ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΑ ΟΦΕΛΗ ΤΩΝ ΦΥΣΙΚΩΝ ΠΡΟΣΩΠΩΝ ΚΑΙ ΟΙ ΠΡΟΚΛΗΣΕΙΣ ΣΤΗ ΔΙΟΙΚΗΣΗ ΟΡΓΑΝΙΣΜΩΝ ΤΕΧΝΟΛΟΓΙΑΣ ΜΕ ΤΗΝ ΕΠΕΡΧΟΜΕΝΗ ΑΝΑΘΕΩΡΗΣΗ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ "ΚΑΝΟΝΙΣΜΟΥ ΓΙΑ ΤΗΝ ΙΔΙΩΤΙΚΗ ΖΩΗ ΚΑΙ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ" (EPRIVACY REGULATION)

ΠΑΡΑΣΚΕΥΑ ΓΕΩΡΓΙΟΣ

ΑΣΚΟΥΝΗΣ ΔΗΜΗΤΡΙΟΣ
ΚΑΘΗΓΗΤΗΣ

ΦΕΒΡΟΥΑΡΙΟΣ 2021

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΑ ΟΦΕΛΗ ΤΩΝ ΦΥΣΙΚΩΝ ΠΡΟΣΩΠΩΝ ΚΑΙ ΟΙ ΠΡΟΚΛΗΣΕΙΣ ΣΤΗ ΔΙΟΙΚΗΣΗ ΟΡΓΑΝΙΣΜΩΝ ΤΕΧΝΟΛΟΓΙΑΣ ΜΕ ΤΗΝ ΕΠΕΡΧΟΜΕΝΗ ΑΝΑΘΕΩΡΗΣΗ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ "ΚΑΝΟΝΙΣΜΟΥ ΓΙΑ ΤΗΝ ΙΔΙΩΤΙΚΗ ΖΩΗ ΚΑΙ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ" (EPRIVACY REGULATION)

ΠΑΡΑΣΚΕΥΑ ΓΕΩΡΓΙΟΣ

ΑΣΚΟΥΝΗΣ ΔΗΜΗΤΡΙΟΣ
ΚΑΘΗΓΗΤΗΣ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή τον Φεβρουάριο 2021.

.....	.....	.....
Ασκούνης Δ.		
Καθηγητής		

ΦΕΒΡΟΥΑΡΙΟΣ 2021

.....

Γεώργιος, Π. Παρασκευά

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Διπλωματούχος Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών Τεχνο-οικονομικών Συστημάτων

Copyright © Γεώργιος Παρασκευά, 2021.

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

Πίνακας Περιεχομένων

Περίληψη

Στη κοινωνία του 21ου αιώνα παρατηρείται ραγδαία ανάπτυξη τεχνολογικών εφαρμογών και υπηρεσιών οι οποίες συλλέγουν, αποθηκεύουν και επεξεργάζονται προσωπικά δεδομένα και πληροφορίες ιδιωτών αλλά και τρίτων οργανισμών. Εύλογα, λοιπόν, τίθενται θέματα ιδιωτικότητας και απορρήτου των επικοινωνιών αλλά και προστασίας των προσωπικών δεδομένων, όχι μόνο σε ευρωπαϊκό αλλά σε παγκόσμιο επίπεδο.

Από πολύ νωρίς, στην Ευρωπαϊκή Ένωση έχουν γίνει προσπάθειες ρύθμισης και εισαγωγής κανονιστικού πλαισίου για την προστασία της επεξεργασίας προσωπικών δεδομένων. Ταυτόχρονα, όμως, τις τελευταίες δεκαετίες και κυρίως σήμερα, η χρήση υπηρεσιών επικοινωνίας που βασίζονται σε πρωτόκολλα διαδικτύου Internet Protocol (IP) αυξάνεται συνεχώς με αποτέλεσμα η νομοθεσία να χρήζει συνεχούς βελτίωσης και επέκτασης με σκοπό τη προστασία του απορρήτου των επικοινωνιών των τελικών χρηστών αλλά και της εξασφάλισης ισότιμων όρων ανταγωνισμού για τους παρόχους ηλεκτρονικών επικοινωνιών.

Σήμερα, προς αυτή τη κατεύθυνση το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (Ε.Δ.Π.Δ) ή European Data Protection Board (E.D.P.B.), σε συνεργασία με την Ευρωπαϊκή Επιτροπή, το Ευρωκοινοβούλιο και το Ευρωπαϊκό Συμβούλιο εργάζονται προς τη νομοθέτηση νέου κανονισμού ο οποίος θα δρα συμπληρωματικά με το *Γενικό Κανονισμό Προστασίας Δεδομένων* (Γ.Κ.Π.Δ.) ή General Data Protection Regulation (G.D.P.R) που τέθηκε σε ισχύ το 2018, αλλά θα αντικαταστήσει τη προηγούμενη *Οδηγία για τη Προστασία της Ιδιωτικής Ζωής στο Τομέα των Ηλεκτρονικών Επικοινωνιών* ή Directive on privacy and electronic communications του 2002. Σε αυτό το πλαίσιο προετοιμάζεται ο *"Κανονισμός του Ευρωκοινοβουλίου και του Ευρωπαϊκού Συμβουλίου σχετικά με το σεβασμό της ιδιωτικής ζωής και την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες και τη κατάργηση της οδηγίας 2002/58/EC"* με τη συνήθη νομοθετική διαδικασία 2017/0003/COD.

Αναμένεται ότι, όπως και ο *Γενικός Κανονισμός Προστασίας Δεδομένων* (που εκδόθηκε το 2016 αλλά τέθηκε σε εφαρμογή και ισχύ τον Μάιο του 2018) έφερε σαρωτικές αλλαγές στους οργανισμούς, κυρίως τεχνολογικού ενδιαφέροντος, έτσι και ο νέος κανονισμός θα αναγκάσει τον εκσυγχρονισμό των υπηρεσιών και θα φέρει προκλήσεις στη Διοίκηση Οργανισμών Τεχνολογίας. Προσδοκούμε ότι το κόστος αλλά και η ταλαιπωρία αυτών των αλλαγών θα ανταμείψει τη κοινωνία με μεγαλύτερη εξασφάλιση του απορρήτου, αύξηση της προστασίας της ιδιωτικότητας

του ατόμου αλλά και επιβολή ισότιμων όρων ανταγωνισμού μεταξύ παρόχων ηλεκτρονικών επικοινωνιών και λειτουργικά ισοδύναμων υπηρεσιών.

