακές και φιλικές σχέσεις, μεταξύ άλλων.

2.2 Βασικές κατηγορίες και λειτουργίες των ΚΠΣ

Οι Beye et all (2010) διαχωρίζουν τα ΚΠΣ σε δύο κατηγορίες: αυτά που προσανατολίζονται στη Διασύνδεση των χρηστών και αυτά που προσανατολίζονται στο Περιεχόμενο. Τα ΚΠΣ που εστιάσουν στη Διασύνδεση των χρηστών είναι πληροφοριακά συστήματα με επίκεντρο τον χρήστη και στη διασύνδεση του με άλλους χρήστες αναπτύσσοντας φιλικές, επιχειρηματικές και άλλες κοινωνικές σχέσεις. Τα ΚΠΣ που εστιάζουν στο Περιεχόμενο είναι εφαρμογές που επικεντρώνονται στο περιεχόμενο (διαμοιρασμός και συνεργασία στην εξέλιξη ανοικτού κώδικα, φόρουμ προτάσεων και αλληλο-υποστήριξης, ανταλλαγής προτάσεων, ιστότοποι με κοινά ενδιαφέροντα, και ειδήσεις) που παρέχεται ή συνδέεται από τους χρήστες.

Μέσα από την βιβλιογραφία, οι περισσότεροι μελετητές των ΚΠΣ καταλήγουν σε δύο βασικές κατηγορίες λειτουργιών ενός ΚΠΣ: υπηρεσίες υποδομής/αρχιτεκτονικής και υπηρεσίες αποθήκευσης/διαχείρισης δεδομένων.



Εικόνα 1. Βασικές λειτουργίες του ΚΠΣ

- Υπηρεσίες υποδομής/αρχιτεκτονικής: καλύπτει τις βασικές υπηρεσίες που παρέχει το ΚΠΣ, όπως η αναζήτηση, ανάκτηση πληροφοριών και η επικοινωνία. Η αναζήτηση είναι ο μηχανισμός εντοπισμού των δεδομένων και των χρηστών στο ΚΠΣ. Η ανάκτηση είναι ο μηχανισμός μέσω του οποίου ανταλλάσσονται δεδομένα μεταξύ των οντοτήτων (χρήστες, πάροχοι υπηρεσιών και τρίτα μέρη). Η επικοινωνία καθορίζει τον τρόπο με τον οποίο τα δεδομένα μεταδίδονται μεταξύ των οντοτήτων.
- Υπηρεσίες αποθήκευσης δεδομένων: περιγράφει τον τρόπο με τον οποίο διατηρούνται οι πληροφορίες στο σύστημα, ειδικά το περιεχόμενο που χρήστες μεταφορτώνουν στο σύστημα, όπως εικόνες, προσωπικά δεδομένα, μεταξύ άλλων. Ο χώρος αποθήκευσης ορίζει τον χώρο όπου αποθηκεύονται τα δεδομένα χρηστών. Ο συγχρονισμός δεδομένων υποδεικνύει ποια οντότητα είναι υπεύθυνη για τον συγχρονισμό προφίλ και πόρων. Ενώ η υπηρεσία απόκρυψης δεδομένων προσδιορίζει τον ρόλο που έχει αρμοδιότητα για τη διαγραφή δεδομένων από το σύστημα (για παράδειγμα, όταν ένας χρήστης κλείνει το λογαριασμό του).

Αυτές οι λειτουργίες μπορούν να υλοποιηθούν με κεντρικοποιημένο ή κατανεμημένο τρόπο, ανάλογα με τις προτιμήσεις του σχεδιαστή.

2.3 Σχεδιασμός Κοινωνικών Πληροφοριακών Συστημάτων

Σήμερα, τα περισσότερα ΚΠΣ βασίζονται σε κεντρικές υπηρεσίες αποθήκευσης και αρχιτεκτονικής. Τα κεντρικοποιημένα ΚΠΣ είναι υπηρεσίες ιστού που έχουν έντονα ιεραρχική αρχιτεκτονική και ενιαία και κεντρική αρχή με αποκλειστικό έλεγχο από τη διοίκηση. Είναι υπεύθυνα για τη συλλογή πληροφοριών, τη διατήρηση όλων των πληροφοριών και των σχέσεων των χρηστών. Αυτά τα κεντρικοποιημένα ΚΠΣ συνήθως υλοποιούνται ως εφαρμογές πελάτη-διακομιστή, στις οποίες η κεντρική

αρχή είναι υποχρεωμένη να διαχειρίζεται τις δραστηριότητες των χρηστών, να είναι υπεύθυνη για τη δρομολόγηση επικοινωνιών, να αναζητά φίλους και δεδομένα και την ανάκτηση περιεχομένου εξ ονόματος των χρηστών κάνοντας χρήση κοινού υλικού και πλατφόρμες λογισμικού. Ένα σημαντικό πλεονέκτημα ενός κεντρικοποιημένου ΚΠΣ είναι η δυνατότητα ενημέρωσης και η διατήρηση του συστήματος. Μερικά από τα πιο κοινά παραδείγματα είναι το Facebook, το Twitter, LinkedIn και MySpace.

Κεντρικές υποδομές αποθήκευσης και διαχείρισης των δεδομένων περιλαμβάνουν όλες τις πληροφορίες και δίκτυα των χρηστών. Αυτές οι συλλογές δεδομένων συγκεντρώνονται μέσα σε ένα σύμπλεγμα ή κέντρο δεδομένων. Περιέχουν πολύτιμη συλλογή προσωπικών πληροφοριών και το προφίλ χρηστών (π.χ., απόψεις, λεπτομέρειες και άλλο περιεχόμενο που δημιουργεί ο χρήστης), το οποίο είναι πολύ χρήσιμο για τη διαφημιστική βιομηχανία (T. Paul et al, 2011). Το επιχειρηματικό μοντέλο του κεντρικοποιημένου ΚΠΣ βασίζεται συνήθως στα κέρδη από τη διαφήμιση. Συνεπώς τα έσοδα και η αξία ενός τέτοιου ΚΠΣ αυξάνεται με τον αριθμό των μελών του (G. Pallis et al, 2011).

Προκειμένου να επιτευχθεί ισχυρότερος έλεγχος, έχει γίνει πολύ προσπάθεια για την αποκέντρωση των ΚΠΣ. Τα αποκεντρωμένα ΚΠΣ είναι κοινωνικά δίκτυα που υλοποιούνται πάνω σε πλατφόρμες διαχείρισης κατανεμημένων πληροφοριών. Έχουν εμφανιστεί τα τελευταία πέντε χρόνια στη βιβλιογραφία. Πράγματι, με την αποκέντρωση των ΚΠΣ, η έννοια ενός παρόχου υπηρεσιών μπορεί να αντικατασταθεί από ένα σύνολο ίσων κατανεμημένων μερών (peers). Αυτές οι διάφορες οντότητες διανέμουν τον έλεγχο και την αποθήκευση, μοιράζοντας το φόρτο εργασίας για την διαχείριση του συστήματος και την επιβολή πολιτικών απορρήτου (A. Datta et al, 2010).

Ωστόσο η αποκέντρωση των υπαρχουσών λειτουργιών του ΚΠΣ έχει να αντιμετωπίσει έναν σημαντικό αριθμό προκλήσεων δεδομένου ότι τμήματα του ΚΠΣ, ή ακόμη και ολόκληρο το σύστημα, δεν λειτουργούν πλέον κεντρικά. Οι Buchegger και Datta (2009) αναφέρουν εννέα προκλήσεις στον σχεδιασμό

αποκεντρωμένων ΚΠΣ: αποθήκευση, ενημερώσεις, αναζήτηση και διευθυνσιοδότηση, τοπολογία, υποδοχή νέων εφαρμογών, ασφάλεια, ευελιξία, επιβολή περιορισμών στα μέλη και γεωγραφικός προσδιορισμός.

Για παράδειγμα, σε αποκεντρωμένα ΚΠΣ, ο τρόπος διατήρησης της διαθεσιμότητας των δεδομένων όταν ο ιδιοκτήτης των δεδομένων δεν είναι συνδεδεμένος, καθώς και ο καθορισμός του απαραίτητου αριθμού αντιγράφων για τον συγχρονισμό του προφίλ ενός χρήστη είναι σημαντικές παράμετροι στον σχεδιασμό του τρόπου κατανεμημένης αποθήκευσης δεδομένων. Συνήθως επιτυγχάνεται με διάθεση πλεονασμού πόρων, υποθέτοντας ότι οι φίλοι ενός χρήστη είναι σε θέση να παρέχουν επαρκή χωρητικότητα αποθήκευσης σε όλα τα δημοσιευμένα δεδομένα.

Σε μία κατανεμημένη αποθήκευση και αναπαραγωγή είναι δύσκολο να συγχρονίζονται οι κοινωνικές ενημερώσεις μεταξύ των συνομηλίκων, ειδικά εάν οι ζώνες ώρας τους είναι διαφορετικές. Ομοίως, η αναζήτηση και η διευθυνσιοδότηση σχετίζονται με ενημερώσεις, με μια έννοια που οι χρήστες θα πρέπει να είναι σε θέση να ανακαλύψουν τους φίλους τους από πραγματικές σχέσεις καθώς και περιεχόμενο που αφορά τα συμφέροντά τους. Μετά τον εντοπισμό των όποιων συνδέσεων, είναι σημαντικό μετά να καθοριστεί ο τρόπος με τον οποίο οι χρήστες μπορούν να συνδεθούν, σχηματίζοντας την τοπολογία του ΚΠΣ.

Γενικότερα, τρια διαφορετικά κίνητρα σχεδιασμού ΚΠΣ περιλαμβάνουν 1) οικονομικά κίνητρα, 2) μη οικονομικά κίνητρα, 2) αλληλεπίδραση και συντονισμός ομαδικών προσπαθειών.

2.3.1 Οικονομικά κίνητρα

Αναμφισβήτητα το πιο σημαντικό ερώτημα στα ΚΠΣ είναι ο τρόπος με τον οποίο οι άνθρωποι παρακινούνται να συνεισφέρουν, να συνεργάζονται και να επενδύουν με άλλο τρόπο στην προσωπική τους ζωή. Η πιο ξεκάθαρη μορφή είναι τα οικονομικά

κίνητρα, όπου οι χρήστες πληρώνονται για το χρόνο και τη προσπάθεια τους. Πολυάριθμες εφαρμογές τύπου crowdsourcing, όπως η Amazon Mechanical Turk (MTurk) αποζημιώνει τους ανθρώπους για τις προσπάθειες τους. Συγκεκριμένα, σε ένα έργο που πραγματοποιείται από ένα πλήθος (crowdsourcing), οι εργαζόμενοι αποζημιώνονται για την ολοκλήρωση των καθηκόντων που δημιουργούνται από τους αιτούντες.

Πράγματι, η Amazon Mechanical Turk αποτελεί το κυρίαρχο παράδειγμα μιας ηλεκτρονικής αγοράς εργασίας που καθιστά μια μεγάλη δύναμη εργαζομένων διαθέσιμη για την ανάθεση εργασιών επί πληρωμή - crowdsourcing ((P. G. Ipeirotis, 2010), (John Joseph Horton and Lydia B. Chilton, 2010)). Το MTurk φιλοξενεί ένα μεγάλο εύρος εργασιών όπως η επαλήθευση των δεδομένων, μεταφράσεις, απομαγνητοφωνήσεις. Άλλα καθήκοντα περιλαμβάνουν ανθρωπο-τεχνικές μελέτες και πειράματα συμπεριφοράς (P. G. Ipeirotis, 2010). Οι εργαζόμενοι που εκτελούν τα καθήκοντα μέσω της MTurk γνωρίζουν συχνά την αποζημίωσή τους και προσπαθούν να εντοπίσουν τα πιο προσοδοφόρα και πιο ενδιαφέροντα καθήκοντα (Chandler et al., 2013). Παρατηρήθηκε επίσης ότι η MTurk διευκολύνει την άμεση συγκέντρωση ομάδας συμμετεχόντων για έρευνα που χρησιμοποιεί ανθρώπους σε πολλούς τομείς (Paolacci et al., 2010, (Jon Sprouse, 2011) , Berinsky et αϊ. 2012, (W. Mason and S. Suri, 2013), Crump et αϊ. 2013).

Οι ηλεκτρονικές αγορές εργασίας περιλαμβάνουν επίσης άλλα συστήματα όπως ODesk, CrowdFlower και MobileWorks, καθώς και υβριδικά ψηφιακά / φυσικά συστήματα όπως το TaskRabbit και το Elance. Ανοιχτού τύπου πλατφόρμες καινοτομίας όπως οι 99designs, InnoCentive και Kaggle οργανώνουν ηλεκτρονικούς διαγωνισμούς υποβολής σχεδίων, αλγορίθμων μηχανικής μάθησης ή άλλων τεχνικών για να αποφασιστεί η καλύτερη επιλογή. Εταιρείες όπως η TaskRabbit και η Uber δημιούργησαν αγορές για crowdsourcing, στις οποίες οι φυσικές συναλλαγές διευκολύνονται από συστήματα επικοινωνιών και αντιστοίχησης αναγκών σε ικανότητες και διαθεσιμότητα (skill/availability matching).

2.3.2 Κοινωνικά και μη-οικονομικά κίνητρα

Παρά την απουσία οικονομικών κινήτρων ή ρητών ανταμοιβών, πολλά ΚΠΣ εξακολουθούν να παρουσιάζουν μεγάλα ποσοστά συμμετοχής των χρηστών. Τα μη χρηματικά κίνητρα συχνά συνδυάζονται ή υποκαθιστούν τα νομισματικά κίνητρα στα λεγόμενα συστήματα ομότιμης παραγωγής (peer production) όπου οι χρήστες μπορούν να ανταμείβονται με φήμη, αναγνώριση ή εγγενές ενδιαφέρον. Άλλοι κοινωνικοί κανόνες όπως η αμοιβαιότητα και ο αλτρουισμός συμβάλλουν επίσης στη συμβολή των χρηστών (Ernst Fehr and Klaus M Schmidt, 2006).

Παραδείγματα ομότιμης παραγωγής περιλαμβάνουν τη Wikipedia, η οποία έχει αντικαταστήσει άλλες προηγούμενες μορφές εγκυκλοπαίδειας από την άποψη της ποσότητας γνώσεων και της ικανότητάς της να συμβαδίζει με τις πρόσφατες εξελίξεις. Ωστόσο λειτουργεί με ένα μοντέλο σχεδόν ανοικτής επεξεργασίας και με βάση τη δυνατότητα των μελών της κοινότητας να ενημερώνουν τα άρθρα και τις όποιες αλλοιώσεις (Priedhorsky et al., 2007, (Aniket Kittur and Robert E. Kraut, 2008)). Η εκτεταμένη συνεργασία σε έργα από κοινότητες ανοιχτού κώδικα, όπως το GitHub βασίζεται επίσης στα ποικίλα κίνητρα των συμμετεχόντων χρηστών (Dabbish et al., 2012).

Πολλά ΚΠΣ εξαρτώνται από τη συμμετοχή των χρηστών για να είναι επιτυχημένα. Διαδικτυακές πύλες όπως το Reddit και το Hacker News χρησιμοποιούν ένα συνδυασμό αλγορίθμων αξιολόγησης της συμμετοχής και κατάταξης των χρηστών για τον εντοπισμό και τη διανομή του επιθυμητού περιεχομένου. Αυτά τα συστήματα πρέπει να σχεδιάζονται και με τα δύο για να προωθήσουν τις συνεισφορές των χρηστών και να προσδιορίσουν τη ποιότητα του περιεχομένου για να δημιουργήσουν μια βιώσιμη κοινότητα (Greg Stoddard, 2015). Τα συστήματα ερωτημάτων-απαντήσεων (Q&A), όπως το StackOver, βασίζονται στις ενέργειες των χρηστών που είναι σταθερά συνδεδεμένοι, όπως και των περιστασιακών επισκεπτών για τη δημιουργία ενός αποθετηρίου χρήσιμων προγραμματιστικών γνώσεων (Anderson et al., 2013).

2.3.3 Αλληλεπίδραση και συντονισμός ομάδων

Η πρόσβαση στο διαδίκτυο έχει δημιουργήσει νέα παραδείγματα διαπροσωπικής επικοινωνίας, επιτρέποντας τη διάδοση των πληροφοριών στα ενδιαφερόμενα μέρη με πολύ ταχύτερο ρυθμό από ότι αν γινόταν με τα παραδοσιακά μέσα. Οι αρχικές μορφές κοινωνικής επικοινωνίας με ηλεκτρονικό τρόπο περιλάμβαναν αποκεντρωμένα συστήματα ηλεκτρονικού ταχυδρομείου, ανταλλαγής άμεσων μηνυμάτων και ιστολόγια, τα οποία απαιτούσαν σημαντική χειροκίνητη προσπάθεια από τους χρήστες. Παρά τις υποψίες ότι τα ηλεκτρονικά μέσα μπορεί να επιτρέψουν την εξαπάτηση των χρηστών, απουσία συναισθηματικών και φυσικών δεικτών στην επικοινωνία (Carlson et al., 2004), Hancock et αϊ. (2007), διαπιστώθηκε ότι μέσα, όπως το ηλεκτρονικό ταχυδρομείο, στην πραγματικότητα αυξήσαν την ειλικρινή επικοινωνία των ανθρώπων.

Πιο πρόσφατα, κοινωνικά δίκτυα όπως το Facebook και το Twitter συνδέουν τους χρήστες που συνδέονται με κάποια διαπροσωπική σχέση μεταξύ τους και διευκολύνουν την εξάπλωση και την κατανάλωση πληροφοριών. Τέτοια δίκτυα ενδέχεται να έχουν σημαντικό αντίκτυπο στη συμπεριφορά των χρηστών τους. Για παράδειγμα, ένα πείραμα του Facebook το 2010 αύξησε την προσέλευση ψηφοφόρων στις εκλογές του Κογκρέσου των ΗΠΑ κατά περίπου 340.000 άτομα (Bond et al., 2012). Η διάδοση των πληροφοριών στο Twitter έχει προταθεί ως ένας τρόπος για την κατασκευή κοινωνικών ανιχνευτών σεισμού (Sakaki et al., 2010) και για την ανάλυση συλλογικών συναισθημάτων στην πρόβλεψη των χρηματιστηριακών κινήσεων.

2.4 Προστασία των προσωπικών δεδομένων σε ΚΠΣ

Το βασικό χαρακτηριστικό ενός ΚΠΣ είναι η δημιουργία προφίλ χρηστών και οι κοινωνικές τους σχέσεις. Μέσα στα ΚΠΣ, οι χρήστες μπορούν να επικοινωνούν μεταξύ τους, να μοιράζονται και να ανταλλάσσουν πληροφορίες. Σαν συνέπεια, μεγάλο μέρος των δεδομένων για τον εαυτό τους και τις κοινωνικές τους σχέσεις, δηλαδή περιεχόμενο που ανεβάζουν σε έναν ιστότοπο και το κοινωνικό τους δίκτυο, αποθηκεύονται στο ΚΠΣ.

Σημαντικές ανησυχίες έχουν προκύψει στο πρόσφατο παρελθόν σχετικά με τα προσωπικά δεδομένα στα προφίλ των χρηστών με αναφορές για πιθανές παραβιάσεις ή απώλειες των προσωπικών πληροφοριών των χρηστών. Η κύρια ανάγκη για προστασία της ιδιωτικής ζωής προέρχεται από την επιθυμία του χρήστη να ελέγχει αυτό που μοιράζεται με άλλους χρήστες, αφού το περιεχόμενο ανταλλαγής σταδιακά έγινε ευκολότερο, ταχύτερο και πιο άμεσο (Ellison και Boyd, 2013). Ωστόσο, τα ζητήματα απορρήτου στα ΚΠΣ σχετίζονται επίσης με το κοινωνικό δίκτυο. Πράγματι, η γνώση των κοινωνικών σχέσεων ενός χρήστη μπορεί να οδηγήσει σε σοβαρές παραβιάσεις στην ιδιωτική του ζωή.

Γενικότερα, οι απειλές ενάντια στην προστασία των προσωπικών δεδομένων ταξινομούνται σε τρεις κατηγορίες: ασφάλεια (π.χ. κλοπή προσωπικών στοιχείων, κλωνοποίηση προφίλ, ηλεκτρονικό ψάρεμα προσωπικών στοιχείων), τη φήμη και την αξιοπιστία (π.χ., εργαζόμενοι έχουν χάσει τη δουλειά τους λόγω της έκθεσης τους στα κοινωνικά μέσα) και στο προφίλ (π.χ. λήψη μηνυμάτων spam, ανεπιθύμητη συλλογή δεδομένων από το χρήστη). Οι απειλές αυτές μπορεί να προέρχονται από πολλές οντότητες σε ένα κοινωνικό δίκτυο (L. A. Cutillo et al, 2009), Chi Zhang et al, 2010):

- Κακόβουλοι χρήστες που έχουν προηγουμένως ταυτοποιηθεί επιτυχώς από το σύστημα

- Κακόβουλοι πάροχοι τρίτων εφαρμογών
- Κακόβουλες οντότητες που παραπλανούν τους χρήστες σε ταυτοποίηση εκ μέρους του συστήματος.

Από τα παραπάνω προκύπτει ότι τόσο τα κεντρικοποιημένα όσο και τα κατανεμημένα ΚΠΣ είναι ευάλωτα σε διάφορα είδη επιθέσεων. Αυτό έχει οδηγήσει στην ανάγκη επαναπροσδιορισμού της βελτίωσης του τρόπου προστασίας των προσωπικών δεδομένων μέσα σε ένα σύστημα. Σε αυτή τη προσπάθεια αναγνωρίζονται τρείς κύριες κατευθύνσεις (Aimeur et al, 2010), (Ho, 2012):

1. Ευαισθητοποίηση των χρηστών στην προστασία των προσωπικών δεδομένων και προσαρμογή: το ΚΠΣ πρέπει να ενημερώνει τον χρήστη σχετικά με τους δυνητικούς κινδύνους για την ανταλλαγή πληροφοριών με άλλους ανθρώπους. Επιπλέον, θα πρέπει να παρέχει έναν εύκολο και εύχρηστο τρόπο για τους χρήστες να εκφράζουν τις ανησυχίες τους για την προστασία των δεδομένων τους σε αναφορά μιας πολιτικής για τα προσωπικά δεδομένα. Έπειτα να τις συγκρίνουν με τις πολιτικές απορρήτου άλλων φορέων, όπως ο πάροχος του ΚΠΣ, οι πάροχοι τρίτων εφαρμογών ή άλλοι χρήστες.

