ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Η επιρροή του Γενικού Κανονισμού για την Προστασία Δεδομένων στο ηλεκτρονικό εμπόριο και τη χρήση cookies.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Ιωάννη Κογχυλάκη

Επιβλέπουσα : Λίλιαν Μήτρου, Καθηγήτρια Πανεπιστημίου Αιγαίου

Σάμος, Μάϊος 2020

Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια μου κα. Λίλιαν Μήτρου για την πολύτιμη βοήθεια που μου παρείχε καθ' όλη την διάρκεια εκπόνησης της διπλωματικής μου εργασίας. Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου για την ηθική και ψυχολογική στήριξη μου που προσέφερε.

Ιωάννη Κογχυλάκη

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Περιεχόμενα

Περίληψη

Ο Γενικός Κανονισμός Προστασίας Δεδομένων, Κανονισμός 2016/679 (εφεξής ΓΚΠΔ), γνωστός και ως General Data Protection Regulation (GDPR), που έχει τεθεί σε εφαρμογή από τις 25 Μαΐου 2018, έχει αλλάξει ριζικά τον τρόπο με τον οποίο οι εταιρίες και οι οργανισμοί, που δραστηριοποιούνται στον τομέα του ηλεκτρονικού εμπορίου, συλλέγουν, επεξεργάζονται και διαχειρίζονται προσωπικά δεδομένα. Τα βασικότερα ζητήματα εστιάζονται στην τήρηση των αρχών του ΓΚΠΔ, δηλαδή της αρχής της νομιμότητας, αντικειμενικότητας και διαφάνειας, της αρχής του σκοπού, της αρχής της ελαχιστοποίησης, της αρχής της ακρίβειας, της αρχής του περιορισμού, της αρχής της ακεραιότητας και εμπιστευτικότητας που προβλέπεται στο άρθρο 5 στην κατοχύρωση των δικαιωμάτων των καταναλωτών και τον ορισμό ενός Υπεύθυνου Προστασίας Δεδομένων, σύμφωνα με το άρθρο 37 του οποίου οι αρμοδιότητες είναι η αξιολόγηση της συμμόρφωσης με τον Κανονισμό, ο έλεγχος των δραστηριοτήτων επεξεργασίας και η παροχή συμβουλών στον υπεύθυνο επεξεργασίας.. Επιπλέον, υποχρεωτική είναι η ανάρτηση εντύπου πολιτικής απορρήτου στην ιστοσελίδα του κάθε ηλεκτρονικού καταστήματος, στο οποίο περιγράφονται όλα τα θέματα σχετικά με τα προσωπικά δεδομένα συμπεριλαμβανομένης της επεξεργασίας των cookies. Αυτά σύμφωνα με τον Κανονισμό θα πρέπει να χρησιμοποιούνται αυστηρά και μόνο με την συγκατάθεση του χρήστη, πέρα των απολύτως απαραίτητων για την σωστή λειτουργία της ιστοσελίδας.

Λέξεις-Κλειδιά: ΓΚΠΔ, Ηλεκτρονικό Εμπόριο, Αρχές, Υπεύθυνος Προστασίας Δεδομένων, Πολιτική Απορρήτου, Cookies

Abstract

General Data Protection Regulation, Regulation 2016/679 (GDPR) in force since 25 May 2018, has radically changed the way companies and organizations, operating in the e-commerce sector, collect, process and manage personal data. The main issues are both the observance of the principles of the GDPR, ie the principle of lawfulness, fairness and transparency, the principle of purpose limitation, the principle of data minimization, the principle of accuracy, the principle of storage limitation, the principle of integrity and confidentiality provided for in Article 5 and assurance of the consumer's rights and designation of Data Protection Officer, according to Article 37 whose responsibilities are to assess compliance with the Regulation, to control the processing activities and to provide advice to the Controller. In addition, mandatory is the privacy policy document posting on the website of each shop, which describes all the issues regarding personal data including cookie processing. According to the Regulation, these should be used strictly only with the consent of the user, in addition to the absolutely necessary for the proper operation of the website.

Keywords: GDPR, E-Commerce, Principles, Data Protection Officer, Privacy Policy, Cookies

1. Εισαγωγή

Λόγω της ταχείας τεχνολογικής εξέλιξης, του τεράστιου όγκου δεδομένων που παράγεται καθημερινά και της αυξανόμενης ποσότητας επεξεργασίας κατέστη σαφές ότι η Ευρωπαϊκή Ένωση (εφεξής ΕΕ) θα έπρεπε να εκσυγχρονίσει το δίκαιο για την προστασία των προσωπικών δεδομένων. Ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (εφεξής ΓΚΠΔ, GDPR ή Κανονισμός), αντικατέστησε και κατάργησε την Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995.

Ο ΓΚΠΔ αφορά όλες τις επιχειρήσεις που συλλέγουν και επεξεργάζονται δεδομένα προσωπικού χαρακτήρα από υποκείμενα εντός της ΕΕ. Το ηλεκτρονικό εμπόριο, τα τελευταία χρόνια, γίνεται όλο και πιο δημοφιλές σε όλο τον κόσμο. Μέσα από αυτό συλλέγεται και επεξεργάζεται τεράστιος όγκος προσωπικών δεδομένων (όνομα, επίθετο, διεύθυνση, τηλέφωνο, αριθμός πιστωτικής/χρεωστικής κάρτας, κ.α.) και για τον λόγο αυτό επηρεάζεται από τον ΓΚΠΔ. Πολλές επιχειρήσεις στο χώρο του ηλεκτρονικού εμπορίου έχουν συμμορφωθεί με τον Κανονισμό, πολλές άλλες, όμως, ακόμα και σήμερα δεν έχουν αφιερώσει την απαραίτητη προσοχή στον Κανονισμό, προβαίνοντας σε παράνομη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα με κυρίαρχο σκοπό το κέρδος.

1.1 Αντικείμενο διπλωματικής

Στην παρούσα εργασία τα βασικά ζητήματα που θα αναλυθούν είναι το πώς ο ΓΚΠΔ επηρεάζει τους οργανισμούς στο ηλεκτρονικό εμπόριο, ποιοι είναι οι κίνδυνοι για τα προσωπικά δεδομένα των πελατών από μια ηλεκτρονική αγορά, ποιες είναι οι βασικές ενέργειες και κινήσεις στις οποίες πρέπει να προβεί ένας οργανισμός που ειδικεύεται στο ηλεκτρονικό εμπόριο ώστε να είναι συμμορφωμένος με τον ΓΚΠΔ. Επίσης, ένα πολύ σημαντικό πρόβλημα για τα ηλεκτρονικά καταστήματα εστιάζεται

στα cookies τα οποία θα μελετηθούν και θα αναλυθούν, καθώς συχνά η χρήση τους συχνά δεν συνάδει με τον ΓΚΠΔ και με την Οδηγία ePrivacy.

1.2 Δομή της διπλωματικής

Η παρούσα εργασία που χωρίζεται σε έξι κεφάλαια έχει ως βασικό θέμα το πώς ο ΓΚΠΔ επηρεάζει το ηλεκτρονικό εμπόριο. Το αρχικό κεφάλαιο έχει σκοπό να εισαγάγει τον αναγνώστη στην έννοια των προσωπικών δεδομένων, τον κατάλογο με τους ορισμούς που καθορίζονται από τον Γενικό Κανονισμό Προστασίας Δεδομένων καθώς επίσης τις βασικές αρχές και την ιδιαιτερότητα της συγκατάθεσης. Το επόμενο κεφάλαιο με τίτλο «Ηλεκτρονικό εμπόριο και οι κίνδυνοι» αφορά στην επιρροή που έχει ο ΓΚΠΔ στο ηλεκτρονικό εμπόριο και τις ιστοσελίδες των ηλεκτρονικών καταστημάτων και επιπλέον τους κινδύνους που κρύβει το ηλεκτρονικό εμπόριο για τα προσωπικά δεδομένα των υποκειμένων. Στη συνέχεια αναλύονται τα δικαιώματα που έχουν τα υποκείμενα των δεδομένων και πώς αυτά συνδέονται με το ηλεκτρονικό εμπόριο. Στο πέμπτο κεφάλαιο περιγράφεται η θέση του υπεύθυνου προστασίας δεδομένων ποια είναι τα καθήκοντα και η ευθύνη του σύμφωνα με τον ΓΚΠΔ. Στο έκτο κεφάλαιο με τίτλο «πολιτική απορρήτου» περιγράφεται πώς πρέπει να είναι η πολιτική απορρήτου μιας ιστοσελίδας ενός ηλεκτρονικού καταστήματος για να τηρεί τις απαιτήσεις του ΓΚΠΔ αναφορικά με το δικαίωμα της ενημέρωσης των χρηστών. Επίσης, στο ίδιο κεφάλαιο διεξάγεται δειγματοληπτική ανάλυση των πολιτικών απορρήτου από δύο μεγάλα ηλεκτρονικά καταστήματα της Ελλάδας. Στο τελευταία κεφάλαιο με τίτλο «cookies» παρουσιάζεται το ζήτημα της χρήσης τους στις ιστοσελίδες των ηλεκτρονικών καταστημάτων και τι επιρροή έχει ο ΓΚΠΔ.

2. Εισαγωγή στον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων

Ο πρωταρχικός στόχος του Κανονισμού είναι να ενισχύσει και να εναρμονίσει την προστασία των προσωπικών δεδομένων για τα άτομα, καθώς και να απλοποιήσει τα κανονιστικά περιβάλλοντα για τους οργανισμούς. Ο ΓΚΠΔ υποχρεώνει τις επιχειρήσεις να εξασφαλίσουν τα συστήματα τους για την αποφυγή παραβιάσεων δεδομένων και την αποτελεσματική αναφορά τους σε περίπτωση αποτυχίας. Ένα από τα μεγαλύτερα οφέλη του ΓΚΠΔ είναι η ανοιχτή διατύπωση και ο σχεδιασμός του με γνώμονα το μέλλον (Jesper Zerlang, 2017). Οι εταιρείες έχουν την ευκαιρία να μην αρκεστούν μόνο στην τυπική συμμόρφωση με τον Κανονισμό, αλλά και να την ξεπεράσουν, ενσωματώνοντας τις σύγχρονες πρακτικές ασφαλείας στο κυβερνοχώρο, αυξάνοντας έτσι την αποτελεσματικότητα τους. Πολλές επιχειρήσεις θέτουν ως βασικό καθήκον τους να συμμορφωθούν με τον νέο Κανονισμό και κάποια άτομα σε σημαντικές θέσεις αναδιαμορφώνουν ακόμα και την στρατηγική ολόκληρου του οργανισμού τους, ώστε να βγουν κερδισμένοι (Jan Philipp Albrecht, 2016). Ο Κανονισμός προβλέπει αρκετές νέες απαιτήσεις σχετικά με τον τρόπο που οι εταιρείες αποθηκεύουν, επεξεργάζονται και διαφυλάσσουν προσωπικές πληροφορίες επιφέροντας οικονομικές κυρώσεις για τη διασφάλιση της εφαρμογής τους.

2.1 Βασικοί Ορισμοί (Άρθρο 4 του ΓΚΠΔ)

«δεδομένα προσωπικού χαρακτήρα» : κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

«επεξεργασία» : κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

«περιορισμός της επεξεργασίας» : η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον.

«υπεύθυνος επεξεργασίας» : το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

«εκτελών την επεξεργασία» : το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

«συγκατάθεση» του υποκειμένου των δεδομένων : κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.

«παραβίαση δεδομένων προσωπικού χαρακτήρα» : η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

«σύστημα αρχειοθέτησης» : κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα

κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση.

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

«εποπτική αρχή» : ανεξάρτητη δημόσια αρχή που συγκροτείται από κράτος μέλος.

«κύρια εγκατάσταση» :

α) **όταν πρόκειται για υπεύθυνο επεξεργασίας** με εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, ο τόπος της κεντρικής του διοίκησης στην Ένωση, εκτός εάν οι αποφάσεις όσον αφορά τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα λαμβάνονται σε άλλη εγκατάσταση του υπευθύνου επεξεργασίας στην Ένωση και η εγκατάσταση αυτή έχει την εξουσία εφαρμογής των αποφάσεων αυτών, οπότε ως κύρια εγκατάσταση θεωρείται η εγκατάσταση στην οποία έλαβε τις αποφάσεις αυτές,

β) **όταν πρόκειται για εκτελούντα την επεξεργασία** με εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, ο τόπος της κεντρικής του διοίκησης στην Ένωση ή, εάν ο εκτελών την επεξεργασία δεν έχει κεντρική διοίκηση στην Ένωση, η εγκατάσταση του εκτελούντος την επεξεργασία στην Ένωση στην οποία εκτελούνται οι κύριες δραστηριότητες επεξεργασίας στο πλαίσιο των δραστηριοτήτων εγκατάστασης του εκτελούντος την επεξεργασία, στον βαθμό που ο εκτελών την επεξεργασία υπόκειται σε ειδικές υποχρεώσεις δυνάμει του παρόντος κανονισμού,

«εκπρόσωπος» : φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ένωση, το οποίο ορίζεται εγγράφως από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία βάσει του άρθρου 27 και εκπροσωπεί τον υπεύθυνο επεξεργασίας ή τον

εκτελούντα την επεξεργασία ως προς τις αντίστοιχες υποχρεώσεις τους δυνάμει του παρόντος κανονισμού.

«συνδρομητής» : κάθε φυσικό ή νομικό πρόσωπο που έχει συνάψει σύμβαση με φορέα παροχής διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών για την παροχή των υπηρεσιών αυτών.

«ηλεκτρονικό εμπόριο» : το εμπόριο παροχής αγαθών και υπηρεσιών που πραγματοποιείται εξ αποστάσεως με ηλεκτρονικά μέσα, βασιζόμενο δηλαδή στην ηλεκτρονική μετάδοση δεδομένων, χωρίς να καθίσταται αναγκαία η φυσική παρουσία των συμβαλλομένων μερών, πωλητή-αγοραστή.

«χρήστης» : κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας.

2.2 Εδαφικό πεδίο εφαρμογής του ΓΚΠΔ

Ο Κανονισμός εφαρμόζεται στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης (άρθρο 2). Αφορά στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπεύθυνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης (άρθρο 3).

Ο ΓΚΠΔ δεν επηρεάζει μόνο οντότητες που είναι εγκατεστημένες στην ΕΕ αλλά και οντότητες που είναι εγκαταστημένες εκτός αυτής, εφόσον επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, υποκειμένων που βρίσκονται εντός της. Ο παρών κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με την προσφορά αγαθών ή υπηρεσιών σε υποκείμενα των δεδομένων στην Ένωση ή αν παρακολουθούν τη συμπεριφορά τους

(δηλ. παρακολούθηση δραστηριοτήτων των ατόμων στο Διαδίκτυο με τη χρήση cookies, ή την δημιουργία προφίλ) (άρθρο 3 παρ. 2).

Σύμφωνα με το άρθρο 3 του ΓΚΠΔ, το πεδίο εφαρμογής του Κανονισμού εκτείνεται στις δραστηριότητες εγκατάστασης υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία που λαμβάνει χώρα εντός ΕΕ, αλλά και στις δραστηριότητες εγκαταστάσεως υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία εκτός ΕΕ, όταν η επεξεργασία αφορά σε υποκείμενα δεδομένων που βρίσκονται εντός ΕΕ (π.χ. περιπτώσεις ηλεκτρονικού εμπορίου και κατάρτισης προφίλ) (Φερενίκη Παναγοπούλου-Κουτνατζή, 2017). Άρα η επιρροή του ΓΚΠΔ εκτείνεται στην ουσία παγκοσμίως όχι μόνο εντός της ΕΕ.

Ένα μεγάλο ποσοστό των οργανισμών αυτών που επηρεάζονται παγκοσμίως είναι τα ηλεκτρονικά καταστήματα, καθώς στη σημερινή εποχή το ηλεκτρονικό εμπόριο δεν περιορίζεται σε ηπείρους, χώρες και σύνορα. Όλοι οι πολίτες του κόσμου μπορούν να αγοράσουν και να λάβουν στο σπίτι τους προϊόντα και υπηρεσίες από όλο το κόσμο. Παγκοσμίως όλα τα ηλεκτρονικά καταστήματα θα πρέπει να συμμορφώνονται με τις απαιτήσεις του ΓΚΠΔ εφόσον συλλέγουν προσωπικά δεδομένα από τους χρήστες της ΕΕ όταν αυτοί κάνουν μια αγορά, αλλά και όταν συνδέονται με τον υπολογιστή τους ή το κινητό τους στην ιστοσελίδα τους (cookies, ip διεύθυνση, κ.α.). Για παράδειγμα, ένα ηλεκτρονικό κατάστημα εγκατεστημένο στην Κίνα από το οποίο προβαίνουν σε ηλεκτρονικές αγορές πολίτες εγκατεστημένοι εντός ΕΕ, θα πρέπει να τηρεί τις απαιτήσεις του ΓΚΠΔ. Με τον τρόπο αυτό ο ΓΚΠΔ καθίσταται ένας Παγκόσμιος Κανονισμός ο οποίος θα αλλάξει όχι μόνο τους ευρωπαϊκούς νόμους περί προστασίας δεδομένων αλλά ολόκληρου του κόσμου.(Jan Philipp Albrecht, 2016) Αυτό φαίνεται και από την τάση χωρών εκτός ΕΕ, όπως η Ιαπωνία, να εισάγουν στη νομοθεσία τους διατάξεις παρόμοιες με αυτές του Κανονισμού(Φερενίκη Παναγοπούλου-Κουτνατζή, 2017).

2.3 Βασικές Αρχές Επεξεργασίας

Κομβικό στοιχείο, αν όχι «σκληρό πυρήνα», της προστασίας προσωπικών δεδομένων, συνιστούν οι αρχές που πρέπει να διέπουν την επεξεργασία τους, αναδιατυπώνονται στο άρθρο 5 του ΓΚΠΔ. (Λίλιαν Μήτρου, 2017)

Η αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας, σύμφωνα με την οποία, τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Αυτό σημαίνει ότι τα υποκείμενα θα πρέπει να γνωρίζουν ότι τα δεδομένα τους θα υποβληθούν σε επεξεργασία και να ενημερωθούν όταν τα δεδομένα τους πρόκειται να επεξεργαστούν (Ειρηνικός Πλατής, 2018).

Η αρχή του σκοπού, όπου σύμφωνα με την συγκεκριμένη αρχή ο σκοπός της επεξεργασίας πρέπει να είναι σαφής, νόμιμος και γνωστοποιημένος στο υποκείμενο των δεδομένων (Λίλιαν Μήτρου, 2017). Συγκεκριμένα, τα δεδομένα προσωπικού χαρακτήρα συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Η επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1.

Η αρχή της ελαχιστοποίησης των δεδομένων υποχρεώνει τα δεδομένα που συλλέγονται και επεξεργάζονται να είναι κατάλληλα, συναφή και να περιορίζονται στα αναγκαία. Η ρητή εισαγωγή της αρχής της ελαχιστοποίησης στον Κανονισμό αποκτά ιδιαίτερη βαρύτητα ακριβώς επειδή η εξέλιξη της υπολογιστικής τεχνολογίας αναιρεί ραγδαία τα όρια των δυνατοτήτων συλλογής, επεξεργασίας και τήρησης δεδομένων (Λίλιαν Μήτρου, 2017).

Η αρχή της ακρίβειας απαιτεί τα δεδομένα προσωπικού χαρακτήρα να είναι ακριβή και να επικαιροποιούνται. Θα πρέπει να ληφθούν όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων, που είναι ανακριβή σε σχέση με τους σκοπούς της επεξεργασίας.

Η αρχή του περιορισμού της περιόδου αποθήκευσης προσδιορίζει ότι τα δεδομένα διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της

επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον αυτά θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.

Η αρχή της ακεραιότητας και εμπιστευτικότητας θεσπίζει ότι τα δεδομένα υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια τους, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρήση κατάλληλων τεχνικών ή οργανωτικών μέτρων.