Στα παραπάνω πλαίσια, στη παρούσα διπλωματική εργασία θα μελετηθεί και αναλυθεί:

(ι) το ευρύτερο πλαίσιο της ιδιωτικότητας του ατόμου και της προστασίας των δεδομένων του σε σχέση με τις Ευρωπαϊκές Οδηγίες του 1995, 2002 αλλά και με τον υπάρχοντα Γενικό Κανονισμό Προστασίας Δεδομένων (G.D.P.R.),

(ιι) οι τρόποι με τους οποίους η πρόταση για τον επερχόμενο συμπληρωματικό κανονισμό θα επηρεάσει τη φύση των τεχνολογικών εφαρμογών αλλά και

(ιιι) τις προκλήσεις που φέρνει στη Διοίκηση Οργανισμών, κυρίως τεχνολογικού ενδιαφέροντος.

Λέξεις Κλειδιά

Κανονισμός ePrivacy

Προστασία δεδομένων

Ιδιωτικότητα του ατόμου

Ηλεκτρονικές επικοινωνίες

Απόρρητο επικοινωνίας

Abstract

Over the recent years, there is a rapid development of technological applications that collect, store and process personal data and information of individuals and companies. Reasonably, there are emerging issues on the privacy of communications, but also on the protection of personal data, not only on a European but also at a global level.

Efforts have been made since a very early age in the European Union to regulate the area by introducing a regulatory framework for the processing of personal data. At the same time however, in recent decades and especially today, the use of communication services based on Internet protocols (IP) is constantly increasing. This results in larger needs for continued legislation improvements and expansion, in order to protect the security and privacy of end-user communications and ensure a level playing field among the competition of electronic communications providers.

Today, the European Data Protection Board (E.D.P.B.), in cooperation with the European Commission, the European Parliament and the European Council, are working towards legislating a new regulation which will act in addition to the *General Data Protection Regulation (G.D.P.R.)* that was published in 2016 but came into effect in 2018, but it will replace the previous *Directive on privacy and electronic communications* of 2002. In this context, the "*Regulation of the European Parliament and of the European Council on respect for privacy and the protection of personal data in electronic communications and repealing Directive 2002/58 / EC*" is being prepared with the ordinary legislative procedure 2017/0003/COD.

Just as the *General Data Protection Regulation* (effective in May 2018) brought sweeping changes to organizations, mainly of technological interest, it is expected that the new regulation will force the modernization of services and will bring challenges to the Management of Technology Organizations. It is expected that the cost of these changes will reward society by ensuring even better data security and confidentiality, increasing the protection of individual privacy and enforcing a level playing field between electronic communications providers and functionally equivalent services.

Concerning the above context, this dissertation will focus on:

(i) the broader context of individual privacy and data protection in relation to the European Union directives of 1995, 2002 and the existing General Data Protection Regulation (G.D.P.R.);

(ii) the ways in which the forthcoming supplementary regulation will affect technological applications as well as

(iii) the challenges it is expected to bring to the Management of Organizations, mainly of technological interest.

Keywords

ePrivacy Regulation

Data protection

Individual privacy

Electronic communications

Confidentiality of communications

Εισαγωγή

Στη κοινωνία του 21ου αιώνα παρατηρείται ραγδαία ανάπτυξη τεχνολογικών εφαρμογών οι οποίες συλλέγουν, αποθηκεύουν και επεξεργάζονται προσωπικά δεδομένα και πληροφορίες ιδιωτών αλλά και τρίτων οργανισμών. Εύλογα, λοιπόν, τίθενται θέματα ιδιωτικότητας των επικοινωνιών αλλά και προστασίας των προσωπικών δεδομένων, όχι μόνο σε ευρωπαϊκό αλλά και σε παγκόσμιο επίπεδο. (Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ), 2018, 1)

Από πολύ νωρίς, στην Ευρωπαϊκή Ένωση έχουν γίνει προσπάθειες ρύθμισης και εισαγωγής κανονιστικού πλαισίου για την επεξεργασία προσωπικών δεδομένων. Οι προσπάθειες αυτές ξεκίνησαν το 1995 και το 2002 δημιουργείται η "*Οδηγία για τη προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Directive 2002/58/EC on privacy and electronic communications)"*. Η οδηγία του 2002 όπως τροποποιήθηκε το 2009 (Directive 2009/136/EC) ισχύει έως σήμερα με σκοπό τη προστασία των προσωπικών δεδομένων και της ιδιωτικότητας του ατόμου. (Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ), 2018, 2-3)

Ταυτόχρονα, όμως, από το 2009 έως σήμερα η χρήση υπηρεσιών επικοινωνίας που βασίζονται σε πρωτόκολλα διαδικτύου Internet Protocol (IP) έχει αυξηθεί σε τέτοιο βαθμό ώστε η νομοθεσία να χρήζει νέου κανονιστικού πλαισίου με σκοπό τη προστασία του απορρήτου των επικοινωνιών των τελικών χρηστών αλλά και της εξασφάλισης ισότιμων όρων ανταγωνισμού για τους παρόχους ηλεκτρονικών επικοινωνιών. (Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ), 2018, 3)

Ως γνωστό, το 2016 εκδόθηκε και το Μάιο του 2018 τέθηκε σε εφαρμογή ο *Γενικός Κανονισμός Προστασίας Δεδομένων ΓΚΠΔ (General Data Protection Regulation GDPR)* με τον Κανονισμό 2016/679/ΕΚ ο οποίος όρισε μια νέα οπτική γωνία, υπό την οποία οι οργανισμοί οφείλουν να διαχειρίζονται, επεξεργάζονται και αποθηκεύουν δεδομένα που αφορούν πολίτες ή άλλους οργανισμούς της Ευρωπαϊκής Ένωσης.