2. Έκθεση των ελάχιστα απαραίτητων δεδομένων: ένα ΚΠΣ θα πρέπει να συλλέγει μόνο προσωπικά δεδομένα που είναι απολύτως απαραίτητα. Ένας χρήστης θα πρέπει να είναι σε θέση να ελέγχει εάν οι πληροφορίες του είναι προσβάσιμες από τον πάροχο του ΚΠΣ ή από παρόχους τρίτων εφαρμογών και πώς χρησιμοποιούνται αυτές οι πληροφορίες. Συγκεκριμένα,οι υπηρεσίες σε ένα ΚΠΣ πρέπει να δηλώνουν με σαφήνεια ποιες προσωπικές πληροφορίες χρειάζονται από τους χρήστες και πώς θα υποβληθούν σε επεξεργασία. Οι Aimer et all (2010) προτείνανε μία διαδικασία που επιτρέπει σε ένα χρήστη να αποφασίσει εάν αποδέχεται ή όχι τις υπηρεσίες του ΚΠΣ. Το ΚΠΣ θα πρέπει να διαθέτει ενσωματωμένο μηχανισμό για τον έλεγχο και

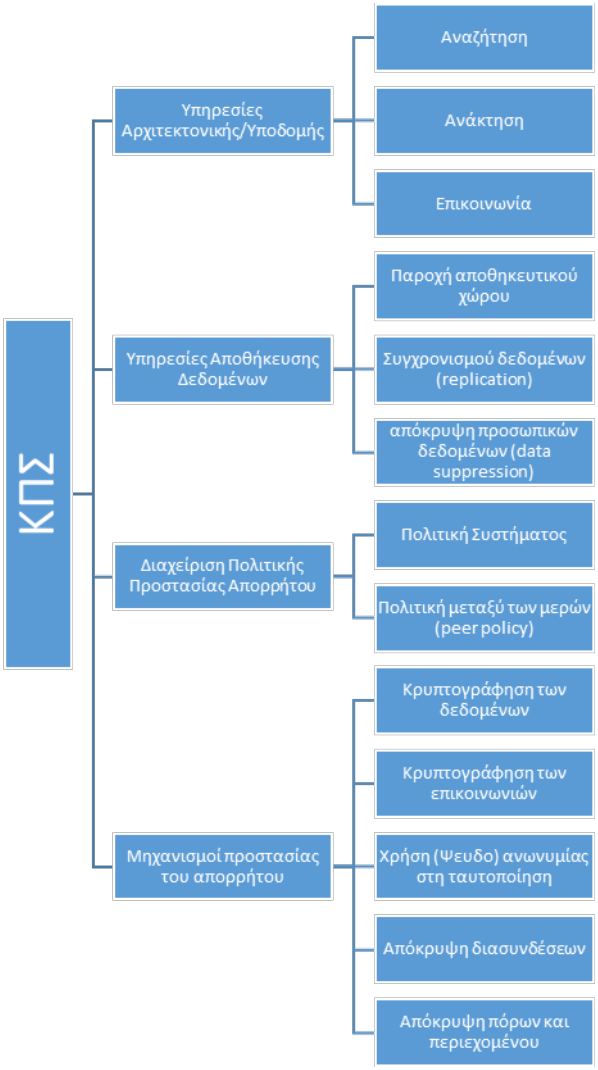
τον περιορισμό της πρόσβασης σε πληροφορίες όπως έχει εγκριθεί προηγουμένως από το χρήστη.

3. Ιδιοκτησία των δεδομένων: θα πρέπει ρητά να δηλώνεται στην πολιτική απορρήτου ότι τα προσωπικά δεδομένα ενός χρήστη ανήκουν αποκλειστικά σε αυτόν και όχι στον πάροχο του ΚΠΣ. Για παράδειγμα, ο πάροχος δεν πρέπει να χρησιμοποιεί προσωπικά δεδομένα χωρίς ρητή συγκατάθεση και δεν θα πρέπει να μπορεί να τα πουλήσει σε άλλες οντότητες. Επιπλέον, αν ο χρήστης αποφασίσει να κλείσει το ΚΠΣ, ο πάροχος θα πρέπει να διαγράψει ρητά όλες τις αποθηκευμένες πληροφορίες του χρήστη. Ένας χρήστης θα πρέπει επίσης να έχει τη δυνατότητα να παρακολουθεί τη διάδοση των πληροφοριών του, αλλά επίσης να ελέγχει προσωπικές πληροφορίες που σχετίζονται με αυτόν και δημοσιεύονται από άλλους χρήστες (π.χ. μια ετικέτα σε μια εικόνα που δείχνει στο προφίλ του).

Η ευαισθητοποίηση σχετικά με την προστασία των προσωπικών δεδομένων είναι σημαντική και ταυτίζεται με την ακριβή ενημέρωση για το ποια προσωπικά στοιχεία έχουν λάβει τα άλλα μέλη και πώς επεξεργάζονται αυτές τις πληροφορίες. Οι χρήστες ενημερώνονται συνήθως για τον τρόπο με τον οποίο οι πάροχοι υπηρεσιών ΚΠΣ διαχειρίζονται τα προσωπικά δεδομένα του χρήστη μέσω της πολιτικής προστασίας απορρήτου που παρέχεται από το σύστημα (Anton et al, 2002). Η έκθεση των ελάχιστα απαραίτητων δεδομένων είναι μία από τις βασικές αρχές για τον περιορισμό της συλλογής προσωπικών πληροφοριών και η ιδιοκτησία των δεδομένων παρέχει τα μέσα προς τον χρήστη για τον έλεγχο των προσωπικών τους πληροφοριών, συμπεριλαμβανομένης της επιλογής να αποφασίσει ποια προσωπικά δεδομένα μπορούν να συλλεχθούν από τρίτους.

Έρευνες δείξανε ότι οι σημαντικότερες απειλές στη παραβίαση ή απώλεια προσωπικών δεδομένων είναι μεγαλύτερες σε κεντρικοποιημένα ΚΠΣ παρά σε κατανεμημένα. Ειδικότερα, η πιο σημαντική απειλή στη προστασία των προσωπικών δεδομένων σε κεντρικοποιημένα ΚΠΣ προέρχεται από έναν κακόβουλο πάροχο, επειδή η αρχιτεκτονική πελάτη-διακομιστή απαιτεί όλες οι

πληροφορίες και η επικοινωνία από όλους τους χρήστες εντός των δικτύων του ΚΠΣ να διέρχεται μέσω κεντρικών εξυπηρετητών που λειτουργούν από τον πάροχο του συστήματος.



Εικόνα 2. Βασικές λειτουργίες και Πολιτικές σχετικά με το απόρρητο των προσωπικών δεδομένων του ΚΠΣ

Αντίθετα, σε κατανεμημένα ΚΠΣ, αποφεύγοντας τη συντήρηση μιας ενιαίας κεντρικής αρχής διοίκησης και κατά συνέπεια η προώθηση της μεγαλύτερης αποκέντρωσης των δεδομένων και των υπηρεσιών μεταξύ των χρηστών, το

επίπεδο προστασίας των προσωπικών δεδομένων είναι ενισχυμένο. Ως εκ τούτου, είναι σημαντικό να εξεταστούν θέματα που σχετίζονται με την προστασία των προσωπικών δεδομένων σε σχέση με το σχεδιασμό των ΚΠΣ και την αρχιτεκτονική σε διάφορα επίπεδα (Εικόνα 2).

Ωστόσο, δεν είναι σαφές ακόμη ένα πλήρες σύνολο ιδιοτήτων για τα ΚΠΣ, δεδομένου ότι τα προσωπικά δεδομένα επηρεάζονται από πολλές επιλογές στο σχεδιασμό. Αφενός, οι προκλήσεις στο σχεδιασμό είναι σε πολλά επίπεδα από την άποψη της προστασίας των προσωπικών δεδομένων, αφετέρου από τη πλευρά της διαθεσιμότητας, της ασφάλειας και της διαχείρισης.

2.5 Η Ευρωπαϊκή Νομοθεσία Προστασίας των Προσωπικών Δεδομένων (General Data Protection Regulation)

Ο κύριος στόχος της νέας νομοθεσίας είναι να προστατεύσει τους πολίτες της ΕΕ από οργανισμούς που χρησιμοποιούν παράνομα προσωπικά στοιχεία όπου αναγνωρίζουν ένα φυσικό πρόσωπο (Personally Identifiable Information - PII). Οι κυρώσεις για παραβιάσεις δεδομένων έχουν επίσης αυξηθεί και οι οργανισμοί έχουν νέες απαιτήσεις π.χ. για ειδοποιήσεις παραβίασης δεδομένων. Οι οργανισμοί που δεν συμμορφώνονται με τον GDPR θα αντιμετωπίσουν ποινές ύψους 20 εκατ. Ευρώ ή 4% του συνολικού ετήσιου κύκλου εργασιών τους.

Οι νέοι κανόνες GDPR πρέπει επίσης να βοηθήσουν τους οργανισμούς να προετοιμάσουν τις σωστές πολιτικές και διαδικασίες για την αντιμετώπιση περιστατικών ασφάλειας στον κυβερνοχώρο. Επιπλέον, ο GDPR θα αλλάξει τον τρόπο με τον οποίο οι οργανισμοί επεξεργάζονται και αποθηκεύουν προσωπικές πληροφορίες για τα φυσικά πρόσωπα. Τα δικαιώματα των πολιτών της ΕΕ πρόκειται να επεκταθούν και ο GDPR ισχύει για όλους τους οργανισμούς που

επεξεργάζονται τα προσωπικά δεδομένα των κατοίκων της ΕΕ (Γενικός κανονισμός της ΕΕ για την προστασία των δεδομένων (GDPR), Duncan 2018).

Ο GDPR τυποποιεί την προστασία των προσωπικών δεδομένων σε κάθε ευρωπαϊκή χώρα. Οι οργανισμοί πρέπει να εξετάσουν το τι προσωπικά δεδομένα επεξεργάζονται και πώς πρέπει να τα προστατεύσουν. Με τον GDPR, υπάρχουν επίσης διαφορετικοί ρόλοι που πρέπει να ανατεθούν μέσα σε κάθε οργανισμό. Συγκεκριμένα θα πρέπει να υπάρχει ο υπεύθυνος επεξεργασίας δεδομένων και ο υπεύθυνος ελέγχου των δεδομένων. Ο ελεγκτής πρέπει να καθορίσει τον τρόπο και τον λόγο για τον οποίο γίνεται επεξεργασία των προσωπικών δεδομένων και ο υπεύθυνος επεξεργασίας είναι αυτός που εκτελεί τη συγκεκριμένη διαδικασία. Ο ελεγκτής μπορεί να είναι μία εταιρεία, ένας μη κερδοσκοπικός ή κρατικός οργανισμός. Ο υπεύθυνος επεξεργασίας μπορεί να είναι μία επιχείρηση πληροφορικής.

Ακόμη και οι οργανισμοί εκτός της Ευρωπαϊκής Ένωσης που δραστηριοποιούνται στην επικράτεια της Ευρωπαϊκής Ένωσης πρέπει να εφαρμόζουν τις απαιτήσεις του κανονισμού. Μετά την ημερομηνία ενεργοποίησης της νομοθεσίας του GDPR, κάθε οργανισμός πρέπει να χειρίζεται τα προσωπικά δεδομένα νόμιμα και με διαφάνεια. Επιπλέον, η επεξεργασία των προσωπικών δεδομένων πρέπει να έχει πραγματικό σκοπό. Όταν οι προσωπικές πληροφορίες για ένα φυσικό πρόσωπο δεν απαιτούνται πλέον, οι οργανισμοί θα πρέπει να τις διαγράψουν (Curtis 2018).

2.5.1 Ορισμός προσωπικών δεδομένων

Οποιαδήποτε δεδομένα σχετίζονται άμεσα ή έμμεσα με ένα αναγνωρίσιμο φυσικό πρόσωπο είναι προσωπικά αναγνωρίσιμα στοιχεία (PII). Παραδείγματα προσωπικών στοιχείων ταυτοποίησης ενός φυσικού προσώπου είναι το όνομα, ο αριθμός ταυτότητας ή διαβατηρίου, τα δεδομένα τοποθεσίας του, η ηλεκτρονική του διεύθυνση ή η διεύθυνση IP των συσκευών του, τα φυσικά, γενετικά ή βιομετρικά δεδομένα, η ψυχική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα

του. Η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων απαγορεύεται εξ ορισμού σύμφωνα με το άρθρο 9 του GDPR. Η φυλετική, εθνική καταγωγή, οι πολιτικές απόψεις, οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τα γενετικά δεδομένα, τα βιομετρικά δεδομένα, η υγεία, η σεξουαλική ζωή ενός ατόμου ή ο σεξουαλικός προσανατολισμός μπορούν να θεωρηθούν ευαίσθητα δεδομένα. Ο GDPR παραθέτει κάποιες περιπτώσεις που επιτρέπουν σε οργανισμούς να επεξεργάζονται μια ειδική κατηγορία προσωπικών δεδομένων (Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 2016).

2.5.2 Βασικές αρχές του GDPR

Το άρθρο 5 του κανονισμού περιγράφει αρχές στις οποίες πρέπει να δίνουν προσοχή οι οργανισμοί κατά την επεξεργασία των προσωπικών στοιχείων (PII). Παρακάτω παρατίθεται ένας κατάλογος με ορισμένες αρχές επεξεργασίας των προσωπικών δεδομένων (Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 2016):

- Η επεξεργασία πρέπει να γίνεται με νόμιμη, δίκαιη και διαφανή μέθοδο.
- Τα προσωπικά δεδομένα πρέπει να συλλέγονται για συγκεκριμένους, σαφείς και νόμιμους σκοπούς και να μην έχουν υποστεί επεξεργασία με τρόπο που δεν είναι συμβατός με αυτούς τους σκοπούς.
- Τα προσωπικά δεδομένα πρέπει να είναι επαρκή, σχετικά και να περιορίζονται στους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.
- Τα προσωπικά δεδομένα πρέπει να είναι ακριβή, να ενημερώνονται, και οι οργανισμοί πρέπει να διασφαλίζουν ότι τα δεδομένα δεν είναι ανακριβή.
- Τα προσωπικά δεδομένα πρέπει να διατηρούνται σε μορφή που επιτρέπει την αναγνώριση των υποκειμένων των δεδομένων μόνο για όσο χρόνο είναι απαραίτητο.

- Τα προσωπικά δεδομένα πρέπει να υποβληθούν σε επεξεργασία κατά τρόπο που να εξασφαλίζονται και να προστατεύονται από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και να μην χαθούν τυχαία, να καταστραφούν ή αλλοιωθούν.
- Ο ελεγκτής είναι υπεύθυνος να αποδείξει ότι τα δεδομένα συμμορφώνονται με τον κανονισμό.

Η νομιμότητα, η δικαιοσύνη και η διαφάνεια μπορούν να εξηγηθούν με τον ακόλουθο τρόπο: ένας οργανισμός πρέπει να ενημερώσει ένα άτομο για τις μεθόδους επεξεργασίας δεδομένων. Επιπλέον, πρέπει επίσης να ενημερώσουν για το είδος των δεδομένων που υποβάλλονται σε επεξεργασία. Οι μέθοδοι επεξεργασίας πρέπει να ταιριάζουν με μια αναφορά ασφάλειας δεδομένων που προσφέρεται από έναν οργανισμό. Στην Εικόνα 3 παρατίθενται έξι αρχές προστασίας της ιδιωτικής ζωής του GDPR. (Οι έξι αρχές προστασίας προσωπικών δεδομένων του GDPR 2017.)

Εικόνα 3. Αρχές ιδιωτικού απορρήτου του GDPR (Οι έξι αρχές προστασίας προσωπικών δεδομένων του GDPR 2017)

Οι επαρκής στόχοι επεξεργασίας σημαίνουν ότι οι προσωπικές αναγνωρίσιμες πληροφορίες μπορούν να υποβάλλονται σε επεξεργασία για συγκεκριμένους, σαφείς και νόμιμους σκοπούς. Το υποκείμενο των δεδομένων γνωρίζει τους προαναφερθέντες σκοπούς και τα προσωπικά δεδομένα δεν χρησιμοποιούνται για περαιτέρω ενέργειες χωρίς τη συγκατάθεση του χρήστη. Συλλέγονται μόνο δεδομένα που είναι απαραίτητα και τίποτα περισσότερο (data minimisation). Ακρίβεια των δεδομένων σημαίνει ότι τα προσωπικά δεδομένα θα πρέπει να ενημερώνονται και να είναι ακριβή. Η αποθήκευση των απαραίτητων δεδομένων και μόνο σημαίνει ότι τα δεδομένα θα αποθηκεύονται μόνο για τον απαιτούμενο χρόνο και όχι πλέον αυτού. Όταν δεν υπάρχει πια σκοπός για την αποθήκευση τους, τα δεδομένα πρέπει να διαγραφούν. Η ακεραιότητα και η εμπιστευτικότητα σημαίνουν ότι τα προσωπικά δεδομένα πρέπει να αντιμετωπίζονται κατά τρόπο που εξασφαλίζονται από την παράνομη επεξεργασία ή την τυχαία καταστροφή ή αλλοίωση (Οι έξι αρχές προστασίας προσωπικών δεδομένων του GDPR 2017).

Το έκτο άρθρο του GDPR ορίζει τη νομιμότητα της επεξεργασίας (Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 2016). Ακολουθούν ορισμένα τέτοια παραδείγματα:

- Το φυσικό πρόσωπο έχει δώσει τη συγκατάθεσή του για την επεξεργασία των προσωπικών του προσωπικών στοιχείων για τουλάχιστον ένα ή περισσότερους σκοπούς.
- Το φυσικό πρόσωπο είναι μέρος μιας σύμβασης που απαιτεί επεξεργασία προσωπικών αναγνωρίσιμων στοιχείων.
- Τα ζωτικά συμφέροντα των εμπλεκομένων φυσικών προσώπων πρέπει να προστατεύονται.
- Η επεξεργασία είναι απαραίτητη από την άποψη του δημόσιου συμφέροντος ή της δημόσιας αρχής.
- Όταν πρέπει να προστατεύονται τα νόμιμα συμφέροντα του υπεύθυνου επεξεργασίας ή ενός τρίτου μέρους.

2.5.3 Τα δικαιώματα των φυσικών προσώπων μέσω του GDPR

2.5.3.1 Το δικαίωμα να ενημερωθεί

Ο κάτοχος ενός μητρώου πρέπει να δώσει τις ακόλουθες πληροφορίες σε ένα εγγεγραμμένο φυσικό πρόσωπο:

- στοιχεία επικοινωνίας του ιδιοκτήτη του μητρώου
- ποιος είναι ο σκοπός και η νομική βάση για την επεξεργασία προσωπικών στοιχείων
- εάν έχουν δοθεί προσωπικά αναγνωρίσιμα στοιχεία σε τρίτους και ποιοι είναι οι παραλήπτες των δεδομένων
- εάν οι προσωπικές αναγνωρίσιμες πληροφορίες θα μεταφερθούν σε τρίτες χώρες και ο τρόπος με τον οποίο ελήφθη υπόψη η ασφάλεια τους
- χρόνος αποθήκευσης για κάθε προσωπικά αναγνωρίσιμη πληροφορία και ποια είναι η νομική βάση για την αποθήκευση
- εάν υπάρχει αυτόματη διαδικασία λήψης αποφάσεων ή προφίλ, ποια είναι η λογική επεξεργασίας και ποιες είναι οι συνέπειες για ένα εγγεγραμμένο πρόσωπο
- τι είδους δεδομένα θα συλλεχθούν
- ποιά είναι η πηγή των προσωπικών αναγνωρίσιμων στοιχείων

2.5.3.2 Το δικαίωμα της πρόσβασης

Ένα φυσικό πρόσωπο έχει το δικαίωμα πρόσβασης στις προσωπικές του πληροφορίες, πράγμα που σημαίνει ότι ο υπεύθυνος του μητρώου πρέπει να ειδοποιήσει το φυσικό πρόσωπο σε περίπτωση επεξεργασίας οποιουδήποτε προσωπικού δεδομένου και στη συνέχεια να παραδώσει ένα αντίγραφο των προαναφερθέντων δεδομένων.

2.5.3.3 Το δικαίωμα της διόρθωσης

Ο κανονισμός GDPR παρέχει στα φυσικά πρόσωπα το δικαίωμα να απαιτούν διόρθωση για λανθασμένες πληροφορίες στα συστήματα του ιδιοκτήτη του μητρώου.

2.5.3.4 Το δικαίωμα της διαγραφής

Ένα φυσικό πρόσωπο έχει το δικαίωμα να ζητήσει από τους κατόχους μητρώων να αφαιρέσουν τις προσωπικές πληροφορίες που έχουν λήξει. Ένα άτομο έχει επίσης το δικαίωμα να ακυρώσει τη συγκατάθεσή του για την επεξεργασία δεδομένων. Επιπλέον, ένα άτομο έχει το δικαίωμα να ζητήσει τη διαγραφή των προσωπικών δεδομένων του από τα συστήματα του ιδιοκτήτη του μητρώου. Στη συνέχεια τα δεδομένα πρέπει να διαγραφούν εάν δεν υπάρχει νόμιμος σκοπός για την αποθήκευση τους.

Ο κανονισμός δεν προβλέπει απαιτήσεις από τεχνική άποψη για τη διαγραφή δεδομένων. Τουλάχιστον τα δεδομένα μπορούν να διαγραφούν, π.χ. αντικαθιστώντας τα έτσι ώστε να μην μπορούν πλέον να αναγνωριστούν φυσικά πρόσωπα από τα δεδομένα. Επιπλέον, τα δεδομένα μπορούν να επισημανθούν ως διαγραμμένα και στη συνέχεια να οριστούν περιορισμοί για τη χρήση τους σε πληροφοριακά συστήματα. Ωστόσο, με αυτόν τον τρόπο τα δεδομένα εξακολουθούν να υπάρχουν, για παράδειγμα σε μια βάση δεδομένων. Παρόλα αυτά, η απαίτηση για καταστροφή των φυσικών συσκευών που θα αποθηκεύουν τα προσωπικά δεδομένα είναι υπερβολική, επειδή μπορεί να είναι δύσκολο να βρεθούν οι θέσεις των δεδομένων, π.χ. από τα συστήματα υπολογιστικού νέφους.