2.4 Νομιμότητα της επεξεργασίας

Σύμφωνα με το Άρθρο 6 του ΓΚΠΔ προκειμένου η επεξεργασία των δεδομένων από ένα ηλεκτρονικό κατάστημα να θεωρείται σύννομη θα πρέπει να ισχύει τουλάχιστον μια από τις ακόλουθες προϋποθέσεις. Αρχικά, το υποκείμενο των δεδομένων θα πρέπει να έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για ένα ή περισσότερους σκοπούς. Θα πρέπει τα ηλεκτρονικά καταστήματα με κάποιον τρόπο να μπορούν να λάβουν τη συγκατάθεση του χρήστη και να μπορούν μελλοντικά να την αποδείξουν στον ίδιο ή στην Αρχή. Επίσης, είναι νόμιμη η επεξεργασία δεδομένων προσωπικού χαρακτήρα όταν είναι απαραίτητη για την εκτέλεση σύμβασης, της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για την λήψη μέτρων κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης. Στον κλάδο του ηλεκτρονικού εμπορίου μια αγορά ενός προϊόντος και η παράδοση του στον χρήστη αποτελεί μια σύμβαση μεταξύ του ηλεκτρονικού καταστήματος και του χρήστη. Στη περίπτωση αυτή το ηλεκτρονικό κατάστημα μπορεί να κάνει επεξεργασία των προσωπικών δεδομένων του υποκειμένου για σκοπούς ολοκλήρωσης της διαδικασίας πώλησης και αποστολής. Επιπλέον, σύμφωνα με το άρθρο 6 του ΓΚΠΔ η επεξεργασία είναι σύννομη όταν είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας. Τέλος, η επεξεργασία είναι σύννομη όταν είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος

επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Στις ακόλουθες περιπτώσεις, σύμφωνα με το άρθρο 9, η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα καθιστάται νόμιμη. Ειδική κατηγορία δεδομένων προσωπικού χαρακτήρα είναι τα δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

α. Το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς,

β. Η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας,

2.5 Κυρώσεις

Σημαντικό ρόλο στον νέο Κανονισμό αποτελούν οι κυρώσεις, οι οποίες αναμφίβολα είναι ένα καθοριστικό κίνητρο για τις εταιρείες και τους οργανισμούς να συμμορφωθούν με τον νέο Κανονισμό. Οι διοικητικές και ποινικές κυρώσεις, επιβεβαιώνουν τη στενή σχέση της προστασίας προσωπικών δεδομένων με την αξία του ανθρώπου και ελευθερία αλλά και την ίδια την δημοκρατική συγκρότηση μιας πολιτείας (Λίλιαν Μήτρου, 2017). Ο βασικότερος κυρωτικός μηχανισμός του ΓΚΠΔ είναι η επιβολή διοικητικού προστίμου, το οποίο κυμαίνεται από δέκα εκατομμύρια ευρώ, σε περίπτωση επιχειρήσεων, έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι

υψηλότερο. Διαφορετικά, επιβάλλονται πρόστιμα από είκοσι εκατομμύρια ευρώ, σε περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο. Οι περιπτώσεις για την επιβολή προστίμου καθορίζονται από τον ΓΚΠΔ στο άρθρο 83 παρ. 4 και παρ. 5. Για την ενίσχυση και την εναρμόνιση των διοικητικών προστίμων του κανονισμού, κάθε εποπτική αρχή θα μπορεί να έχει την εξουσία να επιβάλλει διοικητική πρόστιμα (αιτιολογική σκέψη 150). Κάθε εποπτική αρχή μεριμνά, ώστε η επιβολή διοικητικών προστίμων έναντι παραβάσεων του κανονισμού να είναι για κάθε μεμονωμένη περίπτωση αποτελεσματική, αναλογική και αποτρεπτική (άρθρο 83 παρ. 1).

3. Ηλεκτρονικό εμπόριο και οι κίνδυνοι

Τα τελευταία χρόνια η μεγάλη ανάπτυξη του ηλεκτρονικού εμπορίου προσελκύει ολοένα και περισσότερους ανθρώπους στην αγορά αγαθών και υπηρεσιών μέσω ηλεκτρονικών καταστημάτων. Ο όρος «ηλεκτρονικό επιχειρείν» υιοθετήθηκε για να διακρίνει τις επιχειρήσεις που επενδύουν στη διεξαγωγή των δραστηριοτήτων τους μέσω των τηλεπικοινωνιακών δικτύων. Συγκεκριμένα, στην Ελλάδα, όπως καταγράφεται στην ετήσια έρευνα για το 2016 του Εργαστηρίου Ηλεκτρονικού Εμπορίου και Ηλεκτρονικού Επιχειρείν του Οικονομικού Πανεπιστημίου Αθηνών, που δημοσιεύει ο ΣΕΠΕ, το 29% των online καταναλωτών πραγματοποιεί πάνω από το 50% των συνολικών αγορών του ψηφιακά, όταν αντίστοιχα ποσοστά για το 2015 ήταν στο 25% και το 2014 στο 9%. Η μεγάλη αυτή ανάπτυξη και οι μαζικές ηλεκτρονικές αγορές έχουν ως αποτέλεσμα τα ηλεκτρονικά καταστήματα να συλλέγουν τεράστιες ποσότητες προσωπικών δεδομένων χωρίς όμως να εξασφαλίζουν την προστασία τους.

Το ηλεκτρονικό εμπόριο χωρίζεται σε τρείς βασικές κατηγορίες, οι οποίες είναι το εμπόριο μεταξύ επιχείρησης και καταναλωτή (Business to Customer ή B2C), το οποίο ουσιαστικά είναι το λιανικό ηλεκτρονικό εμπόριο, που αφορά όλους τους οργανισμούς που έχουν ως στόχο την πώληση προϊόντος ή υπηρεσίας απευθείας στους τελικούς καταναλωτές. Στη συνέχεια, είναι το εμπόριο μεταξύ επιχείρησης με επιχείρηση (Business to Business ή B2B), που πρόκειται για το χονδρικό εμπόριο, δηλαδή την αγορά από προμηθευτές. Τέλος, υπάρχουν οι συναλλαγές μεταξύ καταναλωτών (Consumer to Consumer ή C2C), όπου σε αυτή την κατηγορία ένας καταναλωτής πουλά απευθείας σε άλλους καταναλωτές προϊόντα ή υπηρεσίες.

Το ηλεκτρονικό εμπόριο επιπλέον χωρίζεται σε έμμεσο και άμεσο. Έμμεσο είναι όταν πρόκειται για ηλεκτρονικές παραγγελίες υλικών αγαθών, που μπορούν να παραδοθούν μόνο με παραδοσιακούς τρόπους, όπως είναι το ταχυδρομείο ή μέσω μεταφορικών εταιρειών. Αντιθέτως, άμεσο ονομάζεται το ηλεκτρονικό εμπόριο που περιλαμβάνει παραγγελία, πληρωμή και παράδοση άυλων αγαθών και υπηρεσιών. Ένα παράδειγμα άμεσου ηλεκτρονικού εμπορίου είναι η αγορά προγραμμάτων για τους ηλεκτρονικούς υπολογιστές, όπου η πληρωμή από τον χρήστη γίνεται είτε με πιστωτικές κάρτες είτε με ηλεκτρονικό χρήμα με την σύμπραξη των τραπεζών και στη συνέχεια το ηλεκτρονικό κατάστημα στέλνει στον χρήστη κάποιο ηλεκτρονικό

κλειδί ή κάποιον διαδικτυακό σύνδεσμο για να μπορέσει να κάνει λήψη και να το χρησιμοποιήσει.

Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, με τον οποίο πρέπει να συμμορφωθούν τα ηλεκτρονικά καταστήματα, στοχεύει στο να έχουν τα υποκείμενα έλεγχο στα προσωπικά τους δεδομένα και να εξασφαλίζεται η προστασία τους από τρίτους. Τα ηλεκτρονικά καταστήματα θα πρέπει πλέον να σκεφτούν τον νέο Κανονισμό ως κάτι περισσότερο από ένα θέμα πληροφορικής και να συμμορφωθούν με αυτό, ώστε να πετύχουν μεγαλύτερη αξιοπιστία και εμπιστοσύνη προς τους πελάτες, γεγονός που συνεπάγεται με αύξηση των κερδών τους.

3.1 Νομικό πλαίσιο ηλεκτρονικού εμπορίου

Για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, εφαρμόζεται η οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000. Η οδηγία αυτή για το ηλεκτρονικό εμπόριο έχει ενσωματωθεί στην Ελληνική έννομη τάξη από το π.δ. 131 και ρυθμίζει ένα μέρος των υπηρεσιών που παρέχονται ηλεκτρονικά, όπως είναι η πώληση, η παροχή επαγγελματικών υπηρεσιών και η παροχή υπηρεσιών ψυχαγωγίας. Ωστόσο, η προστασία προσώπων σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα ρυθμίζεται αποκλειστικά από τον Κανονισμό 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και από τον νόμο 3471/2006 που ενσωματώνει την Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

3.2 Πώς επηρεάζεται το Ηλεκτρονικό Εμπόριο από τον ΓΚΠΔ

Ο νέος κανονισμός επηρεάζει όλες τις πληροφορίες που μπορούν να προσδιορίσουν ένα άτομο άμεσα ή έμμεσα. Στην περίπτωση του ηλεκτρονικού εμπορίου ο χρήστης που επιθυμεί να ολοκληρώσει μια συναλλαγή με κάποιο ηλεκτρονικό κατάστημα δίνει ορισμένα προσωπικά στοιχεία για την ολοκλήρωση της και στη συνέχεια την αποστολή της παραγγελίας. Τα περισσότερα από τα στοιχεία αυτά, που συλλέγουν τα ηλεκτρονικά καταστήματα, θεωρούνται δεδομένα προσωπικού χαρακτήρα. Αυτά είναι το ονοματεπώνυμο του χρήστη, η διεύθυνση κατοικίας του, η ημερομηνία γεννήσεως, ο αναγνωριστικός αριθμός της κάρτας του και η ηλεκτρονική του διεύθυνση.

Δεδομένα προσωπικού χαρακτήρα δεν είναι μόνο αυτά που δίνονται άμεσα από τον χρήστη, με σκοπό την ολοκλήρωση της παραγγελίας και την αποστολή της σε αυτόν, αλλά και έμμεσα, όπως διευθύνσεις διαδικτυακού πρωτοκόλλου, αναγνωριστικά cookies ή άλλα αναγνωριστικά στοιχεία, για παράδειγμα ετικέτες αναγνώρισης μέσω ραδιοσυχνοτήτων. Αυτά μπορεί να αφήνουν ίχνη, τα οποία, ιδίως όταν συνδυαστούν με μοναδικά αναγνωριστικά στοιχεία ταυτότητας και άλλες πληροφορίες που λαμβάνουν οι εξυπηρετητές, μπορούν να χρησιμοποιηθούν για να δημιουργηθεί το προφίλ των φυσικών προσώπων και να αναγνωριστεί η ταυτότητά τους (αιτιολογική σκέψη 30). Με την δημιουργία ενός προφίλ για κάθε χρήστη τα ηλεκτρονικά καταστήματα μπορούν να λάβουν αποφάσεις που αφορούν τους χρήστες αυτούς, να αναλύσουν ή να προβλέψουν τις προσωπικές τους προτιμήσεις, συμπεριφορές και νοοτροπίες τους.

Όπως αναφέρθηκε προηγουμένως, βασικό στοιχείο του ΓΚΠΔ αποτελούν οι αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπου η κάθε αρχή ξεχωριστά επηρεάζει το τομέα του ηλεκτρονικού εμπορίου με διαφορετικό τρόπο. Με την αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας τα ηλεκτρονικά καταστήματα θα πρέπει να επεξεργάζονται τα δεδομένα με σύννομο, θεμιτό και διαφανή τρόπο. Αυτό σημαίνει ότι τα ηλεκτρονικά καταστήματα οφείλουν να ενημερώσουν τα υποκείμενα των δεδομένων ότι τα προσωπικά δεδομένα που έχουν κοινοποιήσει στο ηλεκτρονικό κατάστημα για την αγορά ενός προϊόντος ή μιας υπηρεσίας, θα υποβληθούν σε επεξεργασία και πότε τα δεδομένα αυτά πρόκειται να επεξεργαστούν.

Η αρχή του σκοπού υποχρεώνει τα ηλεκτρονικά καταστήματα να συλλέγουν και να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία ασύμβατη προς τους σκοπούς αυτούς. Τα ηλεκτρονικά καταστήματα συλλέγουν προσωπικά δεδομένα με συγκεκριμένους σκοπούς και λόγους. Οι λόγοι αυτοί είναι για να ολοκληρωθεί η αγορά ενός προϊόντος ή υπηρεσίας, δίνοντας οι χρήστες τον αριθμό της κάρτας τους, και επίσης δίνοντας τα προσωπικά τους στοιχεία για να μπορέσει να βεβαιωθεί πρώτον ότι το προϊόν ή η υπηρεσία δόθηκε στο χρήστη που το αγόρασε και δεύτερον για να δοθούν τα δεδομένα αυτά σε κάποια μεταφορική εταιρεία, η οποία θα παραδώσει στον χρήστη το προϊόν στη φυσική διεύθυνση που έχει ορίσει. Σύμφωνα με το άρθρο 89 παρ. 1, η επεξεργασία για στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς, εάν μπορούν να περιλαμβάνουν ψευδώνυμα. Δηλαδή τα ηλεκτρονικά καταστήματα μπορούν να βγάζουν στατιστικά για τα ηλεκτρονικά τους κατάστημα και τους χρήστες του χωρίς να είναι δυνατή η ταυτοποίηση τους.

Στη συνέχεια, με την αρχή της ελαχιστοποίησης τα ηλεκτρονικά καταστήματα θα πρέπει να συλλέγουν και να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, τα οποία είναι κατάλληλα, συναφή και περιορισμένα στα αναγκαία. Σύμφωνα με την συγκεκριμένη αρχή, τα προσωπικά δεδομένα που συλλέγονται δεν θα πρέπει να είναι παραπάνω από τα απολύτως απαραίτητα για την ολοκλήρωση μιας διαδικασίας αγοράς ενός προϊόντος ή μιας υπηρεσίες. Για παράδειγμα, ένα ηλεκτρονικό κατάστημα απαγορεύεται να ζητήσει από τους χρήστες να δώσουν τον αριθμό της ταυτότητας τους, καθώς η πληροφορία αυτή δεν εξυπηρετεί πουθενά σε μια διαδικασία ηλεκτρονικής αγοράς.

Με την αρχή της ακρίβειας τα ηλεκτρονικά καταστήματα θα πρέπει τα δεδομένα προσωπικού χαρακτήρα που διαθέτουν για τους πελάτες τους να είναι ακριβή και να επικαιροποιούνται. Αυτό σημαίνει ότι αν κάποιος καταναλωτής έχει δημιουργήσει κάποιο ηλεκτρονικό προφίλ στην ιστοσελίδα ενός καταστήματος και έπειτα από αρκετό χρονικό διάστημα θελήσει να ολοκληρώσει μια ακόμη αγορά από το ίδιο ηλεκτρονικό καταστήματα, τότε τα δεδομένα του θα πρέπει να επαληθευτούν. Για παράδειγμα, σε περίπτωση που ο χρήστης έχει αλλάξει διεύθυνση κατοικίας ή αριθμό κινητού τηλεφώνου το ηλεκτρονικό κατάστημα θα πρέπει να λάβει όλα τα μέτρα, προκειμένου να γίνει η διαγραφή ή η διόρθωση όλων των στοιχείων που έχουν

αλλάξει από τον χρήστη.

Με την αρχή του περιορισμού θα πρέπει τα ηλεκτρονικά καταστήματα να αποθηκεύουν τα προσωπικά δεδομένα των πελατών τους μόνο για το χρονικό διάστημα που απαιτείται για να μπορέσει να ολοκληρωθεί η αγορά και αποστολή της παραγγελίας. Επίσης, αν το ηλεκτρονικό κατάστημα αποφασίσει να κρατήσει τα δεδομένα αυτά για στατιστικούς λόγους θα πρέπει να είναι σε μορφή που δεν επιτρέπει την ταυτοποίηση των χρηστών.

Τέλος, με τη αρχή της ακεραιότητας και εμπιστευτικότητας τα ηλεκτρονικά καταστήματα θα πρέπει να υποβάλλουν τα δεδομένα προσωπικού χαρακτήρα σε επεξεργασία με τρόπο που θα εγγυάται την ασφάλεια τους, δηλαδή την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και πιθανή απώλεια, καταστροφή ή φθορά. Ένας από τους πολλούς τρόπους εξασφάλισης της ασφάλειας των προσωπικών δεδομένων των υποκειμένων είναι η κρυπτογράφηση. Η πρακτική αυτή εγγυάται ότι σε περίπτωση κλοπής δεδομένων από κάποιον εισβολέα οι πελάτες του ηλεκτρονικού καταστήματος δεν θα μπορέσουν να ταυτοποιηθούν.

3.3 Οι διαδικασίες μιας ηλεκτρονικής αγοράς

Προκειμένου να είναι εφικτή η αναγνώριση των κινδύνων που μπορεί να εμφανιστούν σε μια ηλεκτρονική συναλλαγή θα πρέπει πρώτα να αναγνωριστούν οι βασικές λειτουργίες ενός ηλεκτρονικού καταστήματος. Στο παράδειγμα αναλύονται οι κίνδυνοι για τα προσωπικά δεδομένων των πελατών που επιφυλάσσει μια ηλεκτρονική αγορά ενός αγαθού ή μιας υπηρεσίας από κάποιο ηλεκτρονικό κατάστημα. Αρχικά, παρουσιάζονται οι οντότητες που υπάρχουν στο σύστημα αυτό και στη συνέχεια οι κίνδυνοι προς την ιδιωτική ζωή των πελατών.

Οντότητες :

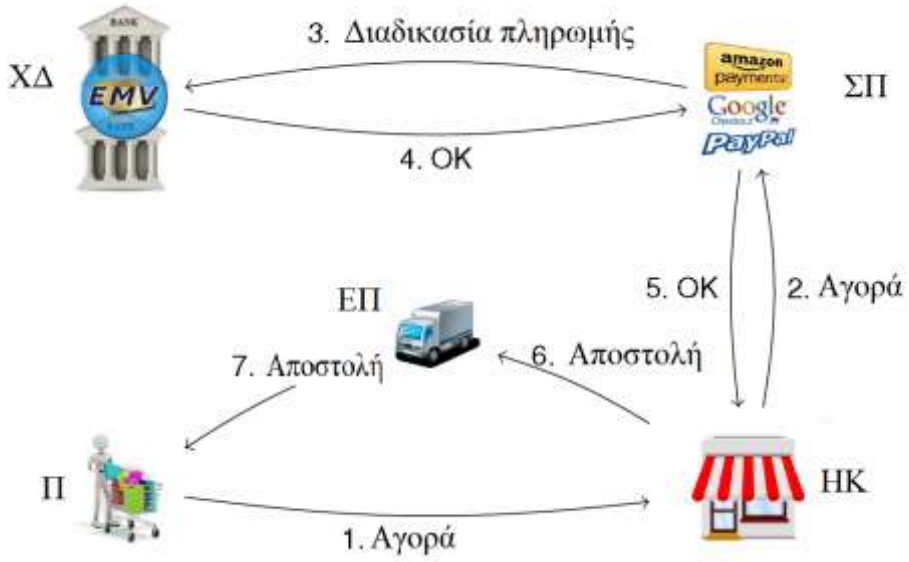
Πελάτης (Π) : Άτομα που αγοράζουν αγαθά ή υπηρεσίες

Ηλεκτρονικό Κατάστημα (ΗΛ) : Πωλούν προϊόντα και προσφέρουν υπηρεσίες στους πελάτες

Σύστημα Πληρωμής (ΣΠ) : Πλατφόρμες που συνδέουν πελάτες και εμπόρους, προσφέροντας υπηρεσίες προστιθέμενης αξίας, πχ. Προγράμματα μάρκετινγκ στους πελάτες και μηχανισμούς πρόληψης της απάτης στους εμπόρους. Για παράδειγμα Amazon, eBay ή Alibaba.

Χρηματοπιστωτικό Δίκτυο (ΧΔ) : Όλες οι οικονομικές οντότητες που επεξεργάζονται και εκτελούν συναλλαγές

Εταιρίες Παράδοσης (ΕΠ) : Υπεύθυνος για την παράδοση των υλικών αγαθών



Εικ. 1 : Οι διαδικασίες μιας ηλεκτρονικής αγοράς (Diaz et. al, 2019)

Για την ολοκλήρωση μιας ηλεκτρονικής αγοράς υπάρχουν τέσσερα βασικά στάδια. Αν υποθέσουμε ότι ο χρήστης έχει ολοκληρώσει την εγγραφή του, τα τέσσερα αυτά στάδια είναι η αγορά, η ολοκλήρωση της παραγγελίας, η παράδοση και η ολοκλήρωση της όλης διαδικασίας. Στη πρώτη φάση τη αγοράς ο Π επιλέγει να αγοράσει ένα προϊόν από το ΗΚ. Στη δεύτερη φάση της ολοκλήρωσης της παραγγελίας, οι πληροφορίες σχετικά με την πληρωμή και την παράδοση που δίνει ο Π κατευθύνονται προς το ΣΠ μέσω του ΗΚ και επεξεργάζονται και εκτελούνται από το ΧΔ. Στην επόμενη φάση της παράδοσης η ΕΠ μεταφέρει στον Π τα φυσικά αγαθά που αγόρασε. Στην τελευταία φάση της ολοκλήρωσης ο Π επιβεβαιώνει ότι όλα είναι σωστά ή αφήνει ένα παράπονο ή μια κριτική εάν συνάντησε κάποιο πρόβλημα.

3.4 Οι κίνδυνοι

Ύστερα από τη διαμόρφωση και την παρουσίαση των βασικών οντοτήτων και διαδικασιών, γίνεται ανάλυση των κύριων κινδύνων για την προστασία της ιδιωτικής ζωής που μπορεί να εμφανιστούν. Στον Πίνακα 1 συνοψίζονται οι απειλές για κάθε μια από τις βασικές διαδικασίες.

