Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Μελέτη και υλοποίηση εφαρμογής για τη διαχείρηση δεδομένων με χρήση του Ευρωπαϊκού Κανονισμού GDPR Study and implementation of an application for data management using the European Regulation GDPR
Ονοματεπώνυμο Φοιτητή	Κωνσταντίνος Γεωργολόπουλος
Πατρώνυμο	Σωτήριος
Αριθμός Μητρώου	ΜΠΠΛ 16006
Επιβλέπων	Μαρία Βίρβου, Καθηγήτρια

Ημερομηνία Παράδοσης ΝΟΕΜΒΡΙΟΣ 2018

Τριμελής Εξεταστική Επιτροπή

Μαρία Βίρβου Καθηγήτρια	Γεώργιος Τσιχριτζής Καθηγητής	Ευθύμιος Αλέπης Επίκουρος Καθηγητής

ΠΕΡΙΛΗΨΗ

Στην παρούσα μεταπτυχιακή διατριβή θα κάνουμε μια ευρύτερη αναφορά στον Ευρωπαϊκό Κανονισμό GDPR που τέθηκε σε ισχύ από τις 25 Μαϊου 2018 και αφορά την προστασία προσωπικών – ευαίσθητων δεδομένων. Θα εξετάσουμε πώς ο νέος Κανονισμός επηρεάζει τις επιχειρήσεις, τους οργανισμούς, καθώς και τους ίδιους τους πολίτες που είναι τα υποκείμενα των δεδομένων, τι προβλέπει, ποιούς κατα κύριο λόγο αφορά και τι αλλαγές επιφέρει. Θα προτείνουμε μέτρα προστασίας σε επίπεδο πολίτη και σε επίπεδο οργανισμού, ώστε να υπάρχει η κατάλληλη και προβλεπόμενη συμμόρφωση όλων με το νέο Ευρωπαϊκό αυτό πλαίσιο. Ιδιαίτερη μνεία έχει δοθεί στα μέσα κοινωνικής δικτύωσης (social media) των οποίων η χρήση αυξάνεται με ραγδαίους ρυθμούς και στα οποία επεξεργάζονται και δημοσιοποιούνται τεράστιος όγκος δεδομένων προσωπικού χαρακτήρα των χρηστων. Επιπρόσθετα υλοποιήσαμε μια εφαρμογή για τον Υπεύθυνο Προστασίας Δεδομένων (DPO) η οποία αποτελεί χρήσιμο εργαλείο, καθώς τον βοηθά να έχει μια πλήρη εικόνα της κατάστασης στην οποία βρίσκεται η εταιρεία ως προς τη συμμόρφωσή της με τις απαιτήσεις του GDPR. Τέλος, με την ολοκλήρωση της εργασίας εξάγουμε κάποια πολύτιμα συμπεράσματα τόσο για την παρούσα μέλετη όσο και για μεταγενέστερη έρευνα.

ABSTRACT

This post graduate dissertation presents an extensive study on the European Regulation GDPR wich concerns the management of personal and sensitive data. It focuses on its application to companies, organizations as well as citizens. More specifically, information about the core aspects of GDPR are provided and the changes that are provoked are discussed. Futhermore, protection measures are suggested either in an organizational or a human level. Special mention has been placed on the management of social media data. Social media manage and publish a huge amount of personal data of all their users. Moreover, as a testbed for this study, an application for Data Protection Officers (DPO) is designed and fully implemented. This application can serve as a valuable tool to any company since it can provide an insight to the situation and compliance requirements of GDPR. This dissertation presents valuable conclusions regarding GDPR and can serve as guideline to stakeholders.

Πίνακας Περιεχομένων

ΚΕΦΑΛΑΙΟ 1ο – ΕΙΣΑΓΩΓΗ

Τα δεδομένα (data), θα λέγαμε είναι το “πετρέλαιο” της 4ης Βιομηχανικής Επανάστασης, όπως πολύ σωστά αναφέρουν και ορισμένες εταιρείες που ασχολούνται με αυτά στις ιστοσελίδες τους. Μάλιστα από στατιστικές μελέτες από επίσημους φορείς αναμένουμε το 2020 η αξία της αγοράς θα αγγίξει το €1 τρις, ενώ το 2025 ο όγκος των δεδομένων πιθανότατα θα αυξηθεί από 16.1 ZB σε 163 ZB (1 ZB = 10^{21} bytes). Είναι προφανές ότι, καθώς αυξάνονται τόσο τα ίδια τα δεδομένα, όσο και η αγορά που πλαισιώνεται γύρω από αυτά, ανάλογη αύξηση επιφέρουν και στους κινδύνους παραβίασή τους με άκρως δυσμενείς επιπτώσεις. Στο Κεφάλαιο 4 θα αναφέρουμε παραδείγματα παραβιάσεων (data breach) ή διαρροής προσωπικών δεδομένων που αντιμετώπισαν κατα το παρελθόν επιχειρηματικοί κολοσσοί, υποθέσεις υποκλοπών προσωπικών και φορολογικών δεδομένων καθώς τέλος και τα μεγαλύτερα cyber σκάνδαλα όλων των εποχών. Με αφορμή λοιπόν αυτών των καταστροφικών επιπτώσεων που επέφεραν αυτές οι παραβιάσεις τόσο σε επίπεδο οικονομικό καθώς απωλέσθηκαν δεδομένα αξίας εκατομμυρίων ευρώ, όσο και σε επίπεδο brand loyalty με την απώλεια της καλής φήμης και αξιοπιστίας, οδήγησαν στην θέσπιση του νέου Γενικού Κανονισμού (GDPR) με έναρξη εφαρμογής την 25η Μαίου 2018. Πρωτού αναπτύξουμε κάποιους από τους ορισμούς και το περιεχόμενο του Κανονισμού όπως επίσης κάποιες από τις σημαντικές αλλαγές που επιφέρει, παρεμπιπτόντως επιβάλλοντας βαριές ποινές και επιπτώσεις σε επιχειρήσεις δημοσίου και ιδιωτικού τομέα με τη μη συμμόρφωσή τους, καλό είναι να δούμε την χρονική εξέλιξη του Κανονισμού αυτού σε επίπεδο Ευρωπαικό αλλά και Ελληνικό.

ΚΕΦΑΛΑΙΟ 2ο - ΧΡΟΝΙΚΗ ΕΞΕΛΙΞΗ ΘΕΜΑΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

2.1 - Το Ευρωπαικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομέμων

Στις 24 Οκτωβρίου 1995 έχουμε την οδηγία 95/46/ΕΚ του Ευρωπαικού Κοινοβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Στις 15 Δεκεμβρίου 1997 η Οδηγία 97/66/ΕΚ αποσκοπεί στην εναρμόνιση των διατάξεων των κρατών – μελών, οι οποίες απαιτούνται ώστε να εξασφαλίζεται ισόποσο επίπεδο προστασίας των θεμελιώδων δικαιωμάτων και ελευθεριών με έμφαση το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα καθώς και στην ελεύθερη κυκλοφορία των δεδομένων αυτών εντός της Κοινότητας. Οι διατάξεις της 97/66/ΕΚ έρχονται να εξειδικεύσουν και να συμπληρώσουν την Οδηγία 95/46/ΕΚ. Το 1997 έχουμε το Νόμο 2472/1997 περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα (ΦΕΚ 50/Α/10-4-1997). Την 12η Ιουλίου 2002 ψηφίζεται η Οδηγία 2002/58/ΕΚ η οποία αντικατέστησε την 97/66/ΕΚ, για να συμπεριλάβει στις διατάξεις της επιπλέον την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Τέσσερα χρόνια αργότερα, τον Μάρτιο του 2006 “έρχεται” η Οδηγία 2006/24/ΕΚ η οποία τροποποιεί την Οδηγία 2002/24/ΕΚ και αφορά τη διατήρηση των δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών ή δημόσιων επικοινωνιών. Εκ των υστέρων, η Οδηγία 2009/136/ΕΚ του 2009 τροποποιεί πέντε Οδηγίες που σχετίζονται με την ρύθμιση ηλεκτρονικών επικοινωνιών, μεταξύ των οποίων και την Οδηγία 2002/58/ΕΚ.

Ο νέος Κανονισμός “πρωτοεμφανίζεται” στις 25 Ιανουαρίου 2012 με την Ευρωπαική Επιτροπή να προτείνει την μεταρρύθμιση των κανόνων προστασίας προσωπικών δεδομένων στην Ευρωπαική Ένωση. Έπειτα από τέσσερα έτη διαπραγματεύσεων και συγκεκριμένα στις 8 Απριλίου 2016 που το Συμβούλιο ενέκρινε τη θέση του σε πρώτη ανάγνωση και στις 14 Απριλίου ο Κανονισμός και η Οδηγία (ΕΕ 2016/680) εγκρίνονται από το Ευρωπαικό Κοινοβούλιο φτάνουμε στις 27 Απριλίου 2016 όπου και ψηφίζεται. Έτσι ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) αποτελεί το κύριο νομοθέτημα της νέας δέσμης κανόνων για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών όπως και την αντικατάσταση της Οδηγίας 95/46/ΕΚ, η οποία δεν ήταν προσαρμοσμένη στην τεχνολογική πραγματικότητα του Διαδικτύου. Μια από τις άμμεσες συνέπειες και αλλαγές που επέφερε ο νέος Κανονισμός και τις οποίες θα τις αναφέρουμε σε επόμενη Ενότητα (Κεφάλαιο 4) είναι η κατάργηση του Ν.2472/97.

Στις 4 Μαίου 2016 ο Κανονισμός και η Οδηγία δημοσιεύονται στην Επίσημη Εφημερίδα της ΕΕ όπου η τελευταία τίθεται σε ισχύ την επομένη μέρα. Έπειτα απο 19 ημέρες (24/05/2016) τίθεται σε ισχύ και ο Κανονισμός, δίνοντας προθεσμία δύο ετών περίπου μέχρί τις 6 Μαίου 2018 στα κράτη – μέλη να συμμορφωθούν με τις διατάξεις του νέου Κανονισμού. Στις 25 Μαίου 2018 ο Κανονισμός τίθεται οριστικά σε εφαρμογή τόσο στις επιχειρήσεις, όσο και στα φυσικά πρόσωπα σε όλη την Ευρώπη. Να επισημάνουμε ότι αφόρα και εφαρμόζεται **μόνο** στην Ευρώπη και όχι σε κάποια άλλη χώρα εκτός αυτής οπώς για παράδειγμα την Αμερική ή την Κίνα.

2.2 - Το Ελληνικό νομικό πλαίσιο

Όσον αφορά την Έλλαδα έπρεπε να ψηφιστεί εφαρμοστικός νόμος πριν την έναρξη ισχύος του Κανονισμού. Άρα έχουμε Συνταγματική κατοχύρωση και το άρθρο 9Α της Συνταγματικής Αναθεώρησης του 2001 που αναφέρει πως ο κάθε πολίτης έχει το δικαίωμα προστασίας από τη συλλογή, την επεξεργασία και την χρήση κυρίως από τα ηλεκτρονικά μέσα, των προσωπικών του δεδομένων. Η προστασία των δεδομένων προσωπικού χαρακτήρα διασφαλίζεται από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) μια ανεξάρτητη Αρχή, συνταγματικά καταχυρωμένη, που σημαίνει πως δεν μπορεί να καταργηθεί. Πρέπει να γίνει αναθεώρηση του Συντάγματος για να υφίσταται τροποποίησης ή κατάργησης. Η ΑΠΔΠΧ να αναφέρουμε πως ιδρύθηκε με τον Νόμο 2472/1997, ο οποίος ενσωματώνει στο Ελληνικό δίκαιο την Ευρωπαική Οδηγία 95/46/ΕΚ. Επίσης για την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, η ΑΠΔΠΧ εφαρμόζει το Νόμο 3471/2006 που αντίστοιχα ενσωματώνει στο Εθνικό δίκαιο την Ευρωπαική Οδηγία 58/2002.

Το 2006 με το Νόμο 3471/2006 έχουμε την αναφορά ειδικά για τις ηλεκτρονικές υπηρεσίες. Ο Νόμος αυτός αναφέρεται δηλαδή στην προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Βλέπουμε πως το 2006 είναι το έτος ορόσημο ώστε να ενταχθεί και το κομμάτι της Πληροφορικής, καθώς πριν από αυτό όλες οι οδηγίες αφορούσαν τα προσωπικά δεδομένα στο κομμάτι των Τηλεπικοινωνιών και κυριότερα τους τηλεπικοινωνιακούς παρόχους και όχι με ότι έχει να κάνει με το Διαδίκτυο ή με τις τεχνολογικές τάσεις όπως για παράδειγμα cloud computing ή social media.

Το 2011 έχουμε την τροποποίηση του Νόμου 3471/2006 και αναφέρεται στην “διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους”. Με λίγα λόγια ο νόμος αυτός **δεν** επιτρέπει σε κάποια εταιρεία ή δημόσιο φορέα να διατηρεί μητρώο ή πελατολόγιο όπως επίσης και δεδομένα προσωπικού χαρακτήρα χωρίς να έχει συμμορφωθεί με κάποιο πλαίσιο ή νομο. Έτσι λοιπόν ένας δημόσιος φορέας δύναται να έχει στην κατοχή του στοιχεία και δεδομένα προσωπικού χαρακτήρα μόνο και εφόσον το επιτρέπει το καταστατικό του ή υπάρχει νομοθεσία που του δίνει το δικαίωμα αυτό. Για παράδειγμα το Ανώτατο Συμβούλιο Επιλογής Προσωπικού (ΑΣΕΠ) δέχεται στοιχεία από υποψήφιους πολίτες κάποια από τα οποία είναι ο βαθμός πτυχίου, η ανεργία, η αναπηρία, η κοινωνική ασφάλιση και άλλα. Από αυτά τα στοιχεία δεν είναι όλα προσωπικά δεδομένα αλλά η αναπηρία ή αν κάποιος είναι έγγαμος ή άγαμος, η εντοπιότητα, είναι στοιχεία που εμπεριέχουν προσωπικά δεδομένα. Παρόλο αυτά υπάρχει στο καταστατικό του διάταξη που αναφέρει πως μπορεί και έχει το δικαίωμα να διαχειρίζεται στοιχεία – δεδομένα προσωπικού χαρακτήρα.

ΚΕΦΑΛΑΙΟ 3ο - ΟΡΙΣΜΟΙ– ΠΕΡΙΕΧΟΜΕΝΟ ΚΑΝΟΝΙΣΜΟΥ

Πρωτού αναφερθούμε που εφαρμόζεται ο Κανονισμός (Κεφάλαιο 5), τι αλλαγές επιφέρει, το πώς και με ποιόν τρόπο “αναγκάζει” επιχειρήσεις του ιδιωτικού τομέα και δημόσιους φορείς να συμμορφωθούν, θα πρέπει να αναπτύξουμε αρχικά κάποιους και από τους πιο σημαντικούς ορισμούς του. Βάσει λοιπόν του άρθρου 4 του Κανονισμού, οι βασικότερες έννοιες είναι:

3.1 - Προσωπικό Δεδομένο

Όρίζεται κάθε πληροφορία που αναφέρεται σε, αλλά και περιγράφει ένα άτομο, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, ΑΦΜ, ΑΜΚΑ, επάγγελμα, οικογενειακή κατάσταση, διεύθυνση κατοικίας κ.α), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες.

3.2 - Υποκείμενο των Δεδομένων

Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα προσωπικά δεδομένα ή το φυσικό πρόσωπο του οποίου η ταυτότητσ μπορεί να εξακριβωθεί άμεσα ή έμμεσα και κυρίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας. *(πηγή: www.sev.org.gr)*

3.3 - Ευαίσθητα Δεδομένα

Χαρακτηρίζονται τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, στις ποινικές διώξεις και καταδίκες του όπως επίσης και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Τα συγκεκριμένα δεδομένα να αναφέρουμε ότι προστατεύονται αυστηρότερα από τον Νόμο, από οτι τα προσωπικά δεδομένα. Στις παραπάνω κατηγορίες, συμπεριλαμβάνονται ακόμη και άλλα νομοθετήματα όπως:

- Τα δεδομένα των ληπτών και δωρητών ανθρώπινων ιστών και οργάνων που περιέχονται στο Εθνικό Μητρώο με τους λήπτες και Αρχείο Δωρητών
- Οι δηλώσεις του αιτούντος άσυλο
- Τα μητρώα και Αρχεία της Εθνικής Αρχής Ιατρικώς Υποβοηθούμενης Αναπαραγωγής

3.4 - Επεξεργασία Δεδομένων

Ορίζεται κάθε εργασία – πράξη ή σειρά εργασιών που υλοποιούνται από το Δημόσιο ή μια εταιρεία ή από φυσικό πρόσωπο με τη βοήθεια ή χωρίς αυτοματοποιημένων μεθόδων και έχει εφαρμογή σε προσωπικά δεδομένα όπως: η συλλογή, η καταχώρηση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η χρήση, η εξαγωγή, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή. *(πηγή: www.inewsgr.com)*

3.5 - Υπεύθυνος Επεξεργασίας Δεδομένων

Ορίζεται εκείνος ο οποίος καθορίζει τον τρόπο με τον οποίο θα γίνει η επεξεργασία των προσωπικών δεδομένων και για ποιο λόγο ή σκοπό. Μπορεί να είναι είτε κάποιο φυσικό ή νομικό πρόσωπο, είτε κάποιος φορέας ή οργανισμός. Ο υπεύθυνος επεξεργασίας ενδέχεται αρκετές φορές να είναι και εκτελών την επεξεργασία που τον όρο αυτό θα αναπτύξουμε παρακάτω. Επίσης έχει στα καθήκοντά του και την γνωστοποίηση στην Αρχή Προστασίας Προσωπικών Δεδομένων την επεξεργασία των δεδομένων που πραγματοποιεί και η τελευταία καταγράφει την γνωστοποίηση αυτή σε ειδικό μητρώο. Σε περίπτωση που η επεξεργασία αφορά ευαίσθητα δεδομένα θα πρέπει να υπάρχει πρωτίστως άδεια της Αρχής και έπειτα ο υπεύθυνος της επεξεργασίας να προχωρήσει στην υλοποιήσή της. Η άδεια επίσης μπορεί να απαιτηθεί και στις περιπτώσεις διαβίβασης δεδομένων εκτός Ευρωπαικής Ένωσης όπως και στην περίπτωση διασύνδεσης αρχείων.