2.5.3.5 Το δικαίωμα της φορητότητας των δεδομένων

Το δικαίωμα στη φορητότητα δεδομένων είναι επίσης μια νέα απαίτηση του GDPR. Ένα άτομο έχει δικαιώματα να συγκεντρώνει όλες τις προσωπικές του πληροφορίες με κοινή δομημένη μορφή και στη συνέχεια να μεταφέρει αυτά τα δεδομένα σε συστήματα άλλου ελεγκτή ή υπεύθυνου μητρώου. Μια πτυχή αυτής της φορητότητας δεδομένων είναι ότι ένα άτομο έχει δικαίωμα να μεταφέρει τα δεδομένα απευθείας από έναν ελεγκτή / καταχωρητή σε ένα άλλο, εάν αυτό είναι τεχνικά εφικτό. Το δικαίωμα στη φορητότητα δεδομένων δεν σημαίνει ότι οι υπεύθυνοι ελέγχου και επεξεργασίας πρέπει να σχεδιάζουν και να εφαρμόζουν συμβατά συστήματα. Όταν τα συστήματα είναι διαφορετικά, τα προσωπικά δεδομένα μπορεί να μεταφερθούν π.χ. χρησιμοποιώντας ένα εξωτερικό μέσο αποθήκευσης και στη συνέχεια να γίνει η μετάπτωση τους σε άλλο σύστημα ελέγχου ή καταχώρησης.

2.5.3.6 Το δικαίωμα ενημέρωσης για παραβιάσεις δεδομένων

Μία ευθύνη για τους ελεγκτές της καταχώρησης προσωπικών δεδομένων είναι να ενημερώνουν τα εγγεγραμμένα πρόσωπα για παραβιάσεις των δεδομένων τους, ή ότι μέρος των δεδομένων αυτών έχουν διαρρεύσει. Το δικαίωμα ισχύει εάν η παραβίαση προκαλεί μεγάλους κινδύνους για τα δικαιώματα και την ελευθερία ενός ατόμου. Οι προαναφερόμενοι κίνδυνοι είναι για παράδειγμα κλοπές ταυτότητας, απάτες πιστωτικών καρτών ή άλλες εγκληματικές δραστηριότητες. Η ειδοποίηση δεν είναι υποχρεωτική εάν οι πληροφορίες διαρροής προσωπικών στοιχείων ήταν κρυπτογραφημένες και τα κλειδιά κρυπτογράφησης δεν έχουν διαρρεύσει. Ένας οργανισμός μπορεί να χρησιμοποιήσει τα κοινωνικά μέσα ενημέρωσης για την ενημέρωση σχετικά με την παραβίαση δεδομένων, εάν η ενημέρωση του εκάστοτε φυσικού προσώπου μπορεί να προκαλέσει πολύ μεγάλο φόρτο εργασίας.

Ο οργανισμός πρέπει να δώσει τα ακόλουθα στοιχεία σχετικά με τις παραβιάσεις δεδομένων στα φυσικά πρόσωπα των οποίων τα δεδομένα έχουν διαρρεύσει:

- ξεκάθαρη και απλή περιγραφή της παραβίασης των δεδομένων
- τρόποι επικοινωνίας για περισσότερες λεπτομέρειες
- περιγραφή των επιπτώσεων των δεδομένων που μπορεί να προκαλέσει η παραβίαση στα δικαιώματα και την ελευθερία ενός ατόμου
- μια περιγραφή των ενεργειών που έχει ήδη κάνει ο ιδιοκτήτης του μητρώου ή θα κάνει για τη μείωση των επιπτώσεων της παραβίασης των δεδομένων.

Εικόνα 4. Τα δικαιώματα των φυσικών προσώπων κάτω από το GDPR

2.5.4 Οι προκλήσεις του GDPR

2.5.4.1 Ενημέρωση για την παραβίαση προσωπικών δεδομένων

Τον Νοέμβριο του 2017 πραγματοποιήθηκε στις Βρυξέλλες το Συνέδριο για την Προστασία Δεδομένων IAPP Europe 2017, όπου εκατοντάδες επαγγελματίες από τον ιδιωτικό τομέα αξιολόγησαν τους κινδύνους που θα μπορούσε να προκαλέσει η νέα νομοθεσία του GDPR. Ο μεγαλύτερος κίνδυνος σχετικά με τη συμμόρφωση με τη νέα αυτή νομοθεσία ήταν για ένα οργανισμό να συμμορφωθεί με τον κανονισμό κοινοποίησης της παραβίασης δεδομένων μέσα σε 72 ώρες.

Το άρθρο 33 του GDPR ορίζει: "Σε περίπτωση παραβίασης των προσωπικών δεδομένων, ο υπεύθυνος της επεξεργασίας ενημερώνει, χωρίς αδικαιολόγητη καθυστέρηση και, εφόσον είναι εφικτό, το αργότερο εντός 72 ωρών από την επίγνωση του γεγονότος αυτού, την παραβίαση των προσωπικών δεδομένων στην αρμόδια εποπτική αρχή με το άρθρο 55, εκτός εάν η παραβίαση των προσωπικών δεδομένων είναι απίθανο να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η κοινοποίηση προς την εποπτική αρχή δεν πραγματοποιηθεί εντός 72 ωρών, πρέπει να συνοδεύεται από λόγους καθυστέρησης. " (Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 2016).

Στις ΗΠΑ υπάρχουν πάνω από 48 διαφορετικοί νόμοι περί παραβίασης. Το συντομότερο χρονικό διάστημα κοινοποίησης είναι 30 ημέρες στη Φλώριδα και για παράδειγμα η Νότια Ντακότα έχει χρονοδιάγραμμα 60 ημερών για την ανακάλυψη της παραβίασης. Η απαίτηση του GDPR είναι 72 ώρες, γεγονός που μετατρέπει ένα πρόβλημα σε αγώνα δρόμο από τη στιγμή που ανακαλύφθηκε η παραβίαση.

Οι οργανισμοί πρέπει να είναι προετοιμασμένοι να εκτελούν συγκεκριμένα καθήκοντα όταν διαπιστωθεί παραβίαση. Αυτά τα καθήκοντα είναι, για παράδειγμα: Μια τοπική εποπτική αρχή και τα φυσικά πρόσωπα πρέπει να ειδοποιούνται, ο οργανισμός πρέπει να παρέχει τη φύση της παραβίασης και να

οργανώνει διαύλους επικοινωνίας μεταξύ διαφόρων μερών σχετικά με τον αριθμό των προσωπικών δεδομένων και τον τρόπο με τον οποίο ο οργανισμός θα χειριστεί το περιστατικό. Όλα αυτά πρέπει να γίνουν σε 72 ώρες ή διαφορετικά θα πρέπει να δοθούν πολύ καλές εξηγήσεις.

Οι παραβιάσεις ασφαλείας μπορούν να κατηγοριοποιηθούν στα παρακάτω:

- παραβίαση της εμπιστευτικότητας: μη εξουσιοδοτημένη ή τυχαία πρόσβαση στα δεδομένα
- παραβίαση της διαθεσιμότητας: τυχαία ή μη εξουσιοδοτημένη απώλεια πρόσβασης στα δεδομένα ή καταστροφή τους
- παραβίαση της ακεραιότητας: μη εξουσιοδοτημένη ή τυχαία αλλοίωση των προσωπικών δεδομένων

Η παραβίαση δεδομένων μπορεί να αφορά ταυτόχρονα όλες τις παραπάνω κατηγορίες ή οποιοδήποτε συνδυασμό αυτών. Ακολουθούν ορισμένα παραδείγματα παραβίασης της διαθεσιμότητας: Τα δεδομένα έχουν διαγραφεί τυχαία ή από μη εξουσιοδοτημένο άτομο, τα δεδομένα δεν μπορούν να αποκατασταθούν από ένα αντίγραφο ασφαλείας ή δεν είναι δυνατή η πρόσβαση στα δεδομένα λόγω επίθεσης άρνησης παροχής υπηρεσιών ή διακοπής ρεύματος.

Από τη σκοπιά της ανάπτυξης λογισμικού, υπάρχει πιθανότητα να συμβούν όλοι οι προαναφερθέντες τύποι παραβιάσεων δεδομένων. Μια παραβίαση εμπιστευτικότητας μπορεί να εμφανιστεί σε ένα λογισμικό ως αποτέλεσμα του σφάλματος ενός χρήστη. Με άλλα λόγια, το προαναφερθέν λάθος μπορεί να είναι κατασκευασμένα διαπιστευτήρια (phishing attack) ή ευαίσθητες πληροφορίες ή απλά να παραχωρούν πάρα πολλά προνόμια σε χρήστες, παρά το γεγονός ότι αυτοματοποιημένες δοκιμές, δοκιμές παλινδρόμησης και χειρωνακτική δοκιμή μειώνουν τις αποτυχίες και τα σφάλματα του λογισμικού.

Υπάρχει πάντοτε μια πιθανότητα ότι ένα σφάλμα στον κώδικα λογισμικού μπορεί να μεταβάλει τα λανθασμένα δεδομένα ή να το διαφθείρει κατά λάθος. Δεν έχει καθοριστεί σαφώς αν π.χ. το προαναφερθέν σφάλμα στο λογισμικό μπορεί να χαρακτηρίζεται ως παραβίαση της ακεραιότητας και αν ένας οργανισμός είναι

υποχρεωμένος να το αναφέρει στις αρχές και στα πρόσωπα των οποίων τα δεδομένα έχουν υποστεί τις συνέπειες.

2.5.4.2 Διαγραφή των προσωπικών δεδομένων

Το άρθρο 17 του GDPR ορίζει ότι: «Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο της επεξεργασίας τη διαγραφή προσωπικών δεδομένων που τον αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει τα προσωπικά δεδομένα χωρίς αδικαιολόγητη καθυστέρηση (Regulation (EU) 2016/679 of the European parliament and of the Council 2016).

Το άρθρο 17 περιγράφει τα δικαιώματα του κατόχου των δεδομένων για την απαίτηση διαγραφής δεδομένων από τον υπεύθυνο επεξεργασίας δεδομένων και ο υπεύθυνος επεξεργασίας πρέπει να τηρεί το αίτημα αυτό. Οι εταιρείες πρέπει να διαθέτουν μηχανισμό και διαδικασίες ώστε να διασφαλίζουν ότι τα αφαιρεθέντα δεδομένα δεν θα επανέλθουν στο μέλλον (Loshin 2017)

Οι ενοποιήσεις μεταξύ των συστημάτων πρέπει να υλοποιηθούν κατά τρόπο ώστε τα δεδομένα που αφαιρούνται κάποτε να μην αποκατασταθούν στο σύστημα, όπως έγραψε ο Malste (2017, 40) στη διατριβή του σχετικά με τα προβλήματα ολοκλήρωσης του συστήματος CRM με ένα άλλο σύστημα. Αυτό είναι επίσης ένα αναγνωρισμένο πρόβλημα με πολλά διαφορετικά συστήματα, όχι μόνο στο CRM.

Εμφανίζεται ένα πολύ συνηθισμένο πρόβλημα με την δημιουργία αντιγράφων ασφαλείας των βάσεων δεδομένων, διότι σε περίπτωση που ένα αντίγραφο ασφαλείας πρόκειται να αποκατασταθεί ποτέ και τα δεδομένα που έχουν αφαιρεθεί εξακολουθούν να υπάρχουν, σίγουρα θα επανέλθουν στο σύστημα. Το προαναφερθέν σενάριο μπορεί να δημιουργήσει προβλήματα για τους οργανισμούς, γι 'αυτό και τα δεδομένα που αφαιρέθηκαν κάποτε δεν θα πρέπει να αποθηκεύονται για πάντα στα αντίγραφα ασφαλείας (Loshin 2017).

Τα αντίγραφα ασφαλείας των βάσεων δεδομένων που λαμβάνονται από ένα περιβάλλον παραγωγής είναι οι μοναδικές τοποθεσίες όπου μπορεί να υπάρχουν προσωπικά δεδομένα. Μπορεί να υπάρχουν διαφορετικά περιβάλλοντα δοκιμών για πολλούς σκοπούς με τις δικές τους βάσεις δεδομένων και αντίγραφα ασφαλείας. Ένας οργανισμός πρέπει να έχει διαδικασίες και εσωτερικό συντονισμό, π.χ. για τους προγραμματιστές πώς να διατηρήσουν το περιβάλλον δοκιμών καθαρό από δεδομένα που περιέχουν προσωπικά δεδομένα.

Πολύ συχνά, ο ευκολότερος τρόπος για να εντοπιστούν τα σφάλματα λογισμικού είναι ότι τα αντίγραφα ασφαλείας των βάσεων δεδομένων έχουν αποκατασταθεί σε περιβάλλον δοκιμής ή στον προσωπικό υπολογιστή εργασίας του προγραμματιστή λογισμικού από ένα περιβάλλον παραγωγής. Ο εντοπισμός σφαλμάτων μπορεί να είναι δύσκολος και απαιτεί δεδομένα του πελάτη για να αναπαραχθεί το πρόβλημα. Η δημιουργία περίπλοκων σεναρίων από μηδενικό σημείο είναι μια χρονοβόρα μέθοδος για να διορθωθεί το πρόβλημα.

Γίνεται αντιληπτό από τη νομοθεσία του GDPR ότι ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να παρέχει στο εκάστοτε λογισμικό ένα ενσωματωμένο μηχανισμό διαγραφής προσωπικών δεδομένων. Αυτός θα μπορεί να χρησιμοποιηθεί από τον υπεύθυνο ελέγχου των δεδομένων. Στο μέλλον, μπορεί να δημιουργηθεί πρόβλημα όπου ένας πελάτης ή ένας ελεγκτής μπορεί να θέλει να μάθει γιατί τα δεδομένα που αποθηκεύτηκαν πριν από χρόνια δεν υπάρχουν πια. Αυτό εξαρτάται από τις πολιτικές κάθε οργανισμού. Ωστόσο, το παλαιότερο αντίγραφο ασφαλείας της βάσης δεδομένων μπορεί να είναι π.χ. 12 μηνών και αυτά τα παλαιότερα δεδομένα δεν μπορούν πλέον να αποκατασταθούν επειδή δεν υπάρχουν σε αντίγραφα ασφαλείας.

Ένας υπεύθυνος επεξεργασίας δεδομένων μπορεί να αντιμετωπίσει το προαναφερθέν πρόβλημα καταγράφοντας τις ενέργειες του χρήστη στο σύστημα. Η προαναφερθείσα διαδικασία ιχνηλασημότητας μπορεί να είναι π.χ. πληροφορίες καταγραφής: Ποιος, πότε, τι και γιατί τα δεδομένα καταργήθηκαν. Εάν ένας υπάλληλος, για παράδειγμα σκοπίμως ή τυχαία καταστρέψει δεδομένα, μπορεί να

βρεθεί στα αρχεία καταγραφής (log files). Η καταγραφή των προαναφερθέντων δυσλειτουργιών πρέπει να γίνεται στο σύστημα.

Οι οργανισμοί πρέπει επίσης να θυμούνται ότι χρειάζονται έναν έγκυρο λόγο για την αποθήκευση πληροφοριών. Επιπλέον, πρέπει να καταργήσουν τις όποιες καταγραφές (logs) όταν δεν υπάρχει νομική βάση για να τα διατηρήσουν περαιτέρω. Τα δεδομένα στα αρχεία καταγραφής πρέπει να έχουν ημερομηνία / ώρα λήξης, η οποία βοηθά στην αφαίρεση των δεδομένων που έχουν λήξει. Μπορεί να υπάρχουν κάποιες περιπτώσεις κατά τις οποίες ο καθορισμός ημερομηνίας λήξης / ώρας για τα δεδομένα στη συνέχεια μπορεί να είναι προβληματικός, επειδή οι οργανισμοί δεν μπορούν να το επισημάνουν με σαφήνεια κατά την δημιουργία των δεδομένων.

2.6 Καταγραφή της ροής των δεδομένων που εισέρχονται στα Κοινωνικά πληροφοριακά Συστήματα σε σχέση με τον GDPR

Οι κύριες πτυχές του τρόπου με τον οποίο η νομοθεσία του GDPR επηρεάζει τη ροή δεδομένων σε ΚΠΣ και διαδικασίες ανάλυσης δεδομένων σε κοινωνικά δίκτυα παρουσιάζεται παρακάτω.

2.6.1 Νομική βάση για την επεξεργασία δεδομένων

Έπειτα από διεξοδική ανάλυση του GDPR, μπορούμε να παρατηρήσουμε ότι όταν πρόκειται για το ερώτημα ποια θα πρέπει να είναι η νόμιμη βάση κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα γενικά, οι σημαντικότερες παράμετροι που πρέπει να ληφθούν υπόψη είναι η ταυτότητα του υπεύθυνου ελέγχου, οι σκοποί της επεξεργασίας καθώς και το πλαίσιο της επεξεργασίας. Ανάλογα με αυτές τις παραμέτρους, ο υπεύθυνος ελέγχου πρέπει να αποφασίσει

ποια νόμιμη βάση πρέπει να χρησιμοποιηθεί για την επεξεργασία. Στην περίπτωση μίας έρευνας ή μίας κοινωνικής εργασίας, φαίνεται ότι οι ακόλουθες νόμιμες βάσεις να είναι οι πιο συναφείς:

- Τα φυσικά πρόσωπα-ομάδες που συμμετέχουν έχουν δώσει τη συγκατάθεσής του για την επεξεργασία των προσωπικών τους δεδομένων
- η επεξεργασία είναι αναγκαία για την εκτέλεση μίας κοινωνικής επεξεργασίας ή δημόσιας αποστολής ή / και
- είναι αναγκαία για τους σκοπούς των νόμιμων συμφερόντων που εκπροσωπεί ο υπεύθυνος ελέγχου.

Το παραπάνω πλαίσιο αντικατοπτρίζεται με λεπτομέρεια στον παρακάτω πίνακα:

Id	**Γενικός κανόνας**	**Εξαιρέσεις**	**Λεπτομέρειες**
1	Προσδιορισμός ρόλων (υπεύθυνοι ελέγχου, επεξεργασίας, υπεύθυνος προστασίας των δεδομένων (DPO), κλπ) και ροών δεδομένων.	Όχι	Αυτό μπορεί να είναι δύσκολο σε ορισμένες περιπτώσεις. Μπορεί να παρέμβει ο υπεύθυνος προστασίας των δεδομένων για να ξεπεραστούν τα όποια εμπόδια.
2	Προσδιορισμός της φύσης των δεδομένων (προσωπικά/ μη προσωπικά / ευαίσθητα).	Όχι	Σε περίπτωση ευαίσθητων δεδομένων, μπορεί να γίνει επεξεργασία (1) αν έχουμε ρητή συγκατάθεση, (2) αν τα δεδομένα είχαν προφανώς γίνει δημόσια από το φυσικό πρόσωπο-πηγή των δεδομένων (και πρέπει να χρησιμοποιηθούν προσεκτικά) ή (3) σε περίπτωση ερευνητικών σκοπών, εάν υπάρχουν κατάλληλες διασφαλίσεις(π.χ., ψευδο- ανωνυμοποίηση, έγκριση από ηθική επιτροπή).
3	Προσδιορισμός σαφών και νόμιμων σκοπών για την επεξεργασία.	Ναι	Μία προδιαγραφή σε περίπτωση έρευνας μπορεί να είναι λίγο περισσότερο γενική (όπως ο ερευνητικός χώρος ή μέρος του έργου, όχι συγκεκριμένα αναλυτικά καθήκοντα). Ωστόσο οι προδιαγραφές που αναφέρονται στον επιδιωκόμενο σκοπό δεν μπορούν να είναι.
4	Προσδιορισμός της νόμιμης βάσης για επεξεργασία δεδομένων.	Όχι	Βάσει της εθνικής νομοθεσίας ορισμένοι φορείς που διεξάγουν έρευνα (π.χ. πανεπιστήμια) μπορεί να θεωρηθεί ότι λειτουργούν προς το δημόσιο συμφέρον και

			ως εκ τούτου μπορεί να ληφθεί υπόψη η δημόσια αποστολή ενός εγχειρήματος. Διαφορετικά θα πρέπει να ληφθεί υπόψη η συγκατάθεση και τα νόμιμα συμφέροντα όσων συμμετέχουν σε αυτή.
5	Καθορισμός σαφών χρονικών ορίων για δεδομένα προς επεξεργασία. Μη ανωνυμοποιημένα δεδομένα δε μπορούν να διατηρηθούν για περισσότερο διάστημα πέρα από αυτό που έχει οριστεί για συγκεκριμένους σκοπούς επεξεργασίας.	Ναι	Μπορεί να ισχύουν μεγαλύτερες προθεσμίες σε περίπτωση έρευνας εφόσον εφαρμόζονται οι κατάλληλες διασφαλίσεις.
6	Εφαρμογή τεχνικών και οργανωτικών μέτρων για την προστασία των δεδομένων, π.χ., η διασφάλιση προστασίας της ιδιωτικότητας από το σχεδιασμό,να εφαρμόζουν ψευδο-ανωνυμοποίηση στα δεδομένα το συντομότερο δυνατό.	Όχι	Τα μέτρα πρέπει να είναι ανάλογα προς τον επιδιωκόμενο στόχο.
7	Σε περίπτωση δημιουργίας προφίλ θα πρέπει να εκτελεστεί μια διαδικασία DPIA (Data Privacy Impact Assessment[1]).	Όχι	Θα πρέπει να γίνει αξιολόγηση μαζί με τον υπεύθυνο της προστασίας δεδομένων για το εάν απαιτείται DPIA. Η δημιουργία προφίλ καθώς και η επεξεργασία μπορεί να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες φυσικών προσώπων.
8	Ενημέρωση των φυσικών προσώπων σχετικά με τους σκοπούς και τα δικαιώματά τους κατά την λήψη των δεδομένων (εάν ληφθούν απευθείας από το φυσικό πρόσωπο) ή εντός εύλογου χρονικού διαστήματος και όχι αργότερα από ένα μήνα	Ναι	Για τα δευτερεύοντα δεδομένα, η παροχή πληροφοριών δεν είναι απαραίτητη εάν η παροχή τέτοιων πληροφοριών αποδεικνύεται αδύνατη ή θα συνεπαγόταν δυσανάλογη προσπάθεια, εάν αυτό είναι πιθανό να καταστήσει αδύνατη ή σοβαρή βλάβη στην επίτευξη των στόχων της επεξεργασίας.