Για παράδειγμα, ο *Γενικός Κανονισμός Προστασίας Δεδομένων ΓΚΠΔ (General Data Protection Regulation)* απαιτεί να υπάρχει σαφής αιτιολόγηση για κάθε είδους ιδιωτική πληροφορία η οποία συλλέγεται και επεξεργάζεται καθώς και να υπάρχει σαφές χρονικό

περιθώριο για το οποίο μπορεί να τηρείται νόμιμα, προτού διαγραφεί με τη προβλεπόμενη διαδικασία.

Με αυτό το τρόπο ο Γενικός Κανονισμός Προστασίας Δεδομένων εισήγαγε για πρώτη φορά κάποια όρια στο πεδίο της συλλογής και επεξεργασίας προσωπικών δεδομένων και έκανε το πρώτο βήμα προς τη κατεύθυνση της προστασίας της ιδιωτικής ζωής. (Ευρωπαϊκό Κοινοβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016)

Πάραυτα, συνεχίζει να υπάρχει περιθώριο βελτίωσης προς αυτή τη κατεύθυνση και για αυτό το λόγο το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (Ε.Δ.Π.Δ) ή European Data Protection Board (EDPB), σε συνεργασία με την Ευρωπαϊκή Επιτροπή, το Ευρωκοινοβούλιο και το Ευρωπαϊκό Συμβούλιο εργάζονται προς τη νομοθέτηση νέου κανονισμού ο οποίος θα δρα *(ι)* συμπληρωματικά με το Γενικό Κανονισμό Προστασίας Δεδομένων ΓΚΠΔ, αλλά θα *(ιι)* αντικαταστήσει τη προηγούμενη Οδηγία για τη Προστασία της Ιδιωτικής Ζωής στο Τομέα των Ηλεκτρονικών Επικοινωνιών του 2002. Σε αυτό το πλαίσιο προετοιμάζεται ο *"Κανονισμός του Ευρωκοινοβουλίου και του Ευρωπαϊκού Συμβουλίου σχετικά με το σεβασμό της ιδιωτικής ζωής και την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες και τη κατάργηση της οδηγίας 2002/58/EC"* με τη συνήθη νομοθετική διαδικασία 2017/0003/COD.

Υπήρξε προσπάθεια ώστε ο Γενικός Κανονισμός Προστασίας Δεδομένων του 2018 να τεθεί σε εφαρμογή ταυτόχρονα με τον νέο κανονισμό αλλά αυτό δεν κατέστει εφικτό τότε.

Ορισμός Βασικών Εννοιών

Προσωπικά Δεδομένα

Προσωπικά δεδομένα αποτελούν όλα τα γεγονότα, δεδομένα ή πληροφορίες τα οποία αφορούν ένα άτομο και το άτομο αυτό δύναται σε οποιαδήποτε χρονική στιγμή να μην επιθυμεί να τα γνωρίζουν άλλοι εκτός από το ίδιο το άτομο. Ακόμη και εάν το άτομο σε συγκεκριμένες περιπτώσεις αποδέχεται ότι συγκεκριμένοι φίλοι, γνωστοί, συνεργάτες ή συγγενείς του γνωρίζουν μέρος ή μέρη αυτών, ενδέχεται το άτομο να μην αποδέχεται ούτε και να συναινεί αυτά τα γεγονότα ή πληροφορίες να τα γνωρίζουν τρίτοι με τους οποίους το άτομο δεν έχει σχέση εμπιστοσύνης ή δεν έχει δώσει ρητή συγκατάθεση. (Parent, 1983, 305-309)

Κάποια δεδομένα χρήζουν ακόμα μεγαλύτερης προστασίας γιατί εμπίπτουν στο σκληρότερο πυρήνα της ιδιωτικότητας και συνήθως αναγνωρίζονται ως "Ευαίσθητα Προσωπικά Δεδομένα". Παραδείγματα αποτελούν η φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα και πεποιθήσεις, η υγεία και το ιστορικό νόσων, οι καταναλωτικές συνήθειες και προτιμήσεις κτλ. (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 1997)

Ιδιωτικότητα ως ανθρώπινο δικαίωμα

Η ιδιωτικότητα του ατόμου ή πιο συγκεκριμένα η πληροφοριακή ιδιωτικότητα του ατόμου αφορά το ανθρώπινο δικαίωμα ενός ατόμου να λαμβάνει εξ ιδίου απόφαση για τα τον τρόπο, το χρόνο και μέχρι ποιό σημείο οι πληροφορίες που το αφορούν θα διαβιβάζονται, συγκεντρώνονται, αποθηκεύονται, επεξεργάζονται ή γίνονται προσβάσιμες σε άλλα άτομα. Σε μία δημοκρατική κοινωνία το δικαίωμα της ιδιωτικότητας πρέπει να προστατεύεται κατά πάγια πρακτική. (Westin, 1968)

Νομοθετικές Πράξεις

Κατά τη μελέτη νομοθετικών πράξεων συχνά συγχέονται τα είδη νομοθετικών πράξεων της Ευρωπαϊκής Ένωσης, όπως οι "οδηγίες" με τους "κανονισμούς". Παρότι υπάρχουν τουλάχιστον πέντε συνηθισμένα είδη νομοθετικών πράξεων, στη παρούσα μελέτη θα αρκεστούμε στο να διακρίνουμε τις οδηγίες από τους κανονισμούς. Αυτό είναι σημαντικό προκειμένου να αντιληφθούμε τη δυναμική των διαπραγματεύσεων και διαβουλεύσεων που λαμβάνουν χώρα πριν από την τελική έγκριση ή έκδοση νομοθετικών πράξεων, το βαθμό στον οποίο επηρεάζει τα μέλη - κράτη της Ευρωπαϊκής Ένωσης και το περιθώριο ελευθερίας που τους αφήνει. (European Union, 2020)