Στάδια	**Κίνδυνοι προστασίας της ιδιωτικής ζωής**
Αγορά	1.1 Οι πληροφορίες για το προϊόν διαρρέουν σε χρηματοπιστωτικές οντότητες ή σε τρίτους 1.2 Γίνεται σύνδεση των πελατών με τους εμπόρους από τρίτους 1.3 Συλλέγονται δεδομένα που δεν χρειάζονται 1.4 Τα δεδομένα αποθηκεύονται για μελλοντική χρήση για άλλους σκοπούς
Ολοκλήρωση παραγγελίας	2.1 Οι πληροφορίες για το προϊόν διαρρέουν σε χρηματοπιστωτικές οντότητες ή σε τρίτους 2.2 Οι πληροφορίες πληρωμής διαρρέουν στους εμπόρους ή σε τρίτους 2.3 Γίνεται σύνδεση των πελατών με τους εμπόρους από τρίτους 2.4 Τα δεδομένα δεν αποθηκεύονται με σωστό τρόπο
Παράδοση	3.1 Η διεύθυνση αποστολής διέρρευσε σε εμπόρους ή τρίτους 3.2 Γίνεται σύνδεση των πελατών με τους εμπόρους από εταιρείες παράδοσης ή τρίτους 3.3 Τα δεδομένα αποθηκεύονται για άλλους σκοπούς
Ολοκλήρωση	4.1 Οι ιδιωτικές πληροφορίες διαρρέουν μέσω σχολίων που δίνει ο χρήστης 4.2 Δεν διαγράφονται τα δεδομένα ή δεν αποθηκεύονται με τρόπο ώστε να είναι μη ταυτοποιήσιμα

Πίνακας 1 : Περίληψη των απειλών στις διάφορες φάσεις(Diaz et. al, 2019)

3.4.1 Κίνδυνοι στη φάση της αγοράς

Όπως αναφέρουν οι Giannakis Antoniou και Lynn Batten (2011) κάποιοι από τους κινδύνους που μπορεί να προκύψουν είναι : «

α. *Ένας εισβολέας παρακολουθεί τις πληροφορίες πληρωμής κατά την μετάβαση τους μεταξύ του πωλητή και του αγοραστή.*

β. *Ένας εισβολέας κλέβει τα στοιχεία πληρωμής του αγοραστή από τον πωλητή και τα καταχράται με ένας από τους δύο τρόπους :*

   1. *Πριν ο πωλητής χρησιμοποιήσει τα στοιχεία πληρωμής.*
   2. *Αφού ο πωλητής χρησιμοποιήσει τα στοιχεία πληρωμής.*

γ. *Ο πωλητής καταχράται τα στοιχεία πληρωμής με τους ακόλουθους τρόπους :*

   1. *Διπλές χρεώσεις στην πιστωτική κάρτα του αγοραστή.*
   2. *Πουλά τα στοιχεία πληρωμής σε άλλες οντότητες.*
   3. *Χρεώνει την πιστωτική κάρτα του αγοραστή με περισσότερα χρήματα από το συμφωνηθέν ποσό.*

δ. *Ο πωλητής καταχράται τις προσωπικές πληροφορίες του αγοραστή με τους ακόλουθους τρόπους :*

   1. *Ο πωλητής μπορεί να πουλήσει / αποκαλύψει τα προσωπικά στοιχεία σε άλλες οντότητες.*
   2. *Ο πωλητής μπορεί να αποκαλύψει στο κοινό προσωπικές πληροφορίες του αγοραστή χωρίς την συγκατάθεση του.*
   3. *Ο πωλητής μπορεί να στείλει ανεπιθύμητο μήνυμα ηλεκτρονικού ταχυδρομείου στον αγοραστή.*

ε. *Ένας εισβολέας μπορεί να κλέψει τις προσωπικές πληροφορίες του αγοραστή από τον πωλητή.*

στ. *Ο πωλητής δεν επιτρέπει στον αγοραστή να ενημερώσει τα προσωπικά του στοιχεία ή τις πληροφορίες πληρωμής.* » (σελ. 4-5)

Πέρα από τους παραπάνω κινδύνους που μπορεί να υπάρχουν στη φάση της αγοράς υφίστανται και άλλοι κίνδυνοι, όπως για παράδειγμα όταν το ηλεκτρονικό κατάστημα δεν τηρεί τις αρχές και γενικότερα τις απαιτήσεις του ΓΚΠΔ. Στη

συγκεκριμένη φάση το ηλεκτρονικό κατάστημα θα πρέπει να τηρεί την αρχή της νομιμότητας, την αρχή του σκοπού, την αρχή της ελαχιστοποίησης και την αρχή της ακρίβειας. Με βάση τις αρχές αυτές τα ηλεκτρονικά καταστήματα θα πρέπει να συλλέγουν συγκεκριμένα δεδομένα, τα οποία είναι απαραίτητα για μπορέσει να ολοκληρωθεί η παραγγελία από τον χρήστη και όχι περισσότερα. Επίσης, στην περίπτωση ενός τακτικού πελάτη, ο οποίος έχει δημιουργήσει στο παρελθόν προφίλ στην ιστοσελίδα του ΗΚ, τα δεδομένα για την νέα αγορά του θα πρέπει να εξακριβωθούν, προκειμένου τα δεδομένα που διαθέτει το ΗΚ να είναι έγκυρα. Επιπροσθέτως, σημαντικό ρόλο στη φάση αυτή είναι η ενημέρωση που πρέπει να παρέχουν όλα τα ηλεκτρονικά καταστήματα. Το δικαίωμα της ενημέρωσης είναι ένα από τα σημαντικότερα δικαιώματα που έχει το υποκείμενο. Σύμφωνα με το δικαίωμα αυτό τα ηλεκτρονικά καταστήματα θα πρέπει να ενημερώνουν τους χρήστες για το πώς συλλέγουν και επεξεργάζονται τα δεδομένα, για το πώς αυτά αποθηκεύονται, και άλλες απαιτήσεις που θα παρουσιαστούν εκτενώς στο κεφάλαιο 6.

Επιπλέον κίνδυνοι και τρωτά σημεία, μπορεί να εμφανιστούν στα προγράμματα αφοσίωσης (loyalty programs). Το ΗΚ μπορεί να εφαρμόσει προγράμματα αφοσίωσης, ώστε να προσελκύσει όλο και περισσότερους πελάτες να αγοράσουν προϊόντα. Οι προσφορές που προσφέρει το ΗΚ με το πρόγραμμα αυτό βασίζονται στο προφίλ του χρήστη, στο ιστορικό αγορών και σε άλλα στοιχεία, που σημαίνει πώς η ανάλυση των προσωπικών πληροφοριών των πελατών είναι σημαντική για τη λειτουργία του προγράμματος. Για τον σκοπό αυτό ηλεκτρονικά καταστήματα (Amazon, eBay, κλπ.) συλλέγουν πληροφορίες, όπως είναι το ιστορικό αγορών, διεύθυνση IP και δεδομένα περιήγησης, προκειμένου να κάνουν την εμπειρία του χρήστη καλύτερη και να αυξήσουν το κέρδος τους.

3.4.2 Κίνδυνοι στη φάση της ολοκλήρωσης της παραγγελίας

Στη φάση αυτή ο Π καθορίζει τα στοιχεία πληρωμής και τη διεύθυνση για την παράδοση του προϊόντος, το ΗΚ ελέγχει τα στοιχεία πληρωμής και τα προωθεί στο ΧΔ. Αφού το ΧΔ ελέγξει τα στοιχεία και ολοκληρώσει την πληρωμή, ενημερώνει το ΗΚ, που με την σειρά του ενημερώνει τον Π.

Στη φάση αυτή δίνονται από τον Π σημαντικές προσωπικές του πληροφορίες

και επομένως ελλοχεύουν πολλοί κίνδυνοι, όπως, για παράδειγμα όλοι όσοι αναφέρθηκαν στη προηγούμενη φάση, καθώς και ο κίνδυνος κατάχρησης από τις οντότητες ΗΚ, ΣΠ ή ΧΔ των προσωπικών πληροφοριών του Π ή των πληροφοριών πληρωμής του Π. Στη φάση αυτή της ολοκλήρωσης της παραγγελίας το ΗΚ θα πρέπει να αποθηκεύσει τα προσωπικά δεδομένα του υποκειμένου για κάποιο χρονικό διάστημα μέχρι να τερματιστεί και η φάση της ολοκλήρωσης. Το ΗΚ θα πρέπει να τηρήσει την αρχή του περιορισμού της περιόδου αποθήκευσης των δεδομένων αυτών και επίσης την αρχή της ακεραιότητας και εμπιστευτικότητας, ώστε τα δεδομένα που θα αποθηκευτούν να είναι προστατευμένα από τυχόν επεξεργασία τους από μη εξουσιοδοτημένη πηγή.

Σε μια έρευνα που έγινε από τους Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh, Alex “Sandy” Pentland, γνωρίζοντας 3 μεταβλητές (τόπος, χρόνος, τιμή) μπορεί να γίνει ταυτοποίησή 90% των ατόμων από τα ανώνυμα οικονομικά στοιχεία ενός καταστήματος. Με άλλα λόγια, οι τράπεζες μέσω του χρηματοπιστωτικού δικτύου μπορούν να κάνουν ταυτοποίηση των πελατών του ΗΚ και να δημιουργήσουν προφίλ για τους πελάτες.

Επιπλέον, οι χρηματοπιστωτικές οντότητες που επεξεργάζονται ευαίσθητες πληροφορίες, όπως είναι οι αριθμοί των καρτών και οι λογαριασμοί, πρέπει να χρησιμοποιούν τεχνικές για την πρόληψη της απάτης. Τέτοιες τεχνικές μπορεί να θέσουν σε κίνδυνο τα προσωπικά στοιχεία των πελατών, στέλνοντας για παράδειγμα κάποιον κωδικό στο προσωπικό τηλέφωνο του χρήστη ή στη διεύθυνση ηλεκτρονικού ταχυδρομείου του. Με τον τρόπο αυτό, οι τράπεζες έχουν περισσότερες προσωπικές πληροφορίες για τους πελάτες, γεγονός που επιφυλάσσει τον κίνδυνο ότι αν κάποιος κάνει κάποια κακόβουλη επίθεση στη τράπεζα, θα έχει στη διάθεση του περισσότερα προσωπικά δεδομένα τους.

3.4.3 Κίνδυνοι στη φάση παράδοσης

Όταν το ΗΚ λάβει την πληρωμή, τότε αποστέλλει στον Π το αγαθό που αγόρασε. Αν πρόκειται για μια υπηρεσία, τότε την αποστέλλει μέσω διαδικτύου. Αν όμως είναι κάποιο προϊόν, τότε το αποστέλλει μέσω μιας εταιρείας παράδοσης. Στη περίπτωση που η παράδοση γίνει μέσω διαδικτύου υπάρχει ο κίνδυνος κάποιος εισβολέας να εμπλακεί στη μεταξύ τους επικοινωνία και να κλέψει προσωπικά

δεδομένα του Π ή ακόμα και την υπηρεσία που αυτός έχει αγοράσει. Στη περίπτωση που η παράδοση γίνει μέσω της ΕΠ, τότε η ΕΠ μαθαίνει και την φυσική διεύθυνση του ΗΚ και του Π, με αποτέλεσμα να μπορεί να τους συνδέσει και να αναγνωρίσει ποιος είναι ο αγοραστής και ποιος είναι ο πωλητής. Ακόμα, με τη σύνδεση αυτή μπορεί να δημιουργήσει ένα προφίλ για τους αγοραστές και να γνωρίζει τις προτιμήσεις τους τόσο σε προϊόντα όσο και σε ηλεκτρονικά καταστήματα.

Η ΕΠ είναι μια ξεχωριστή οντότητα, η οποία θα πρέπει να τηρεί όλες τις αρχές και τις απαιτήσεις του ΓΚΠΔ. Όμως, υπάρχει ο κίνδυνος η ΕΠ να μην συμμορφώνεται με τον Κανονισμό και να εκμεταλλεύεται τα προσωπικά δεδομένα που λαμβάνει από το ΗΚ για τους πελάτες του. Επίσης, η ΕΠ μπορεί να θεωρηθεί και ως εκτελών την επεξεργασία για τα ΗΚ, καθώς είναι ο φορέας που επεξεργάζεται δεδομένα για λογαριασμό του και σύμφωνα με τις εντολές που του απευθύνει ο υπεύθυνος επεξεργασίας, δηλαδή το ΗΚ. Συνεπώς, η ΕΠ δεν μπορεί να λάβει αποφάσεις για την επεξεργασία, αφού τέτοιες αποφάσεις λαμβάνονται μόνο από το ΗΚ. Το κρίσιμο μέλημα της ΕΠ είναι να εξασφαλίσει ότι συμμορφώνεται με τον πλαίσιο προστασίας δεδομένων που θέτει το ΗΚ.

Τέλος, ο πελάτης ενός ΗΚ δεν μπορεί να είναι βέβαιος ότι η ΕΠ συμμορφώνεται όπως θα έπρεπε με τον ΓΚΠΔ και δεν σκοπεύει να καταχραστεί τις προσωπικές πληροφορίες που δίνονται από ΗΚ για την παράδοση του προϊόντος. Ένας τρόπος που η ΕΠ μπορεί να καταχραστεί προσωπικές πληροφορίες, που λαμβάνει από το ΗΚ χωρίς να το γνωρίζει ούτε ο πελάτης ούτε το ΗΚ που κοινοποίησε αυτές τις πληροφορίες, είναι να τις αποθηκεύσει και μελλοντικά να τις πουλήσει σε κάποιον ενδιαφερόμενο οργανισμό, συνήθως για σκοπούς εμπορικής προώθησης.

3.4.4 Κίνδυνοι στη φάση της ολοκλήρωσης

Αφού ο Π λάβει το προϊόν επιβεβαιώνει ότι όλα είναι εντάξει, ότι παρέλαβε το προϊόν χωρίς αυτό να είχε καμία ζημιά και ολοκληρώνεται η όλη διαδικασία. Αν ο Π βρει κάποιο πρόβλημα με το προϊόν ή με την μεταφορά της παραγγελίας του, τότε θα πρέπει να ενημερώσει το ΗΚ.

Στη φάση αυτή επειδή η αγορά έγινε από ένα ηλεκτρονικό κατάστημα και επομένως ο Π στις περισσότερες περιπτώσεις δεν μπορεί να έρθει σε άμεση επαφή με

τους πωλητές είτε γιατί δεν γνωρίζει την τοποθεσία του καταστήματος είτε γιατί βρίσκεται μακριά από αυτό, θα πρέπει να δώσει τα στοιχεία της παραγγελίας του για να γίνει ο έλεγχος. Συνεπώς όλοι οι κίνδυνοι που αναφέρθηκαν προηγουμένως στη φάση της αγοράς είναι πιθανόν να προκύψουν και σε αυτή τη φάση.

Στη φάση αυτή που ακόμα ολοκληρώνεται η όλη διαδικασία το ΗΚ, αλλά επίσης και η ΕΠ θα πρέπει να διαγράψει τα δεδομένα προσωπικού χαρακτήρα που είχε συλλέξει σε προηγούμενη φάση από τον πελάτη. Δεν θα πρέπει να αποθηκευτούν για άλλη χρήση, όπως κατά την αποστολή τους σε τρίτο υπεύθυνο επεξεργασία δεδομένων ή στα προγράμματα αφοσίωσης. Σύμφωνα με τον ΓΚΠΔ ο μόνος λόγος που το ΗΚ ή η ΕΠ μπορεί να αποθηκεύσει τα δεδομένα είναι για στατιστικούς λόγους. Όμως, θα πρέπει να διασφαλιστεί με τεχνικά μέσα ότι τα δεδομένα που έχουν αποθηκευτεί δεν μπορούν να οδηγήσουν στην ταυτοποίηση των πελατών.

3.4.5 Προγράμματα αφοσίωσης (Loyalty programs)

Τα προγράμματα αφοσίωσης είναι μια στρατηγική μάρκετινγκ, που χρησιμοποιείται για να ενθαρρύνει τους πελάτες να συνεχίσουν να αγοράζουν ή να χρησιμοποιούν τα προϊόντα ή τις υπηρεσίες μιας επιχείρησης. Στη σημερινή εποχή τα προγράμματα αφοσίωσης καλύπτουν τους περισσότερους τύπους εμπορίου. Στο ηλεκτρονικό εμπόριο τα προγράμματα αφοσίωσης πελατών επιβραβεύουν τους πελάτες με εκπτώσεις, δώρα, δωρεάν μεταφορικά, κουπόνια, ενώ σε κάποιες περιπτώσεις τους δίνουν πρόσβαση σε προϊόντα που δεν έχουν κυκλοφορήσει ακόμα στο ευρύ κοινό. Τα προγράμματα αφοσίωσης δημιουργούν ένα προφίλ για κάθε πελάτη του οργανισμού που σχετίζεται με το πρόγραμμα. Ακολούθως, παρέχουν μια ολοκληρωμένη πλατφόρμα για τη δημιουργία και την ανάπτυξη διαρκών πελατειακών σχέσεων, αλλά αρκετές εταιρείες δεν γνωρίζουν τον τρόπο που αυτό συμβαίνει. Ο προφανής τρόπος για τα προγράμματα αφοσίωσης είναι η παροχή οφελών, πόντους επιβράβευσης, εκπτώσεις, δωρεάν προϊόντα και άλλα ενδιαφέροντα, αλλά ο πραγματικός οδηγός για την επίτευξη διαρκών πελατειακών σχέσεων είναι τα Big Data. Τα Big Data ή αλλιώς «Μεγάλα Δεδομένα» είναι ο τεράστιος όγκος δεδομένων που δέχονται καθημερινά οι εταιρείες ηλεκτρονικού εμπορίου μέσω των χιλιάδων συναλλαγών από πελάτες.

Μια κοινή ψευδή αντίληψη των εμπόρων είναι ότι τα προγράμματα αφοσίωσης και τα προγράμματα ανταμοιβών (rewards programs) είναι το ίδιο. Στην πραγματικότητα τα προγράμματα ανταμοιβής δεν έχουν καμία σχέση με τα προγράμματα αφοσίωσης. Τα προγράμματα ανταμοιβής είναι απλώς μια πλατφόρμα για προωθήσεις προϊόντων χωρίς να υπάρχει γνώση για το πώς στοχεύονται με ακρίβεια. Αντιθέτως, ένα πρόγραμμα αφοσίωσης παρέχει ένα εξελιγμένο μέσο παρακολούθησης κάθε συναλλαγής μεταξύ ενός πελάτη και ενός οργανισμού, έτσι ώστε τα Big Data να μπορούν να αναλυθούν, με σκοπό την καλύτερη κατανόηση των συνηθειών και των αναγκών του αγοραστή. Τα προγράμματα αφοσίωσης πρέπει να αντιμετωπίζονται ως ανταλλαγή, που σημαίνει ότι προσφέρουν κάτι πολύτιμο στον πελάτη και σε αντάλλαγμα οι πελάτες παρέχουν τα προσωπικά τους στοιχεία μαζί με την άδεια παρακολούθησης της συμπεριφοράς και των ενεργειών τους, που παρέχονται μέσω των Big Data. Η προσφορά ανταμοιβών και κινήτρων στους πελάτες από τα προγράμματα αφοσίωσης δίνει τη δυνατότητα στα ηλεκτρονικά καταστήματα να κερδίσουν τη συγκατάθεση των πελατών για τη λήψη περαιτέρω προσωπικών πληροφοριών. Είναι σημαντικό οι χρήστες να αισθάνονται ότι συνεχίζουν να λαμβάνουν οφέλη και προσφορές που είναι χρήσιμες για αυτούς. Αναπόσπαστο μέρος για την ικανοποίηση αυτών των προσδοκιών είναι η ανάλυση δεδομένων των πελατών.

4. Δικαιώματα του καταναλωτή-υποκειμένου των δεδομένων

Ο νέος Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων προσφέρει στα υποκείμενα των δεδομένων καλύτερο έλεγχο ως προς τα προσωπικά τους δεδομένα, ενισχύοντας τα ήδη υπάρχοντα δικαιώματα τους και προσθέτοντας καινούργια, όπως το δικαίωμα της φορητότητας. Πρωταρχικός στόχος της Ευρωπαϊκής Επιτροπής για τον νέο νομοθετικό πλαίσιο ήταν η ενίσχυση των δικαιωμάτων των υποκειμένων των δεδομένων. Η παραβίαση τους επισύρει στις επιχειρήσεις και στους οργανισμούς υψηλά πρόστιμα.

Σύμφωνα με τον Κανονισμό τα δικαιώματα του υποκειμένου των δεδομένων ορίζονται στα άρθρα 12 έως 22 του Κεφαλαίου ΙΙΙ. Τα δικαιώματα αυτά προσφέρουν στο υποκείμενο καλύτερο έλεγχο στην ιδιωτική του ζωή και ενδυναμώνουν τον ρόλο του. Συγχρόνως, οι υπεύθυνοι επεξεργασίας ή οι εκτελούντες την επεξεργασία θα πρέπει να τροποποιήσουν ακόμα και τις βασικές επιχειρησιακές τους δραστηριότητες, προκειμένου να συμμορφώνονται με τον νέο Κανονισμό και να ικανοποιούν και να σέβονται τα δικαιώματα των υποκειμένων.