[1] Αξιολόγηση του αντίκτυπου στα προσωπικά δεδομένα

	(εάν τα δεδομένα λαμβάνονται έμμεσα).		
9	Συλλογή μόνο κατάλληλων, σχετικών και περιορισμένων δεδομένων σε ό, τι είναι απαραίτητο για την επίτευξη των σκοπούς της επεξεργασίας.	Ναι	Καθώς ο σκοπός μπορεί να διευκρινιστεί με λιγότερο ακριβείς όρους (βλ. την εξαίρεση του κανόνα 3), επηρεάζεται και αυτός ο κανόνας. Τα μη απαραίτητα δεδομένα πρέπει να διαγραφούν το συντομότερο δυνατόν, καταγράφοντας τη διαδικασία και δημιουργώντας τις σχετικές αναφορές.
10	Τα φυσικά πρόσωπα έχουν το δικαίωμα να ελέγξουν αν υπάρχουν προσωπικά τους δεδομένα στις βάσεις δεδομένων Εταιριών και το δικαίωμα να αποκτήσουν αυτά τα δεδομένα.	Όχι	Ακόμη και αν δεν είναι μέρος του GDPR, η εθνική νομοθεσία μπορεί να εξακολουθεί να ισχύει και να περιορίζει αυτό το δικαίωμα.
11	Τα φυσικά πρόσωπα έχουν το δικαίωμα να ζητήσουν τη διαγραφή των δεδομένων τους	Ναι	Δεν είναι απαραίτητο αυτό να γίνει, εάν είναι πιθανό να καταστήσει αδύνατη ή να επηρεάσει σημαντικά την επίτευξη των στόχων προς επεξεργασία. Η εθνική νομοθεσία ενδέχεται επίσης να περιορίσει αυτό το δικαίωμα.
12	Να διατηρούνται τα δεδομένα ακριβή και ενημερωμένα.	Όχι	
13	Αν προκύψει ένας νέος σκοπός, νέες νομικές βάσεις πρέπει να προσδιοριστούν για την επεξεργασία δεδομένων.	Ναι	Εάν ο νέος σκοπός είναι η έρευνα, τότε περαιτέρω επεξεργασία θεωρείται ότι είναι συμβατή με τον αρχικό σκοπό.
14	Αν ο υπεύθυνος ελέγχου αλλάξει τον σκοπό της επεξεργασίας των δεδομένων, τα εμπλεκόμενα φυσικά πρόσωπα πρέπει να ενημερωθούν πριν από την επεξεργασία αυτών.	Ναι	Βλ. την εξαίρεση του κανόνα 3 σχετικά με την αυξημένη ευελιξία στην περιγραφή του σκοπού σε περίπτωση έρευνας.
15	Οι υπεύθυνοι θα πρέπει να διατηρούν γραπτά αρχεία για να αποδείξουν συμμόρφωση.	όχι	

2.6.2 Συλλογή δεδομένων

Τα κοινωνικά δίκτυα μπορούν να δημιουργηθούν μέσω ενός ευρέου φάσματος στρατηγικών συλλογής δεδομένων. Παρακάτω περιγράφουμε διαφορετικές προσεγγίσεις στη συλλογή δεδομένων για ανάλυση κοινωνικών δικτύων και υπό το πρίσμα των απαιτήσεων της νομοθεσίας του GDPR.

1. **Πρωτοβάθμια και δευτερογενή συλλογή δεδομένων και αρχή της διαφάνειας**

Μια σημαντική εννοιολογική και νομική διάκριση έγκειται στην επιλογή των μεθόδων συλλογής δεδομένων. Για παράδειγμα, υπάρχει σημαντική διαφορά μεταξύ δεδομένων που συλλέγονται απευθείας από το φυσικό πρόσωπο (π.χ. δεδομένα μικρής και μεσαίας κλίμακας που λαμβάνονται μέσω ερευνών, online φόρμες) και δεδομένα που συλλέγονται μέσω τρίτου μέσου (π.χ. διαδικτυακά κοινωνικά δίκτυα που λαμβάνονται από API) καθώς και δεδομένα που έχουν ληφθεί από τα φυσικά πρόσωπα χωρίς να το γνωρίζουν.

Σύμφωνα με την αρχή της διαφάνειας, τα φυσικά πρόσωπα πρέπει να είναι σε θέση να γνωρίζουν άμεσα ποιος μπορεί να χρησιμοποιεί τα δεδομένα τους και για ποιους σκοπούς. Παρόλο που τα φυσικά πρόσωπα γνωρίζουν την επεξεργασία και τα δικαιώματά τους, μπορεί να φαίνονται απλά όταν τα δεδομένα συλλέγονται απευθείας από αυτά. Αυτό μπορεί να γίνει πολύ δύσκολο να επιτευχθεί όταν τα δεδομένα αποκτηθούν μέσω μεγάλων δικτύων και μέσω API. Οι δυνητικές δυσκολίες παροχής πληροφοριών υπό συγκεκριμένες συνθήκες αναγνωρίζονται στον GDPR, όπου εισάγονται εξαιρέσεις για την έρευνα και την κοινωνική αποστολή τους ειδικότερα.

Αυτά είναι μερικά παραδείγματα ορισμένων εξαιρέσεων που ενσωματώνονται στον GDPR, κωδικοποιώντας και προσδιορίζοντας τον τρόπο που πρέπει να λειτουργήσει μία κοινωνική εργασία ως προς τη συλλογή δεδομένων. Οι παραπάνω εξαιρέσεις ισχύουν πχ για μία έρευνα μέσω κοινωνικών δικτύων που βασίζεται σε

ηλεκτρονικά δεδομένα και που συλλέγονται από τις πλατφόρμες κοινωνικών μέσων. Υποθέτουμε ότι οι πλατφόρμες κοινωνικών μέσων έχουν ήδη ενημερώσει τους χρήστες τους μέσω κατάλληλων Όρων Υπηρεσιών ότι τα δεδομένα τους θα μοιραστούν με τρίτους ή υποθέτοντας ότι μεγάλη κλίμακα των δεδομένων που συλλέγονται θα απαιτήσει δυσανάλογη προσπάθεια ενημέρωσης όλων των φυσικών προσώπων.

2. Το βάθος των δεδομένων του διαδικτυακού κοινωνικού δικτύου και η αρχή της ελαχιστοποίησης των δεδομένων

Όταν ορισμένα δεδομένα κοινωνικού σκοπού συλλέγονται απευθείας με τη μορφή δικτυακών πληροφοριών, δηλαδή κόμβων και ακμών, πολλά σύνολα δικτυακών δεδομένων λαμβάνονται μέσω επεξεργασίας άλλων τύπων δεδομένων. Για παράδειγμα αυτό συμβαίνει συχνά σε μία έρευνα ή κοινωνική εργασία που βασίζεται σε κοινωνικά μέσα όπως το Twitter. Η επεξεργασία των δεδομένων από το Twitter μπορεί να βασιστεί στη δικτυακή δομή των χρηστών (following-followers), η οποία θεωρείται άμεση δικτυακή πληροφορία. Ταυτόχρονα, μπορούμε να δημιουργήσουμε μία χαρτογράφηση των δικτύων που προκύπτουν από τις διαδικασίες επικοινωνίας, είτε ρητές (μέσα από απαντήσεις, αναφορές του χρήστη) είτε σιωπηρές, για παράδειγμα με τη χρήση κοινών hashtags.

Για τη δημιουργία αυτού του δεύτερου τύπου δικτύου, οι αναλυτές σε ένα ΚΠΣ συλλέγουν το περιεχόμενο των αναρτήσεων των χρηστών και στη συνέχεια εξαγάγουν και συνάπτουν σχεσιακές πληροφορίες. Το πρόβλημα προκύπτει εάν εξετάσουν τις συνέπειες της συλλογής του περιεχομένου των θέσεων για την κατασκευή του δικτύου. Ανάλογα με το θέμα των δημοσιεύσεων, ο τύπος περιεχομένου που ενδέχεται να έχει συλλεχθεί μπορεί να διαφέρει, αλλά μπορεί να περιλαμβάνει δεδομένα που αποκαλύπτουν πληροφορίες που δεν αναγνωρίζουν μόνο φυσικά πρόσωπα, αλλά περιλαμβάνουν και ευαίσθητα δεδομένα όπως πολιτική συμπαράσταση, θρησκευτικές πεποιθήσεις κλπ.

Ο GDPR κάνει διάκριση μεταξύ διαφόρων τύπων προσωπικών δεδομένων, όπως δεδομένα σχετικά με την εθνικότητα και τις σεξουαλικές προτιμήσεις (ευαίσθητα προσωπικά δεδομένα) και για να θεωρηθεί νόμιμη η επεξεργασία, ο υπεύθυνος ελέγχου πρέπει να σέβεται την ουσία των δικαιωμάτων περί προστασίας των δεδομένων και να ακολουθούν κατάλληλες διασφαλίσεις. Σημειώνεται ότι δεδομένα που σε συνδυασμό με άλλα δεδομένα μπορούν να οδηγήσουν στην αποκάλυψη ευαίσθητων δεδομένων μπορούν επίσης να θεωρηθούν ως ευαίσθητα δεδομένα.

Για παράδειγμα το όνομα σε συνδυασμό με τον αριθμό τηλεφώνου, και ενώ κάθε ένα από αυτά τα δεδομένα δεν είναι ευαίσθητο, μπορεί να συνιστούν ευαίσθητα δεδομένα μαζί εάν αποκαλύπτουν πιθανώς την εθνικότητα ενός ατόμου. Είναι εύκολο να δούμε πώς η μέση ροή των μηνυμάτων που γράφεται από έναν μέσο χρήστη μπορεί εύκολα να περιέχει ευαίσθητα προσωπικά δεδομένα ή δεδομένα που μπορούν να συνδυαστούν για να αποκαλύψουν ευαίσθητα προσωπικά δεδομένα σχετικά με το υποκείμενο των δεδομένων. Επιπλέον, τέτοια δεδομένα μπορούν να προκύψουν σχετικά με άτομα απλά από πληροφορίες που παράγονται από τις συνδέσεις τους. Για παράδειγμα, μπορεί να είναι δυνατό να εξακριβωθεί η πολιτική σχέση ενός ατόμου εάν η πλειοψηφία των συνδέσεων τους επικοινωνεί την πολιτική τους ταυτότητα.

3. Ανάλυση και ταξινόμηση δεδομένων

Η ανάλυση δεδομένων στα πλαίσια ενός ΚΠΣ περιλαμβάνει ένα ευρύ φάσμα εργασιών ανάλυσης δεδομένων. Μερικές φορές η συλλογή στατιστικών είναι σημαντική, για παράδειγμα για να συσχετιστεί η δομή επικοινωνίας / αλληλεπίδρασης μιας ομάδας ή ενός οργανισμού με τις επιδόσεις της. Μερικές φορές ενδιαφέρει να προσδιορίσουμε κοινότητες ή άλλες σχετικές υπο-δομές, όπως σε απευθείας σύνδεση συνομιλίες μέσα σε ένα μεγαλύτερο δίκτυο. Οι αναγνωρισμένες ομάδες μπορούν επίσης να χρησιμοποιούνται για την ταξινόμηση μεμονωμένων παραγόντων, για παράδειγμα την ανάθεση σε μια συγκεκριμένη κοινότητα ή ρόλο. Άλλοι τύποι ανάλυσης μικρο-επιπέδων εμπλέκουν τον

χαρακτηρισμό μεμονωμένων παραγόντων, για παράδειγμα όταν εντοπίζονται οι πιο κεντρικοί ή αναγνωρισμένοι συντελεστές. Όταν τα άτομα αποτελούν το αντικείμενο της ανάλυσης, πράγμα που συμβαίνει για τα περισσότερα από τα καθήκοντα που αναφέρονται παραπάνω, μια σημαντική έννοια που πρέπει να ληφθεί υπόψη είναι η δημιουργία προφίλ.

Ο GDPR δίνει ιδιαίτερη έμφαση στην έννοια του προφίλ, καθορίζοντας τον ορισμό και τις πρακτικές αποδεκτής κωδικοποίησης. Κατά συνέπεια, στον GDPR η ταξινόμηση σε προφίλ αποτελείται από τρία βασικά στάδια: α) συλλογή προσωπικών δεδομένων β) αυτοματοποιημένη ανάλυση για τον προσδιορισμό των συσχετισμών γ) εφαρμογή της συσχέτισης [του αποτελέσματος του β)] σε ένα άτομο για τον προσδιορισμό των χαρακτηριστικών της παρούσας ή μελλοντικής συμπεριφοράς.

Σημειώνεται η έννοια της "αυτοματοποιημένης ανάλυσης" που χρησιμοποιείται στον GDPR σε αντίθεση με την "χειροκίνητη ανάλυση". Αν και οι δύο τύποι επεξεργασίας εμπίπτουν στην αρμοδιότητα του GDPR, ο χαρακτηρισμός είναι αναγκαστικά αυτοματοποιημένος. Ωστόσο, αυτοματοποιημένος εδώ θα σημαίνει τόσο τη χρήση ενός στατιστικού λογισμικού για τη διεξαγωγή οποιασδήποτε μορφής ανάλυσης δεδομένων όσο και τη χρήση πιο πολύπλοκων προσεγγίσεων όπως αλγόριθμοι μηχανικής μάθησης. Έτσι οποιαδήποτε ανάλυση δεδομένων που περιλαμβάνει υπολογιστική βοήθεια από το λογισμικό εμπίπτει στην αυτοματοποιημένη ανάλυση και επομένως μπορεί να ταξινομηθεί ως μορφή ταξινόμησης.

Με βάση τα παραπάνω καθήκοντα ανάλυσης δεδομένων που πηγάζουν από κοινωνικά δίκτυα μπορούν να ταξινομηθούν ως ιδιαίτερα χαρακτηριστικά που μπορούν να συσχετιστούν με συγκεκριμένα άτομα. Με άλλα λόγια, κάθε ανάλυση που ξεχωρίζει τα άτομα με βάση τον προσδιορισμό των θέσεων, των ρόλων και των κοινοτήτων είναι μια μορφή ταξινόμησης.

2.7 Εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων

Σύμφωνα με τον Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων και πιο συγκεκριμένα σύμφωνα με αυτά που ορίζονται στο Άρθρο 33, «…κάθε δημόσιος ή ιδιωτικός οργανισμός που επεξεργάζεται συγκεκριμένα προσωπικά δεδομένα, υποχρεούται να εκτελεί μια εκτίμηση για τις πιθανές επιπτώσεις των κινδύνων που ενδέχεται να προκύψουν από την επεξεργασία των δεδομένων αυτών».

Η εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων αποτελεί στην ουσία μια διαδικασία η οποία διενεργείται κυρίως κατά το αρχικό στάδιο σχεδίασης της εφαρμογής. Αποτέλεσμα αυτής της διαδικασίας είναι η σύνταξη μιας έκθεσης στην οποία περιέχονται όλα τα στοιχεία και χαρακτηριστικά της επεξεργασίας, η εκτίμηση των πιθανών κινδύνων καθώς και προτεινόμενα μέτρα ασφαλείας ώστε να επιτυγχάνεται ο περιορισμός ή η εξάλειψη αυτών. Η έκθεση αυτή υπόκειται σε έλεγχο από την εκάστοτε Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ώστε να εκδώσει την απαραίτητη άδεια επεξεργασίας των συγκεκριμένων δεδομένων, όπως προβλέπεται από τον Γενικό Κανονισμό για την Προστασία των Δεδομένων.

Ένα ΚΠΣ όπου έχει μεγάλη επιρροή στον κόσμο τα τελευταία χρόνια είναι το facebook. Κατά την διαδικασία εγγραφής στον εν λόγω κοινωνικό ιστότοπο συλλέγονται προσωπικά δεδομένα ευαίσθητα και μη όπως ορισμένα από τα στοιχεία ταυτότητας του χρήστη, οικογενειακή κατάσταση και προσωπικές φωτογραφίες.

Κατά την διάρκεια παραμονής των χρηστών στο facebook συλλέγονται εκ νέου πληροφορίες για την προσωπικότητα γενικότερα των χρηστών καθώς και την προσωπική τους ζωή. Μετά την παραβίαση του απορρήτου καθώς και τον διαμοιρασμό προσωπικών δεδομένων και πληροφοριών των χρηστών του σε τρίτους, το facebook κατασκεύασε ένα νέο ΄΄κέντρο ιδιωτικότητας΄΄ για τους

χρήστες, γεγονός που δεν μειώνει τον κίνδυνο εκ νέου διαρροής δεδομένων. Πλέον για την επιβεβαίωση των προσωπικών δεδομένων καθώς και την ασφάλεια των λογαριασμών είναι απαραίτητη η αποστολή από τον χρήστη επίσημου εγγράφου ταυτοποίησης δεδομένων.

Η παραβίαση λοιπόν του απορρήτου στην παραπάνω διαδικασία επιφέρει μεγάλες επιπτώσεις καθώς υπάρχει κίνδυνος μη αποτελεσματικής προστασίας προσωπικών δεδομένων και το ρισκό της εν λόγω Εταιρίας είναι μεγάλο.

Σύμφωνα με τον ίδιο διαδικτυακό ιστότοπο του GDPR τα πρόστιμα που χορηγούνται για μη συμμόρφωση και τα ποσά που εισπράττονται εξαρτώνται από 10 βασικά κριτήρια: τη φύση της παράβασης, την πρόθεση, τον μετριασμό, τα προληπτικά μέτρα, το ιστορικό των παραβιάσεων, το επίπεδο συνεργασίας με την αρχές, τους τύπους δεδομένων, την κοινοποίηση, τις πιστοποιήσεις προστασίας δεδομένων και άλλα.

Οι παραβάσεις που θεωρούνται παραβιάσεις "κατώτερου επιπέδου" είναι η μη καταγραφή δεδομένων σε σειρά, η μη κοινοποίηση της εποπτικής αρχής και του υποκειμένου των δεδομένων σχετικά με παραβίαση ή η μη διεξαγωγή εκτιμήσεων αντικτύπου για την προστασία της ιδιωτικής ζωής. Οι εν λόγω παραβάσεις υπόκεινται σε έως και €10.000.000, ή 2% των ετήσιων εσόδων του προηγούμενου οικονομικού έτους, όποιο από τα δυο είναι υψηλότερο.

Παραβάσεις που θεωρούνται παραβιάσεις "ανώτερου επιπέδου" είναι οι παραβιάσεις των βασικών αρχών που σχετίζονται με την ασφάλεια των δεδομένων και τους όρους για τη συγκατάθεση των καταναλωτών, παραβιάσεις των δικαιωμάτων των προσώπων που αφορούν τα δεδομένα και διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτα μέρη ή διεθνείς οργανισμοί που δεν εξασφαλίζουν επαρκές επίπεδο προστασίας των δεδομένων. Οι εν λόγω παραβάσεις υπόκεινται σε έως και €20.000.000 ποινές, ή 4% των παγκόσμιων ετήσιων εσόδων, όποιο από τα δυο είναι υψηλότερο.

2.8 Ανάλυση των αποκλίσεων

Ένα ΚΠΣ όπως το facebook και λαμβάνοντας υπόψη τις απαιτήσεις του GDPR έχει ορισμένα κενά. Πιο συγκεκριμένα οι προσβάσεις ενός χρήστη του εν λόγω ΚΠΣ σε ένα προιόν, ευκαιρία ή όφελος που βασίζονται σε οποιοδήποτε βαθμό στην αυτοματοποιημένη λήψη αποφάσεων (συμπεριλαμβανομένης της κατάρτισης προφίλ).

Η παροχή περαιτέρω υπηρεσιών κάνοντας χρήση πιστωτικών καρτών όπου δίνουν την δυνατότητα στον κατασκευαστη κατοχής ευαίσθητων προσωπικών δεδομένων χωρίς την λήψη μέτρων. Τα εν λόγω κενά δημιουργούν παραβάσεις υψηλού κινδύνου καθώς είναι συχνό φαινόμενο η εισχώρηση τρίτων μέσω κακόβουλων λογισμικών στις βάσεις δεδομένων του facebook. Ο κατασκευαστής πρέπει να θωρακίσει το εν λόγω ΚΠΣ με ισχυρά και προηγμένα συστήματα ασφαλείας προκειμένου να συμμορφωθεί με τον GDPR καθώς επεξεργάζεται τεράστιο όγκο δεδομένων.

Όλοι οι οργανισμοί που επεξεργάζονται δεδομένα υποχρεούνται να αξιολογούν τον κίνδυνο που θέτει η επεξεργασία στα υποκείμενα των δεδομένων, τόσο πριν από την επεξεργασία, όσο και μετά την εφαρμογή ενός συστήματος. Αυτό είναι για να διασφαλιστεί ότι μια εταιρεία έχει σκεφτεί μπροστά για το πώς χρησιμοποιεί τα δεδομένα, έχει προβλέψει πιθανά προβλήματα και έχει εργαστεί για την αντιμετώπισή τους.

Η ελπίδα είναι ότι αυτό θα βοηθήσει στη δημιουργία πιο ισχυρών διεργασιών με ενσωματωμένη προστασία δεδομένων από το μηδέν.

Κεφάλαιο 3
Προστασία των δεδομένων

Μέσα από την ανάλυση των νομικών υποχρεώσεων που προέκυψαν από τον GDPR, έχουμε δει πολλές περιπτώσεις όπου ο νόμος μπορεί να θεωρηθεί ως κατώτατο σημείο για την εφαρμογή ενός κώδικα ηθικής, και κατόπιν οι υπεύθυνοι ενός ΚΠΣ θα εξετάσουν πιο περιοριστικές ενέργειες. Για παράδειγμα, όπως αναφέρθηκε παραπάνω, ο GDPR αναφέρει ρητώς "δυσανάλογη προσπάθεια" ως λόγο για να μην παρέχονται πληροφορίες στα φυσικά πρόσωπα- πηγές των δεδομένων. Αυτό, όταν πλαισιώνεται στο πλαίσιο των ηλεκτρονικών δεδομένων ή της δευτερογενούς ανάλυσης των ήδη συλλεγόμενων μεγάλων συνόλων δεδομένων, θα μπορούσε εύκολα να χρησιμοποιηθεί ως ένας ισχυρός λόγος για την πραγματοποίηση επεξεργασίας τους στο ΚΠΣ χωρίς την ενημέρωση των φυσικών προσώπων.

Μεγάλοι όγκοι ηλεκτρονικών δεδομένων θα μπορούσαν εύκολα να προσδιορίζουν εκατομμύρια δυνητικά πηγές δεδομένων (φυσικά πρόσωπα), μπορεί κανείς να αναμένει ότι για τις ηλεκτρονικές πηγές μπορεί να είναι δυνατή η αυτόματη αποστολή ειδοποιήσεων ή μηνυμάτων που ενημερώνουν τα φυσικά πρόσωπα. Παρόλο που αυτό μπορεί να έχει ως αποτέλεσμα μια σημαντική επιβάρυνση της επικοινωνίας με συγκεχυμένα φυσικά πρόσωπα, η προσπάθεια μπορεί να είναι ένα πρώτο βήμα για να αναγνωριστεί ότι τα άτομα που παράγουν δεδομένα πρέπει να αντιμετωπίζονται με αξιοπρέπεια και σεβασμό, ανεξάρτητα από τους στόχους του ΚΠΣ. Η ανάπτυξη προτύπων για την υλοποίηση διαδικασιών κοινοποίησης σε μεγάλες καμπάνιες συλλογής δεδομένων είναι απαραίτητη και ίσως χρειαστεί να συμβαδίζουν με την ανάπτυξη επαγγελματικού κώδικα δεοντολογίας.