Οδηγίες

Οι οδηγίες είναι νομοθετικές πράξεις οι οποίες καθορίζουν τους στόχους που πρέπει να επιτύχουν τα κράτη-μέλη της Ευρωπαϊκής Ένωσης. Αποτελούν τις κατευθυντήριες γραμμές και συχνά περιγράφουν σε αρκετά αφαιρετικό επίπεδο τη στρατηγική και γενική πολιτική που πρέπει τα κράτη - μέλη της Ευρωπαϊκής Ένωσης να ακολουθήσουν προκειμένου να υπάρχουν συντονισμένες προσπάθειες στο σύνολο της Ευρωπαϊκής Ένωσης. (European Union, 2020)

Το βασικό χαρακτηριστικό των οδηγιών είναι πως οι οδηγίες δεν είναι δεσμευτικές προς τα κράτη - μέλη. Έτσι, εναπόκειται στη κάθε χώρα - μέλος ξεχωριστά να θεσπίσει τους δικούς της νόμους σε εθνικό επίπεδο προκειμένου να πετύχει τους στόχους που περιγράφονται στην κάθε οδηγία της Ευρωπαϊκής Ένωσης.

Άρα οι οδηγίες θεωρούνται και λιγότερο αυστηρά είδη νομοθετικών πράξεων, καθώς πολλά σημεία μιας οδηγίας μπορεί να επιδέχονται διαφορετικές μεταφράσεις ή ερμηνείες από κάθε χώρα, πάντα σε λογικά πλαίσια. Αυτό δίνει τη δυνατότητα στα κράτη - μέλη της Ευρωπαϊκής Ένωσης να λαμβάνουν υπόψη συγκεκριμένα εθνικά χαρακτηριστικά και ιδιαιτερότητες που έχουν κατά τη μεταφορά της οδηγίας από το Ευρωπαϊκό επίπεδο στη δική τους εθνική νομοθεσία. Συχνά, η οδηγία μπορεί να είναι δεσμευτική αλλά μόνο ως προς το τελικό αποτέλεσμα που καλούνται οι χώρες να επιτύχουν, και όχι ως προς τον τρόπο, τον τύπο ή τα μέσα που θα χρησιμοποιήσουν οι εθνικές αρχές.

Η οδηγία δεν έχει άμεση εφαρμογή στις χώρες της Ευρωπαϊκής Ένωσης καθώς η κάθε χώρα θα χρειαστεί διαφορετικό χρονικό περιθώριο για να μεταφέρει και να ενσωματώσει την οδηγία της Ευρωπαϊκής Ένωσης στο δικό της εθνικό δίκαιο, ακολουθώντας το δικό της τρόπο νομοθέτησης. Οι εθνικές αρχές οφείλουν να κοινοποιούν τα μέτρα που παίρνουν στην Ευρωπαϊκή Επιτροπή για την άσκηση καλύτερου ελέγχου. (Lawspot, 2017)

Ένα παράδειγμα οδηγίας είναι η "Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών" η οποία εκδόθηκε και τέθηκε σε εφαρμογή το 1995 και ήταν και η πρώτη απόπειρα νομοθέτησης των θεμάτων περί επεξεργασίας δεδομένων και προστασίας προσωπικών δεδομένων των πολιτών. Θα υποστήριζε κάποιος, πως η πρώτη προσέγγιση νομοθέτησης αυτού του χώρου θα έπρεπε αναγκαστικά να ήταν με οδηγία παρά με όποια άλλη πιο δεσμευτική νομοθετική πράξη καθώς θα έπαιρνε χρόνο ο εναρμονισμός της νομοθεσίας του κάθε κράτους- μέλους ώστε όλα μαζί να πορεύονται προς την ίδια κατεύθυνση.

Η οδηγία αποτελεί ένα ευέλικτο μέσο που χρησιμοποιείται κυρίως για την εναρμόνιση των εθνικών νομοθεσιών. Μπορεί να καθιστά υποχρεωτική την επίτευξη ενός συγκεκριμένου αποτελέσματος και συνήθως δίνοντας ένα συγκεκριμένο χρονοδιάγραμμα - περιθώριο, αλλά αφήνει ελεύθερες τις χώρες να αποφασίσουν τον τρόπο με τον οποίο θα πράξουν σε κάθε περίπτωση για να επιτεύξουν αυτό το στόχο. (Lawspot, 2017)

Κανονισμοί

Οι κανονισμοί, από την άλλη, είναι δεσμευτικές πράξεις για όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης τα οποία είναι και υποχρεωμένα να τις εφαρμόσουν. (European Union, 2020)

Ένα παράδειγμα κανονισμού είναι ο Γενικός Κανονισμός για την Προστασία Δεδομένων (Γ.Κ.Π.Δ.) 2016/679/ΕΚ, γνωστός και ως General Data Protection Regulation (G.D.P.R.).

Οι κανονισμοί έρχονται με συγκεκριμένη ημερομηνία κατά την οποία τίθενται σε ισχύ και εφαρμόζονται άμεσα στο εθνικό δίκαιο της κάθε χώρας - μέλους της Ευρωπαϊκής Ένωσης. Σε περίπτωση που δεν αναφέρεται ρητά η ημερομηνία ισχύος τότε αυτή είναι κατά κανόνα 20 ημέρες μετά τη δημοσίευση του κανονισμού στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. (Lawspot, 2017)

Τεχνικοί Ορισμοί και Ορολογία

Στη παρούσα μελέτη θα χρειαστεί να αναφερθούμε σε κάποιους τεχνικούς ορισμούς και ορολογία. Σε αυτό το κεφάλαιο παρατίθενται οι σημαντικότεροι για να μπορούμε να ανατρέχουμε στον κάθε ορισμό αντίστοιχα.