4.1 Το Δικαίωμα της Ενημέρωσης

Τα φυσικά πρόσωπα έχουν δικαίωμα να ενημερώνονται για τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων. Το δικαίωμα αυτό διέπεται από τη γενική αρχή της διαφάνειας. Ο υπεύθυνος επεξεργασίας οφείλει να καταστήσει τη πληροφόρηση του υποκειμένου επαρκή και σαφή, ώστε το ίδιο το υποκείμενο να είναι σε θέση να ελέγχει ή να επηρεάζει την επεξεργασία των δεδομένων του. Τα άρθρα 13 και 14 του ΓΚΠΔ προσδιορίζουν ποιες πληροφορίες πρέπει να περιλαμβάνει η ενημέρωση ανάλογα με το αν η συλλογή γίνεται από τα ίδια τα υποκείμενα ή από άλλες πηγές.

Ο υπεύθυνος επεξεργασίας ανάλογα με τον τρόπο που έχει γίνει η συλλογή των προσωπικών δεδομένων θα πρέπει να δίνει και αντίστοιχες πληροφορίες στο υποκείμενο με βάση τα παραπάνω άρθρα. Στη περίπτωση που τα προσωπικά δεδομένα έχουν συλλεχθεί από το ίδιο το υποκείμενο, τότε ο υπεύθυνος επεξεργασίας καλείται να δώσει πληροφορίες σχετικά με τους σκοπούς της επεξεργασίας, το

χρονικό διάστημα που θα αποθηκευτούν τα δεδομένα αυτά ή, αν αυτό δεν είναι δυνατόν, τα κριτήρια που καθορίζουν αυτό το χρονικό όριο, τα δικαιώματα που έχει το υποκείμενο και τυχόν αποδέκτες (άρθρο 13 παρ. 2). Στη περίπτωση που η συλλογή των δεδομένων έγινε από κάποια άλλη πηγή, τότε ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει το υποκείμενο ποια είναι η πηγή από την οποία προέρχονται τα δεδομένα (άρθρο 14 παρ. 1 στοιχείο α). Ωστόσο, ο υπεύθυνος επεξεργασίας δεν έχει την υποχρέωση αυτή, και στις δύο περιπτώσεις, αν το υποκείμενο έχει ήδη λάβει τη σχετική πληροφόρηση σε προγενέστερο χρόνο. Για παράδειγμα, αν ο πελάτης έχει δημιουργήσει ένα προφίλ στο ηλεκτρονικό κατάστημα, έχει ολοκληρώσει μια παραγγελία και σε μεταγενέστερο χρόνο επιλέγει να αγοράσει ξανά από το ίδιο ηλεκτρονικό κατάστημα με το ίδιο προφίλ, τότε ο υπεύθυνος επεξεργασίας δεν είναι υποχρεωμένος να ενημερώσει ξανά τον χρήστη (άρθρο 13 παρ. 4 και άρθρο 14 παρ. 5 στοιχείο α).

Η ενημέρωση του υποκειμένου από τον υπεύθυνο επεξεργασίας πρέπει να είναι σε απλή, καθημερινή και σαφή γλώσσα, ώστε να μπορεί να γίνει κατανοητή από οποιονδήποτε ακόμα και από άτομα που έχουν δυσκολίες στην κατανόηση λόγω χαμηλού μορφωτικού επιπέδου, ηλικίας κ.ά. Συνεπώς, πρέπει να αποφεύγεται η χρήση ειδικών όρων (π.χ. οικονομικών, πληροφορικής, νομικών κλπ.) ή όρων ξένων γλωσσών (άρθρο 12 παρ. 1).

Οι πληροφορίες πρέπει να παρέχονται γραπτώς ή με άλλα μέσα και σε κάποιες περιπτώσεις και ηλεκτρονικά. Όταν ζητείται από το υποκείμενο οι πληροφορίες μπορούν να δοθούν και προφορικά με την προϋπόθεση ότι η ταυτότητα του υποκειμένου είναι αποδεδειγμένη (άρθρο 12 παρ. 1). Σύμφωνα με τον ΓΚΠΔ οι πληροφορίες μπορούν να παρέχονται σε συνδυασμό με τυποποιημένα εικονίδια, προκειμένου να δίνεται με ευδιάκριτο, κατανοητό και ευανάγνωστο τρόπο η επισκόπηση της επεξεργασίας. Εάν τα εικονίδια διατίθενται ηλεκτρονικά στα υποκείμενα, θα πρέπει να είναι μηχανικώς αναγνώσιμα (άρθρο 12 παρ. 7).

Όσον αφορά το χρονικό όριο που έχει ο υπεύθυνος επεξεργασίας για να ενημερώσει το υποκείμενο αυτό διαφοροποιείται ανάλογα με το αν οι πληροφορίες συλλέχθηκαν από το ίδιο το υποκείμενο ή από κάποια άλλη πηγή. Αν τα δεδομένα προσωπικού χαρακτήρα συλλέχθηκαν από το ίδιο το υποκείμενο, τότε ο υπεύθυνος επεξεργασίας πρέπει να ενημερώσει το υποκείμενο κατά τη λήψη των δεδομένων (άρθρο 13 παρ. 1). Στη περίπτωση που τα δεδομένα προσωπικού χαρακτήρα

συλλέχθηκαν από κάποια άλλη πηγή, τότε η σχετική ενημέρωση από τον υπεύθυνο επεξεργασίας μπορεί να γίνει εντός ενός μήνα από τη συλλογή των δεδομένων. Αν τα δεδομένα πρόκειται να χρησιμοποιηθούν για επικοινωνία με το υποκείμενο των δεδομένων, η ενημέρωση πρέπει να γίνει κατά την πρώτη επικοινωνία με το εν λόγω υποκείμενο. Επίσης, εάν προβλέπεται να γίνει γνωστοποίηση των δεδομένων σε κάποιον άλλον αποδέκτη, η ενημέρωση πρέπει να γίνει το αργότερο όταν τα δεδομένα προσωπικού χαρακτήρα γνωστοποιούνται για πρώτη φορά (άρθρο 14 παρ. 3).

4.2 Το Δικαίωμα Πρόσβασης

Το δικαίωμα της πρόσβασης αποτελείται από δύο στάδια. Στο πρώτο στάδιο το υποκείμενο των δεδομένων έχει το δικαίωμα να λάβει από τον υπεύθυνο επεξεργασίας μια θετική ή αρνητική απάντηση για το αν τα προσωπικά του δεδομένα υφίστανται σε επεξεργασία. Στο επόμενο στάδιο αν λάβει θετική απάντηση από τον υπεύθυνο επεξεργασίας είναι δυνατή η πρόσβαση του στα δεδομένα του και σε περαιτέρω πληροφορίες για την επεξεργασία, καθώς και για τα δικαιώματα του (άρθρο 15 παρ. 1). Για παράδειγμα, στην περίπτωση ενός ηλεκτρονικού καταστήματος που κρατάει αρχείο των πελατών του, ο κάθε πελάτης έχει το δικαίωμα και μπορεί να ζητήσει πρόσβαση στα δεδομένα που διαθέτει το ηλεκτρονικό κατάστημα για εκείνον, όπως τα στοιχεία επικοινωνίας του, το αρχείο αγορών, η ημερομηνίες αγορών, τα αγορασμένα προϊόντα, οι πληρωμές και το ηλεκτρονικό προφίλ του στο κατάστημα.

Στη συνέχεια, το υποκείμενο μπορεί να ασκήσει το δικαίωμα του να επηρεάσει την επεξεργασία των προσωπικών του δεδομένων. Το υποκείμενο θα πρέπει να υποβάλει μια αίτηση προς τον υπεύθυνο επεξεργασίας, εγγράφως ή με τη χρήση ηλεκτρονικών μέσων για διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα, για περιορισμό της επεξεργασίας τους ή για την άσκηση του δικαιώματος αντίταξης στην εν λόγω επεξεργασία. Ο υπεύθυνος είναι υποχρεωμένος από τον ΓΚΠΔ να παρέχει στο υποκείμενο των δεδομένων πληροφορίες για την ενέργεια που πραγματοποιείται κατόπιν αιτήματος χωρίς καθυστέρηση και σε κάθε περίπτωση εντός ενός μήνα από την παραλαβή του αιτήματος. Η εν λόγω προθεσμία μπορεί να παραταθεί για δύο ακόμα μήνες, εφόσον είναι απαραίτητο, λαμβάνοντας υπόψη τη

πολυπλοκότητα του αιτήματος και τον αριθμό των αιτημάτων. Ο υπεύθυνος επεξεργασίας θα πρέπει να ενημερώσει το υποκείμενο για την παράταση εντός μηνός από την παραλαβή του αιτήματος, καθώς και για τους λόγους της καθυστέρησης.

Στη περίπτωση που το υποκείμενο υποβάλει την αίτηση του με ηλεκτρονικά μέσα, η ενημέρωση παρέχεται, εφόσον είναι εφικτό, με ηλεκτρονικά μέσα, εκτός εάν το υποκείμενο των δεδομένων ζητήσει κάτι διαφορετικό. Ωστόσο, αν το υποκείμενο ζητήσει να λάβει παραπάνω από μια φορές αντίγραφο των δεδομένων ή αν ο αριθμός των αντιγράφων που θα πρέπει να του χορηγηθεί είναι μεγάλος, ενδέχεται ο υπεύθυνος επεξεργασίας να επιβάλει την καταβολή εύλογου τέλους για τα διοικητικά έξοδα (άρθρο 15 παρ. 3).

4.3 Το Δικαίωμα Διόρθωσης

Το δικαίωμα της διόρθωσης συνδέεται άμεσα με την αρχή της ακρίβειας του ΓΚΠΔ βάσει της οποίας τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι ακριβή και να επικαιροποιούνται για την αποφυγή οποιασδήποτε αρνητικής επίπτωσης στο υποκείμενο. Σύμφωνα με το άρθρο 16 του ΓΚΠΔ το υποκείμενο των δεδομένων μπορεί να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Επιπλέον, έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.

4.4 Το Δικαίωμα Διαγραφής

Το δικαίωμα της διαγραφής, ή αλλιώς «δικαίωμα στη λήθη», ορίζεται στο άρθρο 17 του ΓΚΠΔ και αφορά στο δικαίωμα του υποκείμενο των δεδομένων να ζητήσει τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν, εφόσον δεν επιθυμεί πλέον τα δεδομένα του να αποτελούν αντικείμενο επεξεργασίας και εφόσον δεν υφίσταται νόμιμος λόγος να τα κατέχει ο υπεύθυνος επεξεργασίας. Ο υπεύθυνος επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση θα πρέπει να εκτελέσει το αίτημα του υποκειμένου για την διαγραφή των δεδομένων αν ισχύουν οι λόγοι,

που αναγράφονται στο άρθρο 17 παράγραφος 1 του ΓΚΠΔ. Ειδικότερα, το υποκείμενο των δεδομένων μπορεί να ανακαλέσει την συγκατάθεση του επί της οποίας βασίζεται η επεξεργασία. Επομένως, τα δεδομένα πρέπει να διαγραφούν, σε περίπτωση που δεν υπάρχει άλλη νομική βάση για την επεξεργασία. Επίσης, εάν τα δεδομένα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν, αν υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία, εάν υποβάλλονται σε επεξεργασία παράνομα ή αν το υποκείμενο των δεδομένων αντιτάσσεται στην επεξεργασία τους, τότε ο υπεύθυνος επεξεργασίας υποχρεούται να τα διαγράψει.

Ακολούθως, το δικαίωμα αυτό έχει ιδιαίτερη σημασία όταν το υποκείμενο των δεδομένων παρείχε τη συγκατάθεση του ως παιδί, όταν δεν είχε πλήρη επίγνωση των κινδύνων που ενέχει η επεξεργασία και θέλει αργότερα να αφαιρέσει τα συγκεκριμένα δεδομένα προσωπικού χαρακτήρα από το διαδίκτυο ή από οποιαδήποτε οργανισμό είχαν συλλεχθεί. Το υποκείμενο των δεδομένων θα πρέπει να μπορεί να ασκήσει το εν λόγω δικαίωμα παρά το γεγονός ότι δεν είναι παιδί πλέον.

Όταν τα δεδομένα προσωπικού χαρακτήρα έχουν δημοσιοποιηθεί από τον υπεύθυνο επεξεργασίας σε τρίτους και έχει ζητηθεί από το υποκείμενο η διαγραφή τους, ο υπεύθυνος επεξεργασίας θα πρέπει να λάβει εύλογα μέτρα, συμπεριλαμβανομένων των τεχνικών μέτρων, για να ενημερώσει τους υπεύθυνους επεξεργασίας που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, ότι το υποκείμενο των δεδομένων ζήτησε τη διαγραφή από αυτούς πιθανών συνδέσμων με τα δεδομένα αυτά, αντιγράφων ή αναπαραγωγών των εν λόγω δεδομένων προσωπικού χαρακτήρα (άρθρο 17 παρ. 2).

Ωστόσο, το δικαίωμα της διαγραφής δεν είναι ένα απόλυτο δικαίωμα, καθώς ο υπεύθυνος επεξεργασίας μπορεί να αρνηθεί τη διαγραφή των δεδομένων του υποκειμένου για λόγους που προβλέπονται ρητά από τον Κανονισμό στη παράγραφο 3 του άρθρου 17. Τέτοιοι λόγοι είναι για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση, για την τήρηση νομικής υποχρέωσης, για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων. Εν προκειμένω σε μια ηλεκτρονική αγορά ο πωλητής

έχει νομική υποχρέωση τήρησης τιμολογίων για συγκεκριμένο χρονικό διάστημα και συνεπώς ο πελάτης δεν μπορεί να ζητήσει την διαγραφή του τιμολογίου αυτού.

4.5 Το Δικαίωμα Περιορισμού της Επεξεργασίας

Τα φυσικά πρόσωπα έχουν το δικαίωμα να ζητήσουν τον περιορισμό της επεξεργασίας των δεδομένων τους. Συγκεκριμένα, το υποκείμενο των δεδομένων μπορεί να ζητήσει από τον υπεύθυνο επεξεργασίας να περιορίσει την επεξεργασία όταν η ακρίβεια των δεδομένων αμφισβητείται από το υποκείμενο των δεδομένων για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να επαληθεύσει την ακρίβεια των δεδομένων. Επιπλέον, το υποκείμενο διατηρεί το συγκεκριμένο δικαίωμα όταν η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων και ζητεί αντ' αυτού τον περιορισμό της χρήσης τους. Επίσης, όταν ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων και, τέλος, όταν το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπεύθυνου επεξεργασίας υπερισχύουν έναντι των λόγων του υποκειμένου (άρθρο 18 παρ. 1).

Ο Κανονισμός προτείνει τρόπους με τους οποίους μπορεί να περιοριστεί η επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Τέτοιοι τρόποι είναι η προσωρινή μετακίνηση των επιλεγμένων δεδομένων σε άλλο σύστημα επεξεργασίας, η αφαίρεση της προσβασιμότητας των επιλεγμένων δεδομένων προσωπικού χαρακτήρα από τους χρήστες ή την προσωρινή αφαίρεση δημοσιευμένων δεδομένων από ιστοσελίδα. Σε συστήματα αυτοματοποιημένης αρχειοθέτησης ο περιορισμός της επεξεργασίας θα πρέπει να διασφαλίζεται με τεχνικά μέσα με τρόπο ώστε τα δεδομένα να μην υπόκεινται σε περαιτέρω επεξεργασία και να μην μπορούν να αλλάξουν (αιτιολογική σκέψη 67). Το υποκείμενο των δεδομένων θα πρέπει να ενημερώνεται από τον υπεύθυνο επεξεργασίας πριν από την άρση του περιορισμού επεξεργασίας.

Ο υπεύθυνος επεξεργασίας θα πρέπει να ανακοινώσει κάθε διόρθωση, διαγραφή προσωπικών δεδομένων ή περιορισμό της επεξεργασίας των δεδομένων σε

κάθε αποδέκτη, στον οποίο γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, εκτός από τις περιπτώσεις που αυτό αποδεικνύεται ανέφικτο ή συνεπάγεται δυσανάλογη προσπάθεια. Τέλος, εφόσον του ζητηθεί, ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να ενημερώσει το υποκείμενο των δεδομένων σχετικά με τους εν λόγω αποδέκτες (άρθρο 19).

4.6 Το Δικαίωμα Φορητότητας

Το νέο δικαίωμα στη φορητότητα προσφέρει στο υποκείμενο των δεδομένων ένα εύκολο τρόπο να διαχειρίζεται τα ίδια του τα προσωπικά δεδομένα. Σύμφωνα με το άρθρο 20 του ΓΚΠΔ, το υποκείμενο των δεδομένων έχει το δικαίωμα να λάβει από τον υπεύθυνο επεξεργασίας σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνωρίσιμο από μηχανήματα μορφότυπο, καθώς επίσης και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο. Για παράδειγμα, μια πρακτική εφαρμογή σε ένα ηλεκτρονικό κατάστημα που παρέχει τεχνολογικά προϊόντα είναι ο πελάτης να ζητήσει από τον υπεύθυνο επεξεργασίας να του παρέχει μια λίστα με τα προϊόντα που έχει αγοράσει, καθώς επίσης και τα σχόλια που έχει αφήσει για το κάθε προϊόν για να μπορέσει στη συνέχεια να το μεταβιβάσει σε κάποιο άλλο ηλεκτρονικό κατάστημα, ώστε να δουν περισσότεροι πελάτες την αξιολόγηση του στο συγκεκριμένο προϊόν που έχει ήδη αγοράσει από αλλού.

Επιπλέον, το δικαίωμα στη φορητότητα προσφέρει τη δυνατότητα στο υποκείμενο των δεδομένων να ζητήσει από τον υπεύθυνο επεξεργασίας την απευθείας μεταφορά των δεδομένων προσωπικού χαρακτήρα σε άλλον υπεύθυνο επεξεργασίας, εφόσον αυτό είναι τεχνικά εφικτό. Ωστόσο, σύμφωνα με την αιτιολογική σκέψη 68 του ΓΚΠΔ το δικαίωμα φορητότητας δεν θα πρέπει να δημιουργεί υποχρέωση των υπευθύνων επεξεργασίας να υιοθετούν ή να διατηρούν σύστημα επεξεργασίας που είναι συμβατά από τεχνική άποψη.

Το δικαίωμα στη φορητότητα μπορεί να ασκηθεί εφόσον η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πραγματοποιείται με αυτοποιημένα μέσα, δηλαδή χωρίς να προβλέπεται η φορητότητα σε έντυπα αρχεία, καθώς και όταν η νόμιμη βάση της επεξεργασίας είναι είτε η συγκατάθεση του υποκειμένου είτε η σύμβαση στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος. Τέλος,

σύμφωνα με τον Κανονισμό το δικαίωμα στη φορητότητα δεν θα πρέπει να επηρεάζει τα δικαιώματα και τις ελευθερίες άλλων.

4.7 Το Δικαίωμα Εναντίωσης

Σύμφωνα με το άρθρο 21 του ΓΚΠΔ, με το δικαίωμα της εναντίωσης το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν, περιλαμβανόμενης της κατάρτισης προφίλ. Ειδικότερα, το υποκείμενο μπορεί ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του να ασκήσει το συγκεκριμένο δικαίωμα του. Ο υπεύθυνος επεξεργασίας δεν υποβάλλει πλέον τα δεδομένα προσωπικού χαρακτήρα που αφορούν το εκάστοτε υποκείμενο σε επεξεργασία, εκτός εάν ο υπεύθυνος επεξεργασίας αποδείξει ότι υπάρχουν νόμιμοι λόγοι για την επεξεργασία, οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Επιπλέον, δίνεται στο υποκείμενο ένα ιδιότυπο δικαίωμα εναντίωσης στην περίπτωση αυτοματοποιημένης λήψης αποφάσεων (Λίλιαν Μήτρου, 2017). Συγκεκριμένα, σύμφωνα με άρθρο 22 του ΓΚΠΔ το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζουν σημαντικά με παρόμοιο τρόπο. Το δικαίωμα αυτό, επηρεάζει σημαντικά τα ηλεκτρονικά καταστήματα, καθώς χρησιμοποιούν εργαλεία ανάλυσης δεδομένων μεγάλης κλίμακας (big data analytics) για την χρήση προγραμμάτων αφοσίωσης και κάνοντας χρήση cookies για την δημιουργία προφίλ των χρηστών τους. Ωστόσο, το δικαίωμα αυτό δεν εφαρμόζεται όταν η απόφαση είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας των δεδομένων (άρθρο 22 παρ. 2 στοιχείο α) ή όταν βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

4.8 Το Δικαίωμα στην Ανθρώπινη Παρέμβαση

Η τεχνολογική πρόοδος τα τελευταία χρόνια, η ανάλυση μαζικών δεδομένων, η τεχνητή νοημοσύνη και οι μηχανές μάθησης καθιστούν εύκολη την κατάρτιση προφίλ των υποκειμένων και τη λήψη αποφάσεων με αυτοματοποιημένο τρόπο, με κίνδυνο όμως να επηρεαστούν σημαντικά τα δικαιώματα, οι ελευθερίες και τα έννομα συμφέροντα των υποκειμένων (Ειρηνικός Πλάτης, 2018). Με τον νέο Κανονισμό το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο (άρθρο 22 παρ. 1). Συγκεκριμένα, στο ηλεκτρονικό εμπόριο αυτοματοποιημένη απόφαση είναι η αποστολή κουπονιών σε πελάτες που έχουν κάνει ήδη κάποια αγορά στο παρελθόν. Με αυτόν τον τρόπο, τα ηλεκτρονικά καταστήματα θα προσελκύσουν ξανά τους ίδιους χρήστες για μια νέα αγορά.