Σε αυτές τις περιπτώσεις, θα πρέπει επίσης να εξεταστεί η ανάπτυξη εργαλείων που μπορούν να φροντίσουν για την αυτόματη κοινοποίηση, περιορίζοντας την απαίτηση δυσανάλογης προσπάθειας παρά την αξιοποίησή της ως έναν τρόπο για την ανάληψη ευθυνών σε μία εργασία κοινωνικού σκοπού (έρευνα, crowdsourcing, κλπ). Για παράδειγμα, στο αυξανόμενο πεδίο ερευνών μέσα από το Twitter, η αποστολή ενός σύντομου μηνύματος που αναφέρει τους λογαριασμούς χρηστών που περιλαμβάνονται στα δεδομένα μίας κοινωνικής εργασίας θα ήταν ενδεχομένως ενδιαφέρουσες πληροφορίες για τα άτομα στα οποία αναφέρονται τα δεδομένα, συμβάλλοντας στην αύξηση της εγρήγορσης για το πως χρησιμοποιούνται δημοσίως τα δεδομένα.

Εάν γίνει από ένα σχετικό μερίδιο των αναλυτών/προγραμματιστών και όσων άλλων έχουν κύριο ρόλο σε ένα ΚΠΣ (η οποία μπορεί θεωρητικά να επιτευχθεί εάν το κύριο εργαλείο ή τα εργαλεία για τη συλλογή δεδομένων σε ένα ΚΠΣ επεκταθεί με αυτή τη λειτουργικότητα) αυτή η μεγαλύτερη εγρήγορση θα μπορούσε να οδηγήσει σε μια γενική επακόλουθη βελτίωση στον τρόπο με τον οποίο οι άνθρωποι διαχειρίζονται τα δεδομένα τους σε απευθείας σύνδεση και μια αυξημένη εμπιστοσύνη στην επιστήμη, είναι σχετικά με αυτό. Ωστόσο, ενώ η αυτόματη αποστολή των πληροφοριών σε μια λίστα χρηστών φαίνεται να απαιτεί περιορισμένη προσπάθεια, η μετατροπή τους σε πράξη μπορεί να είναι προβληματική.

Τα προβλήματα που προκύπτουν και μπορεί να οδηγήσουν σε αποκλίσεις από βασικές αρχές του GDPR περιλαμβάνουν:

- τη δυσκολία αποστολής πληροφοριών σε εκατομμύρια χρήστες μέσω ενός API τρίτου μέρους που δεν το επιτρέπει
- τα προβλήματα ψευδο-ανωνυμοποίησης των δεδομένων το συντομότερο δυνατόν σε μια συνεχή διαδικασία παρακολούθησης με εργαλεία τρίτων
- το πρόβλημα της διαγραφής των δεδομένων από το χρήστη
- η πρακτική αδυναμία εξασφάλισης της ανωνυμίας των ερωτηθέντων

- η συμπερίληψη δεδομένων σχετικά με άτομα που δεν περιλαμβάνονται σε μία έρευνα ή κοινωνική εργασία

καθώς και γενικότερα ζητήματα που σχετίζονται με την προστασία των δεδομένων που αναδύονται κατά την εφαρμογή ΚΠΣ και κατά την επεξεργασία δεδομένων που προέρχονται από κοινωνικά μέσα.

Έχοντας καταγράψει τα προβλήματα που προκύπτουν εξαιτίας της έλλειψης ενός ΚΠΣ και ειδικά στην εφαρμογή του GDPR, στις επόμενες ενότητες παρουσιάζουμε πως πρέπει να σχεδιαστεί ένα τέτοιο Πληροφοριακό Σύστημα. Κατόπιν παρουσιάζουμε προτάσεις για την εναρμόνιση του συστήματος με τη νομοθεσία του GDPR.

3.1 Χαρτογράφηση των προσωπικών δεδομένων

Ο σχεδιαστής ενός Κοινωνικού Πληροφοριακού Συστήματος (ΚΠΣ) πρέπει να γνωρίζει ποιά προσωπικά αναγνωρίσιμα στοιχεία ενός φυσικού προσώπου επεξεργάζεται. Χωρίς αυτά τα στοιχεία, θα είναι δύσκολο να βεβαιωθεί ότι το ΚΠΣ περιλαμβάνει διαδικασίες διαχείρισης των προσωπικών δεδομένων που είναι συμβατές με τη νομοθεσία του GDPR. Το άρθρο 30 του κανονισμού για την προστασία των γενικών δεδομένων δηλώνει, για παράδειγμα, ότι ο οργανισμός θα πρέπει να ονομάζει έναν σκοπό για κάθε επεξεργασία προσωπικών δεδομένων και να θέτει χρονικά όρια για το χρονικό διάστημα κατά το οποίο θα διατηρούνται τα δεδομένα σε χώρο αποθήκευσης. Επιπλέον, ο υπεύθυνος επεξεργασίας και ελέγχου πρέπει να είναι σε θέση να καταστήσουν τα αρχεία διαθέσιμα στις αρχές και ελέγχου κατόπιν αιτήματος. Το άρθρο 30 του GDPR δεν δίνει οδηγίες σχετικά με το τι θα πρέπει να κάνει ένας οργανισμός, ώστε οι δραστηριότητες επεξεργασίας δεδομένων του οργανισμού να πληρούν τις απαιτήσεις. Η χαρτογράφηση δεδομένων μπορεί να είναι μια καλή μέθοδος για τέτοιου είδους σκοπούς (Biscoe 2017) .

Η χαρτογράφηση δεδομένων βοηθά τον σχεδιαστή ενός ΚΠΣ να προσδιορίσει τις πληροφορίες που διατηρούνται μέσα σε αυτό και τον τρόπο με τον οποίο θα μεταφερθούν από μία τοποθεσία στην άλλη. Η χαρτογράφηση δεδομένων πρέπει να περιλαμβάνει τουλάχιστον τα ακόλουθα στοιχεία (Biscoe 2017):

- Στοιχεία δεδομένων (ονόματα, διευθύνσεις, μηνύματα ηλεκτρονικού ταχυδρομείου κ.λπ.)
- Τύποι (π.χ. βάσεις δεδομένων και αρχεία)
- Μεταφορές (π.χ. API) σε διακομιστές
- Ποιος έχει πρόσβαση στα δεδομένα

3.2 Ποιος έχει πρόσβαση στα δεδομένα και γιατί

Μετά την χαρτογράφηση των προσωπικών δεδομένων, ο σχεδιαστής του ΚΠΣ θα πρέπει να ορίσει ποιος έχει πρόσβαση σε κάθε εγγραφή /αποθηκευτικό χώρο των δεδομένων. Σε αυτή τη φάση καθορίζεται ποιοι είναι οι χρήστες που πραγματικά πρέπει να έχουν πρόσβαση στα συγκεκριμένα δεδομένα. Επιπλέον, ο σχεδιαστής του ΚΠΣ πρέπει να αποφασίσει ποιος μπορεί να τροποποιήσει τα δεδομένα του πελάτη και άλλα προσωπικά στοιχεία. Αυτός είναι ο λόγος για τον οποίο οι πολιτικές και οι διαδικασίες πρέπει να ελέγχονται προσεκτικά για να αποφευχθούν εύκολα λάθη και παραβιάσεις δεδομένων.

3.2.1 Τμήμα εξυπηρέτησης του ΚΠΣ

Ο κύριος ρόλος ενός κέντρου εξυπηρέτησης (helpdesk) είναι να βοηθήσει τους χρήστες μίας κοινότητας ή εξωτερικούς επισκέπτες (ή συνεργάτες) με προβλήματα που μπορεί να εμφανιστούν π.χ. με εφαρμογές. Μερικές φορές απαιτείται ένας εργαζόμενος που εργάζεται στο τμήμα εξυπηρέτησης να έχει πρόσβαση στα δεδομένα του χρήστη, διότι διαφορετικά μπορεί να είναι δύσκολο να εντοπιστεί η

αιτία ενός προβλήματος. Όταν ένας υπάλληλος του τμήματος υποστήριξης χρειάζεται πρόσβαση στα δεδομένα ενός χρήστη, πρέπει να συμπληρώσει μια φόρμα όπου υπάρχει πεδίο για να δοθεί ο λόγος για τον οποίο πρέπει να έχει πρόσβαση στα δεδομένα. Η πρόσβαση στα δεδομένα των χρηστών/επισκεπτών του ΚΠΣ πρέπει να αποτραπεί αρχικά με προγραμματιστικό τρόπο. Επομένως, χωρίς βάσιμο λόγο, ένας υπάλληλος του τμήματος υποστήριξης δεν μπορεί να έχει πρόσβαση στα δεδομένα.

Οι υπάλληλοι του τμήματος υποστήριξης θα πρέπει να έχουν οδηγίες για την υποδοχή αιτημάτων μέσω τηλεφώνου και ηλεκτρονικού ταχυδρομείου, διότι έτσι η εταιρία μπορεί να αποτρέψει παραβιάσεις της ασφάλειας μέσω κοινωνικής μηχανικής (phishing). Μερικές φορές ένα άτομο καλεί το γραφείο υποστήριξης ή στέλνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου και στη συνέχεια π.χ. ζητά τον κωδικό του / της στο σύστημα. Ο κωδικός πρόσβασης δεν μπορεί να δοθεί, επειδή η κλήση μπορεί να είναι κακόβουλη επαφή. Οι πελάτες θα χάσουν την εμπιστοσύνη τους σε έναν οργανισμό που δίνει τους κωδικούς πρόσβασης στο τηλέφωνο. Ως εκ τούτου, μπορούν να δοθούν μόνο απλές οδηγίες σε τηλεφωνική κλήση, ωστόσο δεν μπορούν να εκτεθούν προσωπικές πληροφορίες ή ευαίσθητα δεδομένα. Οι αλλαγές δεδομένων μπορούν να πραγματοποιηθούν π.χ. όταν ένας εγγεγραμμένος χρήστης στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου στο helpdesk.

3.2.2 Ομάδα ανάπτυξης του ΚΠΣ

Η ομάδα ανάπτυξης λογισμικού μπορεί να είναι μία κατανεμημένη ομάδα προγραμματιστών από όλο τον κόσμο. Καλείται να διορθώσει σφάλματα ή να λύσει περίπλοκα προβλήματα που μπορεί να προκύψουν στην τρέχουσα έκδοση του συστήματος. Μερικές φορές είναι αδύνατο να κατανοήσουν τη βασική αιτία ενός προβλήματος χωρίς πραγματικά δεδομένα. Η σύνθεση των δεδομένων για το σενάριο δοκιμής/αναπαραγωγής μπορεί να είναι χρονοβόρα και δύσκολη διαδικασία, επειδή πολύ συχνά τα σφάλματα πρέπει να επιλυθούν σε πολύ σύντομο

χρόνο. Θα είναι πολύ ταχύτερο, ευκολότερο και φθηνότερο για κάθε εμπλεκόμενο μέρος της κοινότητας να χρησιμοποιεί τα πραγματικά δεδομένα για τον εντοπισμό προβλημάτων. Για αυτό το λόγο οι κανόνες για την ομάδα ανάπτυξης είναι ίδιοι με αυτούς που εργάζονται στην εξυπηρέτηση. Ένας προγραμματιστής πρέπει να συμπληρώσει μία φόρμα τεκμηριώνοντας τον λόγο για τον οποίο απαιτεί πρόσβαση στα δεδομένα του πελάτη.

Πρέπει επίσης να υπάρχει μια πολιτική για τον τρόπο με τον οποίο οι προγραμματιστές χειρίζονται τα αντίγραφα ασφαλείας των βάσεων δεδομένων, επειδή υπάρχει μεγάλη πιθανότητα παραβίασης των δεδομένων, εάν πρέπει να αποθηκευτούν αντίγραφα ασφαλείας π.χ. σε εξωτερικές μονάδες μνήμης USB χωρίς κρυπτογράφηση. Κάποιος μπορεί να κλέψει την εξωτερική μνήμη εύκολα ή κατά λάθος, μπορεί να χαθεί έξω από το γραφείο. Στη συνέχεια, προσωπικά αναγνωρίσιμα στοιχεία ενός πελάτη και άλλα ευαίσθητα δεδομένα θα εκτεθούν σε τρίτους.

3.2.3 Διαδικασία συγκατάθεσης

Οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να τηρούν αρχεία για το πώς και πότε ένα άτομο έδωσε τη συγκατάθεσή του για την επεξεργασία των δεδομένων του. Η συγκατάθεση πρέπει να παρέχεται από ένα άτομο και δεν μπορεί να δημιουργηθεί αυτόματα με ένα σύστημα. Ο ελεγκτής πρέπει επίσης να λάβει υπόψη του ότι ένα άτομο έχει δικαίωμα να ακυρώσει μια συγκατάθεση όποτε το θέλει (Curtis 2018)

Η λύση για αυτό είναι ότι όταν ένας χρήστης συνδεθεί στο ΚΠΣ για πρώτη φορά, το σύστημα θα πρέπει να εμφανίσει ένα πλαίσιο στο οποίο θα ζητείται η συγκατάθεση του χρήστη. Το πλαίσιο επιβεβαίωσης περιέχει συνδέσμους προς τους όρους χρήσης και μια έκθεση ασφάλειας των δεδομένων με τις βασικές πληροφορίες για τη νομοθεσία του GDPR. Μετά την ανάγνωση τους ο χρήστης αποφασίζει να δώσει τη συγκατάθεσή του (ή όχι) για την επεξεργασία των προσωπικών του δεδομένων.

3.2.4 Διαδικασία νομιμότητας, δικαιοσύνης και διαφάνειας

Σύμφωνα με τις βασικές αρχές της νομοθεσίας του GDPR που παρουσιάσαμε παραπάνω, τα δεδομένα ενός ατόμου πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που να ικανοποιεί τις απαιτήσεις νομιμότητας, δικαιοσύνης και διαφάνειας. Όπως εξηγήσαμε, αυτό σχετίζεται επίσης με το δικαίωμα της ενημέρωσης και ένα κατάλογος στοιχείων τα οποία ο κάτοχος του μητρώου πρέπει να ενημερώσει, π.χ. τα στοιχεία επικοινωνίας του κατόχου του μητρώου, τον σκοπό της επεξεργασίας των προσωπικών δεδομένων, την πηγή των προσωπικών δεδομένων, τη νομική βάση της επεξεργασίας και το είδος των δεδομένων που πρόκειται να συλλεχθούν. Με βάση αυτή τη διαδικασία, ο σχεδιαστής ενός ΚΠΣ θα πρέπει να δημιουργήσει μία έκθεση ασφάλειας δεδομένων για την επεξεργασία προσωπικών δεδομένων, η οποία να είναι διαθέσιμη για κάθε χρήστη.

Η έκθεση ασφάλειας δεδομένων θα πρέπει να περιέχει επίσης περιγραφές για τον τρόπο παράδοσης των δεδομένων, την αποθήκευση, αρχειοθέτηση και τη διανομή προσωπικών δεδομένων και τη γενική περιγραφή των τεχνικών και βιομετρικών μέτρων ασφαλείας. Επιπλέον, οι χρήστες θα πρέπει να ενημερώνονται για τις όποιες αλλαγές στους όρους.

3.2.5 Διαθεσιμότητα της ελαχιστοποίησης δεδομένων

Σύμφωνα με αυτή την αρχή, και όπως αναφέραμε σε προηγούμενη ενότητα, μόνο οι απαραίτητες πληροφορίες για ένα φυσικό πρόσωπο θα πρέπει να συγκεντρωθούν. Ο σχεδιαστής του ΚΠΣ θα πρέπει να ελέγξει τα αποτελέσματα απογραφής προσωπικών δεδομένων και π.χ. στη φόρμα εγγραφής και άλλα έντυπα

επεξεργασίας προσωπικών δεδομένων δεν θα πρέπει να υπάρχουν ειδικά κατηγοριοποιημένα πεδία δεδομένων. Ειδικά κατηγοριοποιημένα δεδομένα είναι π.χ. πληροφορίες για την εθνική, πολιτική ταυτότητα του χρήστη και την κατάσταση της υγείας του.

3.2.6 Αποθήκευση της ελαχιστοποίησης δεδομένων

Ο σχεδιαστής του ΚΠΣ θα πρέπει να έχει ένα σχέδιο εφαρμογής ενός μηχανισμού διαγραφής προσωπικών δεδομένων. Με την χαρτογράφηση προσωπικών δεδομένων ο σχεδιαστής θα γνωρίζει ποια δεδομένα έχουν αποθηκευτεί σε βάσεις δεδομένων και σε άλλες τοποθεσίες. Στη συνέχεια, η ομάδα ανάπτυξης του συστήματος θα μπορεί να υλοποιήσει αυτοματοποιημένες ρουτίνες καθαρισμού των βάσεων δεδομένων και των αρχείων.

3.2.7 GDPR χαρακτηριστικά του ΚΠΣ

1. **Συντήρηση αρχείων καταγραφής αλλαγών, πρόσβασης και σφαλμάτων**

Οι σχεδιαστές του ΚΠΣ θα πρέπει να καταχωρίσουν όλες τις θέσεις στις οποίες αποθηκεύονται τα δεδομένα καταγραφής και στη συνέχεια θα πρέπει να προσδιορίσουν τον σκοπό αποθήκευσης για κάθε αρχείο καταγραφής. Επιπλέον, θα πρέπει να αξιολογήσουν τον χρόνο για κάθε τύπο καταγραφής και πόσο χρονικό διάστημα θα διατηρούνται οι εγγραφές π.χ. σε κάποιο αποθηκευτικό μέσο. Για κάθε εγγραφή καταγραφής θα πρέπει να ενεργοποιηθεί ένας μηχανισμός ειδοποίησης με βάση την ημερομηνίας λήξης. Στη πληροφορία αυτή έχει πρόσβαση μια αυτοματοποιημένη υπηρεσία για την αυτόματη κατάργηση των αρχείων καταγραφής που έχουν λήξει.

Μία λίστα ελέγχου για την νόμιμη επεξεργασία καταγραφών (Lokiohje 2009) περιλαμβάνει τα παρακάτω:

- να προσδιοριστεί γιατί και ποιος είναι ο σκοπός και η νομική βάση για κάθε επεξεργασία ημερολογίου
- να αξιολογηθεί η ανάγκη για κάθε οντότητα καταγραφικών δεδομένων που αποθηκεύεται
- να προσδιοριστεί ποια προσωπικά δεδομένα μπορούν να αποθηκευτούν σε ημερολόγια
- να μάθουν οι χρήστες πώς πρέπει να προστατεύεται κάθε αρχείο καταγραφής
- να δώσουν προσοχή στις νομικές πτυχές της παρακολούθησης των ημερολογίων και, όταν είναι απαραίτητο, να συνεργαστούν με τους εργαζομένους
- να ειδοποιήσουν τους χρήστες και τους άλλους ενδιαφερόμενους για την επεξεργασία των καταγραφών
- να προσέξουν τις απαιτήσεις σχετικά με το μητρώο φυσικών οντοτήτων που έχει δοθεί από τις αρχές, αν το ημερολόγιο πρόκειται να αποτελέσει ένα τέτοιο μητρώο
- να σχεδιαστεί και τεκμηριωθεί ο σκοπός για την αποθήκευση και τη διασφάλιση της εφαρμογής του.

Τα μέλη της κοινότητας του ΚΠΣ θα πρέπει να εκπαιδευτούν για να ανταποκριθούν στις νέες απαιτήσεις διαχείρισης προσωπικών πληροφοριών. Ειδικά, η πρόσβαση στα δεδομένα των εξωτερικών μερών πρέπει να έχει έγκυρο σκοπό. Ένας χρήστης πρέπει να προσδιορίσει τον σαφή λόγο για τον οποίο επιθυμεί να αποκτήσει πρόσβαση στα δεδομένα ενός επισκέπτη/εξωτερικού συνεργάτη. Ο προαναφερόμενος λόγος είναι οι υποχρεωτικές πληροφορίες καταγραφής και χωρίς αυτό, ο χρήστης δεν μπορεί να έχει πρόσβαση στα δεδομένα. Έχει επίσης ληφθεί υπόψη προγραμματιστικά στην εφαρμογή ότι χωρίς βάσιμο λόγο η πρόσβαση στα δεδομένα είναι αδύνατη. Επιπλέον, οι χρήστες έχουν συμφωνήσει με

κάποιο ηλεκτρονικό τρόπο για χειρισμό προσωπικών στοιχείων, και έχει ενημερωθεί η όποια επιτροπή διοίκησης του ΚΠΣ.

2. Μη αποθήκευση μη χρήσιμων δεδομένων

Υπάρχουν δύο συνήθεις στρατηγικές για τη διαγραφή δεδομένων από μια βάση δεδομένων: μαλακός και σκληρός τρόπος διαγραφής. Ο μαλακός τρόπος διαγραφής σημαίνει ότι σε έναν πίνακα βάσης δεδομένων υπάρχει μια στήλη που ονομάζεται για παράδειγμα isDeleted. Όταν χρησιμοποιείται αυτός ο τύπος διαγραφής, ένα λογισμικό θα ορίσει μια σημαία στην παραπάνω στήλη δηλώνοντας ότι τα δεδομένα διαγράφονται (αρχειοθετούνται). Τα δεδομένα δεν θα αφαιρεθούν από τη βάση δεδομένων και θα παραμείνουν εκεί μέχρι να εκτελεσθεί ο σκληρός τρόπος διαγραφής.

Ο μαλακός τρόπος διαγραφής μπορεί να προκαλέσει σύνθετα ερωτήματα στη βάση δεδομένων στο μέλλον, επειδή οι προγραμματιστές πρέπει πάντα να φιλτράρουν προγραμματιστικά τα αρχειοθετημένα δεδομένα από τα αποτελέσματα των ερωτημάτων. Επιπλέον, τα ερωτήματα στη βάσης δεδομένων ενδέχεται να επιβραδυνθούν στο μέλλον, επειδή τα αρχειοθετημένα δεδομένα εξακολουθούν να βρίσκονται σε μια βάση δεδομένων και θα αντιμετωπίζονται με τον ίδιο τρόπο όπως τα μη αρχειοθετημένα δεδομένα. Όταν ο σκληρός τρόπος διαγραφής εφαρμοστεί, τα δεδομένα θα καταργηθούν οριστικά από μια βάση δεδομένων. Ο σκληρός τρόπος διαγραφής φέρνει, για παράδειγμα, τα ακόλουθα πλεονεκτήματα: είναι ευκολότερη συντήρηση ενός μικρότερου μεγέθους πίνακα. Η αναδημιουργία δεικτών είναι ταχύτερη και το μέγεθός τους θα είναι μικρότερο. Επιπλέον, ένας μικρότερος πίνακας έχει καλύτερες επιδόσεις (Kloeten 2009, Pinal 2010).