3.6 - Εκτελών την Επεξεργασία

Ορίζεται οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του Υπευθύνου Επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός. Τα καθήκοντα του εκτελούντος προς τον Υπεύθυνο Επεξεργασίας θα πρέπει να καθορίζονται σε κάποια σύμβαση ή σε κάποια νομική πράξη.

Στη συνέχεια θα αναφέρουμε ένα παράδειγμα ώστε να κατανοήσουμε καλύτερα τους δύο παραπάνω ορισμούς. Στην περίπτωση λοιπόν του Υπουργείου Εθνικής Άμυνας (ΥΠ.ΕΘ.Α) στο οποίο εργάζονται χιλιάδες εργαζόμενοι, η καταβολή των μισθών τους γίνεται από έναν φορέα, το Κεντρικό Ταμείο Στρατού (ΚΤΣ). Το ΥΠΕΘΑ ενημερώνει το ΚΤΣ για το πότε πρέπει κάποιος εργαζόμενος να πάρει αύξηση ή αντίστοιχα να υποστεί μείωση αναλόγως των αδειών ή αν κάποιος εργαζόμενος συνταξιοδοτηθεί ή αποχωρήσει, παρέχοντας έτσι όλα εκείνα τα στοιχεία που είναι απαραίτητα για το εκκαθαριστικό σημείωμα αποδοχών. Το ΚΤΣ αποθηκεύει τα δεδομένα των εργαζομένων και πραγματοποιεί τις πληρωμές. Στο παράδειγμα αυτό, το ΥΠΕΘΑ είναι ο Υπεύθυνος Επεξεργασίας και το ΚΤΣ είναι ο Εκτελών την επεξεργασία των δεδομένων. Βέβαια υπάρχουν περιπτώσεις στις οποίες μια οντότητα είναι ταυτόχρονα Υπεύθυνος Επεξεργασίας και Εκτελών την επεξεργασία.

3.7 - Διασύνδεση

Είναι μορφή επεξεργασίας δεδομένων και αφορά την δυνατότητα συσχέτισης των δεδομένων ενός αρχείου με δεδομένα αρχείου ή αρχείων που τηρούνται από άλλον ή άλλους Υπεύθυνους Επεξεργασίας. Ένα παράδειγμα διασύνδεσης είναι όταν κάποιος πολίτης είναι εγγεγραμμένος στο ΑΣΕΠ και με το ΑΦΜ του έχει πρόσβαση στο TAXISNET για την πρόσβασή του στα φορολογικά στοιχεία.

Ο νόμος βέβαια σε κάθε περίπτωση διασύνδεσης επιβάλλει ένα σύστημα γνωστοποίησης στην Αρχή Προστασίας Προσωπικών Δεδομένων και ταυτόχρονα ένα σύστημα προηγούμενης άδειας της Αρχής (άδεια διασύνδεσης) εάν εμπεριέχονται ευαίσθητα δεδομένα σε ένα τουλάχιστον αρχείο που επρόκειτο να διασυνδεθεί.

3.8 - Εκτίμηση Αντικτύπου (Data Protection Impact Assessment – DPIA)

Όποιες εταιρείες – φορείς έχουν πληροφοριακά συστήματα υποχρεούνται παράλληλα να έχουν και μια μελέτη Ασφάλειας. Έτσι είναι αναγκαία και η Εκτίμηση Αντικτύπου (ΕΑ) σχετικά με την προστασία των δεδομέμων. Είναι δηλαδή μια διαδικασία – μελέτη που πραγματοποιείται κατά τη φάση του σχεδιασμού μιας εφαρμογής που θα συλλέγει ή θα επεξεργάζεται δεδομένα και διενεργείται πριν την έναρξη της διαδικασίας επεξεργασίας. Ολοκληρώνεται με τη σύνταξη μιας έκθεσης από τον Υπεύθυνο Επεξεργασίας, στην οποία μπορεί να συνδράμει ο εκτελών την επεξεργασία, και περιγράφει συστηματικά τις διαδικασίες, το σκοπό της επεξεργασίας, εκτιμά την αναγκαιότητα και την αναλογικότητα των πράξεων αυτών, εκτιμά επίσης τους κινδύνους που εμπεριέχονται ως προς τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και τέλος αναφέρει όλα εκείνα τα μέτρα ασφαλείας που θα πρέπει να ληφθούν υπόψιν σε περίπτωση κινδύνου ή ζητήματος ασφαλείας. Θα λέγαμε πως είναι ένα κομμάτι του Risk Assessment χωρίς βέβαια να θεωρείται ως μια απλή ανάλυση κινδύνου καθώς όπως αναφέραμε περιλαμβάνει μέτρα ασφαλείας σε συνδιασμό με τους πιθανούς κινδύνους. Με την DPIA γίνεται δηλαδή μια “χαρτογράφηση” των δεδομένων, παρατηρώντας και προβλέπωντας τους κινδύνους, εκτιμώντας παράλληλα το μέγεθος των πιθανών επιπτώσεων.

3.9 - Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer – DPO)

Η θέση του είναι τέτοια ώστε να του επιτρέπει να δρα σε καθεστώς αυτονομίας και ανεξαρτησίας. Ορίζεται από τον Υπεύθυνο Επεξεργασίας και τον εκτελούντα την επεξεργασία, συμμετέχοντας σε όλα τα θέματα – ζητήματα που σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα. Παρέχει συμβουλές και συνδράμει στην παρακολούθηση και υλοποίηση μιας DPIA. Επίσης μπορεί να επικοινωνεί και με τα υποκείμενα των δεδομένων αλλά και με την Αρχή για θέματα προστασίας προσωπικών δεδομένων. Η υπαρξή του είναι υποχρεωτική σε περιπτώσεις που η επεξεργασία δεδομένων διενεργείται από δημόσια αρχή – φορέα, σε περιπτώσεις όπου απαιτείται τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε αρκετά μεγάλη κλίμακα ή όταν υφίσταται επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα ή ποινικές καταδίκες και αδικήματα.

Στις αρμοδιότητές του επίσης είναι η ενημέρωση καθώς και η εκπαίδευση της επιχείρησης στις όποιες απαιτήσεις του Κανονισμού, να τηρεί τα αρχεία καταγραφής και να αποδεικνύει τη συμμόρφωση του εκάστοτε οργανισμού ή επιχείρησης με τις απαιτήσεις του GDPR.

ΚΕΦΑΛΑΙΟ 4ο - ΠΕΡΙΠΤΩΣΙΟΛΟΓΙΚΕΣ ΜΕΛΕΤΕΣ ΥΠΟΚΛΟΠΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΕΛΛΑΔΑ – ΕΞΩΤΕΡΙΚΟ

Στο Κεφάλαιο αυτό θα αναφέρουμε περιπτώσεις κατά τις οποίες υποκλάπηκαν ευαίσθητα προσωπικά δεδομένα καθώς και φορολικά δεδομένα πολιτών επιφέροντας τις όποιες δυσμενείς συνέπειες οικονομικές και μη.

- Το σοκ του 2013[1]

Πρόκειται για την μεγαλύτερη υποκλοπή φορολογικών και προσωπικών δεδομένων στη χώρα μέσα από το σύστημα της Γενικής Γραμματείας Πληροφοριακών Συστημάτων (ΓΓΠΣ). Με το συμβάν αυτό η Αρχή Προστασίας Προσωπικών Δεδομένων επέβαλε στη ΓΓΠΣ το ανώτερο από το νόμο πρόστιμο, ύψους 150.000 Ευρώ, για τη μη λήψη κατάλληλων μέτρων ασφαλείας όπως υποχρεούνταν να πράξει, μετά την αποκάλυψη της διαρροής δεδομένων που αφορούσαν εκατομμύρια Έλληνες φορολογούμενους. Μετά από σειρά διοικητικών ελέγχων σε εταιρείες που σχετίζονταν με την εμπορία προσωπικών δεδομένων διαπιστώθηκε ότι πολλές ήταν αυτές που κατείχαν μεγάλο όγκο φορολογικών δεδομένων φυσικών προσώπων και τα οποία είχαν αντληθεί από τη ΓΓΠΣ. Να επισημάνουμε πως μεταξύ των φορολογικών δεδομένων περιλαμβάνονταν στοιχεία του Ε1, Ε2, Ε9, στοιχεία της έκτακτης εισφοράς, του μητρώου φορολογούμενων, των σημειωμάτων περαίωσης και των τελών κυκλοφορίας.

[1]*http://policenet.gr/article*

- *Αύγουστος 2015*[1]

Τέλος καλοκαιριού του 2015 η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων της ΕΥΠ ενημερώθηκε από ξένη Ευρωπαική υπηρεσία ασφαλείας πως είχαν κλαπεί ευαίσθητα προσωπικά δεδομένα 15.000 Ελλήνων πολιτών. Πιο συγκεκριμένα hackers εξαπέλησαν ηλεκτρονικές επιθέσεις υποκλέπτοντας τα διαπιστευτήρια (credentials) πολιτών που αφορούσαν το email τους, μεταξύ των οποίων ήταν επιχειρηματίες και πρόσωπα «υψηλού ενδιαφέροντος». Στην συνέχεια τα δημοσίευσαν στο Διαδίκτυο με στόχο να τα αχρηστεύσουν. Μετά το περιστατικό αυτό οι κάτοχοι των emails ενημερώθηκαν από την αρμόδια αρχή ώστε να δημιουργήσουν νέους λογαριασμούς.

[1]*http://policenet.gr/article*

- Υπόθεση Βαρουφάκη[1]

Ο πρώην Υπουργός Οικονομικών, Γ. Βαρουφάκης, από κοινού με μια πενταμελή ομάδα στενών συνεργατών και φίλων του σχεδίασαν Plan B για παράλληλο νόμισμα της χώρας με «χακάρισμα» των ΑΦΜ των πολιτών. Το Plan B προέβλεπε τη δημιουργία παράλληλου τραπεζικού συστήματος με παράλληλο νόμισμα (δραχμή) εντός του Ευρώ (IOUS) σε περίπτωση εξόδου της Ελλάδας από την Ευρωπαική Ένωση. Επρόκειτο δηλαδή για σχέδιο ηλεκτρονικής εισβολής στην ιστοσελίδα της Γενικής Γραμματείας Δημόσιων Εσόδων (ΓΓΣΕ) που αποσκοπούσε στην υποκλοπή του λογισμικού και των ΑΦΜ των Ελλήνων φορολογούμενων.

Η δημοσιοποίηση της είδησης αυτής προκάλεσε ισχυρούς τριγμούς στην κυβέρνηση τότε με το σύνολο του πολιτικού και οικονομικού κόσμου αλλά και της ίδιας της κοινωνίας να απαιτούν εξηγήσεις από τον ίδιο τον πρωθυπουργό, Αλ. Τσίπρα. Για πολλούς η υπόθεση Βαρουφάκη αποτέλεσε και συνεχίζει να αποτελεί ένα πολιτικό – οικονομικό σκάνδαλο τεράστιων διαστάσεων στην σύγχρονη ιστορία της χώρας.

[1]*http://policenet.gr/article*

- 29ο Διεθνές Συνέδριο της IFIP[2]

Το 2014 στο 29ο Διεθνές Συνέδριο της IFIP (International Federation for Information Processing) για την Πληροφοριακή Ασφάλεια και Εμπιστευτικότητα, παρουσιάστηκε μια μελέτη του κ. Βασίλη Πρεβελάκη, Επίκουρο Καθηγητή του Πανεπιστημίου Braunschweig της Γερμανίας, και των Δρ. Σωτήρη Ιωαννίδη, Ζαχαρία Τζερμιά από το Ινστιτούτο Πληροφορικής του Ιδρύματος Έρευνας και Τεχνολογίας (FORTH) του Πανεπιστημίου Κρήτης, η οποία καταδείκνυε, μεταξύ άλλων τους κινδύνους που αντιμετωπίζουν οι δημόσιες πηγές δεδομένων.

Ο κ. Πρεβελάκης, σχετικά με το “hacking” της σελίδας της Γενικής Γραμματείας Πληροφοριακών Συστημάτων (ΓΓΠΣ) στην απόκτηση του οποιονδήποτε αντίγραφο των ΑΦΜ, αναφέρει πως είναι εφικτό και πραγματοποιήσιμο και επιπρόσθετα το διαβεβαίωσε και ο ίδιος καθώς το επιχείρησε με απόλυτη επιτυχία μαζί με δύο άλλους ερευνητές από το FORTH. Πιο συγκεκριμένα ο ίδιος σε συνεργασία με τον Δρ. Ιωαννίδη και τον κ. Τζερμιά κατασκευάσανε ένα πρόγραμμα που έκανε επερωτήσεις (querries) στην βάση της ΓΓΠΣ και αντλούσαν πληροφορίες για κάθε πιθανό ΑΦΜ. Για όσους ΑΦΜ η βάση είχε πληροφορίες τους τις έδινε, για τους υπόλοιπους τους ενημέρωνε αν δεν υπήρχαν, αν ήταν ενεργοί ή αν ήταν μεν σωστοί αλλά δεν μπορούσε να “επιστρέψει” συγκεκριμένα στοιχεία. Η “επιχείρηση” διήρκησε μερικές βδομάδες με την βοήθεια ενός cluster υπολογιστών στις ΗΠΑ και το αξιοσημείωτο είναι πως η ΓΓΠΣ δεν αντιλήφθηκε κατι σχετικά με αυτή την επίθεση.

Τέλος, ο κ. Πρεβελάκης επισήμανε πως η συγκεκριμένη έρευνα είχε βασιστεί στην υπηρεσία που πρόσφερε τότε η ιστοσελίδα της ΓΓΠΣ, δίνοντας την δυνατότητα στον οποιονδήποτε να “ρωτά” στοιχεία για το ΑΦΜ του οποιουδήποτε πολίτη, χωρίς την ύπαρξη κάποιας δικλείδας ασφαλείας ώστε να γίνεται ταυτοποιήση του ενδιαφερόμενου, κάτι που σήμερα έχει αλλάξει. Είχε σκοπό επίσης, να καταδείξει ότι υπο ορισμένες προυποθέσεις είναι σχετικά εύκολο για κάποιον, δεδομένων και των δυνατοτήτων που έχουν σήμερα οι ηλεκτρονικοί υπολογιστές, να φτιάξει φακέλους με προσωπικά δεδομένα πολιτών, αντλώντας και συνδυάζοντας δεδομένα από δημόσιες βάσεις δεδομένων, όπως είναι για παράδειγμα η εφαρμογή “Μάθε που ψηφίζεις” του Υπουργείου Εσωτερικών, η “Διαύγεια” και τα λοιπά.

[2]www.capital.gr

- Εταιρεία Τηλεπικοινωνιών Talk Talk

Το 2015 έχουμε την ηλεκτρονική επίθεση στον πάροχο υπηρεσιών διαδικτύου και κινητής τηλεφωνίας Talk Talk που έχει ως έδρα το Ηνωμένο Βασίλειο έχοντας ως αποτέλεσμα τη διαρροή δεδομένων τεσσάρων εκατομμυρίων Βρετανών. Η εκτελεστική διευθύντρια της εταιρείας αποκάλυψε πως οι πληροφορίες που διέρρευσαν αφορούσαν ονόματα, διευθύνσεις, ημερομηνίες γεννήσεως, αριθμοί τηλεφώνου, διευθύνσεις ηλεκτρονικού ταχυδρομείου, στοιχεία των λογαριασμών των πελατών στην Talk Talk όπως επίσης και στοιχεία πιστωτικών καρτών και τραπεζικών λογαριασμών.

Μετά την δημοσίευση της επίθεσης, η εταιρεία με επίσημη επιστολή της προς τους πελάτες δήλωσε ότι «είχε λάβει όλα τα αναγκαία μέτρα για να κάνει την ιστοσελίδα της ασφαλή»

και ανέφερε ότι «είχε επικοινωνήσει με τις μεγάλες τράπεζες» οι οποίες θα παρακολουθούσαν συνεχώς για ύποπτη δραστηριότητα που σχετίζεται με τους λογαριασμούς των πελατών της[3].

[3]www.secnews.gr

- Σκάνδαλο της Ashley Madison

Το “site της αμαρτίας” Ashley Madison, όπως έχει καθιερωθεί να το αποκαλούν, δέχτηκε ηλεκτρονική επίθεση με αποτέλεσμα να κλαπούν στοιχεία 33 εκατομμυρίων λογαριασμών των χρηστών αυτού του ιστότοπου γνωριμιών και τα οποία δημοσιοποιήθηκαν online τον Αύγουστο του 2015. Μεταξύ των στοιχείων που κοινοποιήθηκαν, ήταν οι διευθύνσεις ηλεκτρονικού ταχυδρομείου των χρηστών, οι 16ψήφιοι αριθμοί των πιστωτικών καρτών τους, οι κωδικοί ασφαλείας τους, καθώς ακόμη και οι σεξουαλικές τους προτιμήσεις[4]. Το περιστατικό αυτό έφερε ως αποτέλεσμα, το δικαστήριο των ΗΠΑ να επιδικάσει αποζημείωση ύψους 11.2 εκατομμυρίων δολαρίων για τα “θύματα” αυτής της επίθεσης.