Ο υπεύθυνος επεξεργασίας μπορεί να αρνηθεί την ικανοποίηση του αιτήματος του υποκειμένου εάν η απόφαση που λαμβάνεται βάσει της αυτοματοιημένης επεξεργασίας είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας των δεδομένων ή επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο του κράτους-μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας ή βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

5. Υπεύθυνος Προστασίας Δεδομένων

Σύμφωνα με τον Κανονισμό, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία υποχρεούνται να ορίσουν έναν υπεύθυνο προστασίας δεδομένων (ΥΠΔ). Ο υπεύθυνος προστασίας δεδομένων είναι ένα φυσικό πρόσωπο ή νομικό πρόσωπο, το οποίο αναλαμβάνει συγκεκριμένες αρμοδιότητες, προκειμένου να εξασφαλιστεί η συμμόρφωση με τις απαιτήσεις του Κανονισμού.

5.1 Ορισμός υπεύθυνου προστασίας δεδομένων

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία είναι υποχρεωμένοι να ορίσουν υπεύθυνο προστασίας δεδομένων, όταν η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα, εκτός από τα δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας, ή όταν οι βασικές δραστηριότητες του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα. Επίσης, όταν οι βασικές δραστηριότητες του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα. Ο Κανονισμός επίσης επιτρέπει στα κράτη-μέλη τη θέσπιση νομοθεσίας που θα επιβάλει τον ορισμό ΥΠΔ σε επιπλέον περιπτώσεις.

Η έννοια μεγάλη κλίμακα και η έννοια της τακτικής και συστηματικής παρακολούθησης που προαναφέρθηκαν για το πότε ένας οργανισμός είναι υποχρεωμένος να ορίζει κάποιον στη θέση του υπεύθυνου προστασίας δεδομένων δεν ορίζονται ρητά στον ΓΚΠΔ. Η Ομάδα Εργασίας του άρθρου 29 συνιστά τους ακόλουθους παράγοντες για να προσδιοριστεί εάν η επεξεργασία διενεργείται σε μεγάλη κλίμακα ή όχι. Οι παράγοντες αυτοί είναι ο αριθμός των εμπλεκόμενων υποκειμένων των δεδομένων επί του συναφούς πληθυσμού, ο όγκος των δεδομένων ή/και το εύρος των δεδομένων που υφίστανται σε επεξεργασία, η διάρκεια ή ο μόνιμος χαρακτήρας της επεξεργασίας και η γεωγραφική έκταση της δραστηριότητας επεξεργασίας. Τέτοιοι οργανισμοί είναι σίγουρα τα ηλεκτρονικά καταστήματα που καθημερινώς συλλέγουν και επεξεργάζονται χιλιάδες προσωπικά δεδομένα. Επίσης, στον όρο τακτική και συστηματική παρακολούθηση περιλαμβάνονται όλες οι μορφές

παρακολούθησης και διαμόρφωσης προφίλ στο διαδίκτυο, μεταξύ άλλων τα cookies, η αποστολή κουπονιών από ηλεκτρονικά καταστήματα και η συμπεριφορική διαφήμιση.

Σε περιπτώσεις όπου ο ΓΚΠΔ δεν απαιτεί τον ορισμό υπεύθυνου προστασίας δεδομένων η Ομάδα Εργασίας του άρθρου για τη προστασία των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα ενθαρρύνει τους οργανισμούς να ορίσουν κάποιον υπεύθυνο προστασίας δεδομένων σε εθελοντική βάση, προκειμένου να αποτραπεί πιθανή παραβίαση των διατάξεων του Κανονισμού. Σε μία τέτοια περίπτωση ο υπεύθυνος προστασίας δεδομένων αναλαμβάνει όλα τα καθήκοντα και τις αρμοδιότητες της συγκεκριμένης θέσης.

Οργανισμοί που βάσει του Κανονισμού υποχρεούνται να ορίσουν υπεύθυνο προστασίας δεδομένων και δεν επιθυμούν να ορίσουν κάποιον σε εθελοντική βάση μπορούν να απασχολούν υπαλλήλους ή εξωτερικούς συμβούλους. Σε κάθε περίπτωση για να μην υπάρχει σύγχυση ως προς τον τίτλο, το καθεστώς, τη θέση και τα καθήκοντα των εν λόγω υπαλλήλων ή συμβούλων θα πρέπει να διευκρινίζεται στο πλαίσιο της εταιρικής επικοινωνίας, στις αρχές προστασίας δεδομένων, τα υποκείμενα των δεδομένων και το ευρύ κοινό, ότι ο συγκεκριμένος υπάλληλος ή σύμβουλος δεν χαρακτηρίζεται ως ΥΠΔ. Η απόφαση περί οικειοθελούς ή υποχρεωτικού ορισμού ΥΠΔ είναι μια επιχειρησιακή απόφαση, η οποία εξαρτάται από τις ανάγκες και την στρατηγική της κάθε επιχείρησης ή του κάθε οργανισμού.

5.2 Ορισμός κοινού ΥΠΔ

Σε περιπτώσεις ομίλου επιχειρήσεων ο ΓΚΠΔ προβλέπει ρητά στο άρθρο 37 παρ. 2 τη δυνατότητα ορισμού ενός μόνο υπεύθυνου προστασίας δεδομένων υπό την προϋπόθεση ότι ο υπεύθυνος προστασίας δεδομένων έχει εύκολη πρόσβαση σε κάθε εγκατάσταση. Αυτό είναι σημαντικό για το ηλεκτρονικό εμπόριο, καθώς υπάρχουν ηλεκτρονικά καταστήματα που είναι όμιλοι και έχουν πολλά καταστήματα ή αποθήκες με προϊόντα σε διαφορετικές χώρες. Η επιλογή για τον αν θα οριστεί ένας υπεύθυνος προστασίας δεδομένων σε όλον τον όμιλο είναι απόφαση της επιχείρησης, η οποία εξαρτάται από τις ανάγκες της, τη φύση και την έκταση των δραστηριοτήτων επεξεργασίας της, από οικονομικούς παράγοντες, όπως επίσης και από τον βαθμό

ευκολίας στην πρόσβαση που θα έχει ένας υπεύθυνος προστασίας δεδομένων σε κάθε εγκατάσταση. Ο όρος εύκολη πρόσβαση σε κάθε εγκατάσταση αναφέρεται στα καθήκοντα που έχει ο υπεύθυνος προστασίας δεδομένων ως σημείο επικοινωνίας με τα υποκείμενα των δεδομένων, την εποπτική αρχή, αλλά και το εσωτερικού του οργανισμού. Για τον λόγο αυτό είναι σημαντικό η πρόσβαση στον υπεύθυνο προστασίας δεδομένων να γίνεται είτε μέσω φυσικής παρουσίας, είτε μέσω των απαιτούμενων διαύλων επικοινωνίας και τεχνολογικών εργαλείων, είτε άλλου ασφαλούς μέσου επικοινωνίας.

Ο υπεύθυνος προστασίας δεδομένων θα πρέπει να γνωστοποιεί τα στοιχεία επικοινωνίας του εντός του ομίλου επιχειρήσεων, στις εποπτικές αρχές και στα υποκείμενα των δεδομένων. Επίσης, οφείλει να γνωρίζει άψογα την γλώσσα ή, στην περίπτωση πολυεθνικής εταιρείας, τις γλώσσες που χρησιμοποιούν οι εργαζόμενοι της κάθε εταιρείας του ομίλου, οι ενδιαφερόμενες εποπτικές αρχές και τα υποκείμενα των δεδομένων. Τέλος, θα πρέπει να έχει πλήρη εικόνα των δραστηριοτήτων της κάθε εταιρείας του ομίλου και να βρίσκεται σε επικοινωνία με τα τμήματα της κάθε εταιρείας που εμπλέκονται στην επεξεργασία προσωπικών δεδομένων.

5.3 Καθήκοντα του υπεύθυνου προστασίας δεδομένων

Τα καθήκοντα και οι αρμοδιότητες του υπεύθυνου προστασίας δεδομένων ορίζονται στο άρθρο 39 του ΓΚΠΔ. Συγκεκριμένα, ο υπεύθυνος προστασίας δεδομένων έχει το καθήκον να ενημερώνει και να συμβουλεύει όλους τους υπαλλήλους που επεξεργάζονται δεδομένα, τον εκτελούντα την επεξεργασία και τον υπεύθυνο επεξεργασίας για τις υποχρεώσεις τους ως προς τον ΓΚΠΔ, αλλά ακόμα και τις υποχρεώσεις τους σε άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων. Επιπροσθέτως, μια από τις σημαντικότερες αρμοδιότητες του είναι η παρακολούθηση της συμμόρφωσης με τον ΓΚΠΔ και με άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων. Στο πλαίσιο των καθηκόντων παρακολούθησης, ο υπεύθυνος προστασίας δεδομένων καλείται να συλλέγει πληροφορίες για τον προσδιορισμό δραστηριοτήτων επεξεργασίας, να αναλύει και να ελέγχει τις δραστηριότητες επεξεργασίας, να παρέχει συμβουλές και να ενημερώνει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία.

Σύμφωνα με το άρθρο 35 παράγραφος 1 του ΓΚΠΔ, είναι καθήκον του υπεύθυνου επεξεργασίας η διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων και όχι του υπεύθυνου προστασίας δεδομένων. Ωστόσο, ο υπεύθυνος επεξεργασίας, σύμφωνα με το άρθρο 35 παράγραφος 2, μπορεί να ζητήσει τη γνώμη του υπεύθυνου προστασίας δεδομένων κατά την διάρκεια αυτής της διαδικασίας, ενώ, σύμφωνα με το άρθρο 39 παράγραφος 1 στοιχείο γ), ο υπεύθυνος προστασίας δεδομένων έχει το καθήκον να παρέχει συμβουλές όσον αφορά την εκτίμηση αντικτύπου. Συγκεκριμένα, η Ομάδα Εργασίας του άρθρου 29 συνιστά να ζητεί ο υπεύθυνος επεξεργασίας τη γνώμη του υπεύθυνου προστασίας δεδομένων για τα ακόλουθα ζητήματα :

> «εάν πρέπει ή όχι να διενεργήσει εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων, για το ποια μεθοδολογία πρέπει να ακολουθήσει κατά την διενέργεια της εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων, εάν πρέπει να διενεργήσει την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων εσωτερικά ή να την αναθέσει σε εξωτερικό συνεργάτη, τι εγγυήσεις (περιλαμβανομένων των τεχνικών και οργανωτικών μέτρων) πρέπει να εφαρμόσει προκειμένου να μετριαστούν οι κίνδυνοι για τα δικαιώματα και τα συμφέροντα των υποκειμένων των δεδομένων, εάν διενεργήθηκε σωστά ή όχι η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και εάν τα συμπεράσματα της (σχετικά με το εάν θα δοθεί ή όχι συνέχεια στην επεξεργασία και τι εγγυήσεις θα εφαρμοστούν) είναι σύμφωνα με το ΓΚΠΔ»

Μια ακόμη υποχρέωση του υπεύθυνου προστασίας δεδομένων είναι, σύμφωνα με το άρθρο 39 παράγραφος 1 στοιχείο δ) και ε), να συνεργάζεται με την εποπτική αρχή και να ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή. Ο υπεύθυνος προστασίας δεδομένων οφείλει να έχει τον ρόλο διαμεσολαβητή μεταξύ της εποπτικής αρχής και του οργανισμού. Θα πρέπει να διευκολύνει την πρόσβαση της εποπτικής αρχής στα έγγραφα και τις πληροφορίες που σχετίζονται με την επιτέλεση των καθηκόντων. Ακόμα, ο υπεύθυνος προστασίας δεδομένων ανάλογα με την περίπτωση και για οποιοδήποτε άλλο θέμα κρίνει ο ίδιος δύναται να

πραγματοποιεί διαβουλεύσεις με την εποπτική αρχή.

5.4 Ευθύνη ΥΠΔ

Ο υπεύθυνος προστασίας δεδομένων, όπως προβλέπεται από τον ΓΚΠΔ, δεν φέρει ευθύνη για την ορθή επεξεργασία των δεδομένων. Ο ΓΚΠΔ καθιστά σαφές ότι είναι ευθύνη του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον Κανονισμό (άρθρο 24 παρ. 1). Ωστόσο, ο υπεύθυνος προστασίας δεδομένων οφείλει να εκτελεί τα καθήκοντα του με επιμέλεια και με γνώμονα την προστασία των υποκειμένων των δεδομένων. Αν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία λαμβάνει αποφάσεις που έρχονται σε σύγκρουση με τον ΓΚΠΔ και με τις συμβουλές του υπεύθυνου προστασίας δεδομένων, τότε ο υπεύθυνος προστασίας δεδομένων θα πρέπει να έχει τη δυνατότητα να γνωστοποιήσει την αντίθετη γνώμη του στο ανώτατο διοικητικό επίπεδο του οργανισμού και στους υπευθύνους λήψης αποφάσεων (άρθρο 38 παρ. 3).

6. Πολιτική Απορρήτου

6.1 Τι είναι η πολιτική απορρήτου

Πολιτική απορρήτου είναι μια από τις πιο σημαντικές νομικές απαιτήσεις για τους ιστότοπους. Κάθε οργανισμός που έχει ιστοσελίδα και που συλλέγει προσωπικά δεδομένα από υποκείμενα της ΕΕ χρειάζεται μια πολιτική απορρήτου. Πιο συγκεκριμένα, είναι ένα δημόσιο έγγραφο που θα πρέπει να δημοσιευτεί στην ιστοσελίδα του οργανισμού, ώστε να είναι εύκολα προσβάσιμο από τους επισκέπτες της ιστοσελίδας. Το έγγραφο αυτό θα πρέπει να εξηγεί πώς ο οργανισμός επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα και πώς εφαρμόζει τις αρχές προστασίας δεδομένων σε απλή, εύκολα κατανοητή και ευανάγνωστη γλώσσα. Η πολιτική απορρήτου συνδέεται άμεσα με το δικαίωμα των υποκειμένων στην ενημέρωση. Αν και ο ΓΚΠΔ δεν διευκρινίζει πώς ακριβώς πρέπει να είναι δομημένο το έγγραφο, μέσα από τα άρθρα 12, 13 και 14 ορίζονται έμμεσα ποιες πληροφορίες πρέπει να περιέχει η πολιτική απορρήτου που μοιράζεται ένας οργανισμός με τα υποκείμενα των δεδομένων. Η μη συμμόρφωση του οργανισμού μπορεί να επιφέρει υψηλά πρόστιμα. Στο ηλεκτρονικό εμπόριο, όπου οι οργανισμοί χρησιμοποιούν έναν ιστότοπο για την ολοκλήρωση των αγορών από τους χρήστες, θα πρέπει υποχρεωτικά να έχουν δημοσιεύσει μια πολιτική απορρήτου στην ιστοσελίδα τους.

6.2 Τι πρέπει να περιέχει η πολιτική απορρήτου

Όπως αναφέρθηκε προηγουμένως, ο ΓΚΠΔ δεν ορίζει τι πρέπει να περιέχει η πολιτική απορρήτου. Ωστόσο, κάποια από τα βασικά κεφάλαιο που είναι απαραίτητο να περιέχει το έγγραφο της πολιτικής απορρήτου παρουσιάζονται παρακάτω.

6.2.1 Τι δεδομένα συλλέγονται

Στο συγκεκριμένο κεφάλαιο, ο οργανισμός πρέπει να αναφέρει αναλυτικά ποια δεδομένα συλλέγει. Για παράδειγμα, ένα ηλεκτρονικό κατάστημα πρέπει να

αναφέρει ότι συλλέγει από το υποκείμενο το ονοματεπώνυμο, την διεύθυνση ηλεκτρονικού ταχυδρομείου, την φυσική διεύθυνση, το τηλέφωνο και οτιδήποτε άλλο συλλέγει από το υποκείμενο.

6.2.2 Πώς συλλέγονται τα δεδομένα

Ο οργανισμός πρέπει να αναφέρει όλους τους τρόπους με τους οποίους συλλέγει προσωπικά δεδομένα. Για παράδειγμα, ένα ηλεκτρονικό κατάστημα θα πρέπει να γράφει ότι τα δεδομένα συλλέγονται μεταξύ άλλων όταν κάποιος χρήστης κάνει εγγραφή στην ιστοσελίδα του καταστήματος, όταν κάνει μια αξιολόγηση σε κάποιο προϊόν, όταν στέλνει κάποιο ηλεκτρονικό μήνυμα, όταν επισκέπτεται την ιστοσελίδα, καθώς και όταν το ηλεκτρονικό κατάστημα χρησιμοποιεί cookies. Επίσης, είναι σημαντικό να αναφέρονται και όλες οι πηγές που μπορεί να μεταβιβάζουν δεδομένα στο ηλεκτρονικό κατάστημα.

6.2.3 Πώς επεξεργάζονται τα δεδομένα

Στο κεφάλαιο αυτό ο οργανισμός πρέπει να περιγράψει την επεξεργασία που γίνεται στα δεδομένα που συλλέγονται. Το ηλεκτρονικό κατάστημα γνωστοποιεί πώς ο οργανισμός συλλέγει τα δεδομένα, ώστε να γίνει η ολοκλήρωση της παραγγελίας και διαχείρισης του προφίλ του χρήστη, για την αποστολή email όταν ολοκληρωθεί κάποια παραγγελία με τα στοιχεία της παραγγελίας αυτής ή με την αποστολή email για προσφορές με τα προϊόντα ή τις υπηρεσίες που πιθανόν να ενδιαφέρουν τον χρήστη, το τηλέφωνο του χρήστη σε περίπτωση που προκύψει κάποιο πρόβλημα με την παραγγελία και όλους τους τρόπους που το ηλεκτρονικό κατάστημα επεξεργάζεται τα δεδομένα. Ακόμα, το ηλεκτρονικό κατάστημα θα πρέπει να αναφέρει ότι μεταβιβάζει κάποια από τα δεδομένα που έχει συλλέξει σε τρίτους, όπως είναι η μεταφορική εταιρεία που συνεργάζεται για την αποστολή των παραγγελιών στους χρήστες ή όπως είναι κάποιο σύστημα πληρωμής για την πρόληψη της απάτης.

6.2.4 Πώς αποθηκεύονται τα δεδομένα

Στο σημείο αυτό πρέπει να αναφερθεί πώς ο οργανισμός αποθηκεύει τα δεδομένα που έχουν συλλεχθεί. Πρέπει να αναφερθεί πού αποθηκεύτηκαν και ποιο είναι το μέτρο προστασίας που έχει χρησιμοποιήσει ο οργανισμός. Επιπλέον, πρέπει να γράφει τον τύπο δεδομένων αποθηκεύει, το ακριβές χρονικό διάστημα που θα μείνουν αποθηκευμένα τα δεδομένα αυτά μέχρι να διαγραφτούν, καθώς και ο τρόπος που θα διαγραφτούν.

6.2.5 Marketing

Το μάρκετινγκ είναι ένα πολύ σημαντικό κομμάτι για τους οργανισμούς και ειδικότερα για τα ηλεκτρονικά καταστήματα που υπάρχουν στην Ελλάδα, αλλά και στον κόσμο. Μέσω αυτού προσελκύονται όλο και περισσότεροι χρήστες να επιλέξουν κάποιο κατάστημα έναντι των ανταγωνιστών του. Για να μπορέσει όμως το marketing να είναι αποτελεσματικό θα πρέπει να γίνεται επεξεργασία των δεδομένων, άρα είναι σημαντικό να αναφερθεί στο έγγραφο της πολιτικής απορρήτου. Το εν λόγω κατάστημα θα πρέπει να αναφέρει πως ίσως στέλνει στο μέλλον προσφορές και εκπτώσεις για τα προϊόντα και τις υπηρεσίες που νομίζει ότι θα αρέσουν στους πελάτες. Θα πρέπει να αναφερθεί το δικαίωμα που έχει το υποκείμενο ανά πάσα στιγμή να εμποδίσει την εταιρεία να επικοινωνεί μαζί του για σκοπούς μάρκετινγκ και να παρέχεται κάποιος σύνδεσμος, προκειμένου να γίνει πιο εύκολη η διαδικασία της διακοπής.

6.2.6 Δικαιώματα του υποκειμένου

Στο κεφάλαιο αυτό θα πρέπει να γίνεται αναφορά σε όλα τα δικαιώματα που έχει το υποκείμενο. Πρέπει να γίνει αναλυτική περιγραφή των δικαιωμάτων αυτών, ώστε το υποκείμενο να έχει πλήρη γνώση. Τα έξι δικαιώματα που έχει το υποκείμενο των δεδομένων, πέραν από το δικαίωμα της ενημέρωσης που πραγματοποιείται με το έγγραφο της πολιτικής απορρήτου, είναι το δικαίωμα πρόσβασης, το δικαίωμα

διόρθωσης, το δικαίωμα διαγραφής, το δικαίωμα περιορισμού της επεξεργασίας, το δικαίωμα φορητότητας, το δικαίωμα εναντίωσης και το δικαίωμα στην ανθρώπινη παρέμβαση. Τέλος ο οργανισμός πρέπει να αναφέρει στο υποκείμενο ότι αν θελήσει να ασκήσει κάποια από τα δικαιώματα του η απάντηση αναμένεται εντός ενός μήνα.