Ο περιορισμός της αποθήκευσης δεδομένων είναι μία από τις έξι αρχές προστασίας προσωπικών δεδομένων του GDPR (3.3 Αρχές του GDPR), και σημαίνει ότι τα προσωπικά δεδομένα πρέπει να αφαιρεθούν όταν δεν έχουν κανένα σκοπό ή νομική βάση για τη διατήρησή τους. Επομένως σε ένα ΚΠΣ η παραπάνω διαδικασία του μαλακού τρόπου διαγραφής (λειτουργία αρχειοθέτησης δεδομένων) θα πρέπει να

αντικατασταθεί από τον σκληρό τρόπο διαγραφής, για να μη διατηρούνται άχρηστα και μη –νόμιμα δεδομένα στις βάσεις δεδομένων του συστήματος. Με τον τρόπο αυτό θα υπάρξουν λιγότερες πιθανότητες για συμβάντα που ενδέχεται να προκαλέσουν παλιά και αλλοιωμένα δεδομένα, για παράδειγμα κατά τη μεταφορά δεδομένων, σε ένα άλλο σύστημα.

Μερικές φορές υπάρχει ένας τεχνικός ή νομικός λόγος για τον οποίο, για παράδειγμα, οι λογαριασμοί χρηστών δεν μπορούν να καταργηθούν από το σύστημα. Η διαγραφή ενός ατόμου μπορεί να προκαλέσει την απώλεια της ακεραιότητας αναφοράς των δεδομένων. Αυτό μπορεί εύκολα να προκαλέσει καταστροφή δεδομένων. Ένας τρόπος αντιμετώπισης αυτού του προβλήματος είναι η δημιουργία, για παράδειγμα, μιας προβολής (view) στη βάση δεδομένων που επιστρέφει τους χρήστες που δεν μπορούν να αφαιρεθούν από το σύστημα. Ένας νομικός λόγος για τη διατήρηση αρχειοθετημένων χρηστών σε μια βάση δεδομένων είναι π.χ. όταν τα δεδομένα έχουν ανακτηθεί από ένα API που παρέχεται από τις αρχές. Οι συγκεκριμένες αρχές μπορεί να απαιτούν την αποθήκευση καταγραφών για ερωτήματα ορισμένου χρόνου.

3. Αυτοματοποιημένη διαδικασία καθαρισμού δεδομένων

Σε ένα Πληροφοριακό Σύστημα- και αναμφισβήτητα επίσης στη περίπτωση των ΚΠΣ – η βάση δεδομένων είναι σημαντική συνιστώσα. Ο έλεγχος της πρόσβασης στις διαδικασίες ενημέρωσης των δεδομένων, ανάκτησης δεδομένων όπως επίσης στις διαδικασίες λήψης αντιγράφων ασφαλείας ή αυτόματου καθαρισμού δεδομένων τίθενται πλέον υπό το πρίσμα της προστασίας των δεδομένων.

Στη βάση δεδομένων του ΚΠΣ εκτελούνται προγραμματισμένες εργασίες όπως η λήψη αντιγράφων ασφαλείας βάσεων δεδομένων. Αυτές οι εργασίες μπορούν να ρυθμιστούν ώστε να εκτελούνται αυτόματα, π.χ. κάθε Παρασκευή στις 23:00. Αν η εργασία αντιμετωπίζει κάποιο πρόβλημα, το σύστημα διαχείρισης της βάσης δεδομένων (DBMS) καταγράφει το συμβάν και μπορεί να ρυθμιστεί, για

παράδειγμα, για να στείλει ειδοποιήσεις σε ένα άτομο υπεύθυνο για τις βάσεις δεδομένων και τις προαναφερθείσες εργασίες.

Μια εργασία είναι μια σειρά από βήματα (ενέργειες) που εκτελεί το DBMS στο παρασκήνιο συνήθως μέσω ενός Agent (πχ SQL Server Agent). Οι εργασίες μπορούν να εκτελεστούν μία ή πολλές φορές, ανάλογα με τη φύση μιας εργασίας και ένα πρόγραμμα. Η επιτυχία ή η αποτυχία μιας εργασίας μπορεί να παρακολουθηθεί εύκολα. Μια εργασία μπορεί να εκτελεστεί σε έναν τοπικό ή σε πολλούς απομακρυσμένους διακομιστές (SQL Server Agent 2017).

Επίσης ένα DBMS έχει τη δυνατότητα δημιουργίας και εκτέλεσης ενσωματωμένων διαδικασιών από τον χρήστη (πχ stored procedures). Εάν ένας προγραμματιστής χρειάζεται την ίδια λειτουργία βάσης δεδομένων σε πολλά διαφορετικά σενάρια, ίσως είναι χρήσιμο να γραφτεί μια ενσωματωμένη διαδικασία. Αυτό εξαλείφει την ανάγκη γραφής του ίδιου κώδικα πολλές φορές. Όταν μια λειτουργία βάσης δεδομένων βρίσκεται στη βαθμίδα δεδομένων μόνο, μειώνει την κυκλοφορία δικτύου μεταξύ ενός πελάτη και ενός διακομιστή, ο οποίος επίσης παρέχει ισχυρότερη ασφάλεια, επειδή η διαδικασία ελέγχει ποιες δραστηριότητες μπορούν να εκτελεστούν, π.χ. στις βάσεις δεδομένων αντί να δοθούν δικαιώματα σε πολλούς χρήστες ή προγράμματα.

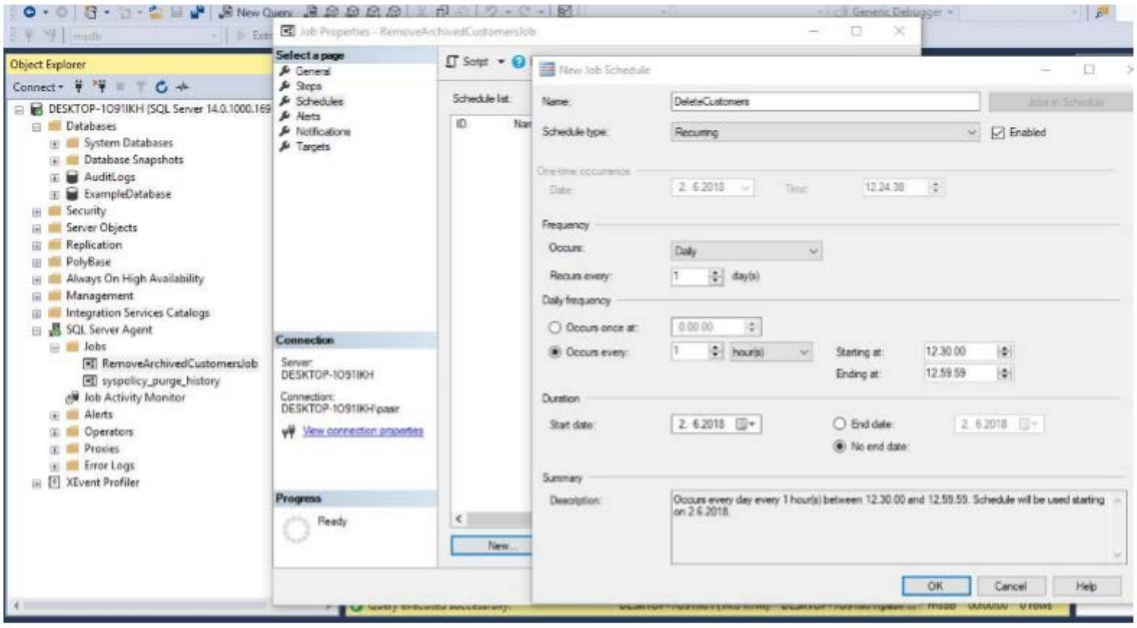
Επιπλέον, όταν χρησιμοποιείται μια διαδικασία μέσω του δικτύου, μια εντολή εκτέλεσης είναι το μόνο ορατό τμήμα της και οι κακόβουλες χρήστες δεν μπορούν να δουν μια υποκείμενη βάση δεδομένων ή ονόματα αντικειμένων πίνακα. Επιθέσεις της μορφής SQL injection δεν μπορούν επίσης να προληφθούν, επειδή οι δηλώσεις SQL του κακόβουλου χρήστη δεν μπορούν να ενσωματωθούν εάν οι παράμετροι μιας διαδικασίας αντιμετωπίζονται ως μία ακέραιη τιμή και όχι ως εκτελέσιμος κώδικας.

Η συντήρηση είναι επίσης ένα από τα οφέλη, επειδή κάποιος μπορεί να αλλάξει μόνο μια συγκεκριμένη δομή στη βάση δεδομένων και το πρόγραμμα-πελάτης δεν χρειάζεται να γνωρίζει τίποτα από αυτές τις αλλαγές. Οι ενσωματωμένες διαδικασίες που δημιουργεί ο χρήστης έχουν επίσης καλύτερο χρόνο απόδοσης,

επειδή θα μεταγλωττιστούν την πρώτη φορά που θα εκτελεσθούν. Επομένως, σε επόμενες εκτελέσεις ο διακομιστής δεν χρειάζεται να επαναλάβει την ίδια διαδικασία ((Stored Procedures (Database Engine) 2017).

Επομένως η ομάδα ανάπτυξης λογισμικού ενός ΚΠΣ μπορεί να υλοποιήσει ενσωματωμένες διαδικασίες και διεργασίες στο παρασκήνιο μίας βάσης δεδομένων για τη συμμόρφωση με τις απαιτήσεις της νομοθεσίας. Η ομάδα καλείται με αυτούς τους μηχανισμούς να σχεδιάσει διαφορετικές διαδικασίες για τον καθαρισμό βάσεων δεδομένων από δεδομένα που είναι άχρηστα.

Επιπλέον, η ομάδα ανάπτυξης λογισμικού μπορεί να δημιουργήσει διαδικασίες για τον έλεγχο των βάσεων δεδομένων, ώστε να μην υπάρχουν μη συμβατά δεδομένα με τον GDPR στη βάση. Όλες οι διαγραφές δεδομένων θα καταγράφονται επίσης, ώστε αργότερα η ομάδα να μπορεί να ελέγξει γιατί π.χ. ένας χρήστης δεν υπάρχει πια και ποιος τον αφαίρεσε. Τα αρχεία με τις καταγραφές των διαγραφών δεδομένων μπορούν να αποθηκευτούν σε άλλη τοποθεσία, διότι αν μια βάση δεδομένων καταστραφεί, τότε είναι σημαντικό να ελεγχθούν τα αρχεία καταγραφών και να εντοπιστούν ποια δεδομένα είχαν προηγουμένως διαγραφεί. Με αυτόν τον τρόπο ο οργανισμός ή η κοινότητα που συντηρεί το ΚΠΣ μπορεί να αποτρέψει ένα πρόβλημα από το γεγονός ότι τα δεδομένα που έχουν διαγραφεί ενδέχεται να αποκατασταθούν ξανά σε μια βάση δεδομένων τυχαία.



Εικόνα 5. Παράδειγμα διεργασίας αυτόματης διαγραφής δεδομένων πελατών

Συνεπώς, αυτοματοποιημένες διαδικασίες για τον καθαρισμό και σχετικό έλεγχο των δεδομένων μπορούν να προγραμματιστούν στον SQL Server Agent ως εργασίες (jobs). Η αυτοματοποίηση βοηθάει καθώς κανείς δεν θα θυμάται να εκτελέσει τις διαδικασίες με το χέρι και επιπλέον θα πρέπει να αφιερώσει χρόνο σε αυτό. Η ομάδα ανάπτυξης λογισμικού σίγουρα θα έχει πιο σημαντικά καθήκοντα από ό, τι η χειρωνακτική εκτέλεση των αποθηκευμένων διαδικασιών, π.χ. κάθε εβδομάδα.

Ο SQL Server Agent καταγράφει επίσης όλα τα σφάλματα, τα οποία μπορεί να αντιμετωπίσει μια διαδικασία κατά την εκτέλεση της. Ο agent μπορεί να διαμορφωθεί επίσης για να στέλνει ειδοποιήσεις στην ομάδα ανάπτυξης λογισμικού. Σε περίπτωση που παρουσιαστεί κάποιο πρόβλημα, κάποιος στην ομάδα μπορεί να ξεκινήσει την εξέταση του προβλήματος που ανέφερε ο πράκτορας. Ως εκ τούτου, η ομάδα πρέπει να παρακολουθεί τακτικά το ιστορικό των εργασιών του πράκτορα για να διασφαλιστεί η εύρυθμη εκτέλεση της αυτοματοποιημένης διαδικασίας.

```
USE [ExampleDatabase]
GO
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE PROCEDURE [dbo].[RemoveArchivedCustomers]
AS
SET NOCOUNT ON;
DECLARE @customerId INT;
DECLARE @dbCursor AS CURSOR;
-- All customers which needs to be deleted
SET @dbCursor = CURSOR FOR SELECT c.Id FROM ExampleDatabase.dbo.Customers c WHERE c.Archived = 1;
-- Open cursor
OPEN @dbCursor;
-- Get customer's id for delete
FETCH NEXT FROM @dbCursor INTO @customerId;
-- Loop through all customers which were found
WHILE @@FETCH_STATUS = 0
BEGIN
    -- Delete customer
    DELETE FROM ExampleDatabase.dbo.Customers WHERE Id = @customerId;
    -- Set log text
    DECLARE @logText VARCHAR(1000);
    SET @logText = 'Deleted customer, id = ' + CAST(@customerId AS VARCHAR(1000));
    -- Write audit log that we know who/what deleted the customer
    INSERT INTO [AuditLogs].[dbo].[AuditLog] (
            [Operation]         -- Name of the operation (Insert, Update, Delete)
           ,[DatabaseName]      -- Name of the database
           ,[TableName]         -- Name of the database table
           ,[TargetId]          -- Target Id (Id of a customer), if we must restore a database, we know which records we should remove automatically
           ,[LogText]           -- Audit log text
           ,[Logger]            -- Script that was executed
           ,[UserName]          -- Name of the user who executed
           ,[PersonName]        -- First- and lastname of the user
           ,[Company]           -- Company of the user
           ,[LogDatetime]       -- Timestamp
           ,[ExpirationDatetime] -- Expiration datetime for a log record
    ) VALUES (
            'Delete'
           ,'ExampleDatabase'
           ,'Customers'
           ,@customerId
           ,@logText
           ,'PROCEDURE dbo.RemoveDeletedCustomers'
           ,'sa'
           ,''
           ,''
           ,GETDATE()
           ,DATEADD(MM, 6, GETDATE()) -- Keep log records for six months as long as database backups will be stored
    );
    -- Get next customer's id for delete
    FETCH NEXT FROM @dbCursor INTO @customerId
END
-- Close cursor
CLOSE @dbCursor;
DEALLOCATE @dbCursor;
GO
```

Εικόνα 6. Παράδειγμα Stored Procedure (SQL Server)

4. Αναζήτηση προσωπικών δεδομένων

Το ΚΠΣ θα πρέπει να διαθέτει φόρμες αναζήτησης προσωπικών δεδομένων μέσω του συστήματος. Με αυτόν τον τρόπο οι χρήστες μπορούν να πραγματοποιούν οι ίδιοι τις αναζητήσεις και δεν θα στέλνουν αιτήματα αναζήτησης σε άλλο τμήμα (πχ το τμήμα υποστήριξης). Στο σύστημα ενδεχομένως να υπάρχουν δεδομένα χιλιάδων ανθρώπων της κοινότητας και αυτό θα εξοικονομήσει σημαντικό χρόνο των υπαλλήλων του helpdesk όταν μπορούν να επικεντρωθούν στην επίλυση άλλων προβλημάτων ενός πελάτη. Επιπλέον, με τον τρόπο αυτό η πρόσβαση στα

προσωπικά δεδομένα περιορίζεται μέσω συγκεκριμένης λειτουργίας και σε συγκεκριμένα τμήματα.

5. Αυτοματοποιημένη διαδικασία διαγραφής αρχείων

Το σύστημα ενδεχομένως να διαθέτει χιλιάδες αρχεία πελατών και μπορεί να είναι αδύνατο να ελεγχθεί ποιο από αυτά περιέχει προσωπικά δεδομένα. Για αυτό το λόγο η διαγραφή των αρχείων μπορεί να αυτοματοποιηθεί δημιουργώντας μια υπηρεσία που θα αναλάβει τη διαγραφή τους από το σύστημα. Όλα τα μη απαραίτητα αρχεία θα καταργούνται αυτόματα όταν δεν υπάρχει λόγος αποθήκευσης τους. Ένας χρήστης μπορεί να επισημαίνει ένα αρχείο που πρέπει να αφαιρεθεί και η υπηρεσία θα διαβάσει από μια βάση δεδομένων τα αρχεία που πρέπει να καταργήσει.

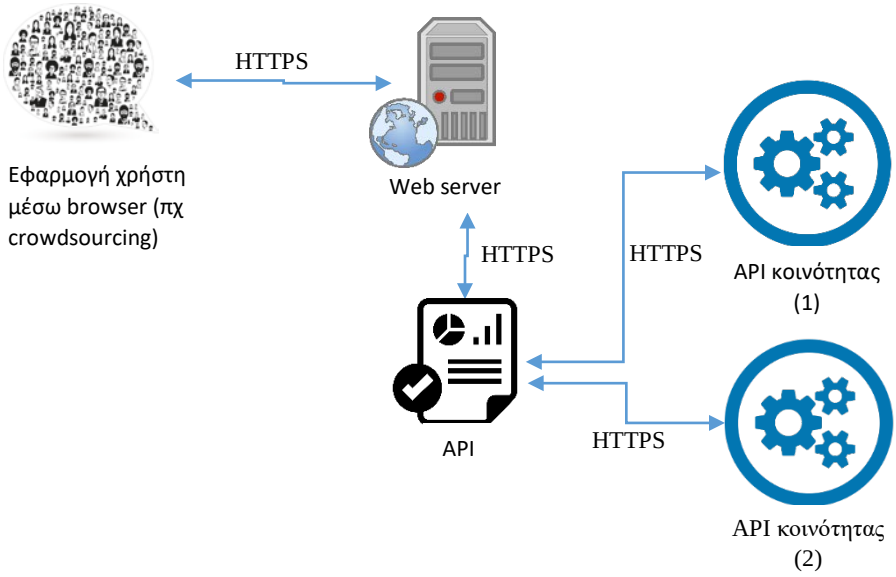
Τα οφέλη του να διαγράφονται τα περιττά αρχεία είναι τα εξής:

- δεν υπάρχουν περιττά αρχεία για λήψη π.χ. δεν καταλαμβάνουν χώρο στο δίσκο
- ο χρήστης δεν χρειάζεται να ελέγξει ένα μεγάλο αρχείο για το ποιά αρχεία πρέπει να αφαιρεθούν
- θα εξοικονομηθεί χρόνος για τον υπεύθυνο ελέγχου των δεδομένων και τον υπεύθυνο επεξεργασίας
- με όλα τα παραπάνω εφαρμόζεται ο περιορισμός αποθήκευσης δεδομένων, μία από τις έξι αρχές προστασίας προσωπικών δεδομένων του GDPR.

6. Πρωτόκολλο HTTPS έναντι του HTTP

Ο ιστότοπος μεταφέρει περιεχόμενο από ένα διακομιστή στο πρόγραμμα περιήγησης ενός χρήστη μέσω του πρωτοκόλλου HTTP και είναι ένα αρχείο κειμένου ουσιαστικά με διακριτά δεδομένα. Οποιοσδήποτε μπορεί να δει το περιεχόμενο αυτού του αρχείου, επειδή δεν είναι κρυπτογραφημένο. Σήμερα, οι

περισσότεροι ιστότοποι χρησιμοποιούν το πρωτόκολλο HTTPS αντί του HTTP για να διασφαλίσουν την ιδιωτικότητα και την ασφάλεια των δεδομένων. Επομένως, το κύριο πλεονέκτημα της χρήσης του HTTPS με πιστοποιητικό SSL είναι η ασφάλεια, επειδή όλο το περιεχόμενο θα κρυπτογραφηθεί και θα μεταφερθεί με ασφαλή τρόπο, π.χ. το όνομα χρήστη, τον κωδικό πρόσβασης και τα δεδομένα του πελάτη (Hopping & Millman 2018).



Εικόνα 7. Δικτυακές συνδέσεις μέσω HTTPS

Όπως φαίνεται και στο παραπάνω διάγραμμα, η δικτυακή κυκλοφορία μεταξύ ενός διακομιστή ιστού και του προγράμματος περιήγησης του χρήστη καθώς και η κυκλοφορία μεταξύ των προγραμματιστικών βιβλιοθηκών (API) και άλλων συστημάτων θα πρέπει να προστατεύονται με τη χρήση HTTPS και του πιστοποιητικού SSL. Αυτό αποτρέπει τις παραβιάσεις δεδομένων που μπορεί να προκύψουν όταν π.χ. το API στέλνει δεδομένα σε άλλο σύστημα μέσω του Διαδικτύου. Με τον τρόπο αυτό γίνεται συμμόρφωση με μέρος των αρχών της νομοθεσίας GDPR, το οποίο απαιτεί την επεξεργασία των προσωπικών δεδομένων κατά τρόπο που διασφαλίζονται και προστατεύονται από μη εξουσιοδοτημένη ή παράνομη επεξεργασία.

7. Φορητότητα δεδομένων

Το άρθρο 20 της νομοθεσίας του GDPR αφορά το δικαίωμα μεταφοράς δεδομένων, δηλαδή ένα φυσικό πρόσωπο έχει το δικαίωμα να λάβει τα προσωπικά δεδομένα που τον αφορούν. Τα δεδομένα πρέπει να είναι π.χ. σε μία κοινά δομημένη και μηχανικά αναγνώσιμη μορφή. Επιπλέον, ένα φυσικό πρόσωπο έχει το δικαίωμα να μεταφέρει τα δεδομένα στο σύστημα άλλου ελεγκτή. (Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 2016).