[4]www.skai.gr

- Wikileaks

Το Wikileaks[5] είναι η ιστοσελίδα ψηφιακών αποκαλύψεων που δημιούργησε το 2006 ο φυσικομαθηματικός, χάκερ και προγραμματιστής Τζούλιαν Ασάνζ, ο οποίος απέκτησε πρόσβαση σε εκατοντάδες χιλιάδες απόρρητα έγγραφα της περιόδου 2006-2009 των μυστικών υπηρεσιών και της διπλωματίας των ΗΠΑ. Πιο συγκεκριμένα δημοσίευσε βίντεο του 2007 στο οποίο φαίνεται Ιρακινός άμαχος πληθυσμός να θανατώνεται από Αμερικανούς στρατιώτες. Δημοσίευσε επίσης το “Ημερολόγιο του Πολέμου στο Αφγανιστάν”, μια συλλογή με 76.900 περίπου έγγραφα σχετικά με τον πόλεμο στο Αφγανιστάν, το “Ημερολογιο του Πολέμου στο Ιράκ” που περιλάμβανε 400.000 έγγραφα καθώς και 251.287 διπλωματικά έγγραφα. Τέλος το 2015 έφερε στη δημοσιότητα λεπτομέρειες σχετικά με τη Συνεργασία των Δύο Πλευρών του Ειρηνικού αναγκάζοντας τον τότε πρόεδρο των ΗΠΑ, Ομπάμα, να δώσει και εκείνος με την σειρά του τη συμφωνία στη δημοσιότητα έπειτα από αυτές τις διαρροές.

[5]www.news247.gr

- 2012. Ο Πρώτος Παγκόσμιος Κυβερνοπόλεμος για το Megaupload[5]

Το 2012 οι Anonymous ανακοίνωσαν την αρχή του Πρώτου Παγκόσμιου Κυβερνοπόλεμου με χιλιάδες ακτιβιστές χάκερ να επιτίθενται μαζικά σε sites είτε χρησιμοποιώντας συντονισμένα το LOIC και πραγματοποιώντας "χτυπήματα" σε πολλές ιστοσελίδες εταιρειών που υποστηρίζουν τα SOPA, PIPA, ACTA, για το κλείσιμο του Megaupload.com και άλλων site παροχής περιεχομένου. Περισσότερα από 5.000 μέλη της οργάνωσης Anonymous συνεργάσθηκαν για να "κατεβάσουν" τους ιστότοπους του υπουργείου Δικαιοσύνης, της ένωσης της κινηματογραφικής βιομηχανίας Motion Picture Association of America και της ένωσης της δισκογραφικής βιομηχανίας Recording Industry Association of America.

- Fappening

Είναι η κωδική ονομασία του σκανδάλου που έλαβε χώρα το 2014 σύμφωνα με το οποίο, χακερ απέκτησε παράνομη πρόσβαση στο iCloud της Apple δίνοντας στη δημοσιότητα γυμνές φωτογραφίες διασήμων. Η επίθεση αυτή εκτιμάται πως έγινε με τη μέθοδο Phishing, η οποία χρησιμοποιείται τις περισσότερες φορές ώστε να ξεγελάσει τον χρήστη που θεωρεί ότι έχει επισκεφθεί το αυθεντικό site αλλά αντιθέτως έχει “μπει” σε ψεύτικο που μοιάζει με το αυθεντικό, υποκλέπτοντάς του με αυτόν τον τρόπο τα διαπιστευτήριά του. Έτσι με την βοήθεια ενός κακόβουλου λογισμικού κάποιος μη εξουσιοδοτημένος χρήστης αποκτά πρόσβαση σε ευαίσθητα προσωπικά δεδομένα, έχοντας στην κατοχή του, τον κωδικό πρόσβασης (password) σε συνδυασμό με το email του χρήστη.

- Κυβερνοεπιθέσεις σε εταιρείες λιανεμπορίου (ΗΠΑ)

Χάκερς της αυτοαποκαλούμενης ομάδας JokerStash, υπέκλεψαν τα δεδομένα πέντε εκατομμυρίων πιστωτικών και χρεωστικών καρτών από πελάτες αμερικανικών καταστημάτων και τα έβγαλαν προς πώληση (περίπου 125.000 αρχεία), γεγονός που αποκάλυψε η εταιρεία κυβερνοασφάλειας Gemini Advisory. «Η συγκεκριμένη κυβερνοεπίθεση είναι μια από τις μεγαλύτερες και τις πιο καταστροφικές που έχουν μέχρι σήμερα σημειωθεί σε εταιρείες λιανεμπορίου», υποστηρίζουν ειδικοί της κυβερνοασφάλειας[6].

[6]www.protothema.gr

ΚΕΦΑΛΑΙΟ 5ο - ΑΛΛΑΓΕΣ ΠΟΥ ΕΠΙΦΕΡΕΙ ΤΟ GDPR

Όπως αναφέραμε στα προηγούμενα Κεφάλαια ο νέος Κανονισμός αποτελεί ένα εγχειρίδιο για τη διαχείριση των προσωπικών δεδομένων των πολιτών και ένα απλοποιημένο πλαίσιο λειτουργίας για τις επιχειρήσεις.

5.1 - Αλλαγές για τους πολίτες

Οι σημαντικές αλλαγές που επιφέρει το GDPR για τους πολίτες είναι:

1. Δικαίωμα πρόσβασης στα δεδομένα όπου ο κάθε πολίτης μπορεί να αιτηθεί πρόσβαση στα προσωπικά του δεδομένα, να ρωτήσει πως αυτά χρησιμοποιούνται και από ποιόν επεξεργάζονται μετά την συλλογή τους.

2. Δικαίωμα εναντίωσης στην επεξεργασία όπου δίνεται η δυνατότητα στον κάθε πολίτη να επιλέξει ποιά από τα δεδομένα του θα επεξεργαστούν και ποιά όχι. Επίσης μπορεί να διακόψει άμεσα την επεξεργασία τους σε περίπτωση εμπορικής τους προώθησης.

3. Δικαίωμα στη λήθη όπου ο κάθε πολίτης μπορεί να αποσύρει τη συγκατάθεση που έχει δώσει για τη χρήση των προσωπικών του δεδομένων από έναν οργανισμό ή εταιρεία ή ακόμη να αιτηθεί και την οριστική διαγραφή τους. Ένα παράδειγμα για να κατανοήσουμε περισσότερο το δικαίωμα αυτό, είναι όταν κάποιος πολίτης “αλλάξει” έναν τηλεπικοινωνιακό πάροχο και “πάει” σε κάποιον άλλον, ο πρώτος είναι υποχρεωμένος να διαγράψει τα προσωπικά δεδομένα του πελάτη μετά από δικιά του απαίτηση. Βέβαια υπάρχουν κάποιες εξαιρέσεις όπως είναι η Ελληνική Αστυνομία (ΕΛΑΣ) που δεν μπορεί να διαγράψει δεδομένα πολιτών καθώς χρειάζεται το πλήρες ιστορικό τους.

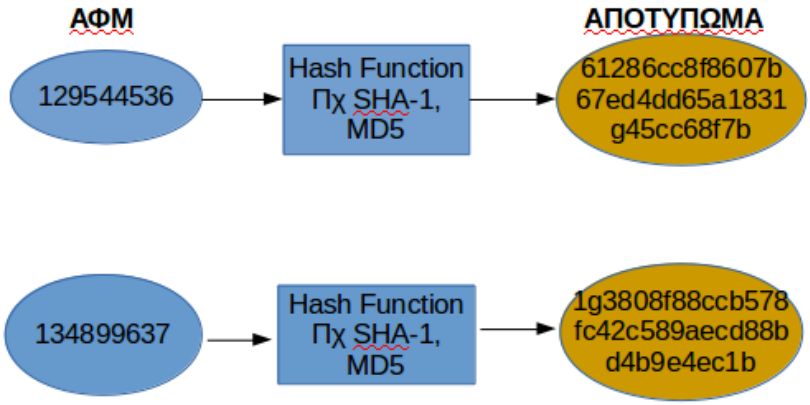
4. Δικαίωμα στη φορητότητα των δεδομένων όπου ο πολίτης μπορεί να μεταφέρει τα δεδομένα του όποτε το επιθυμεί από έναν πάροχο υπηρεσιών σε άλλο. Σε αυτή την περίπτωση υπάρχουν και ακολουθούνται συγκεκριμένοι κανονισμοί ώστε η μια εταιρεια να δώσει τα δεδομένα του πελάτη σε μια άλλη. Δεν μπορεί να τα πουλήσει.

` ***5. Δικαίωμα ειδοποίησης*** Σε περίπτωση παραβίασης δεδομένων που θέτει σε κίνδυνο τα προσωπικά δεδομένα ή σε περίπτωση που μια εταιρεία χάσει τα δεδομένα είτε από κάποια επίθεση είτε από ανθρώπινο λάθος, κάποιου πολίτη, ο τελευταίος θα πρέπει να λάβει σχετική ενημέρωση εντός 72 ωρών από την στιγμή που αναγνωρίστηκε η παραβίαση. Επίσης ενημερώνεται άμεσα και η Αρχή Προστασίας Προσωπικών Δεδομένων. Στο παρελθόν να αναφέρουμε, πριν τον νέο Κανονισμό, δεν υπήρχε αυτή η ειδοποίηση και έτσι για παράδειγμα, αν μια Τράπεζα δεχόταν επίθεση ή παραβίαση στα δεδομένα των πελατών της δεν ενημέρωνε τα υποκείμενα των δεδομένων ώστε να μην χάσει την φήμη της.

6. Προστασία Δεδομένων κατά τον Σχεδιασμό (Data Protection by design) Ο υπεύθυνος επεξεργασίας μαζί με την ομάδα ανάπτυξης εφαρμογών έχουν υποχρέωση προστασίας των δεδομένων ήδη από τον σχεδιασμό των εφαρμογών – υπηρεσιων,

δημιουργώντας εξ' αρχής φιλικές και κατάλληλες συνθήκες. Σε αυτό χρειάζεται η χρήση της τεχνικής της ***ψευδωνυμοποίησης*** (Εικόνα 5.1), σε συνδυασμό με τεχνικές ***κρυπτογράφησης***, σύμφωνα με την οποία επεξεργάζονται προσωπικά δεδομένα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών οι οποίες διατηρούνται χωριστά. Οι τεχνικές αυτές αποσκοπούν στην ανωνυμοποιήση όσο το δυνατόν των προσωπικών δεδομένων που σημαίνει: έχουμε τα δεδομένα μιας βάσης δεδομένων και δεν μπορώ να ανακαλύψω την ταυτότητα του υποκειμένου. Ο GDPR επιβάλει τη χρήση της ψευφωνυμοποίησης και κρυπτογράφησης για περαιτέρω διασφάλιση της ασφάλειας της επεξεργασίας και της προστασίας των θεμελιωδών δικαιωμάτων.

Στην Εικόνα 5.1 βλέπουμε ένα παράδειγμα ανωνυμοποίησης που χρησιμοποείται από πολλούς Υπευθύνους Επεξεργασίας, οι οποίοι συλλέγουν το "αποτύπωμα" (hash value) ενός αναγνωριστικού (identifier) ελπίζοντας πως δεν καθίσταται δυνατόν η αναγνώριση του αρχικού αναγνωριστικού, αφού μια κρυπτογραφική συνάρτηση κατακερματισμού (hash function) είναι μη αναστρέψιμη.



Εικόνα 5.1

Μία άλλη τεχνική ανωνυμοποίησης είναι η ***Γενίκευση (generalization)*** των ψευδοαναγνωριστικών γνωρισμάτων (quasi- identifier) γνωρισμάτων μεταβάλλοντας κατάλληλα τις τιμές των πεδίων όπως φαίνεται στην Εικόνα 5.4.

(α) Ασθενείς

	Ψευδοαναγνωριστικά		Ευαίσθητα
ΦΥΛΛΟ	**ΗΛΙΚΙΑ**	**ΕΠΑΓΓΕΛΜΑ**	**ΑΣΘΕΝΕΙΑ**
Άνδρας	34	Καθηγητής	Διαβήτης
Γυναίκα	28	Δικηγόρος	Ηπατίτιδα Β
Γυναίκα	37	Φαρμακοποιός	Ηπατίτιδα C
Άνδρας	42	Τραπεζ. Υπάλλ.	Λοίμωξη Αναπν
Άνδρας	25	Μουσικός	Γρίπη

Εικόνα 5.2

(β) Εξωτερικός Πίνακας

ΟΝΟΜΑ	ΦΥΛΛΟ	ΗΛΙΚΙΑ	ΕΠΑΓΓΕΛΜΑ
Χρήστος	Άνδρας	40	Δικηγόρος
Ιωάννα	Γυναίκα	27	Τραπεζ. Υπαλλ
Γιώργος	Άνδρας	42	Τραπεζ. Υπαλλ
Κώστας	Άνδρας	28	Νοσοκόμος
Μαρία	Γυναίκα	32	Φυσικοθερα-αυτής

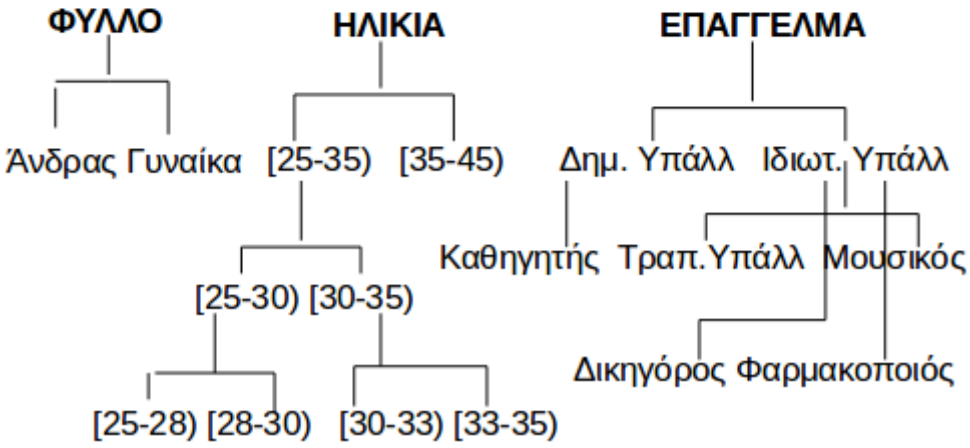
Εικόνα 5.3

Στην Εικόνα 5.2 έχουμε τον πίνακα Ασθενείς με τα δεδομένα ασθενών που έχει ένα νοσοκομείο το οποίο περιέχει προσωπικά και ευαίσθητα δεδομένα όπως είναι για παράδειγμα η ασθένεια. Στην Εικόνα 5.3 βλέπουμε τον πίνακα με τα δεδομένα πολιτών μιας μικρής κοινότητας στα οποία έχει πρόσβαση ο οποιοσδήποτε μέσω κάποιας δημόσιας προσβάσιμης πηγής. Είναι εύκολα αντιληπτό πως με μια συσχέτιση αυτών των δύο πινάκων παίρνουμε την ταυτοποίηση κάποιων πολιτών και συγκεκριμένα από τα τρία γνωρίσματα (ΦΥΛΛΟ , ΗΛΙΚΙΑ, ΕΠΑΓΓΕΛΜΑ) = (Άνδρας, 42, Τραπεζ. Υπαλλ) εξάγουμε το συμπέρασμα ότι ο Γιώργος έχει Λοίμωξη Αναπνευστικού.

Με την τεχνική λοιπόν της *ανωνυμοποίησης,* μεταβάλλουμε κατάλληλα τις τιμές των γνωρισμάτων που είναι ψευδοαναγνωριστικά μέσω γενίκευσή τους (generalization). Για παράδειγμα δεν καταχωρούμε επακριβώς την ηλικία και το επάγγελμα, αλλά ένα εύρος 20-50 ετών και δημόσιος – ιδιωτικός υπάλληλος αντίστοιχα στο κάθε γνώρισμα. Με αυτόν τον τρόπο, η μονοσήμαντη συσχέτιση μιας καταχώρησης του «ανώνυμου» πίνακα με μία του «επώνυμου» καθίσταται πιο δύσκολη. Όσο πιο μεγάλη είναι η γενίκευση, τόσο ενισχύουμε την ανωνυμοποίηση αλλά αντιθέτως έχουμε την απώλεια χρήσιμης πληροφορίας για ερευνητικούς σκοπούς. Στόχος μας επομένως είναι η επίτευξη της μέγιστης ανωνυμοποίησης με όσο το δυνατόν μικρότερη απώλεια πληροφορίας. Στην Εικόνα 5.4 βλέπουμε τον πίνακα με την γενίκευση των ψευδοαναγνωριστικών γνωρισμάτων.

(α) Ασθενείς

ΦΥΛΛΟ	ΗΛΙΚΙΑ	ΕΠΑΓΓΕΛΜΑ	ΑΣΘΕΝΕΙΑ
Άνδρας	30-35	Δημ. Υπάλλ	Διαβήτης
Άνδρας	40-45	Ιδιωτ. Υπάλλ	Λοίμωξη Αναπν
Άνδρας	25-30	Ιδιωτ. Υπάλλ	Γρίπη
Γυναίκα	25-30	Ιδιωτ. Υπάλλ	Ηπατίτιδα Β
Γυναίκα	35-40	Ιδιωτ. Υπάλλ	Ηπατίτιδα C



Εικόνα 5.4

Επομένως με τον νέο Πίνακα (Εικόνα 5.4) δεν μπορεί να επιτευχθεί η συσχέτιση και η εξαγωγή ευαίσθητων προσωπικών δεδομένων κάποιου υποκειμένου, όπως προηγουμένως είχαμε πετύχει.

7. Προστασία Δεδομένων εξ' ορισμού (Data Protection by Default). Πρέπει να υπάρχει εξ' αρχής μια πολιτική ασφαλείας από οποιονδήποτε φορέα ο οποίος συλλέγει προσωπικά δεδομένα, την οποία θα μπορεί να διαβάζει ο καθένας πρωτού παραχωρήσει τα προσωπικά του δεδομένα και να του δίνεται η δυνατότητα ώστε να προχωρήσει ή μη στην επεξεργασία των δεδομένων του αναλόγως με το αν συμφωνεί ή όχι. Για να κατανοήσουμε περισσότερο αυτή την παροχή απορρήτου από προεπιλογή, έχουμε το παράδειγμα όπου κάποιος επισκέπτης μιας ιστοσελίδας, συμπληρώνει ένα ηλεκτρονικό έντυπο για να εγγραφεί σε μια λίστα ενημερωτικών δελτίων, υποβάλλοντας το όνομά του και την διεύθυνση ηλεκτρονικού ταχυδρομείου, όπως και τυχόν πρόσθετες πληροφορίες για τον εαυτό του. Θα πρέπει λοιπόν να υπάρχει μια φόρμα από προεπιλογή ώστε να τον ενημερώνει και να αναμένει πως αυτά τα δεδομένα που καταχώρησε επρόκειτο να επεξεργαστούν πριν πατήσει το κουμπί "Submit" και υποβάλλει την αίτηση εγγραφής του στην λίστα ενημερωτικών δελτίων.