6.2.7 Cookies

Τα cookies είναι και αυτά ένα σημαντικό μέρος για τις ιστοσελίδες στο διαδίκτυο. Ο οργανισμός σε αυτό το κεφάλαιο της πολιτικής απορρήτου θα πρέπει να αναφέρει τους σκοπούς για τους οποίους χρησιμοποιεί τα cookies, για παράδειγμα κάποιοι λόγοι μπορεί να είναι για να μένει ο χρήστης συνδεδεμένος στο προφίλ του ή για να μπορέσει ο διαχειριστής του ιστότοπου να αξιολογήσει πώς χρησιμοποιούν οι χρήστες τον ιστότοπο και στη συνέχεια να κάνει τις απαραίτητες αλλαγές, προκειμένου να γίνει η περιήγηση του χρήστη πιο εύκολη. Επίσης, ο οργανισμός οφείλει να αναφέρει το είδος των cookies που χρησιμοποιεί, καθώς και μια περιγραφή των cookies αυτών. Κάποιες από τις κατηγορίες χρήσης των cookies που ενδέχεται να χρησιμοποιεί η ιστοσελίδα ενός ηλεκτρονικού καταστήματος είναι η κατηγορία μάρκετινγκ για να γίνουν οι διαφημίσεις πιο ελκυστικές για τους χρήστες, η κατηγορία λειτουργικότητα που χρησιμοποιεί ένας ιστότοπος για να αναγνωρίσει τους χρήστες και να θυμάται τις προτιμήσεις που έχει επιλέξει ο χρήστης προηγουμένως. Τέλος, θα πρέπει να αναφέρει ότι ο χρήστης έχει τη δυνατότητα να μην δέχεται τα cookies από το πρόγραμμα περιήγησής του, άλλα να του γίνεται κατανοητό ότι κάποιες από τις λειτουργίες της ιστοσελίδας ενδέχεται να μην λειτουργούν αποτελεσματικά.

6.2.8 Τρόποι επικοινωνίας

Στο σημείο αυτό θα πρέπει να αναγράφονται από τον οργανισμό που αναρτά το έγγραφο της πολιτικής απορρήτου όλους τους τρόπους με τους οποίους κάποιος χρήστης θα μπορέσει να επικοινωνήσει με τον οργανισμό για οποιοδήποτε λόγο, είτε αυτός είναι για απορίες με την πολιτική απορρήτου είτε απορίες και ερωτήσεις για τα δεδομένα που συλλέγονται και επεξεργάζονται, είτε για λόγους άσκησης των

δικαιωμάτων του, είτε και για λόγους πέραν τον προσωπικών δεδομένων και την επεξεργασία αυτών. Οι συνήθεις τρόποι επικοινωνίας είναι το email του οργανισμού, το τηλέφωνο και η φυσική διεύθυνση, όταν υφίσταται, του οργανισμού.

6.2.9 Τρόπος επικοινωνίας της Αρχής

Στο τελευταίο αυτό κεφάλαιο της πολιτικής απορρήτου, ο οργανισμός είναι σημαντικό να αναφέρει στον χρήστη πώς μπορεί να επικοινωνήσει με την δημόσια Αρχή αν θελήσει να αναφέρει κάποιο πρόβλημα που είχε με τον οργανισμό όσον αφορά θέματα με τα προσωπικά του δεδομένα. Θα πρέπει ο οργανισμός να γνωστοποιήσει όλους τους τρόπους που μπορεί να επικοινωνήσει ο χρήστης με την Δημόσια Αρχή, όπως είναι το τηλέφωνο, το email ή οποιοσδήποτε άλλος τρόπος.

6.3 Αξιολόγηση δειγματοληπτικών Πολιτικών Απορρήτου

6.3.1 E-shop

Η πρώτη αξιολόγηση της πολιτικής απορρήτου εστιάζεται στο ηλεκτρονικό κατάστημα E-Shop, το οποίο έχει αποθήκες με προϊόντα σε πολλές περιοχές της Ελλάδας. Η ιστοσελίδα του ηλεκτρονικού καταστήματος είναι (https://www.e-shop.gr) όπου στο κάτω μέρος της ιστοσελίδας υπάρχει link για τους όρους χρήσης, το οποίο μεταφέρει τους πελάτες στην πολιτική απορρήτου. Στη νέα αυτή διεύθυνση (https://www.e-shop.gr/protection) που είναι χωρισμένη σε κεφάλαια, ο χρήστης μπορεί να ενημερωθεί για διάφορα θέματα. Ένα από αυτά είναι η Προστασία Προσωπικών Δεδομένων, το οποίο και αυτό χωρίζεται σε υποκεφάλαια. Με μια πρώτη ματιά το κύριο αρνητικό της συγκεκριμένης πολιτικής απορρήτου είναι τα μικρά γράμματα και η μικρή απόσταση μεταξύ των γραμμών, το οποίο δυσκολεύει την ανάγνωση της από τους χρήστες.

Σε θέματα που αφορούν τις απαιτήσεις του ΓΚΠΔ και το δικαίωμα του πελάτη στην ενημέρωση, η πολιτική απορρήτου του συγκεκριμένου καταστήματος είναι αρκετά περιεκτική. Στο υποκεφάλαιο «Συγκέντρωση πληροφοριών» το

ηλεκτρονικό κατάστημα αναφέρει αναλυτικά όλους τους τρόπους με τους οποίους συλλέγει τα προσωπικά δεδομένα και ποια δεδομένα είναι αυτά. Συγκεκριμένα, αναφέρει ότι συλλέγει δεδομένα κατά την εγγραφή ενός πελάτη, στοιχεία που δίνει ο πελάτης προκειμένου να εκτελεστεί η παραγγελία του, στοιχεία που δίνει ο πελάτης όταν συμμετέχει σε διαγωνισμούς κ.α. Στη συνέχεια, το ηλεκτρονικό κατάστημα έχει διαφορετικό υποκεφάλαιο για το πώς επεξεργάζονται τα δεδομένα με τίτλο «Χρήση προσωπικών δεδομένων», που σε αυτό αναφέρει όλους τους σκοπούς και τους τρόπους που επεξεργάζονται τα δεδομένα. Στο υποκεφάλαιο αυτό το ηλεκτρονικό κατάστημα αναφέρει πώς μόνο με την παροχή της συγκατάθεσης από τον χρήστη θα χρησιμοποιηθούν τα προσωπικά του στοιχεία πέρα από τους αρχικούς σκοπούς που αφορούν την ολοκλήρωση της παραγγελίας, όπως για παράδειγμα για σκοπούς μάρκετινγκ. Για τον τρόπο αποθήκευσης των δεδομένων προσωπικού χαρακτήρα δεν γίνεται κάποια συγκεκριμένη αναφορά από το ηλεκτρονικό κατάστημα. Στο υποκεφάλαιο «Διατήρηση των προσωπικών σας δεδομένων» το e-shop αναφέρει ότι τα προσωπικά δεδομένα θα διαγραφούν αν δεν είναι πλέον αναγκαία για τους σκοπούς που συλλέχθηκαν αρχικώς, εκτός κι αν υπάρχουν νομικά ζητήματα ή αν ο χρήστης βρίσκεται στην λίστα που το e-shop διατηρεί με όλους όσους δεν επιθυμούν επικοινωνία στο μέλλον.

Για το θέμα τον νομικών δικαιωμάτων του πελάτη στο υποκεφάλαιο «Τα νόμιμα δικαιώματά σας» γίνεται πλήρη αναφορά και περιγραφή όλων των δικαιωμάτων που ορίζονται από τον ΓΚΠΔ. Ακολούθως, στο τέλος του κεφαλαίου το e-shop παρέχει τρόπο επικοινωνίας με τον ΥΠΔ σε περίπτωση που ο πελάτης θελήσει να ασκήσει κάποιο ή κάποια από τα δικαιώματα του. Στη συνέχεια, για το θέμα των cookies το ηλεκτρονικό κατάστημα με συγκεκριμένο υποκεφάλαιο ορθώς αναφέρει την σημασία των cookies, τί είναι, για ποιον λόγο το ηλεκτρονικό κατάστημα κάνει την χρήση των cookies και ποιες κατηγορίες των cookies χρησιμοποιεί. Ακόμα, αναφέρει ότι υπάρχουν τρίτες συνεργαζόμενες εταιρείες που κάνουν χρήση δικών τους cookies και πώς αυτά δεν ελέγχονται από το e-shop. Τέλος, αυτό που δεν υπάρχει από την συγκεκριμένη πολιτική απορρήτου είναι ο τρόπος επικοινωνίας με την Αρχή Προστασίας Δεδομένων της Ελλάδας. Το τελικό συμπέρασμα για την πολιτική απορρήτου της ιστοσελίδας του e-shop είναι πώς είναι ως επί το πλείστον συμμορφωμένη με τον ΓΚΠΔ και ότι τηρεί τις περισσότερες απαιτήσεις για το δικαίωμα ενημέρωσης του πελάτη.

6.3.2 Public

Η δεύτερη αξιολόγηση αφορά στην πολιτική απορρήτου των καταστημάτων Public που, πέρα από το φυσικά καταστήματα που έχουν σε όλη τη χώρα, διαθέτουν και ιστοσελίδα για ηλεκτρονικό εμπόριο (https://www.public.gr). Ο πελάτης μπορεί να δει την πολιτική απορρήτου του συγκεκριμένου καταστήματος στο κάτω μέρος της ιστοσελίδας και στη συνέχεια μεταφέρεται στην παρακάτω ιστοσελίδα (https://www.public.gr/cat/corporate/oroi/politiki-aporritoy/). Εκ πρώτης όψεως η πολιτική απορρήτου είναι ευκρινώς διαμορφωμένη, δηλαδή με αριθμημένα κεφάλαια, και εύκολη οπτικά για ανάγνωση από τον χρήστη.

Αναλυτικότερα, στα κεφάλαια 4 και 5 της πολιτικής απορρήτου αναφέρονται ποια δεδομένα συλλέγονται από την ιστοσελίδα και για ποιους σκοπούς γίνεται η συλλογή τους. Επίσης, στο κεφάλαιο 5 υπάρχει συγκεκριμένος σύνδεσμος που μεταφέρει τους χρήστες σε διαφορετική ιστοσελίδα (Πολιτική cookies), όπου σε αυτή γίνεται ανάλυση για όλα τα θέματα που αφορούν τα cookies και τη χρήση τους από το ηλεκτρονικό κατάστημα Public. Στη συνέχεια, στα κεφάλαια 6 και 7 τα Public αναφέρουν λεπτομερώς, με την χρήση υποκεφαλαίων και διαχωριστικών bullet, τον τρόπο που χρησιμοποιούνται τα δεδομένα που συλλέγονται από τους χρήστες και για ποιους σκοπούς γίνεται η επεξεργασία τους. Στο κεφάλαιο 9 και 11 τα Public γνωστοποιούν αναλυτικά όλους τους αποδέκτες των δεδομένων και στην ενότητα 10 περιγράφεται ο τρόπος εξασφάλισης της προστασίας των δεδομένων από τους εκτελούντες την επεξεργασία. Μέσα από το κεφάλαιο 12 οι χρήστες ενημερώνονται για το χρονικό διάστημα που τα προσωπικά τους δεδομένα παραμένουν αποθηκευμένα, ενώ μέσα από το επόμενο κεφάλαιο τον τρόπο που τα Public διαφυλάσσουν τα δεδομένα των χρηστών. Συγκεκριμένα, τα Public χρησιμοποιούν πρωτόκολλο TLS για τις ασφαλείς ηλεκτρονικές εμπορικές συναλλαγές. Με τον τρόπο αυτό, κρυπτογραφούνται όλα τα δεδομένα που παρέχει ο χρήστης, όπως είναι το όνομα, η διεύθυνση και ο αριθμός πιστωτικής κάρτας, ώστε να μην μπορούν να αποκρυπτογραφηθούν ή να τροποποιηθούν με την μεταφορά τους στο διαδίκτυο.

Ακολούθως, όπως είναι απαραίτητο από κάθε ηλεκτρονικό κατάστημα, τα Public στο κεφάλαιο 14 περιγράφουν και αναλύουν όλα τα δικαιώματα που έχουν οι χρήστες και στην επόμενη ενότητα παρουσιάζουν τους τρόπους επικοινωνίας με το

ηλεκτρονικό κατάστημα, για να ασκήσουν τα δικαιώματα αυτά, εφόσον το επιθυμούν. Ακολούθως, στο κεφάλαιο 16 γίνεται λόγος για το πώς και το πότε τα Public απαντάνε στα αιτήματα που αποστέλλουν οι χρήστες. Τέλος, σημαντικό για την πολιτική απορρήτου είναι το κεφάλαιο 18, στο οποίο υπάρχει ο τρόπος επικοινωνίας με την Αρχή Προστασίας Προσωπικών Δεδομένων. Συνοψίζοντας, η πολιτική απορρήτου των καταστημάτων Public συμμορφώνεται πλήρως με τον ΓΚΠΔ και τηρεί το δικαίωμα του καταναλωτή για ενημέρωση. Συνεπώς θα πρέπει να θεωρείται παράδειγμα για τα υπόλοιπα ηλεκτρονικά καταστήματα.

6. Cookies

6.1 Ιστορική αναδρομή

Για να μπορέσει να γίνει κατανοητή η έννοια των cookies και η επιρροή αυτών στους χρήστες του διαδικτύου, θα πρέπει πρώτα να γίνει μια ιστορική αναδρομή. Τα cookies εφευρέθηκαν από τον προγραμματιστή Lou Montulli το 1994, ο οποίος εργαζόταν για το πρόγραμμα περιήγησης Netscape, το οποίο ήταν από τα μεγαλύτερα εκείνης της εποχής. Το Netscape ήθελε να δημιουργήσει "μάτια και αυτιά" για τα ηλεκτρονικά καταστήματα και έτσι δημιουργήθηκαν τα cookies. Τα cookies θα έμοιαζαν με έναν υπάλληλο σε ένα ηλεκτρονικό κατάστημα, ο οποίος θα ήταν σε θέση να εκτιμήσει την αγοραστική συμπεριφορά ενός ατόμου. Ωστόσο, ο Montulli προσπάθησε να εξελίξει αυτή την ιδέα, θέλοντας πέρα από τα μάτια και τα αυτιά να δώσει στην ιστοσελίδα και μνήμη. Η μνήμη θα θυμόταν τους χρήστες και τις προσωπικές τους πληροφορίες από την πρώτη επίσκεψη τους σε μια ιστοσελίδα. Με την βοήθεια των λειτουργιών της μνήμης, αποθηκεύονταν οι πληροφορίες, ακόμα και όταν αποσυνδεόταν ή εξερχόταν ο χρήστης από τον ιστότοπο, με σκοπό η εμπειρία του να γίνει καλύτερη και πιο λειτουργική. Από την αρχή τα cookies ήταν ένα απλό εργαλείο, που επέτρεπε σε έναν ιστότοπο να παρακολουθεί τις δραστηριότητες μόνο ενός χρήστη τη φορά.

Το όνομα cookie προήλθε από τον ήδη υπάρχοντα όρο στον προγραμματισμό magic cookies, ο οποίος χρησιμοποιείται για να περιγράψει τη διαδικασία κατά την οποία ένα σύστημα δέχεται δεδομένα και στη συνέχεια τα στέλνει χωρίς να τα έχει αλλάξει. Στα τέλη της δεκαετίας του 1990 άρχισαν και άλλες εταιρείας να πειραματίζονται και να αναπτύσσουν νέες λειτουργίες για τα cookies. Τελικά, τα cookies μπορούσαν να παρακολουθούν τις δραστηριότητες πολλών χρηστών σε διάφορους ιστότοπους, καταφέρνοντας να δημιουργήσουν ένα πλήρες προφίλ για κάθε χρήστη. Στη συνέχεια, οι εταιρείες παρακολουθούσαν τις τιμές που είχαν καταγραφεί από τα cookies, με αποτέλεσμα να είναι σε θέση να γνωρίζουν τις προτιμήσεις των χρηστών. Γνωρίζοντας τις προτιμήσεις των χρηστών, οι εταιρείες πλέον μπορούσαν να δώσουν στους πελάτες τους πιο σχετικές διαφημίσεις, οι οποίες οδηγούν σε ευκαιρίες πωλήσεων. Σήμερα η καινοτομία αυτή, που ανέπτυξε ο

Montulli, χρησιμοποιείται από όλα τα προγράμματα περιήγησης και παρέχει πλεονεκτήματα τόσο στους χρήστες όσο και στους οργανισμούς που την αξιοποιούν.

6.2 Γενικές Πληροφορίες των cookies

Στη μελέτη που πραγματοποιήθηκε από τον ENISA το 2010, το 80% των παρόχων υπηρεσιών διαδικτύου συλλέγει δεδομένα από τα cookies. Αυτή η έρευνα πραγματοποιήθηκε πριν περίπου 10 χρόνια και μπορούμε να φανταστούμε πως αυτό το ποσοστό ίσως αγγίζει το 100% στην σημερινή εποχή, με τις τεχνολογικές εξελίξεις στο χρονικό αυτό διάστημα. Οι περισσότερες εταιρείες χρησιμοποιούν τα cookies ως ένα εργαλείο για τις ιστοσελίδες τους για να ενισχύσουν την ευκολία τόσο των χρηστών όσο και των ίδιων των εταιρειών. Τα cookies είναι αρχεία κειμένου ή HTTP (Hypertext Transfer Protocol). Όταν ένας χρήστη επισκέπτεται κάποιον ιστότοπο, το πρόγραμμα περιήγησης ζητά από τον ιστότοπο την εν λόγω διαδικτυακή τοποθεσία της ιστοσελίδας. Στη συνέχεια, ο διακομιστής εντοπίζει και αποστέλλει την ιστοσελίδα μαζί με κάποια δεδομένα. Η σελίδα που λαμβάνει το πρόγραμμα περιήγησης από τον διακομιστή είναι αυτή που εμφανίζεται στον χρήστη, ενώ τα δεδομένα που στάλθηκαν μαζί με την σελίδα είναι τα cookies. Τα δεδομένα αυτά αποθηκεύονται στον υπολογιστή του χρήστη και χρησιμοποιούνται κάθε φορά που επισκέπτεται την ίδια ιστοσελίδα, εκτός αν ο χρήστης διαγράψει τα cookies μετά από κάθε επίσκεψη του στη σελίδα. Τα δεδομένα που αποθηκεύονται στα αρχεία κειμένου διαφέρουν ανάμεσα στους ιστότοπους και οι αποθηκευμένες πληροφορίες εξαρτώνται αποκλειστικά και μόνο από το τι θέλει να αποθηκεύσει ο ιδιοκτήτης του ιστότοπου.

Τα cookies λειτουργούν ως αναγνωριστικό, δηλαδή θυμούνται το όνομα του κάθε χρήστη ξεχωριστά, το οποίο δεν είναι το πραγματικό, αλλά ένα κωδικό για αυτόν, όπως είναι για παράδειγμα το “user=1856”. Κάποιες από τις πληροφορίες που μπορεί να αποθηκεύονται είναι η χώρα, η γλώσσα προτίμησης και ο κωδικός σύνδεσης. Συγκεκριμένα, στο ηλεκτρονικό εμπόριο οι πληροφορίες που μπορεί να αποθηκεύονται είναι τα στοιχεία στο καλάθι αγορών, τα μεγέθη, εάν πρόκειται για ένα ηλεκτρονικό κατάστημα με ρούχα, ή η προτίμηση σε μια γλώσσα, αν το ηλεκτρονικό κατάστημα βρίσκεται εκτός της χώρας του χρήστη, όπως επίσης άλλα φίλτρα που παρέχονται στην ιστοσελίδα.

Η καθημερινή ηλεκτρονική δραστηριότητα καθίσταται πολύ πιο εύκολη και λειτουργική με τη χρήση του cookies. Αντί να πρέπει κάθε φορά ο χρήστης να επιλέγει την γλώσσα της αρεσκείας του ή να συνδέεται στον λογαριασμό του, οι πληροφορίες ανακτώνται αυτόματα από το cookie που έχει αποθηκευτεί στη συσκευή του. Ωστόσο, οι λειτουργίες των cookies υπερβαίνουν κατά πολύ τις τεχνικώς απαραίτητες, καθώς μπορούν να επιτρέπουν ένα ευρύτερο φάσμα λειτουργιών, από την προβολή οπτικοακουστικού περιεχομένου και τον διαμοιρασμό ενός άρθρου στα μέσα κοινωνικής δικτύωσης μέχρι την ανάλυση συμπεριφοράς των χρηστών και την προβολή εξατομικευμένων διαφημίσεων (Βασίλης Καρκατζούνης, 2019).