Ανωνυμοποίηση Δεδομένων

Η ανωνυμοποίηση δεδομένων είναι ένα είδος επεξεργασίας των δεδομένων με σκοπό τη προστασία της ιδιωτικής ζωής. Συγκεκριμένα, είναι η διαδικασία της αφαίρεσης ή αλλοίωσης στοιχείων από το σύνολο δεδομένων τα οποία μπορούν να ταυτοποιήσουν μοναδικά κάποιο άτομο ή υποκείμενο. (Karras et al., 2007, 758-769)

Για παράδειγμα, μια κοινή πρακτική στην έναρξη της ανωνυμοποίσης δεδομένων είναι η αφαίρεση του ονόματος, του αριθμού φορολογικού μητρώου ή αριθμού δελτίου ταυτότητας και μέρους (ή και ολόκληρης) της διεύθυνσης κατοικίας ενός ατόμου. Αυτά τα στοιχεία θα ταυτοποιούσαν μοναδικά ένα άτομο καθώς δεν θα υπήρχε δεύτερο άτομο με ακριβώς ίδια τιμή σε κάποιο από αυτά τα πεδία.

Στη συνέχεια των κοινών πρακτικών αφαιρούνται ή αλλοιώνονται μερικώς κάποιοι συνδυασμοί δεδομένων - τιμών, π.χ. το φύλο και η ημερομηνία γέννησης μαζί, ώστε να αποφευχθεί η έμμεση αναγνώριση. Για παράδειγμα, σε πολλές περιπτώσεις συνόλων δεδομένων ενδέχεται να υπάρχει μόνο μία εγγραφή η οποία να πληρεί τα κριτήρια "άνδρας" και "01/01/2021" ταυτόχρονα, παρότι υπάρχουν πολλές εγγραφές για "άνδρας" και πολλές εγγραφές για "01/01/2021" ξεχωριστά. Αυτό που μας ενδιαφέρει είναι ο συνδυασμός. Εάν εμείς προσπαθούμε να αναγνωρίζουμε ένα συγκεκριμένο άτομο ανάμεσα στο σύνολο των δεδομένων, και γνωρίζουμε ότι πληροί αυτά τα δύο κριτήρια ταυτόχρονα, τότε ο συνδυασμός των πεδίων θα αρκούσε για να πεισθούμε ότι η συγκεκριμένη εγγραφή αντιστοιχεί στο άτομο που προσπαθούμε να αναγνωρίσουμε. Δεν χρειάζεται να αφαιρέσουμε το φύλο ή την ημερομηνία από όλες τις εγγραφές και εξ ολοκλήρου, παρά μόνο να μελετήσουμε με αλγόριθμο το σύνολο των δεδομένων και να αφαιρέσουμε μόνο συγκεκριμένα ψηφία, π.χ. να αφαιρέσουμε μόνο την ημέρα και το μήνα από το πεδίο της ημερομηνίας αφήνοντας το έτος ως έχει, και αυτό μόνο σε κάποιες περιπτώσεις συνδυασμών με λιγότερες εγγραφές.

Υπάρχουν διάφορες τεχνικές ανωνυμοποίησης δεδομένων και ανοιχτού κώδικα λογισμικό που μπορούμε να χρησιμοποιήσουμε για την εισαγωγή δεδομένων, αυτοματοποιημένη ανάλυση, λήψη αποφάσεων για τις παραμέτρους ανωνυμοποίησης (πιο χαλαρή ή πιο αυστηρή), επεξεργασία (δηλαδή ανωνυμοποίηση) και εξαγωγή της νέας έκδοσης του συνόλου δεδομένων σε ξεχωριστό αρχείο.

Οι τεχνικές ανωνυμοποίησης δεδομένων προτείνεται να χρησιμοποιούνται ευρέως σε κάθε περίπτωση όπου αναμεταδίδουμε, αποστέλλουμε ή αποθηκεύουμε δεδομένα τα οποία δε χρειαζόμαστε ως έχουν στην αρχική τους μορφή, για τους νόμιμους λόγους που τα συλλέξαμε και αποθηκεύουμε.

Για παράδειγμα, τα ιατρικά δεδομένα εν γένει ή για παράδειγμα τα αποτελέσματα αιματολογικών εξετάσεων ενός νοσοκομείου για το τελευταίο ημερολογιακό έτος πρέπει να αποσυνδέονται από τους ασθενείς με τέτοιο τρόπο ώστε να προστατεύεται το ιατρικό απόρρητο καθώς τα ιατρικά δεδομένα αποτελούν ευαίσθητα προσωπικά δεδομένα. Στο παράδειγμα αυτό, εάν θέλουμε να μελετήσουμε τα δεδομένα στατιστικά και να αναγνωρίσουμε κάποια τάση ανάμεσα στους ασθενείς με τη πάροδο του χρόνου στο σύνολο, τότε δεν χρειάζεται τα δεδομένα αυτά να περιλαμβάνουν στοιχεία των ασθενών παρά μόνο τα αποτελέσματα. (ISO, 2017)

Η ανωνυμοποίηση δεδομένων οφείλει να προκαλεί μόνιμες αλλοιώσεις στα αρχικά δεδομένα ή σε μια νέα έκδοση των δεδομένων αυτών, σε ικανοποιητικό βαθμό ώστε να εξασφαλίζεται η ανωνυμία των υποκειμένων. Δηλαδή, να γίνεται όλο και δυσκολότερο να αναγνωρίσουμε συγκεκριμένο υποκείμενο ανάμεσα στο σύνολο των δεδομένων.

Απο την άλλη όμως, το αρνητικό είναι πως όσο πιο ενδελεχείς και αναλυτικοί γινόμαστε κατά την ανάλυση του συνόλου δεδομένων και κάνοντας όλο και πιο ευρεία χρήση τεχνικών ανωνυμοποίησης, τόσο περισσότερο αλλοιώνουμε τα δεδομένα χάνοντας πολύτιμη πληροφορία. Επομένως αναλόγως με τη κάθε περίπτωση χρήσης αλλά και με το είδος των δεδομένων οφείλουμε να κάνουμε κάποιες παραδοχές ώστε να εξασφαλίζεται η προστασία της ιδιωτικής ζωής σε ικανοποιητικό βαθμό ενώ ταυτόχρονα τα δεδομένα να συνεχίζουν να εξυπηρετούν τους νόμιμους σκοπούς που επιδιώκουμε. (Karras et al., 2007, 758-769)

Ψευδοανωνυμοποίηση

Η ψευδοανωνυμοποίηση είναι μια διαδικασία διαχείρισης δεδομένων με σκοπό την αποσύνδεση τους από τα υποκείμενα τα οποία αφορούν. Συγκεκριμένα, κάθε προσωπικά αναγνωρίσιμο πεδίο πληροφορίας σε μία εγγραφή δεδομένων αντικαθίσταται από ένα ή περισσότερα τεχνητά αναγνωριστικά ή ψευδώνυμα. Υπάρχει δηλαδή μια συγκεκριμένη αντιστοιχία δεδομένων που αντικαταστήσαμε και συμβόλων που χρησιμοποιούμε σε κάθε περίπτωση.