8. Προστασία Δεδομένων για τα παιδιά. Υπάρχει ειδική πρόβλεψη από τον νέο Κανονισμό, καθώς υπάρχει μεγάλη έκθεση στην δημοσιότητα μέσω τον social media, για παιδιά κάτω των 18 ετών. Σύμφωνα με το GDPR η διάθεση ψηφιακών υπηρεσιών θα επιτρέπεται μόνα αν το παιδί είναι τουλάχιστον 16 ετών και ορίζει για ελεύθερη πρόσβαση στο διαδίκτυο το κατώτατο επιτρεπόμενο όριο τα 13 έτη, ενώ για παιδιά ηλικίας από 13-16 ετών θα απαιτείται η συναίνεση του γονέα ή κηδεμόνα. Σύμφωνα μ' αυτό είναι ευθύνη λοιπόν των παρόχων και των μέσων κοινωνικής δικτύωσης να έχουν ορισμένες διαδικασίες που θα ελέχγουν τις ηλικίες των ανθρώπων όταν εκείνοι εγγράφονται ή χρησιμοποιούν τις υπηρεσίες τους, να αλλάξουν την μορφή των όρων χρήσης της κάθε εφαρμογής και τέλος η ενημέρωση των παιδιών και των κηδεμόνων τους να γίνεται σε γλώσσα απλή και σαφή.

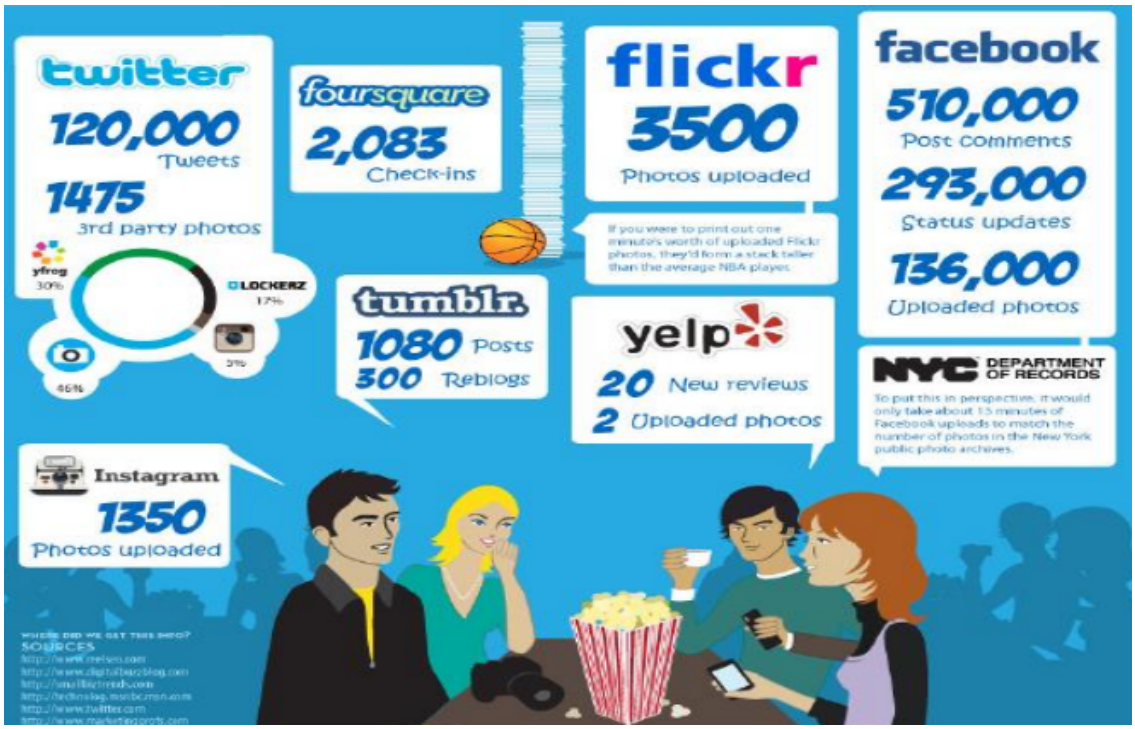
5.2 - Αλλαγές για τις επιχειρήσεις

Υποχρεώνει τις επιχειρήσεις να ορίζουν έναν Υπεύθυνο Προστασίας Δεδομένων (DPO) ο οποίος θα κληθεί να αναλάβει τον θεματοφύλακα των προσωπικών δεδομένων και να προλαμβάνει περιπτώσεις παραβίασης προσωπικών δεδομένων διασφαλίζοντας την ομαλή λειτουργία και τις προϋποθέσεις του νέου Κανονισμού. Για τους χειριστές Δεδομένων ορίζει τον Υπεύθυνο Επεξεργασίας και τον Εκτελών την Επεξεργασία που αναπτύξαμε στο Κεφάλαιο 1. Άλλη υποχρέωσή τους είναι η «εκτίμηση αντικτύπου» σχετικά με την προστασία των δεδομένων (DPIA) και σχετική υποχρέωση διαβούλευσης με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Επίσης θα πρέπει οι επιχειρήσεις ή οι δημόσιοι φορείς να τηρούν αρχείο δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων.

Εν κατακλείδι το GDPR δίνει μεγαλύτερη εξουσία στα άτομα – υποκείμενα των δεδομένων, παρέχει προστασία της ιδιωτικότητας ήδη από τον σχεδιασμό εφαρμογών που τον αφορούν, υπάρχουν μέσα επιβολής κυρώσεων και προστίμων, υπάρχει αυξημένη υποχρέωση λογοδοσίας αυτών που διατηρούν δεδομένα και τα επεξεργάζονται και όλα αυτά δεν είναι σε διάσπαρτους νόμους αλλά σε έναν ενιαίο νόμο – σε έναν ενιαίο Κανονισμό.

ΚΕΦΑΛΑΙΟ 6ο - GDPR ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

Στο Κεφάλαιο αυτό θα εξετάσουμε το πώς ο νέος Κανονισμός επηρεάζει τα Μέσα Κοινωνικής Δικτύωσης, καθώς είναι η κύρια πηγή δεδομένων στις μέρες μας, πώς εφαρμόζεται και τι προβλέπει. Να αναφέρουμε πως από στατιστικές μελέτες στον Ελληνικό χώρο υπάρχει εντυπωσιακή αύξηση στη χρήση των social media καθώς 1 στους 2 Έλληνες διαθέτει λογαριασμό σε μέσο κοινωνικής δικτύωσης. Επίσης υπάρχει αύξηση 79% των λογαριασμών στο youtube (634.050 λογαριασμοί), 49% αύξηση των λογαριασμών στο twitter (509.448 λογαριασμοί) και 20% αύξηση των λογαριασμών στο Facebook (6,7 εκατ. Λογαριασμοί) και σύμφωνα με τις μελέτες υπολογίζεται πως ο μέσος χρόνος ημερησίως όπου οι Έλληνες περνούν στα social media είναι 80 λεπτά.



Τελευταία παρατηρούμε πως υπάρχει μια «κινητοποίηση» στις πλατφόρμες των μέσων κοινωνικής δικτύωσης σχετικά με την συμμόρφωσή τους με τον νέο Κανονισμό. Έτσι γινόμαστε αποδέκτες μηνυμάτων, σχετικά με τους νέους όρους, νέες ρυθμίσεις αναφορικά με τα προσωπικά μας δεδομένα, νέες λειτουργίες και νέες πολιτικές προστασίας προσωπικών δεδομένων, τα οποία καταφθάνουν σε εμάς με διάφορους πρωτότυπους ή μη τρόπους (όπως για παράδειγμα με τη μορφή αναδυόμενων παραθύρων διαλόγων, μενού επιλογών, emails, μηνυμάτων μέσω chatbots, banners υπυνθύμισης, μηνυμάτων sms κτλ).

6.1 - Σκάνδαλο Facebook - Cambridge Analytica

Πρωτού αναπτύξουμε το GDPR στα μέσα κοινωνικής δικτύωσης αξίζει να θυμηθούμε το μεγαλύτερο σκάνδαλο περί «διαρροής πληροφοριών και στοιχείων» που γνώρισε ο “βασιλιάς” των social media το Facebook. Πιο συγκεκριμένα η εταιρεία ανάλυσης δεδομένων Cambridge Analytica με ιδιοκτήτη τον Στιβ Μπανον, σύμβουλο του προέδρου των ΗΠΑ, αναπτύσσοντας ένα λογισμικό παραβίασε τα προσωπικά δεδομένα 50 εκατομμυρίων χρηστών της πλατφόρμας με στόχο να επηρεάσει την τελική τους ψήφο προς όφελος της προεκλογικής καμπάνιας του Ντοναλντ Τραμπ το 2016[7]. Η ανικανότητα του facebook να σταματήσει τις επιθέσεις αυτές, έφερε την άμεση παραίτηση του επικεφαλής του τομέα ασφάλειας του μέσου, Alex Stamos. Τα στοιχεία αντλήθηκαν μέσω της εφαρμογής «thisisyourdigitallife» η οποία είχε δημιουργηθεί το 2013 από αναλυτή του Πανεπιστημίου του Κέιμπριτζ, με ένα κουιζ προσωπικότητας, που στην ουσία συνέλεγε πληροφορίες με τις οποίες στη συνέχεια “έχτιζε” το ψυχολογικό προφιλ του χρήστη. Ο αλγόριθμος της εφαρμογής παραβίαζε λογαριασμούς των συμμετέχοντων αλλά και των φίλων τους, έτσι ώστε οι 320.000 περίπου μοναδικοί χρήστες που έκαναν επί πληρωμή το τεστ και συμφώνησαν να συλλεχθούν τα προσωπικά δεδομένα τους για πανεπιστημιακή χρήση, μια τακτική αντίθετη με τους κανονισμούς του facebook, να πολλαπλασιαστούν και να φτάσουν τα 50.000.000.

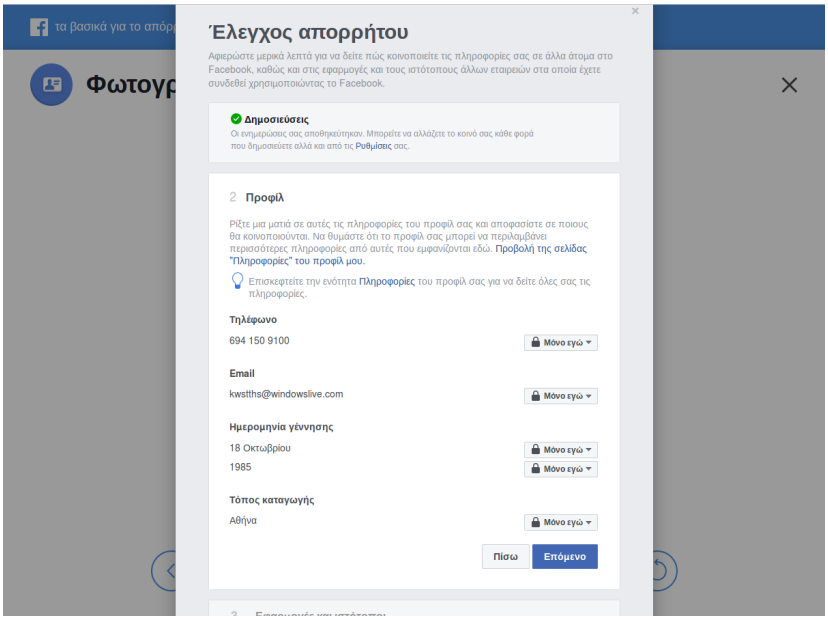
Οι εισαγγελικές αρχές της Μασαχουσέτης και της Νέας Υορκης ζήτησαν με επιστολή τους στην δημοφιλή πλατφόρμα κοινωνικής δικτύωσης να τους δοθεί ολόκληρη η αλληλογραφία που είχε η εταιρεία με την Cambridge Analytica ώστε να διελευκάνουν την υπόθεση και να αποδώσουν ευθύνες. Το facebook από την πλευρά του, με τον Μαρκ Ζουκερμπεργκ να απολογείται για την «διαρροή» επί δύο 24ωρα ενώπιον του Κονγκρέσου, δηλώνει ότι εξαπατήθηκε καθώς έβλεπε παράλληλα τη μετοχή να πέφτει επικίνδυνα στα διεθνή χρηματιστήρια προκαλώντας απώλειες δισεκατομμυρίων.

[7]www.politis.com

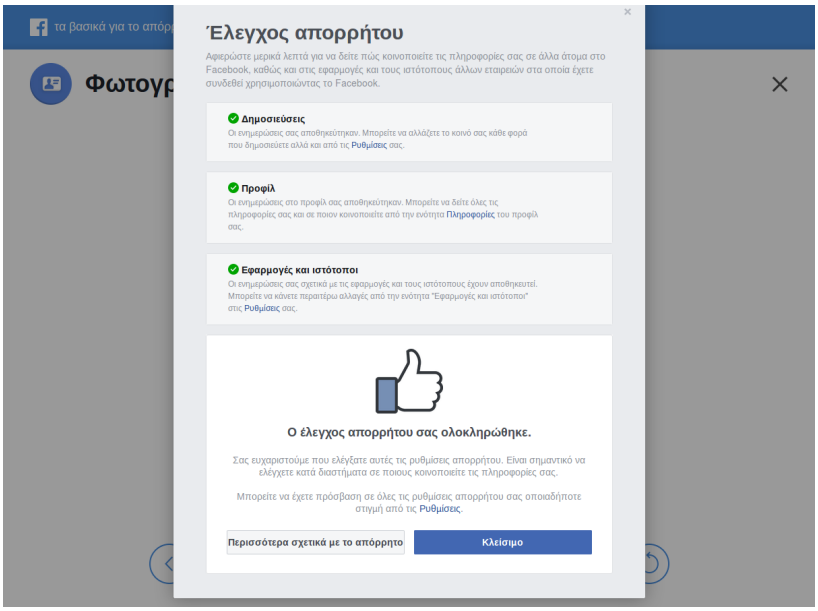
6.2 - Facebbok και GDPR

Αυτό που ζητείται από το GDPR είναι η ρητή και ξεκάθαρη συγκατάθεση του χρήστη με άμεσο και ξεκάθαρο τρόπο. Ο κάθε χρήστης λοιπόν στην περίπτωση του facebook δίνει τη σαφή και αδιαμφισβήτητη συγκατάθεσή του να λαμβάνει επικοινωνία (αλληλεπιδρά με δεδομένα άλλων χρηστών) κάνοντας Like ή Follow στη σελίδα που τον ενδιαφέρει. Η συγκεκριμένη πλατφόρμα εφαρμόζει αυστηρά το ***απόρρητο από προεπιλογή*** που σημαίνει πως ο χρήστης δεν μεταβαίνει στις ρυθμίσεις ώστε να κάνει ο ίδιος χειροκίνητες αλλαγές για να έχει αυστηρότερες ρυθμίσεις καθώς είναι ήδη προκαθορισμένες από την εταιρεία. Για την μεγαλύτερη προστασία των προσωπικών δεδομένων των χρηστών κάνει χρήση της τεχνολογίας ***αναγνώρισης προσώπου (face recognition)***, όπου η χρήση της είναι προαιρετική, θέλωντας έτσι να αποτρέψει και το ενδεχόμενο μιας πιθανής απόπειρας από τρίτους να χρησιμοποίησουν την εικόνα κάποιου χρήστη ως φωτογραφία προφίλ. Επίσης επιλέγοντας κάποιος τη χρήση της τεχνολογίας αυτής ενημερώνεται από την πλατφόρμα σε περίπτωση που εμφανίζεται σε φωτογραφίες ή βίντεο και δεν έχει προστεθεί σε ετικέτα (tag).

Με τον ***Έλεγχο Απορρήτου*** (Εικόνα 6.1 & 6.2) ο κάθε χρήστης μπορεί να δεί και να παραμετροποίηση ποιές από τις πληροφορίες του (προσωπικά και ευαίσθητα δεδομένα) θα κοινοποιηθούν και σε ποιούς.