6.3 Τύποι των cookies

Τα cookies χωρίζονται σε τέσσερις βασικές κατηγορίες, οι οποίες είναι αποδεκτές και αναγνωρισμένες από την Ομάδα Εργασίας του άρθρου 29, τα «προσωρινά», τα «έμμονα», καθώς και τα «πρώτου μέρους» και «τρίτου μέρους». Στη σύγχρονη διαδικτυακή πραγματικότητα χρησιμοποιείται εκτενώς η διάκριση των cookies που προέρχεται από το Διεθνές Εμπορικό Επιμελητήριο (International Chamber of Commerce) του Ηνωμένου Βασιλείου. Σύμφωνα με την κατηγοριοποίηση αυτή, τα cookies διακρίνονται σε «αυστηρώς απαραίτητα», «επιδόσεων» και «στόχευσης ή διαφήμισης». Ο διαχωρισμός αυτός δεν συνάδει με τη νομική αξιολόγηση των cookies, αλλά αποτελεί μια βάση, προκειμένου να καταστεί εύκολα κατανοητή η λειτουργία των cookies στους χρήστες.

6.3.1 Έμμονα cookies

Τα έμμονα ή αλλιώς επίμονα cookies είναι αυτά που αποθηκεύονται στη συσκευή ενός χρήστη τη στιγμή που επισκέπτεται μια ιστοσελίδα και παραμένουν αποθηκευμένα και μετά το κλείσιμο του προγράμματος περιήγησης. Τα cookies αυτά ενεργοποιούνται αυτόματα κάθε φορά που ο χρήστης ανοίξει εκ νέου το πρόγραμμα περιήγησης του. Για την απαλλαγή από αυτά τα cookies ο χρήστης θα πρέπει είτε ο ίδιος να τα διαγράψει είτε να περιμένει μέχρι την ημερομηνία λήξης τους, η οποία εξαρτάται από τον δημιουργό τους. Ένα παράδειγμα των επίμονων cookies σε κάποιο

ιστότοπο ενός ηλεκτρονικού καταστήματος είναι η απομνημόνευση του προφίλ του χρήστη, έτσι ώστε όταν μετά από κάποιο διάστημα, αφού έχει κλείσει το πρόγραμμα περιήγησης του, θελήσει να κάνει καινούρια αγορά από το ίδιο κατάστημα, η σύνδεση με το προφίλ του πραγματοποιείται αυτόματα χωρίς να απαιτείται επιπλέον ενέργεια από το άτομο. Εάν τα επίμονα cookies παρακολουθούν δεδομένα που ορίζονται ως προσωπικά σύμφωνα με τον ΓΚΠΔ, τότε η συγκατάθεση του χρήστη είναι απαραίτητη για τη χρήση τους.

6.3.2 Προσωρινά cookies

Τα προσωρινά ή αλλιώς παροδικά cookies έχουν τις ίδιες δυνατότητες με τα μόνιμα cookies. Η μόνη διαφορά τους είναι η χρονική περίοδος που παραμένουν αποθηκευμένες οι πληροφορίες του χρήστη. Τα παροδικά cookies αποθηκεύουν τις πληροφορίες που δημιουργούνται κατά τη διάρκεια της επίσκεψης του χρήστη στην ιστοσελίδα, προκειμένου να διευκολυνθεί η εμπειρία του χρήστη κατά την χρονική διάρκεια της επίσκεψης του. Μόλις ο χρήστης εγκαταλείψει την ιστοσελίδα ή κλείσει το πρόγραμμα περιήγησης, οι πληροφορίες που έχουν δημιουργηθεί θα διαγραφούν αυτόματα. Ένα τέτοιο παράδειγμα των cookies αυτών είναι οι ιστοσελίδες των τραπεζών, όπου οι χρήστες κάθε φορά καλούνται να καταχωρήσουν τα στοιχεία σύνδεσης τους για να αποκτήσουν πρόσβαση στο προφίλ τους. Ένα άλλο παράδειγμα στον τομέα του ηλεκτρονικού εμπορίου είναι τα cookies αυτά που χρησιμοποιούνται για την διατήρηση στοιχείων στο καλάθι αγορών. Τα cookies αυτά σπάνια υπόκεινται στον ΓΚΠΔ, καθώς δεν χρησιμοποιούνται για την παρακολούθηση των προσωπικά δεδομένων του χρήστη, αλλά για την απαραίτητη λειτουργία του ιστότοπου.

6.3.3 Cookies πρώτου μέρους

Τα cookies πρώτου μέρους ανήκουν και εκδίδονται από τον ίδιο τον ιστότοπο και χρησιμοποιούνται από την ιστοσελίδα για να δώσουν μνήμη στον ιστότοπο σχετικά με τα δεδομένα και τις προτιμήσεις των χρηστών.

6.3.4 Cookies τρίτου μέρους

Τα cookies τρίτου μέρους είναι τα cookies που ορίζονται από τρίτους σε κάποιον ιστότοπο, δηλαδή από οντότητες πέραν της εταιρείας που έχει την ιστοσελίδα. Τα cookies αυτά ενεργοποιούνται όταν ο διαχειριστής της ιστοσελίδας χρησιμοποιεί αναλυτικά στοιχεία, εμφανίζει στην ιστοσελίδα διαφημίσεις ή έχει ενσωματωμένα περιεχόμενα. Ο διαχειριστής της ιστοσελίδας συνήθως δεν γνωρίζει πώς ακριβώς λειτουργούν τα cookies αυτά ή τι ακριβώς πληροφορίες συλλέγουν, καθώς ανανεώνονται συνεχώς και αυτόματα. Ο κύριος στόχος των cookies αυτών είναι η συλλογή ορισμένων πληροφοριών για τη διεξαγωγή διάφορων ερευνών σχετικά με την συμπεριφορά, τη δημογραφία και κυρίως για το στοχοθετημένο μάρκετινγκ.

6.4 Νόμοι και Κανονισμοί που επηρεάζουν τα cookies

Τα cookies γίνονται όλο και μεγαλύτερο μέρος της καθημερινής χρήσης του διαδικτύου και χρησιμοποιούνται σήμερα, σχεδόν από κάθε ιστοσελίδα. Ένα cookie, όπως αναφέρθηκε προηγουμένως, μπορεί να παρακολουθεί τη διαδρομή του χρήστη και να αποθηκεύει προσωπικές πληροφορίες. Για τον λόγο αυτό, υπάρχουν ορισμένοι κανονισμοί και νόμοι για το πώς πρέπει να αξιοποιούνται. Σήμερα όλες οι εταιρείες και οργανισμοί εντός της ΕΕ, που αποθηκεύουν προσωπικά δεδομένα σχετικά με τους πολίτες, οφείλουν να ακολουθούν τους νόμους και τον Κανονισμό για την προστασία των προσωπικών δεδομένων.

Η νομοθεσία των cookies της ΕΕ, ή όπως είναι γνωστή η οδηγία για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγία 2009/136/ΕΚ, ενσωματωμένη στην ελληνική έννομη τάξη με τον Ν 3471/2006), αποτελεί παλαιότερη νομική πράξη, η οποία εγκρίθηκε το 2002 και ενημερώθηκε το 2009 και αφορά στη διατήρηση δεδομένων και την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Περιγράφει τι επιτρέπεται να κάνουν και τι όχι οι τρίτοι με τα ψηφιακά δεδομένα των χρηστών χωρίς να έχουν την συγκατάθεση από αυτούς, για ποιους σκοπούς και με ποιον τρόπο. Η οδηγία για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών δηλώνει ότι απαγορεύεται η

τοποθέτηση των cookies και ιχνηλατών πριν από τη συναίνεση του χρήστη, εκτός από τα απολύτως απαραίτητα για τη βασική λειτουργία ενός διαδικτυακού τόπου.

Σε αντίθεση με τον νόμο των cookies, ο ΓΚΠΔ είναι πολύ νεότερος και είναι ένας κανονισμός, ο οποίος είναι δεσμευτικός για όλα τα κράτη μέλη της ΕΕ από το Μάιο του 2018. Έχει πολύ μεγαλύτερη εμβέλεια από την οδηγία για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, δεδομένου ότι επικεντρώνεται στην προστασία των προσωπικών δεδομένων, ανεξάρτητα από το είδος των δεδομένων και τον τρόπο με τον οποίο οι εταιρείες και οι οργανισμοί πρέπει να διασφαλίζουν τη διαφάνεια και να λαμβάνουν τη συγκατάθεση των χρηστών.

Η αλληλεπίδραση μεταξύ των δύο νομοθετημάτων διαμορφώνει ένα πλαίσιο, στο οποίο ο υπεύθυνος επεξεργασίας για να επεξεργαστεί τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να συμμορφώνεται με τις απαιτήσεις της οδηγίας ePrivacy και του ΓΚΠΔ. Σύμφωνα με το ισχύον πλαίσιο, ο υπεύθυνος επεξεργασίας δύναται, πλην συγκεκριμένων εξαιρέσεων, να εγκαταστήσει cookies, μόνο εάν ο εκάστοτε χρήστης έχει δώσει τη συγκατάθεση του, ύστερα από σαφή ενημέρωση για την εγκατάσταση και τη χρήστη τους. Η υποχρέωση του υπεύθυνου επεξεργασίας αποτελεί έναν από τους βασικούς άξονες του ΓΚΠΔ για τη θεμιτή επεξεργασία και για τον λόγο αυτό η ενημέρωση από τον υπεύθυνο επεξεργασίας, στο πλαίσιο του ΓΚΠΔ, θα πρέπει να επεκταθεί, καλύπτοντας το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα ή τα κριτήρια που καθορίζουν το εν λόγω διάστημα ή την λήψη αυτοματοποιημένων αποφάσεων. Σύμφωνα με την Ομάδα Εργασίας του άρθρου 29, το δικαίωμα ενημέρωσης του υποκειμένου ισχύει και για τα απολύτως απαραίτητα cookies για την λειτουργία της ιστοσελίδας, ακόμα και αν δεν χρειάζεται η συγκατάθεση του χρήστη για την χρήση τους. Ακολούθως, η επιλογή του ύφους της γλώσσας και των λέξεων, που χρησιμοποιούνται στα κείμενα που ενημερώνουν τους χρήστες, θα πρέπει να συνεπάγονται με τις αρχές της διαφάνειας και να μην λειτουργούν παραπλανητικά, με σκοπό να καθοδηγήσει τους χρήστες στην παροχή συγκατάθεσης για την χρήση cookies.

6.5 Η επιρροή του ΓΚΠΔ ως προς την συγκατάθεση των cookies

Ένα ενδιαφέρον ζήτημα αναφορικά με τα cookies είναι το γεγονός ότι η Οδηγία ePrivacy απευθύνεται στην αποθήκευση πληροφοριών ή στην απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον υπολογιστή του χρήστη και όχι στην επεξεργασία των δεδομένων που συλλέγονται μέσω των cookies. Στον ΓΚΠΔ γίνεται λόγος μόνο μια φορά για τα cookies στην αιτιολογική σκέψη 30, όπου αναφέρει :

> (30) « Τα φυσικά πρόσωπα μπορεί να συνδέονται με επιγραμμικά αναγνωριστικά στοιχεία ταυτότητας, τα οποία παρέχονται από τις συσκευές, τις εφαρμογές, τα εργαλεία και τα πρωτόκολλά τους, όπως διευθύνσεις διαδικτυακού πρωτοκόλλου, αναγνωριστικά cookies ή άλλα αναγνωριστικά στοιχεία όπως ετικέτες αναγνώρισης μέσω ραδιοσυχνοτήτων. Αυτά μπορεί να αφήνουν ίχνη τα οποία, ιδίως όταν συνδυαστούν με μοναδικά αναγνωριστικά στοιχεία ταυτότητας και άλλες πληροφορίες που λαμβάνουν οι εξυπηρετητές, μπορούν να χρησιμοποιηθούν για να δημιουργηθεί το προφίλ των φυσικών προσώπων και να αναγνωριστεί η ταυτότητά τους. »

Αυτό σημαίνει πώς η διαδικασία αναγνώρισης ενός ατόμου μέσω των cookies θεωρείται πώς αφορά προσωπικά δεδομένα εκείνου. Παρόλο που δεν χρησιμοποιούνται όλα τα cookies με τρόπο που θα μπορούσαν να ταυτοποιήσουν κάποιον χρήστη, η πλειοψηφία τους το κάνει. Για τον λόγο αυτό θα πρέπει να διαχειρίζονται τα cookies με τρόπο ώστε να συμμορφώνονται με τον ΓΚΠΔ. Τέτοια παραδείγματα είναι τα cookies για αναλυτικές, διαφημιστικές και λειτουργικές υπηρεσίες. Για να συμμορφωθεί ένας οργανισμός με τους κανονισμούς που διέπουν τα cookies στο πλαίσιο του ΓΚΠΔ και με την οδηγία για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών οφείλει, όπως προαναφέρθηκε, να λαμβάνει την συγκατάθεση των χρηστών, προτού χρησιμοποιήσει οποιαδήποτε cookies, εκτός από τα απολύτως απαραίτητα. Επιπροσθέτως, θα πρέπει να παρέχει ακριβείς και συγκεκριμένες πληροφορίες σχετικά με τα δεδομένα που κάθε cookie παρακολουθεί και για τον σκοπό που τα χρησιμοποιεί, σε απλή και κατανοητή γλώσσα, πριν από τη λήψη της συναίνεσης. Σύμφωνα με το Δελτίου Τύπου της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα με αρ. Πρωτ Γ/ΕΞ/1525

στις 25/2/2020, ένας τρόπος για να γίνει αυτό είναι κατά την επίσκεψη κάποιου χρήστη στον ιστότοπο ενός οργανισμού αυτόματα να του εμφανίζεται ένα pop-up παράθυρο, που θα περιλαμβάνει όλες τις απαραίτητες πληροφορίες των cookies και στην συνέχεια την επιλογή για αποδοχή ή απόρριψη αυτών. Στις πληροφορίες αυτές, πρέπει να παρέχεται ειδική ενημέρωση για τον σκοπό του κάθε ιχνηλάτη που χρησιμοποιείται, και όχι γενική ενημέρωση για την χρήση τους. Επίσης, στην ενημέρωση αυτή πρέπει να αναφέρονται η διάρκεια λειτουργίας, η ταυτότητα του υπεύθυνου της επεξεργασίας, οι αποδέκτες ή οι κατηγορίες των δεδομένων. Η Αρχή Προστασίας Δεδομένων στο Δελτίου Τύπου, τονίζει ότι το περιεχόμενο της ενημέρωσης θα πρέπει να είναι ευανάγνωστο ανεξαρτήτως της τερματικής συσκευής από όπου γίνεται η πρόσβαση (φορητή ή σταθερή συσκευή) και ότι είναι θεμιτή η παροχή της ενημέρωσης μέσω πολλών επιπέδων, αρκεί να εξασφαλιστεί ότι η συγκατάθεση του χρήστη ζητείται αφού έχει ενημερωθεί ειδικά ο χρήστης για τις κατηγορίες ιχνηλατών που χρησιμοποιούνται.

Ο ΓΚΠΔ ορίζει ότι η συγκατάθεση δεν θα πρέπει να θεωρείται ελεύθερη στην περίπτωση που το υποκείμενο των δεδομένων δεν έχει αληθινή ή ελεύθερη επιλογή ή αν δεν είναι σε θέση να αρνηθεί. Η συγκατάθεση, σύμφωνα με την αιτιολογική σκέψη 32 του ΓΚΠΔ, θα πρέπει να παρέχεται με σαφή θετική ενέργεια, η οποία να συνιστά ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επίγνωση ένδειξη της συμφωνίας του υποκειμένου των δεδομένων υπέρ της επεξεργασίας των δεδομένων που το αφορούν, για παράδειγμα με γραπτή δήλωση, μεταξύ άλλων με ηλεκτρονικά μέσα ή προφορική δήλωση. Αυτό θα μπορούσε να περιλαμβάνει τη συμπλήρωση ενός τετραγωνιδίου κατά την επίσκεψη σε διαδικτυακή ιστοσελίδα, την επιλογή των επιθυμητών τεχνικών ρυθμίσεων για υπηρεσίες της κοινωνίας των πληροφοριών ή μια δήλωση ή συμπεριφορά που δηλώνει σαφώς, στο συγκεκριμένο πλαίσιο, ότι το υποκείμενο των δεδομένων αποδέχεται την πρόταση επεξεργασίας των οικείων δεδομένων προσωπικού χαρακτήρα. Επομένως, η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια δεν θα πρέπει να εκλαμβάνονται ως συγκατάθεση. Στο σημείο αυτό η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα καθορίζει ότι δεν υπάρχει συγκατάθεση από τον χρήστη αν το πρόγραμμα πλοήγησης έχει ως επιλογή την αποδοχή των cookies.

Εάν η συγκατάθεση του υποκειμένου των δεδομένων πρόκειται να δοθεί κατόπιν αιτήματος με ηλεκτρονικά μέσα, το αίτημα πρέπει να είναι σαφές, περιεκτικό

και να μην διαταράσσει αδικαιολόγητα τη χρήση της υπηρεσίας για την οποία παρέχεται. Σύμφωνα με τις παραπάνω παρατηρήσεις, προκύπτει ο βαθμός νομιμότητας της εξάρτησης της πρόσβασης σε μια ιστοσελίδα από την αποδοχή των cookies. Πολλές ιστοσελίδες χρησιμοποιούν το cookie wall, που αποτελεί έναν τρόπο ώστε οι χρήστες που δεν επιλέγουν τη χρήση όλων των cookies και των trackers να μην έχουν πρόσβαση στην ιστοσελίδα. Η πρακτική αυτή, σύμφωνα με τον Ευρωπαίο Επόπτη για την Προστασία Δεδομένων[1] όσο και η Ολλανδική Αρχή προστασίας δεδομένων[2], υποστηρίζει ότι η απαγόρευση της εισόδου σε μια ιστοσελίδα λόγω της μη αποδοχής των cookies δεν είναι συμβατή με το ισχύον πλαίσιο για την προστασία δεδομένων.

Ένα ακόμη ζήτημα είναι αν η συνέχιση της περιήγησης σε μια ιστοσελίδα χωρίς την αποδοχή των cookies ισοδυναμεί, ως θετική ενέργεια, με συγκατάθεση, εφόσον υπάρχει σαφής και πλήρης ενημέρωση. Η σιωπή, σύμφωνα με τον ΓΚΠΔ, δεν θα πρέπει να εκλαμβάνεται ως συγκατάθεση. Στο συγκεκριμένο ζήτημα έχει τοποθετηθεί και η Ομάδα Εργασίας του άρθρου 29 στις κατευθυντήριες γραμμές σχετικά με την έννοια της συγκατάθεσης, όπου αναφέρει ότι η απλή συνέχιση της συνήθους χρήσης διαδικτυακού τόπου δεν συνιστά συμπεριφορά του υποκειμένου των δεδομένων να συμφωνήσει σε πράξη επεξεργασίας. Επιπλέον, ένα ακόμη ζήτημα είναι η ανάκληση, δηλαδή, σύμφωνα με τον σύμφωνα με τον ΓΚΠΔ, το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεση του ανά πάσα στιγμή χωρίς να ζημιωθεί. Στη περίπτωση της ανάκλησης της συγκατάθεσης όσον αφορά τη χρήση των cookies, αν και ενδέχεται να είναι αρκετά περίπλοκη από τεχνική άποψη, οι υπεύθυνοι επεξεργασίας καλούνται να ανακαλύψουν τρόπους, προκειμένου να είναι εφικτή. Ένας τρόπος είναι η δημιουργία ενός κέντρου διαχείρισης cookies, όπου με φιλικό και εύκολο τρόπο προς τον χρήστη να μπορεί να πραγματοποιηθεί η ανάκληση της συγκατάθεσης.

Τελευταίο ζήτημα που προκύπτει είναι η δυνατότητα του υπεύθυνου επεξεργασίας να αποδείξει ότι το υποκείμενο των δεδομένων έχει δώσει τη

[1] EDPS Opinion 6/2017 for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation) https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

[2] Βλ. Dutch Data Protection Authority: Websites must remain accessible when refusing tracking cookies https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigerentracking-cookies

συγκατάθεση του για την επεξεργασία τους στην περίπτωση των cookies. Ενώ η σχετική υποχρέωση τίθεται στο άρθρο 7 παρ. 1 του ΓΚΠΔ, στη πράξη δεν είναι ιδιαίτερα πιθανό ο ΥΕ να μπορεί να ταυτοποιήσει ένα φυσικό πρόσωπο μόνο μέσω των πληροφοριών που συλλέγονται από τον ίδιο μέσω αρχείων cookies (Βασίλης Καρκατζούνης, 2019). Συνεπώς, η απόκτηση συμπληρωματικών πληροφοριών προκειμένου να ταυτοποιήσει το υποκείμενο των δεδομένων, με σκοπό τη συμμόρφωσή του προς τις διατάξεις του ΓΚΠΔ, δεν θα πρέπει να θεωρείται υποχρέωση του ΥΕ.