Αυτή η διαδικασία είναι παρόμοια με την ανωνυμοποίηση δεδομένων που αναφέραμε παραπάνω με τη διαφορά ότι εδώ εισάγουμε νέα τεχνητά αναγνωριστικά όπως κωδικούς ή αριθμούς όπου χρειάζεται, αντί να αφαιρούμε τα δεδομένα εντελώς. Επομένως στην ψευδοανωνυμοποίηση κάθε βήμα αντικατάστασης καθιστά τη συγκεκριμένη εγγραφή ως λιγότερο αναγνωρίσιμη, ενώ διατηρεί το σύνολο δεδομένων πιο κατάλληλο για ανάλυση και επεξεργασία χωρίς μεγάλη απώλεια πληροφορίας.

Η ψευδοανωνυμοποίηση αποτελεί μια εύκολη προσέγγιση με σκοπό την συμμόρφωση με το Γενικό Κανονισμό Προστασίας Δεδομένων (Γ.Κ.Π.Δ.) τον οποίο μελετάμε πιο κάτω εκτενώς.

Το όφελος της ψευδοανωνυμοποίησης για τον εμπορικό κόσμο και τις εταιρείες πληροφορικής, σε αντίθεση με την ανωνυμοποίηση δεδομένων, είναι ότι με την ψευδοανωνυμοποίηση μπορούμε να επαναφέρουμε τα δεδομένα στην αρχική τους μορφή εάν κρατήσουμε στην άκρη και έχουμε στη κατοχή μας τα δεδομένα που αφαιρέσαμε κατά την ψευδοανωνυμοποίηση με τη σωστή αντιστοιχία. (Neubauer & Heurix, 2011, 190-204)

Κρυπτογράφηση

Η κρυπτογράφηση είναι μια διαδικασία κωδικοποίησης δεδομένων κατά την οποία η αρχική μορφή των δεδομένων, λεγόμενη και "απλό κείμενο", μετατρέπεται σε μια εναλλακτική μορφή την οποία ονομάζουμε "κρυπτογράφημα" ή "κωδικοποιημένο κείμενο".

Το κρυπτογράφημα δεν είναι αναγνώσιμο από τον άνθρωπο ή τον υπολογιστή ως έχει. Η αναπαράστασή του κρυπτογραφήματος μοιάζει με μία ακατανόητη και τυχαία σειρά αλφαριθμητικών ή άλλων συμβόλων.

Χρησιμοποιώντας ξανά έναν υπολογιστή με μία παρόμοια διαδικασία, είναι εφικτό να αποκρυπτογραφήσουμε το κωδικοποιημένο κείμενο ώστε ξαναπάρουμε την αρχική του μορφή, αλλά μόνο εάν γνωρίζουμε το "κλειδί κρυπτογράφησης" που χρησιμοποιήθηκε κατά τη διαδικασία της κρυπτογράφησης. Δηλαδή, εάν έχουμε το κατάλληλο κλειδί μπορούμε να αναιρέσουμε τη κρυπτογράφηση χωρίς κάποια απώλεια πληροφορίας και να διαβάσουμε το απλό κείμενο όπως πριν.

Τα κρυπτογραφημένα δεδομένα μπορούν να αποσταλούν ή να διαμοιραστούν στο δίκτυο με τον ίδιο τρόπο που κοινοποιούμε το απλό κείμενο, καθώς αποτελούν και αυτά κείμενο. Δηλαδή, η κρυπτογράφηση εξασφαλίζει ότι τα δεδομένα μπορούν να διαβαστούν από όποιον γνωρίζει το κλειδί. Η κρυπτογράφηση δεν μπορεί να προλάβει ούτε να σταματήσει τη υποκλοπή δεδομένων από το δίκτυο, όμως εξασφαλίζει ότι κρυπτογραφημένα δεδομένα που ενδεχομένως έχουν υποκλαπεί δεν θα είναι χρήσιμα ούτε αναγνώσιμα από κάθε μη επιθυμητό παραλήπτη, καθώς οι παραλήπτες δεν γνωρίζουν πως να τα αποκρυπτογραφήσουν.

Για τεχνικούς λόγους, η κρυπτογράφηση χρησιμοποιεί ένα ψευδο-τυχαίο κλειδί κρυπτογράφησης το οποίο συνήθως παράγεται από κάποιο αλγόριθμο.

Σε θεωρητικό επίπεδο είναι εφικτό να αποκρυπτογραφίσει κανείς ένα κρυπτογραφημένο κείμενο, ενώ δεν γνωρίζει το σωστό κλειδί κρυπτογράφησης, απλά και μόνο δοκιμάζοντας ξανά και ξανά διαφορετικά πιθανά κλειδιά μέχρι σε κάποια από αυτές τις προσπάθειες το αποτέλεσμα που προκύπτει να είναι κείμενο που αναγνωρίζει ο άνθρωπος. (Katz & Lindell, 2021)

Πρακτικά όμως, είναι ανέφικτο να γίνει αυτό με τις σύγχρονες μεθόδους κρυπτογράφησης καθώς οι υπολογιστικοί πόροι και ο ελάχιστος χρόνος που χρειάζεται αυτή η διαδικασία είναι πολύ μεγαλύτερος από την αναμενόμενη διάρκεια ωφέλιμης ζωής αυτών των δεδομένων ή και πολύ μεγαλύτερος από τη διάρκεια ζωής των ανθρώπων που το επιχειρούν.