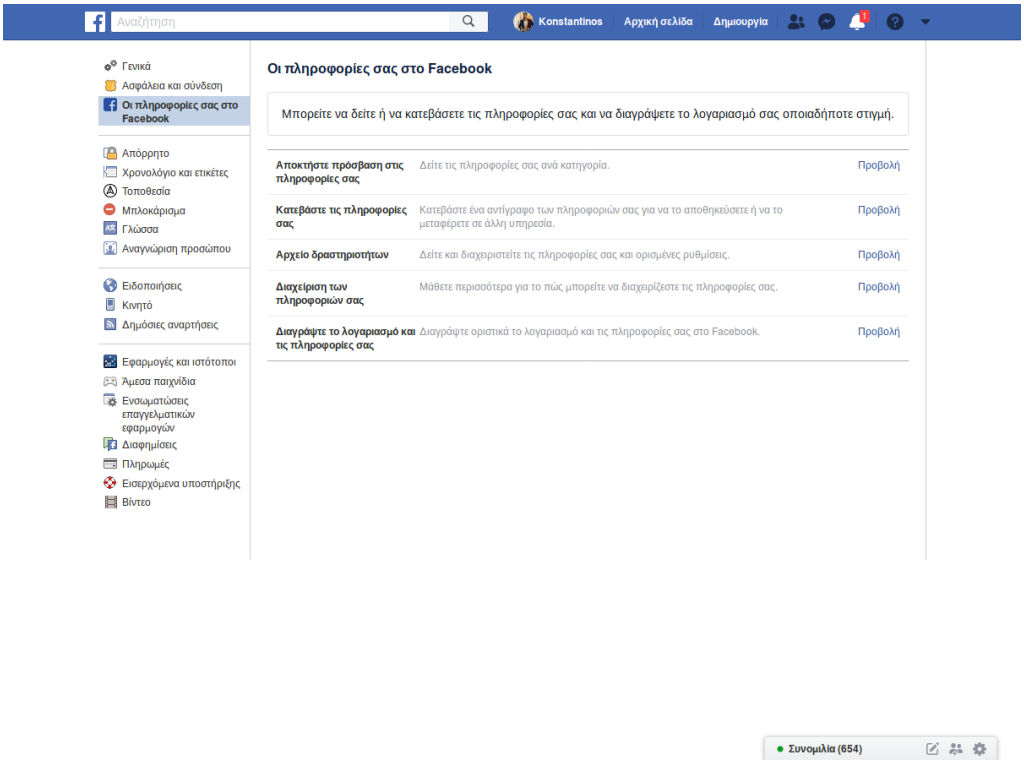


Εικόνα 6.1



Εικόνα 6.2

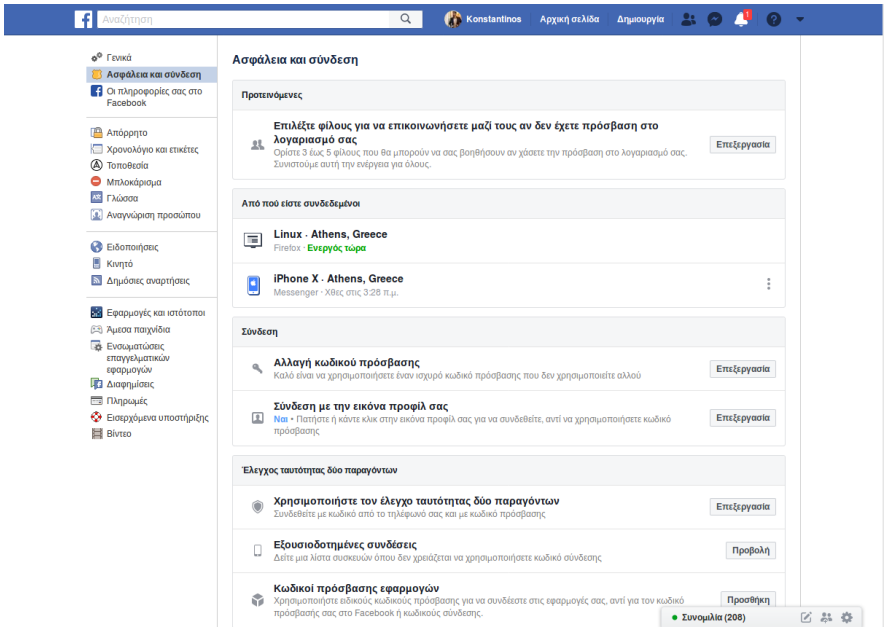
Μια άλλη επιλογή που δίνεται από την πλατφόρμα είναι ***Οι πληροφορίες σας στο Facebook*** μέσα από την επιλογή ρυθμίσεις (Εικόνα 6.3). Σύμφωνα μ' αυτή ο κάθε χρήστης μπορεί να αποκτήσει πρόσβαση στις πληροφορίες και να κατεβάσει αντίγραφο αυτών οποιαδήποτε στιγμή. Του δίνεται η δυνατότητα να κατεβάσει όλα τα δεδομένα μαζί, ή κατηγορίες δεδομένων, σε μορφή HTML, ώστε να μπορεί να τα δεί εύκολα ή σε μορφή JSON για την εύκολη εισαγωγή τους σε άλλη υπηρεσία.



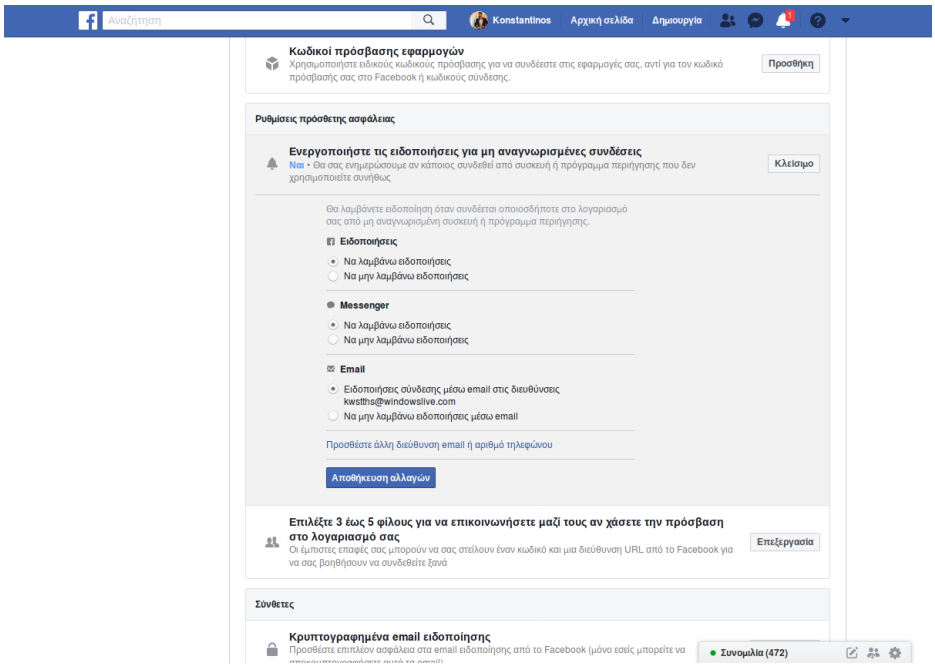
Εικόνα 6.3

Όσον αφορά την προστασία δεδομένων μας, προσωπικών και ευαίσθητων στην πλατφόρμα του facebook θα λέγαμε πως είναι αποκλειστικά δική μας ευθύνη. Ενώ καμία σελίδα δεν είναι απαραβίαστη, στις περισσότερες φορές των περιπτώσεων που κάποιος απώλεσε την πρόσβασή του στον λογαριασμό του, ήταν από δικό του λάθος παρά κάποιας αδυναμίας του facebook, μετά μάλιστα από την εναρμόνισή του με τον νέο Κανονισμό. Έτσι σαν πρώτο μέτρο προστασίας θα προτείναμε, να έχουμε τον απόλυτο έλεγχο όλων των συσκευών με τις οποίες πραγματοποιούμε απομακρυσμένη σύνδεση στον λογαριασμό μας, μια δυνατότητα που μας την παρέχει η πλατφόρμα με την επιλογή *Ρυθμίσεις → Ασφάλεια και Σύνδεση* (Εικόνα 6.4) καθώς επίσης να επιλέξουμε να λαμβάνουμε ειδοποιήσεις σε περίπτωση που κάποιος έχει τον κωδικό μας και επιχειρήσει να συνδεθεί στον λογαριασμό μας (Εικόνα 6.5). Στην ίδια καρτέλα ορίζουμε αν θα μας έρχεται ένα απλό notification στο Facebook ή στο Messenger ή ένα email όταν ο λογαριασμός μας συνδέεται από μια νέα συσκευή.

Ένα άλλο μέτρο είναι να ενεργοποιήσουμε τον ***έλεγχο ταυτότητας δύο παραγόντων,*** ένα πρόσθετο επίπεδο που μας παρέχει το facebook. Με την μέθοδο αυτή κάθε φορά που θα θέλουμε να κάνουμε σύνδεση στον λογαριασμό μας, αφού εισάγουμε τον κωδικό πρόσβασής μας, θα μας ζητηθεί ο κωδικός σύνδεσης, ένας μοναδικός κωδικός, ο οποίος προηγουμένως θα μας έχει σταλθεί ως sms στο κινητό μας. Έτσι και να καταφέρει κάποιος να μας υποκλέψει τον κωδικό πρόσβασής μας μέσω της μεθόδου phishing ή με κάποιο malware που καταγράφει το πληκτρολόγιό μας, δεν θα καταφέρει να έχει στην κατοχή του ταυτόχρονα και τον κωδικό σύνδεσης που όπως αναφέραμε απαιτείται για να πραγματοποιηθεί η τελική σύνδεσή μας στο λογαριασμό.

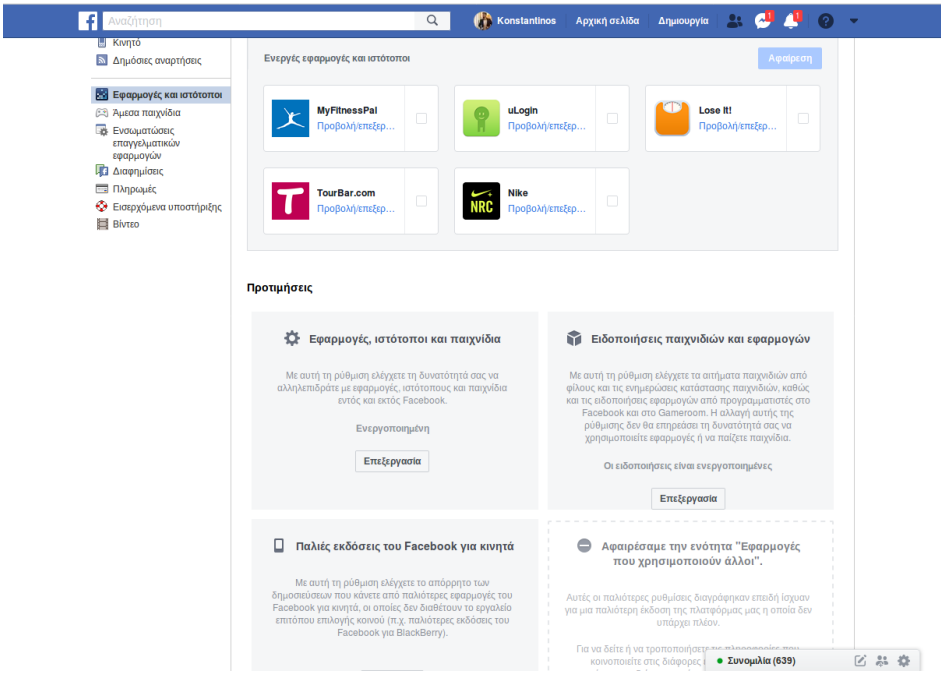


Εικόνα 6.4



Εικόνα 6.5

Τέλος να επισημάνουμε πως με τις νέες ρυθμίσεις που επέβαλε το GDPR, το Facebook αφαίρεσε την ενότητα “Εφαρμογές που χρησιμοποιούν άλλοι”, θέλωντας να προστατεύσει τους χρήστες από την «επεξεργασία» των δεδομένων τους από εφαρμογές ξένες. Έτσι από τις *Ρυθμίσεις → Εφαρμογές και ιστότοποι* έχουν τον απόλυτο έλεγχο οι χρήστες να επιλέξουν με ποιές εφαρμογές, ιστότοπους και παιχνίδια θα αλληλεπιδρούν (Εικόνα 6.6).



Εικόνα 6.6

Σε αντίστοιχες ενέργειες με το Facebook έχουν προβεί σταδιακά και όλα τα υπόλοιπα μέσα δικτύωσης όπως το Instagram, Snapchat, LinkedIn, WhatsApp, Twitter και Viber.

ΚΕΦΑΛΑΙΟ 7ο - ΜΕΘΟΔΟΛΟΓΙΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟ GDPR -ΤΕΧΝΙΚΑ ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Στο Κεφάλαιο αυτό θα αναλύσουμε τον « οδικό χάρτη» και την μεθοδολογία που χρειάζεται ώστε οι επιχειρήσεις, οι οργανισμοί να συμμορφωθούν με τον νέο Κανονισμό προκειμένου να μην έχουν προβλήματα και κυρώσεις σε περίπτωση που τους γίνει έλεγχος από την αρμόδια εποπτική αρχή ή υπάρξουν καταγγελίες εις βάρος τους. Έτσι λοιπόν συστήνονται τα εξής:[8]

[8]www.webtralls.gr

1) Διαμόρφωση συνείδησης προστασίας προσωπικών δεδομένων. Εντός της επιχείρησης θα πρέπει να υπάρχει ενημέρωση τόσο της διοίκησης όσο και του προσωπικού για το ότι ο Κανονισμός επιφέρει αλλαγές στην προστασία των δεδομένων και ενδεχομένως και στη λειτουργία της επιχείρησης. Επομένως όλοι οι εργαζόμενοι της επιχείρησης επιβάλλεται να γνωρίζουν, στο βαθμό που είναι αναγκαίο για την ορθή άσκηση των καθηκόντων τους τί επιτρέπεται και τί απαγορεύεται, τί είναι υποχρεωτικό και τί προαιρετικό με βάση τον Κανονισμό. Ακόμη και αν όλα τα τεχνικά μέτρα προστασίας που η επιχείρηση ή ο οργανισμός εφαρμόζει είναι άψογα, εάν δεν υπάρχει ευαισθητοποίηση και κινητοποίηση του ανθρώπινου δυναμικού, θα ανακύπτουν συνεχώς προβλήματα συμμόρφωσης.

2) ***Χαρτογράφηση ροής δεδομένων (Data Flow Mapping).*** Η επιχείρηση ή ο οργανισμός θα πρέπει να χαρτογραφήσει τα προσωπικά δεδομένα που επεξεργάζεται, τις πηγές τις οποίες τα αντλεί καθώς και τους αποδέκτες τους. Συγκεκριμένα πρώτα από όλα θα πρέπει να διαχωρίσει στο τι είδους δεδομένα υπόκεινται σε επεξεργασία και σε ποιά κατηγορία εμπίπτουν, αν είναι για παράδειγμα δεδομένα υγείας, ποινικό μητρώο, δεδομένα θέσης κλπ. Επίσης θα πρέπει να εξετάσουν σε ποιά μορφή αποθηκεύονται (έντυπη, ψηφιακή, βάση δεδομένων, κινητά τηλέφωνα κλπ), πως συλλέγονται (ταχυδρομείο, τηλέφωνο, κοινωνικά μέσα) και πως τα μοιράζεται εσωτερικά εντός της επιχείρησης και εξωτερικά (με τρίτους). Ποιές τοποθεσίες εμπλέκονται στη ροή δεδομένων αν είναι για παράδειγμα γραφεία ή cloud και γενικά θα πρέπει η επιχείρηση να αναλύσει όλο τον κύκλο ζωής των δεδομένων προκειμένου να εντοπίσει απρόβλεπτες ή ακούσιες χρήσεις αυτών.

3) Αναθεώρηση της πολιτικής απορρήτου. Θα πρέπει να γίνει αναθεώρηση της πολιτικής απορρήτου γνωστή και ως πολιτική προστασίας δεδομένων (privacy notice) ώστε να είναι συμβατή με τις διατάξεις του νέου Κανονισμού. Προκειμένου η πολιτική απορρήτου να καταστεί όσο γίνεται περισσότερο προσπελάσιμη και ευρύτερα γνωστή, συνίσταται η ανάρτησή της στην αρχική ιστοσελίδα της επιχείρησης ή του οργανισμού. Οι Υπεύθυνοι Επεξεργασίας υποχρεώνονται πλέον από τον Κανονισμό να γνωστοποιούν στο υποκείμενο των δεδομένων τη νόμιμη βάση επεξεργασίας των δεδομένων του, το χρόνο τήρησής τους και το δικαίωμά του για υποβολή καταγγελίας στην αρμόδια εποπτική αρχή. Η πληροφόρηση αυτή πρέπει πάντα να γίνεται σε ύφος “λακωνικό” και σε γλώσσα σαφή και εύκολα κατανοητή από το μέσο πολίτη. Επίσης στο κείμενό της θα πρέπει να αναφέρεται σχετικά με τον έλεγχο πρόσβασης των

χρηστών στις εφαρμογές και στα αποθηκευμένα δεδομένα βάσει των ρόλων και των δικαιωμάτων τους. Ανάλογα με τις ανάγκες ασφαλείας του οργανισμού, πολλές φορές είναι απαραίτητη η χρήση πλατφόρμας μέσω της οποίας ελέγχονται και άλλες παράμετροι που εμπλέκονται στην πρόσβαση του εκάστοτε χρήστη στους εταιρικούς πόρους όπως για παράδειγμα το ενημερωμένο OS & antivirus engine του τερματικού, η ώρα, ο τύπος του τερματικού και το σημείο από το οποίο γίνεται η προσπάθεια πρόσβασης στους πόρους του οργανισμού. Τέλος στην πολιτική απορρήτου θα πρέπει να συμπεριλαμβάνεται η αρχή της «ελαχιστοποίησης των δεδομένων» σύμφωνα με την οποία γίνεται επεξεργασία των απολύτως αναγκαίων δεδομένων για την επίτευξη του εκάστοτε σκοπού και όχι περισσοτέρων δεδομένων από ότι χρειάζεται.

4) Έλεγχος των υφιστάμενων διαδικασιών της επιχείρησης ώστε να εξακριβωθεί αν και κατά πόσο διασφαλίζουν την υλοποίηση των νέων καθώς και των ήδη υφιστάμενων αλλά ενισχυμένων πλέον από τον Κανονισμό, δικαιωμάτων των υποκειμένων των δεδομένων. Πρόκειται για τα:

- δικαίωμα ενημέρωσης
- δικαίωμα πρόσβασης
- δικαίωμα διόρθωσης
- δικαίωμα στη λήθη (δικαίωμα διαγραφής)
- δικαίωμα στον περιορισμό της επεξεργασίας
- δικαίωμα στη φορητότητα των δεδομένων
- δικαίωμα εναντίωσης

τα οποία αναπτύξαμε και εξηγήσαμε στο Κεφάλαιο 5.