Τέλος, υπάρχουν κατηγορίες cookies και συναφών τεχνολογιών που αποτελούν εξαίρεση ως προς την λήψη συγκατάθεσης για τη χρήση τους. Σύμφωνα με την Αρχή Προστασία Δεδομένων Προσωπικού Χαρακτήρα στο Δελτίο Τύπου ως προς τις συστάσεις για τη συμμόρφωση υπευθύνων επεξεργασίας δεδομένων με την ειδική νομοθεσία για τις ηλεκτρονικές επικοινωνίες, τα cookies που εξαιρούνται είναι όσα είναι απαραίτητα για την αναγνώριση ή/και διατήρηση του περιεχομένου, που εισάγει ο συνδρομητής ή χρήστης κατά τη διάρκεια μια σύνδεση σε ιστοσελίδα καθ' όλη τη διάρκεια της συγκεκριμένης σύνδεσης, όπως είναι το καλάθι αγορών. Επιπρόσθετα, εξαιρούνται όσα είναι απαραίτητα για τη σύνδεση του συνδρομητή ή χρήστη σε υπηρεσίες, που απαιτούν αυθεντικοποίηση, όσα είναι απαραίτητα για την ασφάλεια του χρήστη, όσα είναι αναγκαία για την πραγματοποίηση της τεχνικής της κατανομής φορτίου (load balancing) σε μια σύνδεση σε ιστοσελίδα του διαδικτύου και, τέλος, όσα απαιτούνται για τη διατήρηση των επιλογών του χρήστη σχετικά με την παρουσίαση της ιστοσελίδας, όπως για παράδειγμα η επιλογή γλώσσας και αποθήκευση ιστορικού αναζητήσεων. Τα cookies που εγκαθίστανται με σκοπό τη διαδικτυακή διαφήμιση (online advertising) και τα η χρήση cookies τρίτων όπως η υπηρεσία Google Analytics με σκοπό την στατιστική ανάλυση (web analytics) δεν εμπίπτουν στην εξαίρεση, επομένως επιτρέπονται μόνο εφόσον έχει ληφθεί η συγκατάθεση από τον χρήστη.

6.6 Κακές πρακτικές χρήσης των cookies

Τα cookies έχουν την δυνατότητα να αποθηκεύουν προσωπικές πληροφορίες σχετικά με τους χρήστες, γεγονός που αποτελεί μεγάλη ευθύνη για τους ιδιοκτήτες

των ιστοσελίδων, που κάνουν χρήση των cookies. Με την συγκεκριμένη ικανότητα των cookies είναι αναπόφευκτη η ύπαρξη ανθρώπων που θα προβούν στην κακόβουλη χρήση τους. Τα cookies ως εργαλείο δεν είναι απειλή, δεν είναι ιοί και δεν μπορούν να εκτελέσουν κακόβουλες πράξεις, καθώς είναι ένα αρχείο κειμένου που δεν μπορεί να περιέχει κώδικα. Ωστόσο, για ανθρώπους που ξέρουν πώς μπορούν να τα αξιοποιήσουν είναι πιθανό να αποτελέσουν ένα εργαλείο για την απόκτηση προσωπικών πληροφοριών, όπως επίσης για να «ανοίξουν μια πόρτα» στον υπολογιστή ενός χρήστη. Ένα παράδειγμα για το πώς ένα cookie μπορεί να χρησιμοποιηθεί από έναν χάκερ με κακόβουλο τρόπο για να αποκτήσει πρόσβαση στον υπολογιστή είναι με την αποστολή ενός Trojan ιού σε ένα διακομιστή, που θα διαγράψει τα cookies του προγράμματος περιήγησης του χρήστη και θα τοποθετήσει κακόβουλα cookies στο πρόγραμμα περιήγησης. Όταν ο χρήστης ανοίξει το πρόγραμμα περιήγησης, αυτό αυτόματα θα συνδεθεί σε μια νέα αρχική σελίδα, η οποία είναι η ιστοσελίδα του χάκερ. Αφού συνδεθεί με την ιστοσελίδα αυτή, το κακόβουλο cookie, ενημερώνει τον χάκερ ότι η επίθεση πραγματοποιήθηκε με επιτυχία. Έπειτα, ο χάκερ έχει ελεύθερη πρόσβαση στον υπολογιστή του χρήστη, καθώς και σε όλες τις πληροφορίες του. Παρόλα αυτά, συνήθως τα cookies δεν αποτελούν απειλή και οι ιστοσελίδες των ηλεκτρονικών καταστημάτων σπάνια μπορεί να περιέχουν ένα κακόβουλο cookie.

Εκτός από την κακόβουλη χρήση τους από κάποιον που θέλει να επιδιώξει μια επίθεση στον υπολογιστή ενός χρήστη, τα cookies χρησιμοποιούνται με λάθος τρόπο από πολλές ιστοσελίδες στο διαδίκτυο. Σύμφωνα με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στο Δελτίο Τύπου, που εκδόθηκε στις 25/2/2020 με Αρ. Πρωτ Γ/ΕΞ/1525, ως προς τις συστάσεις για τη συμμόρφωση υπευθύνων επεξεργασίας δεδομένων με την ειδική νομοθεσία για τις ηλεκτρονικές επικοινωνίες, κακές πρακτικές ως προς τη λήψη συγκατάθεσης για την χρήση των cookies θεωρείται η χρήση των απαραίτητων cookies για τη λειτουργία της ιστοσελίδας, χωρίς καμία ενημέρωση του χρήστη, αλλά και η χρήση Google Analytics, με σκοπό τη στατιστική ανάλυση (web analytics) μόνο με ενημέρωση στο χρήστη, χωρίς να δίνεται η δυνατότητα απόρριψης, ή ακόμη και χωρίς την εν λόγω ενημέρωση.

Σε θέματα ενημέρωσης κακές πρακτικές, σύμφωνα με το Δελτίο Τύπου, είναι η παροχή μόνο μιας γενικής ενημέρωσης σχετικά με τη χρήση ιχνηλατών μέσα σε ένα

γενικό κείμενο πολιτικής προστασίας δεδομένων. Όταν η ενημέρωση για τη χρήση cookies, στο πρώτο επίπεδο του αναδυόμενου παραθύρου, περιορίζεται μόνο σε γενικό κείμενο, το οποίο αναφέρει ότι χρησιμοποιούνται τέτοιες τεχνικές, όπως είναι τα cookies για την καλύτερη εμπειρία και την καλύτερη παρουσίαση. Τέλος, μία άλλη περίπτωση είναι όταν το κείμενο της ενημέρωσης δεν είναι ευανάγνωστο λόγω της μη προσαρμογής στο είδος της τερματικής συσκευής από όπου γίνεται η πρόσβαση (φορητή ή σταθερή συσκευή).

Το τελευταίο θέμα λανθασμένων πρακτικών αφορά στον τρόπο λήψης συγκατάθεσης από το υποκείμενο των δεδομένων. Σύμφωνα με την Αρχή Προστασίας, τέτοιες κακές πρακτικές είναι όταν για τη λήψη συγκατάθεσης υπάρχει μόνο μια επιλογή της μορφής «Ενημερώθηκα» ή «Συμφωνώ», χωρίς τη δυνατότητα να συνεχιστεί απρόσκοπτα η πλοήγηση (με απομάκρυνση του εν λόγω μηνύματος), αν ο χρήστης δεν επιλέξει το ανωτέρω. Ακόμα, θεωρείται λάθος η μη ύπαρξη δυνατότητας απόρριψης της χρήσης ιχνηλατών στο αναδυόμενο παράθυρο, παρά μόνο αποδοχής όλων, καθώς και όταν η δυνατότητα απόρριψης της χρήσης cookies δίνεται μόνο σε δεύτερο επίπεδο πληροφοριών, δηλαδή μετά το «κλικ» σε υπερσύνδεσμο με «περισσότερες πληροφορίες» ή «ρυθμίσεις». Επιπροσθέτως, κακή πρακτική είναι όταν το κλείσιμο του αναδυόμενου παραθύρου/ενημερωτικού πλαισίου, η συνέχιση πλοήγησης ή το κύλισμα οδηγεί σε χρήση ή εγκατάσταση των μη απαραίτητων cookies. Κακή πρακτική, επίσης, είναι όταν το μέγεθος και το χρώμα του κουμπιού «αποδοχή» ή «συγκατάθεση» για τη χρήση των cookies προδιαθέτει έντονα τον χρήστη στην επιλογή του, για παράδειγμα όταν είναι πολύ μεγάλο και με έντονο χρώμα ή/και είναι προεπιλεγμένο. Μια άλλη σημαντικά κακή πρακτική, σύμφωνα με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, προκύπτει όταν το αναδυόμενο παράθυρο δίνει μόνο τη δυνατότητα αποδοχής των μη απαραίτητων cookies, ενώ σε περιπτώσεις που υπάρχει και η επιλογή απόρριψης είτε δεν προβλέπεται κάποιος τρόπος αλλαγής των προτιμήσεων του χρήστη είτε αυτή επιτρέπεται να πραγματοποιηθεί μόνο μέσω αλλαγής ρυθμίσεων του προγράμματος περιήγησης και όχι του ιστότοπου. Τέλος, στο θέμα του τρόπου λήψης συγκατάθεσης από τον υποκείμενο κακή πρακτική θεωρείται η περίπτωση όπου όταν ο χρήστης έχει απορρίψει τα cookies μια φορά με την επίσκεψη του στην ιστοσελίδα καλείται συνεχώς μέσω αναδυόμενο παραθύρου να προχωρήσει σε νέα επιλογή, ενώ αυτό δεν ισχύει όταν τα έχει αποδεχτεί.

Συμπεράσματα

Η παρούσα εργασία είχε ως κύριο σκοπό την διερεύνηση της επιρροής του Γενικού Κανονισμού για την Προστασία Δεδομένων στο ηλεκτρονικό εμπόριο και τη χρήση cookies. Προκειμένου να εκπληρωθεί ο στόχος αυτός, κατά την βιβλιογραφική ανασκόπηση, αναζητήθηκαν βασικοί ορισμοί και έννοιες και μελετήθηκαν τα σχετικά με το ηλεκτρονικό εμπόριο άρθρα του Κανονισμού. Παρόλο που ο ΓΚΠΔ στο ηλεκτρονικό εμπόριο και τα cookies αποτέλεσαν τις κεντρικές μεταβλητές της εν λόγω βιβλιογραφικής έρευνας, πραγματοποιήθηκε εκτενής αναφορά στους κινδύνους που ελλοχεύουν για τα δεδομένα προσωπικού χαρακτήρα σε μια αγορά μέσω διαδικτύου.

Ο Κανονισμός εισάγει νέους μηχανισμούς με σκοπό την ριζική αλλαγή του τρόπου με τον οποίο οι εταιρείες και οι οργανισμοί, συλλέγουν, επεξεργάζονται και διαχειρίζονται δεδομένα, εντός και εκτός της Ευρωπαϊκής Ένωσης. Οι οργανισμοί που δραστηριοποιούνται στον τομέα του ηλεκτρονικού εμπορίου οφείλουν να συλλέγουν και να επεξεργάζονται δεδομένα σύμφωνα με τις βασικές αρχές του Κανονισμού, που προβλέπονται στο άρθρο 5, δηλαδή της αρχής της νομιμότητας, αντικειμενικότητας και διαφάνειας, της αρχής του σκοπού, της αρχής της ελαχιστοποίησης, της αρχής της ακρίβειας, της αρχής του περιορισμού και της αρχής της ακεραιότητας και εμπιστευτικότητας. Σε κάθε στάδιο της διαδικασίας της ηλεκτρονικής αγοράς η τήρηση των παραπάνω αρχών είναι επιτακτική. Παρόλα αυτά, συχνό φαινόμενο είναι τα ηλεκτρονικά καταστήματα να μην τηρούν τις αρχές αυτές, με αποτέλεσμα να θέτουν σε κίνδυνο την ιδιωτική ζωή των πελατών τους. Η μη τήρηση των αρχών και των απαιτήσεων του Κανονισμού επιφέρει στα ηλεκτρονικά καταστήματα υψηλά πρόστιμα.

Σημαντική παράμετρος του ΓΚΠΔ αναδεικνύεται η αναβάθμιση του ρόλου του υποκειμένου μέσω τον δικαιωμάτων του. Πρόκειται για το δικαίωμα της ενημέρωσης, το δικαίωμα πρόσβασης, το δικαίωμα διόρθωσης, το δικαίωμα διαγραφής, το δικαίωμα περιορισμού της επεξεργασίας, το δικαίωμα φορητότητας, το δικαίωμα εναντίωσης και το δικαίωμα στην ανθρώπινη παρέμβαση. Στη παρούσα εργασία παρουσιάστηκε η εφαρμογή των δικαιωμάτων του υποκειμένου στο ηλεκτρονικό εμπόριο. Τα ηλεκτρονικά καταστήματα πρέπει παρέχουν στο πελάτη τη

δυνατότητα άσκησης των δικαιωμάτων αυτών. Η διασφάλιση αυτή αποτελεί ένα από τα καθήκοντα του Υπεύθυνου Προστασίας Δεδομένων, του οποίου ο ρόλος είναι κυρίως συμβουλευτικός προς τον Υπεύθυνο Επεξεργασίας. Στις υπόλοιπες υποχρεώσεις του συγκαταλέγεται η αξιολόγηση της συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Δεδομένων και ο έλεγχος της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

Από τα προαναφερθέντα δικαιώματα από την βιβλιογραφική ανασκόπηση φάνηκε ότι ιδιαίτερη έμφαση δίνεται σε αυτό της ενημέρωσης των χρηστών μέσω της Πολιτικής Απορρήτου. Πρόκειται για ένα έντυπο πληροφόρησης που οφείλει να είναι δημοσιευμένο στην ιστοσελίδα του κάθε ηλεκτρονικού καταστήματος. Στην εργασία αναλύθηκαν οι απαιτήσεις σχετικά με το περιεχόμενο της Πολιτικής Απορρήτου που ισχύουν, ώστε να συμμορφώνεται με τον Κανονισμό. Συγκεκριμένα θα πρέπει να αναφέρεται το είδος των δεδομένων, ο τρόπος συλλογής, επεξεργασίας και αποθήκευσης τους, η χρήση τους για σκοπούς μάρκετινγκ, η περιγραφή των δικαιωμάτων των υποκειμένων, καθώς και ο τρόπος επικοινωνίας με το ηλεκτρονικό κατάστημα και με την Αρχή.

Επιπροσθέτως, στην ενημέρωση συμπεριλαμβάνονται όλες οι απαραίτητες πληροφορίες για τα cookies, δηλαδή γίνεται μια αναλυτική περιγραφή του είδους τους, τον σκοπό χρήσης τους, όπως επίσης και του τρόπου μη αποδοχής και διαγραφής. Τα cookies, που διακρίνονται σε έμμονα, προσωρινά, πρώτου και τρίτου μέρους, προσφέρουν στις επιχειρήσεις ευκαιρίες πωλήσεων μέσω στοχευμένων διαφημίσεων προς τους πελάτες του, καθώς απομνημονεύουν τις προτιμήσεις τους, διαμορφώνοντας έτσι ένα προφίλ για τον καθένα. Βασική προϋπόθεση για την χρήση τους είναι η ρητή συγκατάθεση του υποκειμένου πέρα από των απαραίτητων για την ορθή λειτουργία των ιστοσελίδων. Τέλος, κατά την μελέτη του Δελτίου Τύπου της Αρχής Προστασίας Προσωπικών Δεδομένων εντοπίστηκαν περιπτώσεις άνομης χρήσης των cookies.

Ύστερα, λοιπόν, από την βιβλιογραφική ανασκόπηση και την μελέτη των άρθρων του Γενικού Κανονισμού Προστασίας Δεδομένων, προκύπτει πώς ο Κανονισμός καλύπτει επαρκώς θέματα που αφορούν στην συλλογή, επεξεργασία και διαχείριση των προσωπικών δεδομένων των πελατών από τα ηλεκτρονικά καταστήματα. Συνεπώς, σημαντική αξία στο ηλεκτρονικό εμπόριο έχει η διεξαγωγή ελέγχου ως προς τον σύννομο τρόπο συλλογής, επεξεργασίας και διαχείρισης

δεδομένων προσωπικού χαρακτήρα, αλλά και της σύννομης χρήσης των cookies σε όλες τις ηλεκτρονικές επιχειρήσεις, ανεξάρτητα από το πόσο μεγάλα είναι, ώστε να μην ελλοχεύει ο κίνδυνος αθέμιτου ανταγωνισμού. Έτσι, θα αποτραπεί η ανεξέλεγκτη άνθιση των μικρών καταστημάτων με μη σύννομο τρόπο. Ωστόσο, δεν είναι δυνατός ο επαρκής έλεγχος της συμμόρφωσης των οργανισμών, που εδρεύουν εκτός Ευρωπαϊκής Ένωσης, καθώς, όσον αφορά σε θέματα εδαφικού πεδίου εφαρμογής του Κανονισμού, διαπιστώνονται κενά.

Η εν λόγω βιβλιογραφική έρευνα, όμως, διαθέτει και ορισμένους περιορισμούς. Αρχικά, δεν γίνεται λόγος ως προς την επιρροή του Κανονισμού στις κατηγορίες ηλεκτρονικού εμπορίου μεταξύ επιχείρησης με επιχείρηση (Business to Business ή B2B) και μεταξύ καταναλωτών (Consumer to Consumer ή C2C). Ακολούθως, στην δειγματοληψία δεν συμπεριλαμβάνονται επιχειρήσεις που δραστηριοποιούνται στον χώρο του ηλεκτρονικού εμπορίου και εδρεύουν εκτός Ευρωπαϊκής Ένωσης, για παράδειγμα στην Ασία ή την Αμερική, γεγονός που δεν οδηγεί στη διεξαγωγή ενός ολοκληρωμένου και γενικεύσιμου συμπεράσματος σχετικά με την γενική συμμόρφωση στον Κανονισμό. Προτείνεται, λοιπόν, οι μελλοντικοί ερευνητές να πραγματοποιήσουν έναν εκτενέστερο δειγματοληπτικό έλεγχο, όπου θα μελετούν μεγάλο όγκο ηλεκτρονικών καταστημάτων σε παγκόσμια κλίμακα και διαβαθμιζόμενης δημοτικότητας. Τέλος, χρήσιμη θα ήταν σε μια ανάλογη μελέτη η αναφορά στις υπόλοιπες κατηγορίες ηλεκτρονικού εμπορίου, κατά την οποία θα μπορούσε να μελετηθεί ο σωστός τρόπος λειτουργίας και δράσης τους για την αποφυγή άνομων χρήσεων προσωπικών δεδομένων και την συμμόρφωση τους με τον ΓΚΠΔ.

Βιβλιογραφία

Albrecht, J. P. (2016). How the GDPR will change the world. *Eur. Data Prot. L. Rev.*, *2*, 287.

Antoniou, G., & Batten, L. (2011). E-commerce: protecting purchaser privacy to enforce trust. *Electronic commerce research*, *11*(4), 421.

Bader, C., Castefelt, E. L., & Gunnarsson, L. (2018). The Recipe for Cookies: A studies about cookies & the GDPR-law.

Cookiebot. EU cookie law – a right to privacy. Retrieved from https://www.cookiebot.com/en/cookie-law/

Cookiebot. GDPR and cookies | What do I need to know? | Is my use of cookies compliant? Retrieved from https://www.cookiebot.com/en/gdpr-cookies/

De Montjoye, Y. A., Radaelli, L., & Singh, V. K. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*, *347*(6221), 536-539.

Diaz, J., Choi, S. G., Arroyo, D., Keromytis, A. D., Rodriguez, F. B., & Yung, M. (2019). A Methodology for Retrofitting Privacy and Its Application to e-Shopping Transactions. In *Advances in Cyber Security: Principles, Techniques, and Applications* (pp. 143-183). Springer, Singapore.

Freris, Y. GDPR κανονισμός: Τι είναι και πως θα επηρεάσει την επιχείρησή σας. Retrieved from https://www.addicted.gr/gdpr-kanonismos-ti-einai-kai-pos-tha-epireasei-tin-epicheirisi-sas/

GDPR.EU. Cookies, the GDPR, and the ePrivacy Directive. Retrieved from https://gdpr.eu/cookies/

GDPR.EU. Writing a GDPR-compliant privacy notice (template included). Retrieved from https://gdpr.eu/privacy-notice

Lawspot.gr. Cookies : Προθεσμία 2 μηνών για συμμόρφωση δίνει στις ιστοσελίδες η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Retrieved from https://www.lawspot.gr/nomika-nea/cookies-prothesmia-2-minon-gia-symmorfosi-dinei-stis-istoselides-i-arhi-prostasias

Maria, P. GDPR Privacy Policy Template. Retrieved from https://www.privacypolicies.com/blog/gdpr-privacy-policy/

Wood, A. BIG DATA: THE SECTER WEAPON BEHIND LOYALTY PROGRAMS. Retrieved from https://www.chiefmarketer.com/big-data-secret-weapon-behind-loyalty-programs/

Zerlang, J. (2017). GDPR: a milestone in convergence for cyber-security and compliance. *Network Security*, *2017*(6), 8-11.

Καρκατζούνης, Β. (2019). Cookies και προστασία δεδομένων προσωπικού χαρακτήρα, *ΔίΜΕΕ*

Μήτρου, Λ. (2017). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων. *Νέο Δίκαιο-Νέες Υποχρεώσεις-Νέα Δικαιώματα, 1η έκδοση, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη*.

Παναγοπούλου-Κουτνατζή, Φ. (2017). Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ. *Εισαγωγή και Προστασία Δικαιωμάτων, 1η έκδοση, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη*.

Πλατής, Ε. (2018). Προσωπικά Δεδομένα, Προστασία GDPR. *Εκδόσεις Παπαδόπουλος*