Για παράδειγμα, ακόμα και εάν επιστρατεύαμε δύο δισεκατομμύρια σύγχρονους υπολογιστές ταυτόχρονα για να μοιραστούν τον φόρτο εργασίας των δοκιμών, θα χρειαζόμασταν τουλάχιστον κάποια τρισεκατομμύρια χρόνια για να βρούμε με βεβαιότητα το σωστό κλειδί κρυπτογράφησης. (Scrambox, 2016)

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (Γ.Κ.Π.Δ.) που θα μελετήσουμε παρακάτω απαιτεί να χρησιμοποιηθούν τεχνικές ανωνυμοποίησης ή και κρυπτογράφησης πριν

από κάθε μετάδοση δεδομένων για την εξασφάλιση της προστασίας των προσωπικών δεδομένων των πολιτών.

Αντίγραφο Ασφαλείας

Το αντίγραφο ασφαλείας (backup ή data backup) είναι ένα αντίγραφο των δεδομένων το οποίο δημιουργούμε τακτικά και φυλάσσουμε σε διαφορετικό μέρος από τα πραγματικά μας δεδομένα με σκοπό να το χρησιμοποιήσουμε σε περίπτωση απώλειας ή καταστροφής των αρχικών δεδομένων.

Για παράδειγμα, κάθε Παρασκευή σε ένα νοσοκομείο μπορεί να υπάρχει μια αυτόματη ή χειροκίνητη διαδικασία με την οποία τα δεδομένα ασθενών, είτε εξ ολοκλήρου από την αρχή είτε μόνο τα δεδομένα της τελευταίας εβδομάδας, αντιγράφονται σε ένα δεύτερο μέσο (π.χ. εξωτερικό σκληρό δίσκο) και αποθηκεύονται σε διαφορετικό όροφο ή κτίριο. Εάν υπάρξει κάποια απώλεια δεδομένων εντός εβδομάδας, μπορούμε να ανατρέξουμε στο τελευταίο αντίγραφο ασφαλείας και να ανακτήσουμε τα δεδομένα προκειμένου να συνεχίσουμε τη συνηθισμένη λειτουργία του οργανισμού.

Σε πολλές περιπτώσεις ενώ τα αρχικά, πραγματικά δεδομένα είναι κρυπτογραφημένα με σκοπό τη προστασία των προσωπικών δεδομένων των ατόμων, τα αντίγραφα ασφαλείας που κρατάμε ξεχωριστά μπορεί να μην αποθηκεύονται σε κρυπτογραφημένη μορφή. Αυτό συνήθως είναι συνειδητή επιλογή καθώς η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης κοστίζει σε υπολογιστικούς πόρους και χρόνο. Αυτό εγείρει κάποια θέματα ασφάλειας των προσωπικών δεδομένων, καθώς τα δεδομένα των ατόμων πρέπει να προστατεύονται από επεξεργασία ή κλοπή σε κάθε αντίγραφο που υπάρχει. (New Cyber-attack Advice for European Hospitals, 2021)

Το πρόβλημα της ιδιωτικότητας στη ψηφιακή εποχή

Με την ένταξή μας στο ψηφιακό κόσμο, όλο και περισσότεροι οργανισμοί συλλέγουν και παράγουν δεδομένα για κάθε άνθρωπο.

Το κόστος για τη συλλογή, επεξεργασία και παρουσίαση δεδομένων γίνεται όλο και φθηνότερο, με μικρότερες απαιτήσεις σε χρόνο και υλικό, γεγονός που δίνει όλο και μεγαλύτερη αξία στα ανθρώπινα δεδομένα και ώθηση στους οργανισμούς για συλλογή αυτών. Ως αξία εννοούμε την δυνατότητα εμπορικής ή άλλου είδους εκμετάλλευσης των δεδομένων αυτών.

Η επεξεργασία μπορεί να διαχωριστεί στην απαραίτητη επεξεργασία για την παροχή της αντίστοιχης υπηρεσίας (π.χ. αποστολή ηλεκτρονικού μηνύματος με συνημμένη φωτογραφία), αλλά μπορεί να εκτείνεται και σε επιπρόσθετη επεξεργασία (π.χ. ανάλυση φωτογραφίας, αναγνώριση αντικειμένων και χαρακτηρισμός της φωτογραφίας βάσει προϋπάρχουσας ταξινομίας) η οποία δύναται να προσφέρει επιπρόσθετες υπηρεσίες στο χρήστη ή να χρησιμοποιείται για τρίτους εμπορικούς σκοπούς. Σε πολλές περιπτώσεις, η φύση των δεδομένων δεν επιτρέπει σαφή διαχωρισμό στα είδη της επεξεργασίας.

Σημειώνουμε ότι προσωπικά δεδομένα δεν αποτελούν μόνο όλα τα δεδομένα που ο χρήστης αποφάσισε να παρέχει συνειδητά σε μία υπηρεσία, πλατφόρμα ή εταιρεία αλλά περιλαμβάνουν και όλα τα γεγονότα που καταγράφει το σύστημα για κάθε συγκεκριμένο χρήστη τα οποία συνδέονται με αυτόν και περιγράφουν τη συμπεριφορά ή τις προτιμήσεις του.

Σε πολλές περιπτώσεις η συλλογή δεδομένων δεν είναι μόνο χρήσιμη αλλά και απαραίτητη προκειμένου να προσφερθεί συγκεκριμένη υπηρεσία, η οποία ενδέχεται να είναι και καθαρά ηλεκτρονικής φύσεως, όπως η ψηφιακή επικοινωνία μεταξύ ατόμων χρησιμοποιώντας μια πλατφόρμα.

Από τη μία, κάθε είδους πληροφορία που καταγράφεται για κάθε άτομο κάνει όλο και μεγαλύτερη την ανάγκη για ιδιωτικότητα, δηλαδή το σωστό χειρισμό των δεδομένων, την ασφαλή διακίνηση αυτών στο δίκτυο και τη προστασία τους από κάθε παράγοντα που θα ήθελε να εκμεταλλευτεί την αποθηκευμένη ή διακινούμενη πληροφορία για σκοπό διαφορετικό από αυτόν που ρητά συναίνεσε ο χρήστης.