5) Υιοθέτηση κατάλληλων οργανωτικών και τεχνικών μέτρων. Έλεγχος εάν έχουν υιοθετηθεί τα κατάλληλα οργανωτικά και τεχνικά μέτρα προκειμένου η επιχείρηση ή ο οργανισμός να μπορεί αμέσως και ευχέρως να ανταποκρίνεται σε αιτήματα των υποκειμένων των δεδομένων για πρόσβαση σ' αυτά, ιδίως μάλιστα αν αναμένονται πολλά τέτοια αιτήματα. Πρέπει να υπάρχει μεγάλη προσοχή στην άσκηση του δικαιώματος πρόσβασης του υποκειμένου διότι τις πεισσότερες φορές το δικαίωμα αυτό παρέχεται δωρεάν, ενώ η προθεσμία απάντησης είναι μόνο ένας μήνας. Σε περίπτωση άρνησης ικανοποίησης του δικαιώματος πρόσβασης, ο Υπεύθυνος Επεξεργασίας οφείλει να εξηγήσει στο υποκείμενο των δεδομένων χωρίς αναίτια καθυστέρηση και το αργότερο εντός ενός μηνός το λόγο άρνησης και ταυτόχρονα ενημερώνει το υποκείμενο για το δικαίωμα του να υποβάλει καταγγελία στην αρμόδια εποπτική αρχή και να προσφύγει δικαστικά κατά του Υπευθύνου Επεξεργασίας. Μια «καλή πρακτική» θα λέγαμε αποτελεί η εγκατάσταση IT συστήματος που επιτρέπει την online πρόσβαση των υποκειμένων στα προσωπικά τους δεδομένα.

6) Έλεγχος επαλήθευσης της ηλικίας. Έλεγχος αν υπάρχει ανάγκη υιοθέτησης μέτρων επαλήθευσης της ηλικίας των υποκείμενων των δεδομένων καθώς και μέτρων λήψης της συγκατάθεσης των γονέων ή των κηδεμόνων για κάθε επεξεργασία δεδομένων παιδιών.

7) Υιοθέτηση της προστασίας της ιδιωτικότητας εξ' ορισμού, εκ' σχεδίου και δια σχεδιασμού. Απαιτείται η προστασία της ιδιωτικότητας εξ' ορισμού (Privacy by Default) καθώς και εκ σχεδίου και δια σχεδιασμού (Privacy by Design) όπως αναπτύξαμε στο Κεφάλαιο 5. Εν συντομία με το πρώτο επιτυγχάνουμε:

- ελαχιστοποίηση των υπο επεξεργασία δεδομένων ως προς τον όγκο τους καθώς και ως προς την ένταση της επεξεργασίας
- παροχή στο χρήστη της δυνατότητας ο ίδιος ενεργά να προσδιορίζει την «ορατότητα» στο προφίλ του

ενώ με το δεύτερο επιτυγχάνουμε:

- πάλι την ελαχιστοποίηση της επεξεργασίας δεδομενων
- την ψευδωνυμοποίηση
- την διαφάνεια όσον αφορά την επεξεργασία ώστε να μπορεί το υποκείμενο των δεδομένων να παρακολουθεί την επεξεργασία τους.

Να τονίσουμε επίσης ότι η λήψη μέτρων προστασίας εκ σχεδίου και δια σχεδιασμού θα πρέπει να γίνεται λαμβάνοντας υπόψη όχι μόνο τις τελευταίες τεχνολογικές εξελίξεις αλλά και το κόστος εφαρμογής των μέτρων αυτών καθώς και την πιθανότητα και σοβαρότητα των κινδύνων που μπορεί να προκύψουν (riskassessement).

8) Κρυπτογράφηση των δεδομένων. Τα δεδομένα θα πρέπει να κρυπτογραφούνται τόσο κατά τη μεταφορά όσο και κατά την παραμονή τους στα συστήματα αποθήκευσης. Πάρα πολλές είναι οι λύσεις θα λέγαμε σ' αυτόν τον τομέα αναλόγως βέβαια με τις ανάγκες της κάθε επιχείρησης. Οι δημοφιλέστερες εκ αυτών υλοποιούνται μέσω ενεργοποίησης της συγκεκριμένης δυνατότητας του συστήματος αποθήκευσης, το οποίο για τον σκοπό αυτό χρησιμοποιεί ξεχωριστά cpus ώστε να μην επιβαρύνεται η πρωταρχική λειτουργικότητα του συστήματος.

9*) Πρόληψη Απώλειας Δεδομένων (Data Loss Prevention – DLP).* Θα λέγαμε ότι είναι ίσως το σημαντικότερο εργαλείο στο πλαίσιο προφύλαξης των δεδομένων μιας επιχείρησης ή οργανισμού. Η συγκεκριμένη πλατφόρμα, σε συνδυασμό με την την Ταξινόμηση των Δεδομένων (Classification of Data) που είναι η αυτόματη κατηγοριοποίηση των ευαίσθητων δεδομένων που εμπεριέχονται σε αρχεία κειμένων (documents, pdf, text κτλ) αλλά και σε συγκεκριμένα πεδία μιας φόρμας (τιμολόγια, έντυπα εγγραφής πελατών), αναλαμβάνει να εκτελέσει τις εταιρικές πολιτικές ώστε να προστατευτούν τα ευαίσθητα δεδομένα της επιχείρησης – οργανισμού.

Η συγκεκριμένη υπηρεσία DLP έχει τρεις προκαθορισμένες αποκρίσεις σε περίπτωση που κάποιος χρήστης προσπαθήσει να στείλει ή να ανεβάσει ευαίσθητα δεδομένα:

- Να στείλει μια *ειδοποίηση* στον διαχειριστή συστήματος

- Να *αποτρέψει* την αποστολή δεδομένων
- Να *κρυπτογραφήσει* τα δεδομένα πριν αποσταλούν

10) Perimeter Security Systems. Η υποδομή IT και ειδικότερα το σύστημα αποθήκευσης θα πρέπει να προστατεύεται από ισχυρά συστήματα ασφαλείας δικτύων όπως για παράδειγμα firewalls, antispam & antimalware systems, intrussion protection systems κλπ. Τα συγκεκριμένα συστήματα μπορούν να λειτουργούν ως ανεξάρτητρα Vms πάνω στην υποδομή, εκμεταλλευόμενοι τα πλεονεκτήματα του virtualization.

11) Συστήματα endpoint security. Κάθε σταθμός εργασίας θα πρέπει να διαθέτει ένα ενημερωμένο και αξιόπιστο λογισμικό endpoint protection (firewall, Antivirus κλπ)

12) Λήψη Αντιγράφων Ασφαλείας (Backup). Η λήψη αντιγράφων ασφαλείας είναι απαραίτητη καθώς επιτρέπει την προστασία των δεδομένων και των εφαρμογών μιας επιχείρησης με ένα δομημένο τρόπο. Αυτά λαμβάνονται σύμφωνα με την πολιτική της επιχείρησης και την κρισιμότητα των δεδομένων που προστατεύουν. Υπάρχει πληθώρα λύσεων backup – restore ανάλογα με το μέγεθος και την πολυπλοκότητα του εταιρικού περιβάλλοντος. Υπάρχουν περιπτώσεις όπου γίνεται σε tape ή σε δίσκο ή επίσης σε συνδυασμό αυτών. Πολλές είναι βέβαια οι επιχειρήσεις που προτιμούν να υλοποιούν το backup δεδομένων σε κάποια άλλη ιστοσελίδα, για ακόμη μεγαλύτερη προστασία αυτών. Σε αυτές τις περιπτώσεις είναι απαραίτητη και η χρήση μεθόδων κρυπτογράφησης καθώς ο κίνδυνος να υποπέσουν ευαίσθητα δεδομένα σε λάθος χέρια είναι αυξημένος.

Έτσι λοιπόν κλείνουμε το Κεφάλαιό μας συνοψίζοντας τα βήματα προετοιμασίας για τον νεό Κανονισμό που απαιτούνται από μικρό – μεσαίες και μεγάλες επιχειρήσεις να ακολουθήσουν:

Βήμα 1ο: *Μελέτη του Κανονισμού και εντοπισμός πτυχών.*
Βήμα 2ο: *Συζήτηση με συναδέλφους και νομικούς συμβούλους της εταιρείας.*
Βήμα 3ο: *Καταγραφή δραστηριοτήτων του οργανισμού που εμπίπτουν στον Κανονισμό*
Βήμα 4ο: *Έλεγχος αν η πληροφόρηση που παρέχεται χρειάζεται διαφοροποίηση για να προσαρμοστεί αναλόγως.*
Βήμα 5ο: *Κατάλληλη εκπαίδευση ανθρώπινου δυναμικού.*
Βήμα 6ο: *Έλεγχος πώς τα νέα δικαιώματα του GDPR επηρεάζουν τις δραστηριότητες του οργανισμού.*
Βήμα 7ο: *Εξασφάλιση ότι κάθε δραστηριότητα της επιχείρησης υπακούει στις προυποθέσεις για νόμιμη επεξεργασία.*
Βήμα 8ο: *Εξασφάλιση ότι διαθέτουν κατάλληλα και εκσυγχρονισμένα τεχνικά και διαδικαστικά μέτρα ασφαλείας.*
Βήμα 9ο: *Προσοχή στην επεξεργασία ευαίσθητων δεδομένων και μέριμνα για την ενσωμάτωση δικλείδων ασφαλείας ειδικά για τα παιδιά.*

Βήμα 10ο: *Κατανόηση των κινδύνων που δημιουργούνται και ανάλυση των επιπτώσεων (DPIA)*
Βήμα 11ο: *Σχεδιασμός προϊόντων και υπηρεσιών λαμβάνοντας υπόψη την προστασία της ιδιωτικότητας.*
Βήμα 12ο: *Ενημέρωση των αρμόδιων αρχών ή και των επηρεαζόμενων προσώπων εντός 72 ωρών.*
Βήμα 13ο: *Ορισμός Υπευθύνου Προστασίας Δεδομένων (DPO).*
Βήμα 14ο: *Δημιουργία πλάνου αντιμετώπισης περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων (Incident Response Plan).*
Βήμα 15ο: *Ετοιμότητα για αποζημίωση των πελατών των οποίων τα δεδομένα δεν κατάφεραν να προστατευτούν.*

ΚΕΦΑΛΑΙΟ 8ο - ΛΟΓΙΣΜΙΚΑ ΥΠΟΣΤΗΡΙΞΗΣ ΚΑΙ ΕΝΣΩΜΑΤΩΣΗΣ ΤΟΥ GDPR

8.1 - Συστήματα και λογισμικά της εταιρείας SYMANTEC

Η εταιρεία Symantec είναι μία από τις μεγαλύτερες εταιρείες παγκόσμιας ασφάλειας στον κυβερνοχώρο και παρέχει ολοκληρωμένες λύσεις για την προστασία σε επιθέσεις σε clouds, υποδομές πληροφορικής και λειτουργικά συστήματα. Χρησιμοποιεί την τεχνολογία Control Compliance Suite (CCS) σύμφωνα με την οποία επιτυγχάνεται η *αρχική αξιολόγηση της ετοιμότητας,* βοηθώντας τους οργανισμούς να εκτιμήσουν πόσο απέχουν από την εκπλήρωση σημαντκών απαιτήσεων του GDPR, και να εφαρμόσουν μια αποδοτική, ολιστική προσέγγιση στη διαδικασία αυτοματοποίησης συμμόρφωσης με την αξιοποίηση των παρακάτω λειτουργικών εργαλείων της CCS:

- ***Symantec CCS Policy Manager:*** Αυτοματοποιεί τον ορισμό της πολιτικής του οργανισμού και της διαχείρισης του κύκλου ζωής.
- ***Symantec CCS Assessment Manager:*** Χρησιμοποιείται για να συλλέξει πληροφορίες για την ανταπόκριση τόσο στην ετοιμότητα όσο και στο πλήρες ερωτηματολόγιο περιεχομένου του GDPR.
- ***Symantec CCS StandartsManager:*** Χρησιμοποιείται για τη συλλογή τεχνικών στοιχείων σχετικά με την επιβολή της ασφάλειας δεδομένων.

Επίσης με τη χρήση της τεχνολογίας ***Information Centric Security*** επιτυγχάνεται ένας καινοτόμος συνδυασμός βασικής τεχνολογίας προστασίας δεδομένων και αναλυτικών στοιχείων, ώστε οι οργανισμοί να μπορούν να εντοπίζουν, να παρακολουθούν και να προστατεύουν ευαίσθητα δεδομένα, συμπεριλαμβανομένων των δεδομένων που μετακινούνται στο cloud και χρησιμοποιούνται από οργανισμούς τρίτων.

8.2 - Συστήματα και λογισμικά της εταιρείας IBM

Η IBM διαθέτει έναν από τους μεγαλύτερους στον κόσμο, οργανισμούς έρευνας, ανάπτυξης και διάθεσης λύσεων στον τομέα της ασφάλειας πληροφοριακών συστημάτων. Δημιούργησε ένα από τα πιο εξελιγμένα και ολοκληρωμένα χαρτοφυλάκια προϊόντων και υπηρεσιών ασφαλείας το **IBM Resilient[9].** Τα εργαλεία του είναι:

- Το **Resilient GDPR Preparatory Guide**, ένα διαδραστικό εργαλείο με οδηγίες για την ετοιμότητα της επιχείρησης ως προς τον Κανονισμό GDPR, το οποίο αξιοποιεί την ευελιξία της πλατφόρμας **Resilient IRP (Incident Response Plattform)** και κάνει την προετοιμασία και το σχεδιασμό, μια διαδραστική και δυναμική διαδικασία.

- Το **Resilient GDPR – Enhanced Privacy Module,** μια παγκόσμια βάση δεδομένων για την προστασία της ιδιωτικότητας με συνεχείς ενημερώσεις σχετικά με τις απαιτήσεις του GDPR.
- Το **Resilient GDPR Simulation,** μια νέα λειτουργία της πλατφόρμας **Resilient IRP** που βοηθάει τους αναλυτές ασφαλείας της επιχείρησης να προσοιμοιάσουν τις ενέργειες στις οποίες θα χρειαστεί να προβούν σε περίπτωση παραβίασης.
- Το **Incident Response Platform (IRF),** μια πλατφόρμα που δίνει στις ομάδες ασφαλείας της επιχείρησης τα απαραίτητα εργαλεία για να αναλύουν, να αντιμετωπίζουν και να εξουδετερώνουν τα περιστατικά, εξυπνότερα και αποτελεσματικότερα.

[9] www.insuranceworld.gr

8.3 - Συστήματα και λογισμικά της εταιρείας SAP

Οι διαδικασίες προστασίας δεδομένων από την SAP περιέχουν την πρόβλεψη (predict), την πρόληψη (prevent), την ανίχνευση (detect), και την ανταπόκριση (respond). Κάθε κατηγορία περιγράφει συγκεκριμένες διαδικασίες προστασίας όπως για παράδειγμα τη διαχείριση περουσιακών στοιχείων, τη διαχείρισση περιστατικών ή την απειλή πληροφοριών. Το αποθετήριο του συστήματος πληροφοριών στο SAP μπορεί να χρησιμοποιηθεί για να απαριθμήσει όλους τους πίνακες που περιέχουν πεδία με προσωπικές πληροφορίες. Επίσης με το λογισμικό της SAP παρέχεται προστασία δεδομένων σε διάφορα στάδια:

- Στάδιο επεξεργασίας → να είναι προσιτά για τον επιδωκόμενο σκοπό
- Στάδιο αποκλεισμού → να είναι προσβάσιμα μόνο για χρήστες με ρητή άδεια
- Ολοκλήρωση δέσμευσης → σε περίπτωση λήξης του σκοπού να διαγράφονται
- Περιορισμός της πρόσβασης σε ευαίσθητες προσωπικές πληροφορίες και της διαθεσιμότητάς τους όσο απαιτείται
- Εφαρμογή ελέγχων για την αποτροπή της λήψης προσωπικών πληροφοριών
- Εφαρμογή βέλτιστων πρακτικών για τη μεταφορά και τη διαγραφή προσωπικών δεδομένων σε ένα σύστημα SAP σε παραγωγικά και μη παραγωγικά περιβάλλοντα.

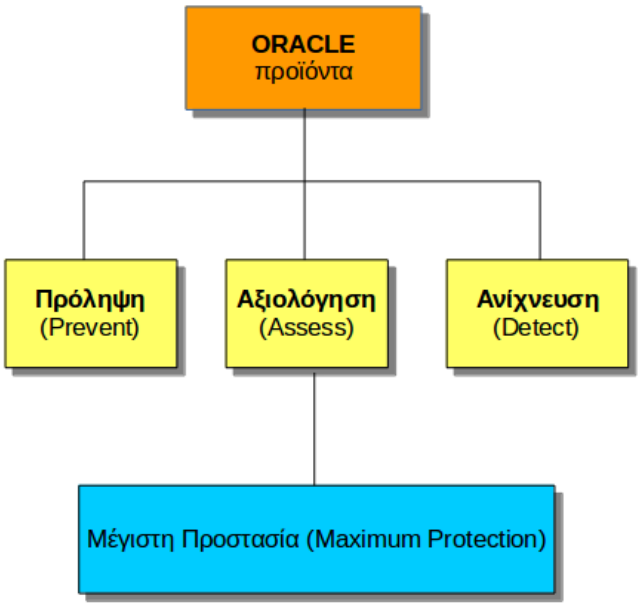
8.4 - Συστήματα και λογισμικά της εταιρείας MICROSOFT

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

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

8.5 - Συστήματα και λογισμικά της εταιρείας ORACLE

Η εταιρεία Oracle παρέχει προστασία δεδομένων σύμφωνα με το παρακάτω διάγραμμα (Εικόνα 8.1).



Εικόνα 8.1

Πρόληψη (Prevent)

Χρησιμοποιεί μια σειρά προληπτικών ελέγχων που βοηθά τους οργανισμούς να εφαρμόσουν τις βασικές προληπτικές τεχνικές σύμφωνα με το GDPR με τις παρακάτω λειτουργίες:

- Transparent Data Encryption (TDE): Κρυπτογράφηση δεδομένων
- Oracle Key Vault (OKV): Διαχείριση κεντρικών κλειδιών κρυπτογράφησης
- Oracle Database Network Encryption and Data Integrity: Κρυπτογράφηση δεδομένων σε μεταφορά
- Oracle Data Masking and Subsetting: Ανωνυμοποίηση και ελαχιστοποίηση

- Oracle Virtual Private Database: Επιλεκτική απόκρυψη δεδομένων
- Oracle Label Security: Έλεγχος Πρόσβασης

Αξιολόγηση (Assess)

Προχωρά στην ανάλυση των ρόλων και των δικαιωμάτων των βάσεων δεδομένων για τον καθορισμό του τρόπου με τον οποίο οι ελεγκτές, οι επεξεργαστές, τα τρίτα μέρη και οι παραλήπτες μπορούν να έχουν πρόσβαση σε προσωπικά δεδομένα. Έτσι έχουμε τις υπηρεσίες:

- **Oracle Application Data Modeling:** Αξιολόγηση ευαίσθητων δεδομένων
- **Oracle Database Security Assessment Tool:** Αξιολόγηση του προφίλ ασφάλειας των βάσεων δεδομένων.
- **Oracle Database Vault Privilege Analysis:** Αξιολόγηση της προνομιακής πρόσβασης.