Αυτή είναι μια προβληματική απαίτηση του GDPR, επειδή δεν μπορούν να μεταφερθούν όλα τα δεδομένα στο σύστημα ενός άλλου ελεγκτή. Τα δεδομένα σε ένα ΚΠΣ μπορεί να είναι σημαντικά από επιχειρηματική άποψη σε έναν υπεύθυνο επεξεργασίας δεδομένων και έχουν έναν λεγόμενο επιχειρηματικό σκοπό για την επεξεργασία και την αποθήκευση τους. Οι χρήστες ενδέχεται να έχουν κάποια επαγγελματικά προσόντα, π.χ. πιστοποιήσεις για επικίνδυνη εργασία. Οι προαναφερόμενες πιστοποιήσεις είναι μερικές φορές δεδομένα προσωπικού χαρακτήρα και μπορούν να θεωρηθούν ότι μεταφέρονται μεταξύ διαφορετικών εταιρειών. Μία τυπική κατάσταση είναι π.χ. όταν ένας εργολάβος μισθώνει τους υπαλλήλους του σε έργα άλλης εταιρείας. Φυσικά, εκεί θα πρέπει να τεθούν κανόνες για το ποια χαρακτηριστικά περιλαμβάνονται στο πλαίσιο της φορητότητας δεδομένων. Στο παραπάνω παράδειγμα η αυθαίρετη φορητότητα θα διευκολύνει την ενοικίαση των εργαζομένων μεταξύ έργων.

8. Αξιολόγηση των χαρακτηριστικών του ΚΠΣ

Όταν ένα ΚΠΣ έχει π.χ. πάνω από 15 χρόνια ιστορίας πίσω από αυτό και πολλοί προγραμματιστές έχουν εργαστεί σε αυτό, ίσως είναι καλή ιδέα να αναθεωρηθούν ποια χαρακτηριστικά εξακολουθούν να ισχύουν και ποιά θα πρέπει να καταργηθούν. Ορισμένες λειτουργίες έχουν προστεθεί και καταργηθεί στο κύκλο ζωής της εφαρμογής. Βεβαίως, θα υπάρχουν δεδομένα μη συμβατά με τη νομοθεσία του GDPR που βρίσκονται χωρίς σκοπό, π.χ. σε βάσεις δεδομένων, επειδή πιθανώς

κανείς δεν τα διέγραψε από τη βάση δεδομένων όταν απενεργοποιήθηκαν τα παλιά χαρακτηριστικά.

Μια πολύ κοινή τεχνική για την αποτροπή των προαναφερθέντων καταστάσεων είναι η αναδόμηση (refactoring), πράγμα που σημαίνει ότι η εσωτερική δομή μιας εφαρμογής θα αλλάξει χωρίς να αλλάξει η εξωτερική της συμπεριφορά. Υπάρχουν τουλάχιστον τρεις διαφορετικές περιοχές refactoring: αναδόμηση πηγαίου κώδικα, βάσης δεδομένων και διεπαφής χρήστη (Veerraju & Srinivasa & Murali 2010).

Η αναδόμηση του κώδικα έχει τα ακόλουθα πλεονεκτήματα (Veerraju & Srinivasa & Murali 2010):

- Κάνει τον κώδικα αναγνώσιμο για άλλους προγραμματιστές.
- Διευκολύνει τη συντήρηση και την αναβάθμιση του κώδικα.
- Αυξάνει την ποιότητα σχεδιασμού και υλοποίησης εφαρμογών.
- Μπορεί να θεωρηθεί ως επένδυση για το μέλλον.

Η διαγραφή των περιττών δεδομένων και πινάκων από τη βάση δεδομένων όχι μόνο βελτιώνει την ποιότητα της εφαρμογής, αλλά βοηθά επίσης ένα οργανισμό να απαλλαγεί από τα μη συμβατά δεδομένα ως προς τον GDPR. Για παράδειγμα, οι πάροχοι υπηρεσιών υπολογιστικού νέφους (ΥΝ) χρεώνουν για την αποθήκευση δεδομένων στους δίσκους που είναι διαθέσιμοι στο ΥΝ. Το κόστος δεν είναι μεγάλο για μικρές βάσεις δεδομένων. Ωστόσο, όταν το μέγεθος της βάσης δεδομένων είναι π.χ. 1000 Gigabytes, ο καθαρισμός της βάσης δεδομένων από περιττά δεδομένα βελτιώνει την απόδοση και μειώνει το κόστος. Η αναδόμηση του πηγαίου κώδικα ενδέχεται επίσης να μειώσει την πιθανότητα κυβερνοεπίθεσης από κακόβουλους χρήστες. Έτσι, ο επανασχεδιασμός ενός ΚΠΣ για τη πλήρη συμμόρφωση με την νομοθεσία του GDPR δεν είναι μόνο ένα βαρύ φορτίο για τους οργανισμούς αλλά είναι επίσης μια ευκαιρία βελτίωσης των χαρακτηριστικών τους. Οι εταιρείες θα πρέπει να επαναπροσδιορίσουν τις απαιτήσεις τους ακόμη και αν δεν υπήρχε GDPR.

3.3 Διαδικασία κοινοποίησης πιθανής παραβίασης δεδομένων

Μία από τις απαιτήσεις του GDPR είναι ότι η τοπική εποπτική αρχή πρέπει να ενημερώνεται για τις παραβιάσεις δεδομένων το συντομότερο δυνατό. Ο οργανισμός – ιδιοκτήτης ενός ΚΠΣ- πρέπει να δημιουργήσει μια πολιτική για αυτή τη διαδικασία. Πρέπει να υπάρχει μια καθορισμένη ομάδα ανθρώπων που θα αναλάβουν την ευθύνη όταν υπάρχει υποψία ή ένα συμβάν που αφορά την ασφάλεια των πληροφοριών.

Η γενική απαίτηση είναι ότι σε περίπτωση που μια παραβίαση δεδομένων προκαλεί κίνδυνο για τα δικαιώματα και την ελευθερία ενός φυσικού προσώπου, η κοινοποίηση πρέπει να αποσταλεί χωρίς αδικαιολόγητη καθυστέρηση (μέσα σε 72 ώρες) όταν ο ελεγκτής έχει λάβει γνώση της παραβίασης. Οι τυπικές παραβιάσεις δεδομένων είναι κλοπή υπολογιστών ή φορητών μέσων αποθήκευσης, εισβολή στο δίκτυο ή υπολογιστή του οργανισμού, μολύνσεις από κακόβουλο λογισμικό, πυρκαγιά σε υπολογιστικό κέντρο, μία γενικότερης κλίμακας κυβερνο-επίθεση και η αποστολή μιας επίσημης δήλωσης σε λάθος άτομο.

Ο υπεύθυνος ελέγχου πρέπει να παρέχει π.χ. τις ακόλουθες πληροφορίες:

- περιγραφή της παραβίασης των προσωπικών δεδομένων
- στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων ή άλλης επαφής που θα παρέχει περισσότερες πληροφορίες
- συνέπειες της παραβίασης
- ενέργειες που έλαβε ο ελεγκτής για να μετριάσει τις επιπτώσεις της παραβίασης των δεδομένων

3.4 Προτάσεις για την μελλοντική εναρμόνιση με τις απαιτήσεις του GDPR

Ο κάθε οργανισμός που καλείται να διαχειριστεί ένα ΚΠΣ είναι εις γνώση του ότι δεν είναι δυνατόν να τηρούνται οι εφαρμοζόμενες διαδικασίες, πολιτικές και δυνατότητες λογισμικού σε συμμόρφωση με την οδηγία του GDPR για πάντα. Σίγουρα θα υπάρξουν αλλαγές στη νομοθεσία και θα σχεδιαστούν και θα εφαρμοστούν νέα χαρακτηριστικά λογισμικού.

3.4.1 Παρακολούθηση των αλλαγών στον GDPR

Ο οργανισμός πρέπει να ενεργεί γρήγορα όταν η κυβέρνηση/ΕΕ αλλάζει τη νομοθεσία και μάλλον πριν από την έναρξη ισχύος της. Οι αρχές ενδέχεται να διατάξουν πρόστιμα, αγωγές ή κλείσιμο σε μη συμμορφούμενες εταιρείες. Η νέα νομοθεσία ενδέχεται να επιφέρει αλλαγές στις υπάρχουσες διαδικασίες και πολιτικές και η δημιουργία νέων απαιτεί πάντα κάποια προσπάθεια. Επιπλέον, οι εργαζόμενοι πρέπει να εκπαιδεύονται για τους νέους ρόλους και τις ευθύνες τους. Μια επιχείρηση δεν μπορεί να απαλλαγεί από τους νόμους και είναι σημαντικό να διασφαλιστεί η συνέχεια της επιχείρησης (Masson 2017).

Ο οργανισμός πρέπει να παρακολουθεί τις αλλαγές στην οδηγία του GDPR για να διασφαλίσει ότι λαμβάνονται υπόψη οι νεότερες ενημερώσεις στους κανονισμούς, π.χ. στις πολιτικές και τις διαδικασίες της εταιρείας. Όπως αναφέρθηκε προηγουμένως, η νομοθεσία χρειάζεται ορισμένες γενικά καθορισμένες οδηγίες σχετικά με το τι πρέπει να κάνουν οι επιχειρήσεις με τον κανονισμό, διότι ο κανονισμός αφήνει πολλά κενά προς ερμηνεία. Συνεπώς είναι σημαντικό για τον οργανισμό να παρακολουθεί τις αλλαγές της νομοθεσίας και να αντιδρά με τον απαραίτητο τρόπο σε αυτές.

3.4.2 Τακτική εκπαίδευση του προσωπικού

Οι καλύτεροι έλεγχοι ασφαλείας και το τείχος προστασίας δεν θα βοηθήσουν τον οργανισμό αν π.χ. ένας εισβολέας αποκτήσει πρόσβαση στο δίκτυο ή σε ευαίσθητα πληροφοριακά συστήματα χρησιμοποιώντας τεχνικές κοινωνικής μηχανικής. Ένας εισβολέας μπορεί να επικοινωνήσει με το γραφείο εξυπηρέτησης μιας εταιρείας και να προσποιηθεί ότι είναι εξωτερικός συνεργάτης ή προμηθευτής για να αποκτήσει ευαίσθητες πληροφορίες. Επιπλέον, ένας υπάλληλος μπορεί να εξαπατηθεί για να κάνει κλικ σε έναν κακόβουλο σύνδεσμο που προέρχεται από ένα ηλεκτρονικό ταχυδρομείο ή μια ψεύτικη πηγή στα κοινωνικά μέσα. Ένας εισβολέας μπορεί να επισκεφθεί για μη ελεγχόμενο λόγο τις εγκαταστάσεις του οργανισμού και να εγκαταστήσει κακόβουλα USB sticks, να κλέψει περιουσιακά στοιχεία ή ακόμα και να βλάψει τους ανθρώπους (Goodchild & Hulme 2017).

Οι εργαζόμενοι θα πρέπει να εκπαιδεύονται τακτικά για να αποτρέπουν π.χ. παραβιάσεις μέσω κοινωνικής μηχανικής, για αυτό ένας οργανισμός θα πρέπει να πραγματοποιεί σεμινάρια ασφάλειας και συμμόρφωσης στις οδηγίες του GDPR για τους υπαλλήλους της. Επιπλέον, οι οδηγίες του helpdesk θα ενημερώνονται συνεχώς και όταν συμβαίνει κάτι καινούργιο, αυτές οι αλλαγές θα πρέπει να κοινοποιούνται στους υπαλλήλους, τις κοινότητες εξωτερικών χρηστών και συνεργατών (πχ crowdsourcing). Είναι επίσης σημαντικό να εκπαιδεύονται τα μέλη της ομάδας ανάπτυξης στις πολιτικές ασφάλειας, τη νέα τεχνολογία, τους ελέγχους ασφαλείας και τα εργαλεία.

3.4.3 Εσωτερικός έλεγχος

Είναι σημαντικό να διασφαλιστεί ότι η ασφάλεια των πληροφοριών και η κανονιστική συμμόρφωση έχουν εφαρμοστεί σωστά. Ο εσωτερικός έλεγχος είναι ένα καλό εργαλείο που βοηθά τους οργανισμούς να καθορίσουν ποιες περιοχές

μπορεί να χρειαστούν βελτίωση καθώς επίσης εκθέτει πιθανούς κινδύνους. Το πεδίο εφαρμογής ενός εσωτερικού ελέγχου συνίσταται στην παρακολούθηση, ανάλυση και αξιολόγηση π.χ. των κινδύνων ενός οργανισμού. Επιπλέον, η συμμόρφωση με το νόμο ενδέχεται να επανεξεταστεί. Οι συστάσεις είναι επίσης αποτέλεσμα των εσωτερικών ελέγχων.

Οι νόμοι θα αλλάξουν και είναι σημαντικό να παρακολουθούνται αυτές οι αλλαγές έτσι ώστε ο οργανισμός να παραμένει συμμορφούμενος με αυτούς. Μια εταιρεία πρέπει να αλλάξει τις διαδικασίες και τις πολιτικές της ως αποτέλεσμα αλλαγών στο νόμο, για αυτό και ο οργανισμός πρέπει να διενεργεί τακτικούς εσωτερικούς ελέγχους για να παραμείνει π.χ. συμβατός με τον GDPR. Οι πολιτικές ασφάλειας και οι διαδικασίες ανάπτυξης λογισμικού πρέπει να ελέγχονται έτσι ώστε η εταιρεία να μπορεί να μειώσει τις παραβιάσεις της ασφάλειας και η συνολικής της απόδοση να παραμένει υψηλή.

3.4.4 Ενσωμάτωση του GDPR στο σχεδιασμό και την εφαρμογή λειτουργιών

Οι διαδικασίες ανάπτυξης λογισμικού θα πρέπει να περιλαμβάνουν φάσεις εργασίας για την ανάλυση των απαιτήσεων της ασφάλειας των πληροφοριών και τη διαχείριση των προσωπικών δεδομένων. Οι απαιτήσεις ασφάλειας ποικίλλουν ανάλογα με τον τομέα στον οποίο ειδικεύεται η εταιρεία. Οι τεχνικές εφαρμογές πρέπει να σχεδιάζονται κατά τρόπο ώστε να συμβαδίζουν με το επίπεδο κινδύνου των δεδομένων. Είναι σημαντικό να συμπεριληφθεί η εκτίμηση των επιπτώσεων στη διαδικασία ανάπτυξης λογισμικού από την αρχή για να ληφθούν π.χ. οι απαιτήσεις ασφάλειας δεδομένων εάν εφαρμόζονται σωστά.

Τα συστήματα που έχουν σχεδιαστεί λανθασμένα μπορεί να είναι δύσκολο να αλλάξουν για να είναι συμβατά με τις απαιτήσεις ασφάλειας δεδομένων. Είναι επίσης σημαντικό να διασφαλιστεί ότι οι έλεγχοι ασφαλείας εφαρμόζονται σωστά κατά τη διάρκεια της φάσης ανάπτυξης και στη συνέχεια. Οι τεχνικές μέθοδοι

ασφαλείας μπορεί να είναι, για παράδειγμα, ο έλεγχος πρόσβασης και η κρυπτογράφηση / ανωνυμοποίηση δεδομένων.

Όταν σχεδιάζονται και εφαρμόζονται λειτουργίες σε ένα ΚΠΣ, πρέπει να λαμβάνονται υπόψη οι έλεγχοι συμμόρφωσης στον GDPR και στην ασφάλεια πληροφοριών. Με αυτόν τον τρόπο ο οργανισμός δημιουργεί αυτόματα συμβατές με τον GDPR εφαρμογές. Για παράδειγμα, αν η ομάδα ανάπτυξης λογισμικού ακολουθεί τη μεθοδολογία Scrum, τότε αναπτύσσει τα χαρακτηριστικά της εφαρμογής σε sprints (μικρές φάσεις ανάλυσης, σχεδιασμού, υλοποίησης, δοκιμών). Οι απαιτήσεις της νομοθεσίας GDPR μπορούν να ληφθούν υπόψη πριν, κατά τη διάρκεια και μετά τα sprints.

Όταν ξεκινά ένα sprint, υπάρχει μια συνάντηση σχεδιασμού και η ομάδα σχεδιάζει τα καθήκοντα για την υλοποίηση συγκεκριμένων απαιτήσεων για το επερχόμενο sprint. Μια εργασία περιέχει μια περιγραφή πώς πρέπει να υλοποιηθεί μια λειτουργία. Ως εκ τούτου, μια συνάντηση σχεδιασμού sprint θα μπορούσε να είναι με σκοπό εάν οι λειτουργίες προς υλοποίηση πρέπει να λάβουν υπόψη τις απαιτήσεις της οδηγίας GDPR.

Κατά τη διάρκεια ενός sprint, όταν έχει γίνει μια εργασία, τα μέλη της ομάδας θα εξετάσουν και θα δοκιμάσουν τις υλοποιήσεις. Οι απαιτήσεις του GDPR μπορούν να αναθεωρηθούν και να δοκιμαστούν ταυτόχρονα. Μετά το sprint, θα υπάρξει μια συνάντηση για ανατροφοδότηση και η ομάδα θα έχει την ευκαιρία να αξιολογήσει τις διαδικασίες, τα εργαλεία, τις υλοποιήσεις και να δημιουργήσει συστάσεις για το μελλοντικό της έργο. Με αυτόν τον τρόπο οι απαιτήσεις GDPR μπορούν να ληφθούν υπόψη κατά τη διάρκεια ολόκληρου του κύκλου ζωής ανάπτυξης κάθε λογισμικού.

3.4.5 Έλεγχος των λειτουργιών και των δεδομένων του λογισμικού

Ο GDPR και άλλα λειτουργικά χαρακτηριστικά που εφαρμόζονται σε ένα ΚΠΣ και οι διαδικασίες αυτόματου καθαρισμού πρέπει να ελέγχονται και να δοκιμάζονται

τακτικά για το αν λειτουργούν σωστά. Επιπλέον, πρέπει να αφαιρεθούν άχρηστα δεδομένα και αρχεία. Το ιστορικό εργασιών του καθαρισμού της βάσης δεδομένων μπορεί να προβληθεί στη διεπαφή διεργασιών του πράκτορα του SQL Server. Αυτό μπορεί να γίνει με μια δέσμη ενεργειών SQL για τον έλεγχο όλων των απαραίτητων πινάκων στη βάση δεδομένων που ενδέχεται να περιέχουν προσωπικά δεδομένα, ώστε να μην υπάρχουν περιττά δεδομένα.

Η υπηρεσία καθαρισμού αρχείων χρειάζεται επίσης αυτοματοποίηση για τον έλεγχο ότι όλα τα αρχεία που έχουν επισημανθεί προς απομάκρυνση έχουν διαγραφεί. Χωρίς αυτοματοποίηση μπορεί να είναι μια επίπονη χειρωνακτική εργασία για την εύρεση αρχείων που πρέπει να αφαιρεθούν. Με αυτό τον τρόπο μπορεί να ελεγχθεί ότι π.χ. η εργασία στη βάση δεδομένων είναι πλήρως λειτουργική.

Όταν ένα νέο χαρακτηριστικό έχει εφαρμοστεί ή μια υπάρχουσα λειτουργία τροποποιηθεί, οι προγραμματιστές πρέπει να αλλάξουν και να ελέγξουν τις αυτόματες υπηρεσίες καθαρισμού για να πιστοποιήσουν ότι λειτουργούν σωστά. Το λογισμικό πρέπει επίσης να ελέγχεται από την πλευρά του GDPR, έτσι ώστε όλα τα προσωπικά δεδομένα να έχουν νόμιμο σκοπό για επεξεργασία και αποθήκευση.

Κεφάλαιο 4
Επίλογος

Μέσα από την ανασκόπηση της βιβλιογραφίας και της μελέτης προτάσεων για τον τρόπο προσαρμογής του σχεδιασμού των ΚΠΣ στη νομοθεσία του GDPR, προκύπτει ότι αυτό γίνεται ακόμα εμπειρικά χωρίς τη καθοδήγηση κάποιου μοντέλου. Αυτό γιατί η νέα νομοθεσία αφήνει πολλά θέματα προς ερμηνεία και δεν καθορίζει με ακρίβεια το επίπεδο που είναι νομικά αποδεκτό για την προστασία των προσωπικών δεδομένων. Αυτός είναι και ο κύριος λόγος για τον οποίο ο ίδιος ο σχεδιαστής του ΚΠΣ πρέπει να αξιολογήσει και να καθορίσει σε ποιο λογικό επίπεδο πρέπει να αλλάξουν οι λειτουργίες του Συστήματος για να ανταποκριθούν στις απαιτήσεις του GDPR.

Ο σχεδιαστής του ΚΠΣ θα πρέπει να μελετήσει με ποιο τρόπο ανάλογα συστήματα εφάρμοσαν τη νομοθεσία και αν παρουσιάζουν αποκλίσεις και σε ποιους τομείς. Σημαντική πηγή εμπειριών προκύπτει από συστήματα διαχείρισης κοινωνικών δικτύων που φέρνουν σε επαφή μία ανοιχτή κοινότητα μελών για μία αποστολή ή εφαρμογές που επιζητούν τον εντοπισμό εθελοντών για τη πραγματοποίηση κοινωνιών/ιατρικών μελετών. Η παροχή συμβουλών από εξειδικευμένους συμβούλους είναι επίσης μία άλλη επιλογή. Στη συνέχεια θα μπορούσε κανείς να προσλάβει έναν συνεργάτη (δικηγόρο) που ειδικεύεται στη νομοθεσία του GDPR και σε άλλη νομοθεσία για την ασφάλεια των δεδομένων. Επιπλέον, θα πρέπει να συνάπτονται συμβάσεις με κάθε πελάτη, συνεργαζόμενες εταιρείες, συνεργαζόμενες κοινότητες χρηστών (πχ ανοικτή κοινότητα προγραμματιστών, ή crowdsourcing) ώστε να διασφαλίζεται ότι οι ευθύνες μεταξύ των μερών έχουν κατανοηθεί και συμφωνηθεί.

Ένας οργανισμός πρέπει να γνωρίζει ποια δεδομένα επεξεργάζονται στα συστήματά του, όπου βρίσκονται τα δεδομένα και πού θα μεταφερθούν. Είναι μια μεγάλη πρόκληση, π.χ. όταν ένα λογισμικό έχει μεγάλης διάρκειας κύκλο ζωής ή συνεχώς μεταβαλλόμενη κοινότητα χρηστών. Η καταγραφή δεδομένων και η χαρτογράφηση παρέχουν γνώση σχετικά με τα επεξεργασμένα δεδομένα, τις μορφές δεδομένων, τις μεθόδους μεταφοράς, τις τοποθεσίες και το ποιος έχει πρόσβαση στα δεδομένα. Επιπλέον, οι αρχές του GDPR περί απορρήτου πρέπει να ληφθούν υπόψη κατά την επεξεργασία των προσωπικών δεδομένων.