Ανίχνευση (Detect)

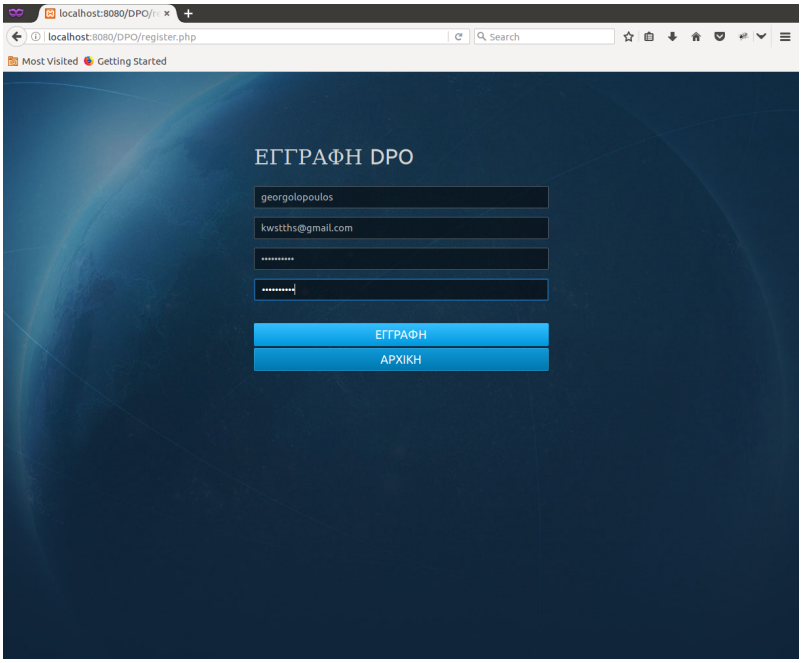
Η Oracle Database Security παρέχει έναν εκτεταμένο μηχανισμό συλλογής και υποβολής εκθέσεων σε περίπτωση εντοπισμού παραβιάσεων. Επίσης με το Oracle Audit Vault και Database Firewall (AVDF) παρέχεται μια ολοκληρωμένη και ευέλικτη παρακολούθηση μέσω της ενοποίησης δεδομένων από βάσεις δεδομένων Oracle και μη Oracle. Να αναφέρουμε ότι το Database Firewall μπορεί να λειτουργήσει και ως πρώτη γραμμή υπεράσπισης στο δίκτυο, επιβάλλοντας την αναμενόμενη συμπεριφορά των εφαρμογών.

ΚΕΦΑΛΑΙΟ 9ο - ΕΦΑΡΜΟΓΗ ΓΙΑ ΤΟΝ ΥΠΕΥΘΥΝΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (DPO)

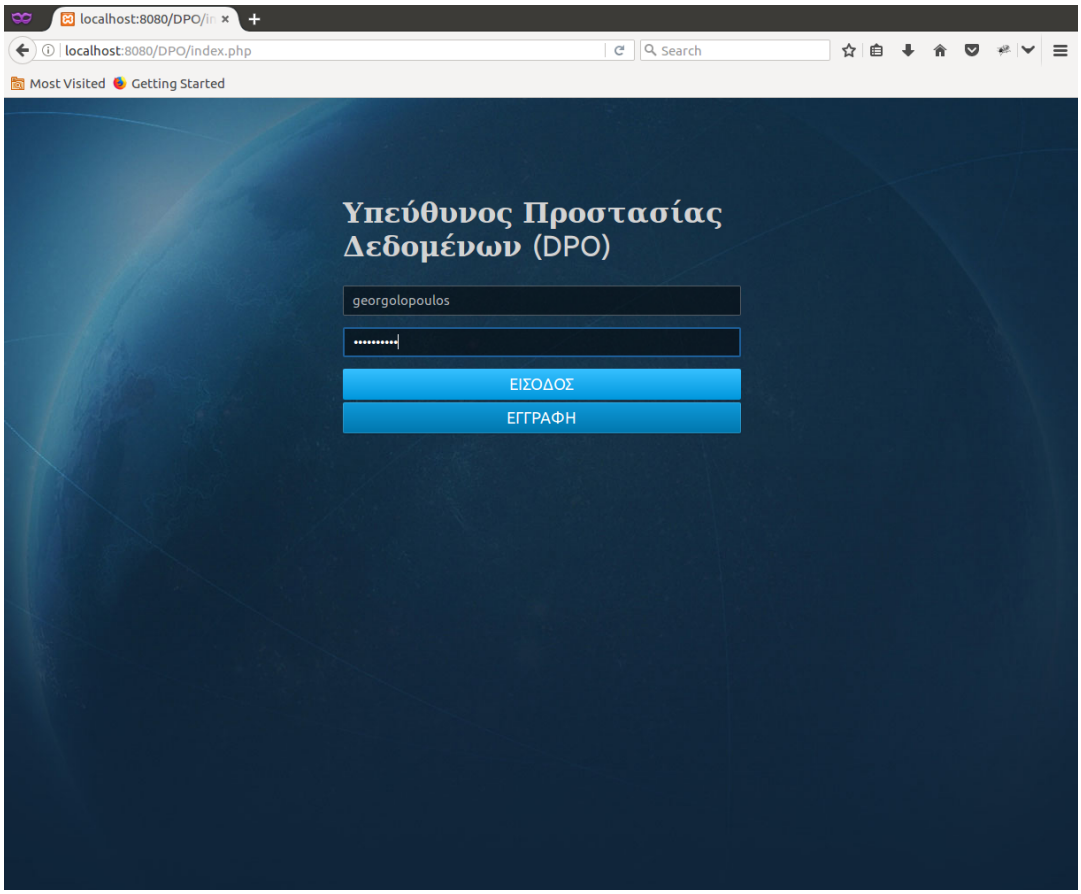
Στο Κεφάλαιο 3 αναφέραμε τον ορισμό του DPO, τον ρόλο του καθώς και τα καθήκοντά του. Ένα από αυτά λοιπόν είναι να γνωρίζει σε άριστο βαθμό τις υποχρεώσεις τόσο του **Υπεύθυνου Επεξεργασίας** όσο και του **Εκτελούντα την Επεξεργασία,** μέσα στον Οργανισμό ή στην Εταιρεία. Για τον σκοπό αυτό υλοποιήσαμε μια εφαρμογή για τον ίδιο, μέσα στην οποία έχουμε μια λίστα με όλους τους σημαντικούς ελέγχους που θα πρέπει να γίνονται εντός του Οργανισμού ή της εταιρείας που ασχολούνται – διαχειρίζονται δεδομένα πελατών. Η συγκεκριμένη εφαρμογή αποτελεί χρήσιμο εργαλείο για τον οποιοδήποτε που εκτελεί καθήκοντα DPO καθώς τον βοηθά να έχει μια πλήρη εικόνα της κατάστασης στην οποία βρίσκεται η εταιρεία και να γνωρίζει το ποσοστό ανάγκης που απαιτείται για την συμμόρφωση με τον νέο Κανονισμό. Να συμπληρώσουμε πως οι ερωτήσεις που έχουμε εισάγει στην εφαρμογή και καλείται να απαντήσει ο DPO, είναι στα καθήκοντα – υποχρεώσεις του Υπεύθυνου και του Εκτελών την Επεξεργασία. Ορισμένες εξ' αυτών αφορούν μόνο τον ένα από τους δύο, ενώ άλλες και τους δύο ταυτόχρονα. Παρακάτω περιγράφουμε με απλά βήματα πώς λειτουργεί η εφαρμογή μας:

Βήμα 1ο - Εγγραφή – Είσοδος

Στην συγκεκριμένη εφαρμογή ο DPO, θα πρέπει πρώτα να κάνει εγγραφή με τα στοιχεία του *(username, email, password)* και εφόσον την πραγματοποιήσει επιτυχώς, μεταφέρεται στην αρχική σελίδα που του ζητείται να κάνει είσοδο με το *username* και το *password* του (Εικόνα 9.1 & 9.2).

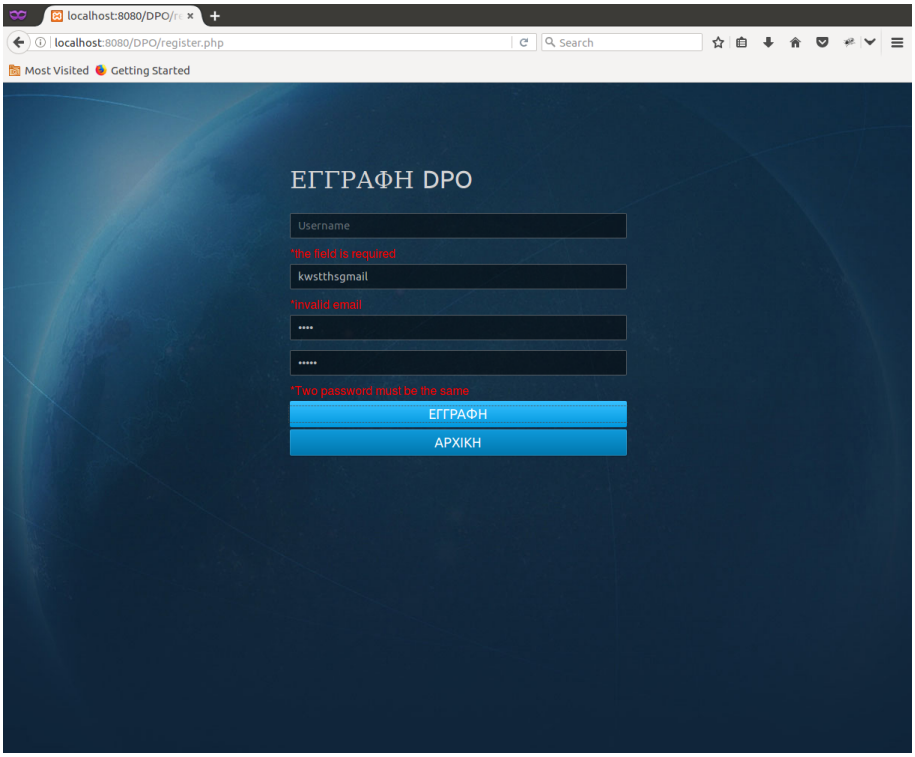


Εικόνα 9.1

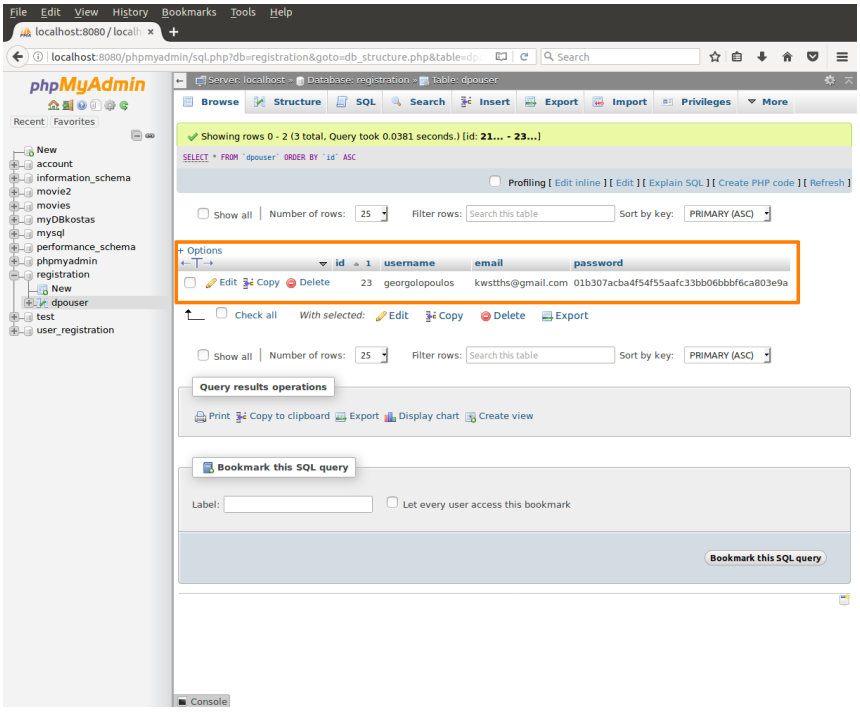


Εικόνα 9.2

Στην Εικόνα 9.3 φαίνονται τα μηνύματα που εμφανίζει η εφαρμογή στον χρήστη, σε περίπτωση που δεν εισάγει σωστά το *email* του για παράδειγμα. Ανάλογα μηνύματα επίσης εμφανίζονται σε περίπτωση που δεν συμπληρώσει όλα τα πεδία της φόρμας ή όταν ο κωδικός του δεν είναι ίδιος με το πεδίο *confirm password.* Στην Εικόνα 9.4 φαίνεται η επιτυχής καταχώρηση των στοιχείων του στην βάση δεδομένων της εφαρμογής *(phpMyAdmin)* μετά την επιλογή *ΕΓΓΡΑΦΗ* και εφόσον προηγουμένως έχει συμπληρώσει σωστά τα στοιχεία του.



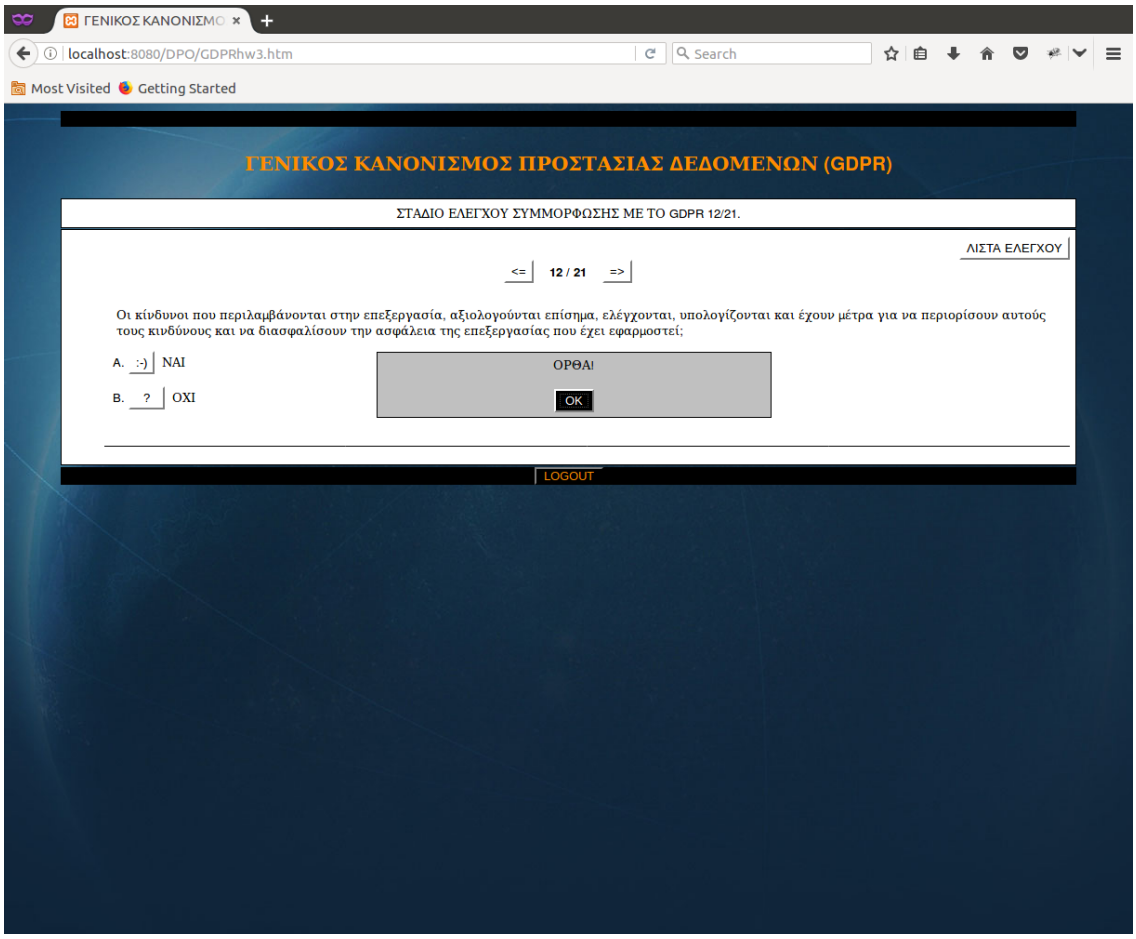
Εικόνα 9.3



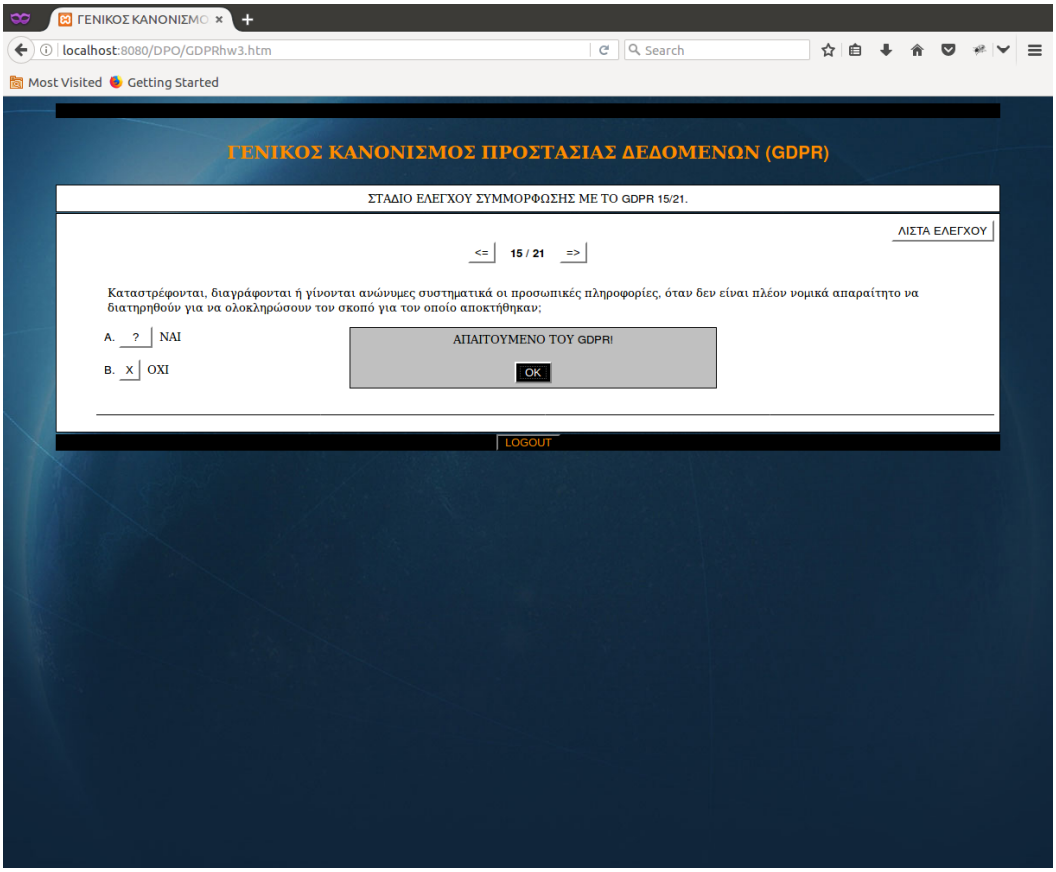
Εικόνα 9.4

Βημα 2ο – Λίστα ελέγχου συμμόρφωσης με το GDPR

Μετά την είσοδό του DPO στην εφαρμογή βλέπουμε τις ερωτήσεις (Εικόνα 9.5 & 9.6) που καλείται να απαντήσει με ΝΑΙ ή ΟΧΙ αναλόγως τι ισχύει στον Οργανισμό ή την εταιρεία στην οποία εργάζεται. Εάν απαντήσει ΝΑΙ τότε του εμφανίζεται ένα μήνυμα ΟΡΘΑ! Σε περίπτωση που απαντήσει ΟΧΙ εμφανίζεται σχετικό μήνυμα που τον ενημερώνει πως είναι ΑΠΑΙΤΟΥΜΕΝΟ ΤΟΥ GDPR. Οι ερωτήσεις είναι στο σύνολό τους 21 και με το τέλος αυτών παίρνουμε το συνολικό ποσοστό συμμόρφωσης της εταιρείας με τον νέο Κανονισμό..



Εικόνα 9.5



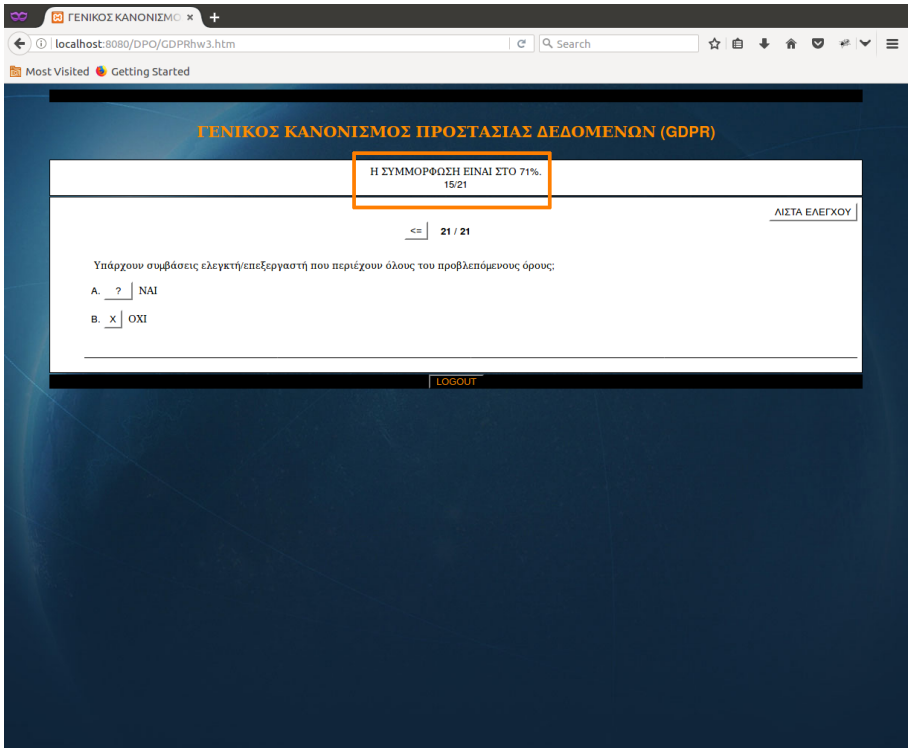
Εικόνα 9.6

Βήμα 3ο – Ποσοστό συμμόρφωσης

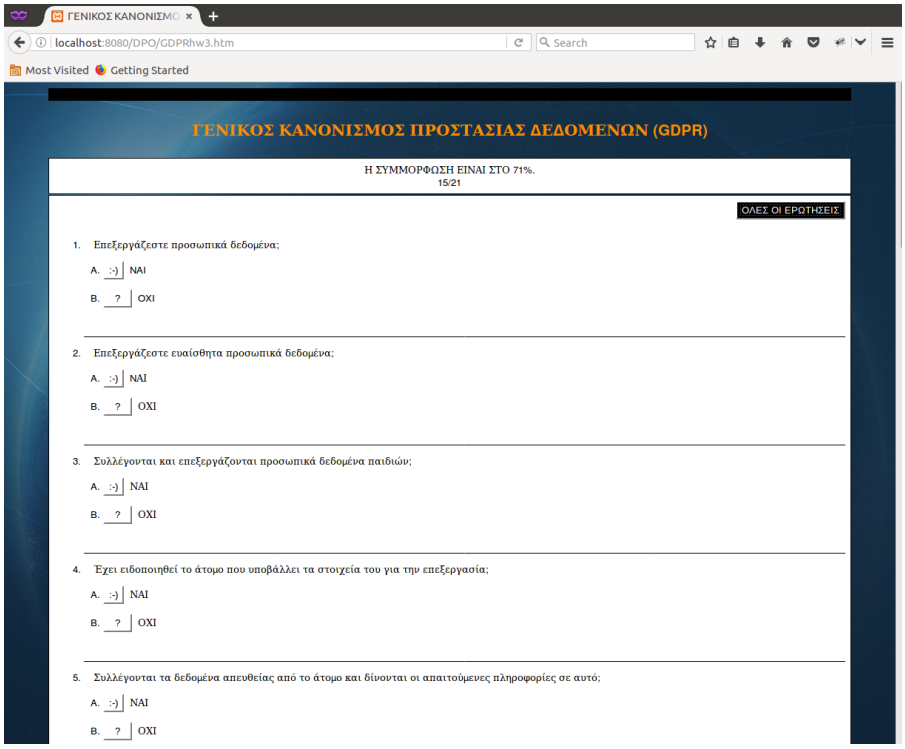
Στην Εικόνα 9.7 βλέπουμε το τελικό ποσοστό συμμόρφωσης της εταιρείας βάσει των συνολικών απαντήσεων που έχει δώσει ο DPO. Έχουμε επίσης ορίσει μια κλίμακα η οποία περιλαμβάνει:

- Από **50% εώς 70%** → **Απαιτείται άμεση συμμόρφωση**
- Από **71% εώς 90%** → **Μερικώς συμμόρφωση**
- Από **91% εώς 100%** → **Συμμόρφωση με το GDPR**

Τέλος εάν ο χρήστης επιλέξει το πλήκτρο ΛΙΣΤΑ ΕΛΕΓΧΟΥ βλέπει το σύνολο των ερωτήσεων καθώς και σε ποιά σημεία είναι σύμφωνος με τους κανονισμούς του GDPR και σε ποιά δεν είναι (Εικόνα 9.8).



Εικόνα 9.7



Εικόνα 9.8

ΚΕΦΑΛΑΙΟ 10ο - ΣΥΜΠΕΡΑΣΜΑΤΑ

Στο Κεφάλαιο αυτό θα κάνουμε μια ανακεφαλαίωση με τις ουσιαστικές αλλαγές που επέφερε ο νέος Κανονισμός στις επιχειρήσεις και θα εξάγουμε μερικά συμπεράσματα. Με την μελέτη των παραπάνω ενοτήτων, επισημάνουμε πως το GDPR δεν αφορά αποκλειστικά τη Διεύθυνση Πληροφοριακών Συστημάτων μιας εταιρείας αλλά το σύνολο του οργανισμού. Οι βασικές αλλαγές για τις επιχειρήσεις είναι:

- ✔ Συνολική υποχρέωση εναρμόνισης και συμμόρφωσης των οργανισμών με τον Κανονισμό
- ✔ Αυξημένη διαφάνεια εσωτερικών διαδικασιών και ανάγκη ύπαρξης του εσωτερικού μητρώου δεδομένων
- ✔ Εισαγωγή του ρόλου του Υπεύθυνου Προστασίας Δεδομένων (DPO)
- ✔ Υποχρέωση αναφοράς και γνωστοποίησης περιστατικών παραβίασης προστασίας δεδομένων
- ✔ Σαφής και ακριβής συγκατάθεση εκ μέρους των ατόμων κατά την επεξεργασία των προσωπικών του δεδομένων
- ✔ Περιορισμός της πρόσβασης στα δεδομένα όταν πραγματοποιείται η επεξεργασία τους
- ✔ Εκτέλεση εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων (DPIA)
- ✔ Συνεχής παρακολούθηση των κινδύνων προστασίας – προσωπικών δεδομένων σε ολόκληρο τον οργανισμό
- ✔ Επιβολή υψηλών προστίμων (4 % παγκοσμίου τζίρου ή 20 εκατομμύρια ευρώ)

Σαν συμπεράσματα λοιπόν αναφέρουμε πως οι περισσότερες επιχειρήσεις δεν είναι ακόμα έτοιμες να υποδεχτούν και να συμμορφωθούν με τις επιταγές του GDPR. Οι διαδικασίες εφαρμογής του συγκεκριμένα στον δημόσιο τομέα είναι σχεδόν ανύπαρκτες σε αντίθεση με τον ιδιωτικό. Επίσης το χρονικό διάστημα από την έναρξη ισχύος του Κανονισμού που ήταν 25 Μαίου 2018 μέχρι και σήμερα, είναι πάρα πολύ μικρό ώστε να δούμε αντικειμενικά και να αξιολογήσουμε τα πραγματικά αποτελέσματα εφαρμογής όλων αυτών των αλλαγών πέρα από την θεωρητική πλευρά της μεθοδολογίας του Κανονισμού.

Όσον αφορά τους πολίτες, που άνθρωποι μεγαλύτερης ηλικίας, εν αγνοία τους μοιράζονται προσωπικά στοιχεία στο διαδίκτυο θα λέγαμε πως είναι θέμα «ψηφιακού αναλφαβητισμού» καθώς δεν είναι εξοικειωμένοι αρκετά με την πληροφορική, την εξέλιξη της τεχνολογίας, το Διαδίκτυο και τους όποιους κινδύνους κρύβει με την δημοσιοποίηση των δεδομένων τους σ’ αυτο. Βέβαια το «ψηφιακό» αυτό χάσμα, με τον καιρό εξαλείφεται καθώς οι γενιές περνούν και οι νέοι μεγαλώνοντας γίνονται πιο έμπειροι και υποψιασμένοι θα λέγαμε με τη χρήση του Διαδικτύου.

Το αρνητικό επακόλουθο που φέρνει μαζί του ο Ευρωπαϊκός Κανονισμός είναι πως πολλές εταιρείες που δραστηροποιούνται εκτός των συνόρων της Ευρώπης και έχουν στο πελατολόγιό τους ευρωπαίους χρήστες, δεν συμφωνούν με τις ρυθμίσεις του GDPR, επομένως αρνούνται και τους ευρωπαίους χρήστες προκαλώντας σειρά αντιδράσεων. Για παράδειγμα στην Κίνα, η ευαισθησία στα θέματα της ιδιωτικής ζωής είναι πολύ λιγότερο ισχυρή και ο Ευρωπαϊκός Κανονισμός θα θεωρηθεί περισσότερο ως καταναγκασμός παρά ως πλεονέκτημα. Αποκτά έτσι μεγάλο ενδιαφέρον να δούμε σε μελλοντικές μελέτες πώς όλες αυτές οι αντιδράσεις θετικές και αρνητικές, μπορούν να συνυπάρξουν και τι πραγματικά αποτελέσματα θα επιφέρει ο GDPR.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]http://www.sev.org.gr/Uploads/Documents/50953/SPECIAL%20REPORT_14_3_2018.pdf
[2]http://web.ihu.edu.gr/mdt2017/media-files/documents/i.iglezakis-nomos-prostasia-dedomenon.pdf
[3]https://www.taxheaven.gr/laws/circular/view/id/28194
[4]https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32006L0024&from=GA
[5]https://www.inewsgr.com/96/poia-einai-ta-evaisthita-prosopika-dedomena-kai-poia-ta-katochyromena-dikaiomata-mas.htm
[6]https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_el
[7]https://www.amcham.gr/wp-content/uploads/2017/11/VIKTORIA-HATZARA.pdf
[8]https://www.beautifeye.co/qualitative-market-research-insights-trends-blog/2018/3/29/cambridge-analytica-what-happened
[9]https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el
[10]http://www.iefimerida.gr/news/418789/ti-allazei-sta-prosopika-dedomena-me-gdpr-10-erotiseis-apantiseis
[11]http://policenet.gr/article/%CE%B1%CF%85%CF%84%CE%AD%CF%82-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CE%BF%CE%B9-%CF%80%CE%B9%CE%BF-%CE%BA%CE%B1%CF%81%CE%B1%CE%BC%CF%80%CE%B9%CE%BD%CE%AC%CF%84%CE%B5%CF%82-%CF%85%CF%80%CE%BF%CE%B8%CE%AD%CF%83%CE%B5%CE%B9%CF%82-%CF%85%CF%80%CE%BF%CE%BA%CE%BB%CE%BF%CF%80%CF%8E%CE%BD-%CF%80%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CF%8E%CE%BD-%CE%BA%CE%B1%CE%B9-%CF%86%CE%BF%CF%81%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CE%BA%CF%8E%CE%BD-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD
[12]http://www.capital.gr/epikairotita/3047784/i-upoklopi-afm-apo-tin-istoselida-tis-ggps-exei-idi-sumbei
[13]https://www.news247.gr/technologia/ta-megalytera-cyber-skandala-olon-ton-epochon.6392107.html
[14]https://www.protothema.gr/world/article/775442/ipahakers-eklepsan-dedomena-apo-5-ekatommuria-kartes-pelaton-megalon-katastimaton/
[15]https://palopro.io/social-media-el/gdpr-social-media-monitoring/
[16]https://www.cnn.gr/news/kosmos/story/128913/pistoi-sto-facebook-oi-amerikanoi-para-to-skandalo-tis-cambridge-analytica
[17]http://politis.com.cy/article/cambridge-analytica-ena-skandalo-gia-chari-tou-tramp-ke-tou-brexit
[18]https://www.lawspot.gr/nomika-nea/infographic-ta-dikaiomata-ton-politon-me-vasi-ton-gdpr

[19]https://www.news.gr/tech/article/1116245/ti-ine-o-kanonismos-gdpr-ke-giati-allazi-to-diadiktio.html
[20]https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en
[21]http://www.edemocracy2017.eu/wp-content/uploads/2018/01/%CE%91%CE%BD%CF%89%CE%BD%CF%85%CE%BC%CE%BF%CF%80%CE%BF%CE%AF%CE%B7%CF%83%CE%B7-%CE%BA%CE%B1%CE%B9-%CF%88%CE%B5%CF%85%CE%B4%CF%89%CE%BD%CF%85%CE%BC%CE%BF%CF%80%CE%BF%CE%AF%CE%B7%CF%83%CE%B7.pdf
[22]http://www.infocomsecurity.gr/presentations/2018/day2/papachristofis.pdf
[23]http://eclass.uth.gr/eclass/modules/document/file.php/DIB256/Lectures/04.personal_data_limniotis.pdf
[24]http://cgi.di.uoa.gr/~klimn/edemocracy_2017.pdf
[25]https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/
[26]https://magazine.joomla.org/issues/issue-apr-2018/item/3318-privacy-by-default-and-gdpr-examples-and-best-practises
[27]https://gr.pcmag.com/asphaleia/28799/prostasia-ton-paidion-me-base-to-neo-kanonismo-gia-ta-prosop
[28]https://www.jit.gr/gdpr/
[29]https://webtrails.gr/articles/12-praktika-vimata-gdpr/
[30]https://www.newsbeast.gr/world/arthro/3634727/i-allages-sta-prosopika-dedomena-ke-i-pagkosmies-epiptosis-tou-gdpr
[31]https://www.dreamweaver.gr/gdpr-%CF%80%CE%BF%CE%B9%CE%BF%CF%8D%CF%82-%CE%B1%CF%86%CE%BF%CF%81%CE%AC.php
[32]https://www.dikaiologitika.gr/eidhseis/kosmos/209486/ti-allazei-sto-facebook-me-to-gdpr
[33]https://www.socialactive.gr/blog/social-media-gdpr/
[34]http://nestor.teipel.gr/xmlui/bitstream/handle/123456789/13433/STE_MHP_00188_Medium.pdf?sequence=1
[35]https://insuranceworld.gr/40469/eidiseis/nees-dinatotites-sto-tomea-tis-asfalia-apo-tin-ivm/