Ο καθορισμός ρόλων και δικαιωμάτων προσβάσεων στα δεδομένα είναι σημαντικός για να καταγράφεται ποιος έχει πρόσβαση στα δεδομένα των πελατών και γιατί. Επιπλέον, ο οργανισμός πρέπει να εμποδίσει την πρόσβαση σε δεδομένα χωρίς έγκυρο λόγο. Το όποιο τμήμα εξυπηρέτησης θα χρειαστεί οδηγίες για να αποτραπούν επιθέσεις κοινωνικής μηχανικής. Το προσωπικό πρέπει επίσης να εκπαιδεύεται για τις νέες απαιτήσεις και οδηγίες χειρισμού δεδομένων.

Η αυτοματοποίηση συμβάλλει στην εξοικονόμηση χρόνου και ο οργανισμός μπορεί να επικεντρωθεί στις κύριες διαδικασίες του, π.χ. στην ανάπτυξη λογισμικού. Η ανάγνωση ή η κατάργηση των δεδομένων με μη αυτόματο τρόπο από πολλές βάσεις δεδομένων και αρχεία από χιλιάδες φακέλους ίσως να είναι επίπονη διαδικασία. Οι αυτοματοποιημένες διαδικασίες καθαρισμού βάσεων δεδομένων και αρχείων εξακολουθούν να απαιτούν την παρακολούθηση ότι εκτελούνται σωστά.

Ο προγραμματισμός των υπηρεσιών καθαρισμού δεδομένων απαιτεί επίσης αυστηρό προγραμματισμό, π.χ. μια βάση δεδομένων μπορεί να περιέχει αρκετές αυτοματοποιημένες διεργασίες οι οποίες μπορεί να θέτουν, για παράδειγμα, κλειδώματα σε πίνακες βάσης δεδομένων. Αυτό μπορεί να οδηγήσει σε πρόβλημα όταν η ανάγνωση ή η εγγραφή δεδομένων από μια βάση δεδομένων μπορεί να αποτύχει και μια διαδικασία καθαρισμού ή άλλη αυτοματοποιημένη διαδικασία δεν μπορεί να ολοκληρώσει την εκτέλεση της. Μια βάση δεδομένων μπορεί επίσης να χρησιμοποιείται καθόλη τη διάρκεια της εγγραφής ή της ανάγνωσης δεδομένων, π.χ. μέσω API Web ή το λογισμικό να έχει πολλούς χρήστες σε απευθείας σύνδεση.

Η παρακολούθηση της νομοθεσίας του GDPR και άλλων νομοθετικών αλλαγών είναι σημαντική, ώστε ο οργανισμός να είναι σε θέση να ανταποκριθεί στις απαιτήσεις που προκαλούνται από τις προαναφερθείσες αλλαγές. Επιπλέον, με αυτόν τον τρόπο ο οργανισμός μπορεί να αποφύγει τα ακριβά πρόστιμα που ενδέχεται να καθορίσουν οι αρχές εάν δεν έχουν αντιμετωπιστεί σωστά τα θέματα. Είναι επίσης ένα καλό σημάδι για τους πελάτες και τις ευρύτερες κοινότητες συνεργατών, αν ο οργανισμός προσαρμοστεί σωστά στις νομοθετικές αλλαγές και καταβάλλει προσπάθεια για την ασφάλεια στον κυβερνοχώρο.

Η τακτική εκπαίδευση των υπαλλήλων από την άποψη της ασφάλειας είναι σημαντική, διότι συμβάλλει στην αποφυγή εύκολων λαθών, π.χ. στο γραφείο εξυπηρέτησης. Ένας κωδικός πρόσβασης ή άλλες ευαίσθητες πληροφορίες που διαρρέουν μέσω της κοινωνικής μηχανικής μπορεί να προκαλέσει μεγάλη οικονομική ζημιά στον οργανισμό. Για το λόγο αυτό, είναι σημαντικό να εκπαιδευτούν και να δημιουργηθούν οδηγίες για τους υπαλλήλους ώστε το προσωπικό να μπορεί να αναγνωρίσει πιθανές απειλές κοινωνικής μηχανικής.

Οι διαχειριστές ενός ΚΠΣ πρέπει να ενημερώνονται σχετικά με τις αρχές επεξεργασίας δεδομένων προσωπικού χαρακτήρα και τις απειλές για την ασφάλεια. Οι εσωτερικοί έλεγχοι και ενδεχομένως η εξωτερική βοήθεια βοηθούν να ελεγχθούν αν π.χ. οι διαδικασίες και οι πολιτικές ενός οργανισμού έχουν γίνει σωστά και οι εργαζόμενοι ακολουθούν τις οδηγίες. Επιπλέον, σε περίπτωση αλλαγής της νομοθεσίας, ενδέχεται να προκληθούν αλλαγές στις διαδικασίες και τις πολιτικές του οργανισμού.

Όταν δημιουργείται μια ανάγκη για δημιουργία νέου λογισμικού κοινωνικού σκοπού, είναι σημαντικό να δοθεί προσοχή στο είδος δεδομένων που θα εισέρχονται σε αυτό και θα επεξεργάζονται. Επίσης, πρέπει να δοθεί προσοχή στο είδος των ελέγχων ασφαλείας που πρέπει να εφαρμοστούν για να διασφαλιστεί η τήρηση των απαιτήσεων της νομοθεσίας. Είναι σημαντικό να διασφαλιστεί ότι ένα λογισμικό δεν επεξεργάζεται ή αποθηκεύει πληροφορίες που δεν έχουν νομική βάση (π.χ. ειδικές κατηγορίες προσωπικών πληροφοριών).

Όταν η ομάδα σχεδιασμού και υλοποίησης του συστήματος αρχίζει να σχεδιάζει τις απαιτήσεις και τα χαρακτηριστικά των νέων λειτουργιών, πρέπει να υπάρχουν ορισμοί της επιχειρησιακής λογικής, το είδος των δεδομένων και οι έλεγχοι ασφαλείας που πρέπει να εφαρμοστούν. Στη συνέχεια, η ομάδα θα σχεδιάσει τα καθήκοντά της από τεχνική άποψη ως προς το πώς η λειτουργία θα εφαρμοστεί, δοκιμαστεί και διατεθεί στον κοινωνικό της σκοπό.

Ο γενικός κανονισμός για την προστασία των δεδομένων αποτελεί σημαντική δυσκολία για πολλούς οργανισμούς αφού αφήνει πολλά ερωτήματα ανοιχτά προς απάντηση. Μέχρι τώρα έχουν υλοποιηθεί πολλές σημαντικές λειτουργίες σχετικές με το GDPR όπως η τυποποίηση του τρόπου συλλογής, επεξεργασίας και αποθήκευσης προσωπικών δεδομένων, των ρόλων και των αρμοδιοτήτων γύρω από αυτό, και οι οργανισμοί έχουν καλύτερη κατανόηση για το πώς το GDPR επηρεάζει την καθημερινή τους λειτουργία. Η πιο σημαντική συνεισφορά αυτής της εργασίας είναι τα βήματα που πρέπει να ληφθούν υπόψη στη πορεία συμμόρφωσης προς το GDPR. Επιπλέον, απαιτείται ένα κοινό μοντέλο GDPR για το τι είδους λειτουργίες οι κοινότητες προγραμματιστών πρέπει να σχεδιάσουν και να εφαρμόσουν π.χ. ώστε να ανταποκρίνονται στις απαιτήσεις GDPR. Απαιτείται επίσης περαιτέρω μελέτη του τρόπου με τον οποίο θα επιτυγχάνεται συμμόρφωση με τα θέματα του GDPR στο μέλλον. Σε αυτή την εργασία, αναφερθήκαμε σε πιθανούς τρόπους που ωστόσο χρειάζονται ακόμη μια βαθύτερη ανάλυση.

Βιβλιογραφία

A. Anderson, D. Huttenlocher, J. Kleinberg, and J. Leskovec. (2014). Engaging with massive online courses. *Proceedings of the 23rd International World Wide Web Conference (WWW)*, (pp. 687–698).

Adam J Berinsky, Gregory A Huber, and Gabriel S Lenz. (2012). Evaluating online labor markets for experimental research: Amazon. com's mechanical turk. *Political Analysis, 20(3):351–368*.

Aniket Kittur and Robert E. Kraut. (2008). Harnessing the wisdom of crowds in wikipedia: quality through coordination. *Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work (CSCW)*, (pp. 37-46). New York, NY, USA.

Ernst Fehr and Klaus M Schmidt. (2006). The economics of fairness, reciprocity and altruism– experimental evidence and new theories. *In Handbook of the economics of giving, altruism and reciprocity, volume 1*, 615–691.

Gabriele Paolacci, Jesse Chandler, and Panagiotis G Ipeirotis. (2010). Running experiments on amazon mechanical turk. *Judgment and Decision making, 5(5):411–419*.

Greg Stoddard. (2015). Popularity dynamics and intrinsic quality on reddit and hacker news. *Proceedings of the 9th AAAI Conference on Web and Social Media (ICWSM).*

Jeffrey T Hancock, Lauren E Curry, Saurabh Goorha, and Michael Woodworth. (2007). On lying and being lied to: A linguistic analysis of deception in computer-mediated communication. *Discourse Processes, 45(1):1–23*.

Jesse Chandler, Pam Mueller, and Gabriele Paolacci. (2013). Nonna¨ıvet´e among amazon mechanical turk workers: Consequences and solutions for behavioral researchers. *Behavior Research Methods*.

John Joseph Horton and Lydia B. Chilton. (2010). The labor economics of paid crowdsourcing. *Proceedings of the 11th ACM Conference on Electronic Commerce (EC)* (pp. 209-218). New York, NY, USA, 2010. ACM. ISBN 978-1-60558-822-3. doi: 10.1145/1807342.1807376. URL http://doi.acm.org/10.1145/1807342.1807376.

John R Carlson, Joey F George, Judee K Burgoon, Mark Adkins, and Cindy H White. (2004). Deception in computer-mediated communication. *Group decision and negotiation, 13(1): 5-28*.

Jon Sprouse. (2011). A validation of amazon mechanical turk for the collection of acceptability judgments in linguistic theory. *Behavior research methods, 43(1):155–167*.

Laura Dabbish, Colleen Stuart, Jason Tsay, and Jim Herbsleb. (2012). Social coding in github: transparency and collaboration in an open software repository. *Proceedings of the 15th ACM Conference on Computer Supported Cooperative Work (CSCW)*, (pp. 1277–1286).

Matthew JC Crump, John V McDonnell, and Todd M Gureckis. (2013). Evaluating amazon's mechanical turk as a tool for experimental behavioral research. *PloS one, 8(3): e57410*.

P. G. Ipeirotis. (2010). Analyzing the amazon mechanical turk marketplace. *XRDS, 17 (2):16–21, December 2010*, ISSN 1528-4972. doi: 10.1145/1869086.1869094. URL http: //doi.acm.org/10.1145/1869086.1869094.

Reid Priedhorsky, Jilin Chen, Shyong Tony K Lam, Katherine Panciera, Loren Terveen, and John Riedl. (259-268). Creating, destroying, and restoring value in wikipedia. *Proceedings of the 2007 international ACM conference on Supporting group work*, 2007.

Robert M Bond, Christopher J Fariss, Jason J Jones, Adam DI Kramer, Cameron Marlow, Jaime E Settle, and James H Fowler. (2012). A 61-million-person

experiment in social influence and political mobilization. *Nature, 489(7415): 295–298*.

Takeshi Sakaki, Makoto Okazaki, and Yutaka Matsuo. (2010). Earthquake shakes twitter users: realtime event detection by social sensors. *Proceedings of the 19th International World Wide Web Conference (WWW)* (pp. 851-860). ACM.

W. Mason and S. Suri. (2013). Conducting behavioral research on amazon's mechanical turk. *Behavior Research Methods, 44(1):1–23*.

ARTICLE 29 DATA PROTECTION WORKING PARTY. Directorate General Justice. 2017. PDF document published by Directorate General Justice 3 October 2017. Accessed 17 March 2018. Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=47741

Biscoe, C. 2017. Data mapping: Where to start for GDPR compliance. Accessed 6 June 2018. Retrieved from https://www.itgovernance.co.uk/blog/data-mapping-where-tostart-for-gdpr-compliance/

Curtis, J. 2018. What is GDPR? Everything you need to know post-compliance deadline. Accessed 11 May 2018. Retrieved from http://www.itpro.co.uk/itlegislation/27814/what-is-gdpr-everything-you-need-to-know

DeRose, J. 2018. How Do Internal Audits Work? 27 April 2018. Accessed 1 July 2018. Retrieved from https://www.ispartnersllc.com/blog/how-do-internal-audits-work/

Do 72 Hours Really Matter? Data Breach Notifications in EU GDPR. 2018. Trend Micro. Accessed 13 May 2018. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/online-privacy/do-72-hoursreally-matter-data-breach-notifications-in-eu-gdpr

Duncan, E. 2018. What is GDPR in a nutshell? Accessed on 4 June 2018. Retrieved from https://www.ftadviser.com/regulation/2018/04/12/what-is-gdpr-in-a-nutshell/

EU General Data Protection Regulation (GDPR) Overview. Vigilant software. Accessed 4 June 2018. Retrieved from https://www.vigilantsoftware.co.uk/topic/eu-gdpr

Goodchild, J. Hulme, G. 2017. What is social engineering? How criminals take advantage of human behavior. Accessed 30 June 2018. Retrieved from https://www.csoonline.com/article/2124681/social-engineering/what-is-socialengineering.html

Gunathunga, S. 2017. Individual's rights under GDPR. Accessed 6 July 2018. Retrieved from https://medium.com/@sagarag/individuals-rights-under-gdpr-3256fb3f356c

Hart, C. 2001. Doing a Literature Search. First edition. SAGE Publications Ltd.

Hart, C. 2018. Doing a Literature Review. Releasing the Research Imagination. 2nd Edition. SAGE Publications Ltd.

Hopping, C. Millman, R. 2018. HTTP vs HTTPS: what difference does it make to security? Accessed 20 June 2018. Retrieved from http://www.itpro.co.uk/networkinternet/30416/http-vs-https-what-difference-does-it-make-to-security

Kloeten, O. 2009. Soft-deletes are bad, m'kay? Accessed 18 June 2018. Retrieved from https://weblogs.asp.net/fbouma/soft-deletes-are-bad-m-kay

Kylmänen, A. 2018. General Data Protection Regulation - Requirement Analysis of Customer Personal Data: Case Study. Master's thesis, university. Tampere University of Technology. Degree programme in industrial and information management. Accessed 25 January 2019. Retrieved from http://URN.fi/URN:NBN:fi:tty201808292218

Lehtisalo, I. 2018. GDPR-Six Months After the D-Day. Master's thesis, polytechnic. Haaga-Helia University of applied sciences. Degree programme in information systems management. Accessed 28 January 2019. Retrieved from http://urn.fi/URN:NBN:fi:amk-2018112718374

Lemminki, R. 2018. Sahaammeko omaa oksaamme liian tiukalla GDPR:n ja ePrivacyn tulkinnalla [Do we cut our own branches with too strict an interpretation of GDPR and ePrivacy]? Accessed 26 June 2018. Retrieved from https://www.marmai.fi/blogit/mainostajien_blogi/sahaammeko-omaa-oksaammeliian-tiukalla-gdpr-n-ja-eprivacyn-tulkinnalla-6704012

Lokiohje [Log guidelines]. Valtiovarainministeriö [The Ministry of Finance]. 2009. PDF document published by The Ministry of Finance. Accessed 24 June 2018. Retrieved from https://www.vahtiohje.fi/c/document_library/get_file?uuid=775179cb-6c544dfb-b65d-e925d47c61d2&groupId=10229

Loshin, P. 2017. The GDPR right to be forgotten: Don't forget it. Accessed 13 May 2018. Retrieved from http://searchsecurity.techtarget.com/feature/The-GDPR-rightto-be-forgotten-Dont-forget-it

Masson, D. 2017. Adapting to regulation: How to cope when government changes the rules. Accessed 29 June 2018. Retrieved from https://www.theglobeandmail.com/report-on-business/careers/leadershiplab/adapting-to-regulation-how-to-cope-when-government-changes-therules/article34862926/

Mast, J. 2018. SAP authorization concept renewal project and GDPR in company X. Master's thesis, polytechnic. Turku University of applied sciences. Degree programme in international business. Accessed 28 January 2019. Retrieved from http://urn.fi/URN:NBN:fi:amk-2018060713056

Mononen, M. 2019. GDPR-Strategy Management at a SAP Organization. Master's thesis, polytechnic. Karelia University of applied sciences. Degree programme in

technology competence management. Accessed 29 January 2019. Retrieved from http://urn.fi/URN:NBN:fi:amk-201901281616

Pedro, B. 2017. What are Web APIs. Accessed 10 June 2018. Retrieved from https://hackernoon.com/what-are-web-apis-c74053fa4072 Personal data breaches. OFFICE OF THE DATA PROTECTION OMBUDSMAN. Accessed 24 June 2018. Retrieved from https://tietosuoja.fi/en/personal-data-breaches

Pinal, D. 2010. SQL SERVER – Soft Delete – IsDelete Column – Your Opinion. Accessed 18 June 2018. Retrieved from https://blog.sqlauthority.com/2010/09/03/sql-serversoft-delete-isdelete-column-your-opinion/

Pulkkinen, T. 2018. Cloud outsourcing guidelines and data protection regulation in Europe : Context of online banking self-service channels. Master's thesis, polytechnic. Jyväskylä University of applied sciences. Degree programme in cyber security. Accessed 26 January 2019. Retrieved from http://urn.fi/URN:NBN:fi:amk201805107482

Regulation (EU) 2016/679 of the European parliament and of the council. 2016. Official Journal of the European Union 4 May 2016. Accessed 25 February 2018. Retrieved from http://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FI

SQL Server Agent. Microsoft. 2017. Technical document in docs.microsoft.com page 19 January 2017. Accessed 7 June 2018. Retrieved from https://docs.microsoft.com/en-us/sql/ssms/agent/sql-server-agent?view=sql-server2017

Stored Procedures (Database Engine). Microsoft. 2017. Technical document in docs.microsoft.com page 14 March 2017. Accessed 4 June 2018. Retrieved from https://docs.microsoft.com/en-us/sql/relational-databases/storedprocedures/stored-procedures-database-engine?view=sql-server-2017

Survey Reveals Biggest GDPR Compliance Risks are Breach Notification, Data Mapping, Managing Consent, and Data Transfer. 2017. TrustArc. Accessed 13 May 2018. Retrieved from https://www.prnewswire.com/news-releases/survey-revealsbiggest-gdpr-compliance-risks-are-breach-notification-data-mapping-managingconsent-and-data-transfer-300551549.html

The Six Privacy Principles of GDPR. 2017. MTHREE Consulting. Accessed 12 May 2018. Retrieved from https://www.mthreeconsulting.com/blog/2017/04/the-6-privacyprinciples-of-gdpr

Veerraju, A. Srinivasa, R. Murali, G. 2010. Refactoring and Its Benefits. Accessed 5 June 2018. Retrieved from https://aip.scitation.org/doi/abs/10.1063/1.3516393?journalCode=apc

What is SCRUM? Scrum.org. 2018. Accessed 25 February 2018. Retrieved from https://www.scrum.org/resources/what-is-scrum

Antonio Tapiador and Diego Carrera. 2012. A survey on social network sites' functional

features. Computing Research Repository (CoRR), abs/1209.3650.

Facebook. 2007. Facebook platform.

Google. 2007. Open social.

How tech-giants like Facebook and whats-app are affected by gdpr. 2019. Accesed 27 April 2019. Retrieved from https://www.cyberdefensemagazine.com/how-tech-giants-like-facebook-and-whats-app-are-affected-by-gdpr/

How to perform a data protection impact assessment (DPIA) under GDPR. 2019. Accesed 17 September 2019. Retrieved from https://www.itpro.co.uk/data-protection/34416/how-to-perform-a-data-protection-impact-assessment-dpia-under-gdpr

M. Beye, A. J. P. Jeckmans, Z. Erkin, P. H. Hartel, R. L. Lagendijk, and Q. Tang. 2010. Literature overview - privacy in online social networks. Technical Report TR-CTIT-

10-36, Centre for Telematics and Information Technology University of Twente, Enschede, October 2010.

T. Paul, S. Buchegger, and T. Strufe. 2011. Decentralizing social networking services. In Luca Salgarelli, Giuseppe Bianchi, and Nicola BlefariMelazzi, editors, Trustworthy Internet, pages 187–199. Springer Milan.

G. Pallis, D. Zeinalipour-Yazti, and Dikaiakos M. D. 2011. Online social networks: Status and trends. In Athena Vakali and LakhmiC. Jain, editors, New Directions in Web Data Management 1, volume 331 of Studies in Computational Intelligence, pages 213–234. Springer Berlin Heidelberg.

A. Datta, S. Buchegger, Le-Hung Vu, T. Strufe, and K. Rzadca. 2010. Decentralized online social networks. In Borko Furht, editor, Handbook of Social Network Technologies and Applications, pages 349–378. Springer US.

S. Buchegger and A. Datta. 2009. A case for p2p infrastructure for social networks - opportunities & challenges. In Wireless On-Demand Network Systems and Services, 2009. WONS 2009. Sixth International Conference on, pages 161–168, Feb 2009.

N. B. Ellison and D. Boyd. 2013. Sociality through social network sites. In The Oxford Handbook of Internet Studies, pages 151–172. Oxford University Press.

L. A. Cutillo, R. Molva, and T. Strufe. 2009. Safebook: A privacy-preserving online social network leveraging on real-life trust. Comm. Mag., 47(12):94–101, dec 2009.

Chi Zhang, Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang. 2010. Privacy and security for online social networks: challenges and opportunities. Network, IEEE, 24(4):13–18, July 2010.

E. Aimeur, S. Gambs, and A. Ho. 2010. Towards a privacy-enhanced social networking site. In International Conference on Availability, Reliability, and Security (ARES), pages 172–179. IEEE Computer Society.

Ai T. Ho. 2012. Towards a Privacy-Enhanced Social Networking Site. PhD thesis, Montreal University.

A.I. Anton, J.B. Earp, and A. Reese. 2002. Analyzing website privacy requirements using a privacy goal taxonomy. In IEEE Joint International Conference on Requirements Engineering, pages 23–31.