Από την άλλη, η επεξεργασία δεδομένων βοηθάει τους οργανισμούς και τις επιχειρήσεις να δημιουργήσουν περισσότερες υπηρεσίες προς τους καταναλωτές ή να βελτιώσουν τη ποιότητα

και το κόστος των υπηρεσιών, εντείνοντας τον ανταγωνισμό. Για παράδειγμα, η ανάλυση των ενδιαφερόντων και αντίστοιχα των διαφημιστικών προτιμήσεων του ατόμου βοηθάει στη παραγωγή προϊόντων ή υπηρεσιών που θα έχουν μεγαλύτερη ωφέλεια για τον ίδιο τον καταναλωτή αλλά και μεγαλύτερη εμπορική επιτυχία για την ίδια την επιχείρηση.

Στη ψηφιακή εποχή και όσο οι ηλεκτρονικές υπηρεσίες πληθαίνουν και μεγαλώνουν συνεχώς, θα πρέπει να γίνουν κάποιες συμβάσεις ιδιωτικότητας και να εισαχθούν κάποια όρια με σκοπό την ικανοποίηση και των δύο πλευρών σε κάθε περίπτωση, χωρίς καταχρήσεις ή αλόγιστη εκμετάλλευση. Αυτό το θέμα έχει απασχολήσει τόσο κοινωνικά όσο και νομικά την Ευρωπαϊκή Ένωση και όχι μόνο.

Προηγούμενες Οδηγίες της Ευρωπαϊκής Ένωσης

Στη παρούσα μελέτη είναι σημαντικό να ανατρέξουμε στη πρόσφατη νομοθετική δραστηριότητα της Ευρωπαϊκής Ένωσης με σκοπό να καταλάβουμε την εξέλιξη της νομοθεσίας, σε αντίθεση με τον ρυθμό της τεχνολογική ανάπτυξης ο οποίος και δημιουργεί συνεχώς μεγαλύτερες ανάγκες για νομοθέτηση. Η νομοθετική δραστηριότητα της Ευρωπαϊκής Ένωσης ουσιαστικά αρχίζει από το 1995 και συνεχίζει ενεργά μέχρι και σήμερα.

Οδηγία 95/46/ΕΚ

Τον Οκτώβριο του 1995 εκδόθηκε και τέθηκε σε ισχύ η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Αποτέλεσε τη πρώτη προσπάθεια της Ευρωπαϊκής Ένωσης στο μονοπάτι της νομοθέτησης και καθοδήγησης της αγοράς αλλά και της κοινωνίας, ως προς τον τρόπο χειρισμού και επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

Παρότι η οδηγία 95/46/ΕΚ καταργήθηκε από την οδηγία τον Κανονισμό ΕΕ 2016/679, έθεσε τους πρώτους ορισμούς, πυλώνες και αρχές πάνω στις οποίες στηρίχθηκαν οι οδηγίες που εκδόθηκαν σε μεταγενέστερο στάδιο. (Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 119, 4 Μαΐου 2016, 2016, 1)

Βασικοί Πυλώνες

Η οδηγία 95/46/ΕΚ στηρίχθηκε σε δύο βασικούς πυλώνες. Από τη μία θεσπίζεται και προστατεύεται η ελεύθερη διακίνηση των δεδομένων αυτών στην Ευρωπαϊκή Ένωση, κάτι που εντείνει τον ανταγωνισμό στην ενιαία αγορά της Ευρωπαϊκής Ένωσης, βοηθάει την ανάπτυξη επιχειρήσεων πέραν των γεωγραφικών ορίων μιας συγκεκριμένης χώρας - μέλους της Ευρωπαϊκής Ένωσης και εν γένει επιταχύνει την αύξηση της ποιότητας των υπηρεσιών. Από την άλλη, η οδηγία στηρίζεται στη προστασία των ανθρωπίνων δικαιωμάτων και ιδιαίτερα της

ιδιωτικότητας του ατόμου, τα οποία αποτελούσαν ανέκαθεν βασικές αρχές της Ευρωπαϊκής Ένωσης.

Εισαγωγή Βασικών Εννοιών

Η οδηγία του 1995 εισήγαγε επίσημα τις έννοιες των "προσωπικών δεδομένων" και περιγράφει τη σύνδεση των δεδομένων με συγκεκριμένο άτομο σε κάθε περίπτωση. Ακόμη, όρισε ως "επεξεργασία δεδομένων" την κάθε πράξη ή σύνολο πράξεων που εφαρμόζονται σε προσωπικά δεδομένα, ανεξαρτήτως εάν αυτό προκύπτει από χειροκίνητες αλλαγές ή από αυτοματοποιημένη μέθοδο, δηλαδή με τη χρήση υπολογιστών και αλγορίθμων. Η επεξεργασία δεδομένων περιλαμβάνει τις έννοιες της συλλογής, καταγραφής, ταξινόμησης, οργάνωσης, φύλαξης, αποθήκευσης, προσαρμογής, ανάκτησης, χρήσης, διακίνησης, διάδοσης, συνδυασμού, διαγραφής και καταστροφής δεδομένων.

Όσον αφορά την ευθύνη για την εφαρμογή των οδηγιών που προβλέπονται, ορίστηκε η έννοια του "διαχειριστή δεδομένων" η οποία δεν περιορίζεται μόνο σε ένα συγκεκριμένο φυσικό πρόσωπο σε κάθε περίπτωση, αλλά επεκτείνεται και σε κάθε τεχνικό ή τεχνητό παράγοντα (μηχανή, αλγόριθμο, λογισμικό ή υπολογιστικό πρόγραμμα), αρχή, οργανισμό ή συνδυασμό αυτών που εκτελούν πράξεις ή ενέργειες επί προσωπικών δεδομένων.

Πεδίο Εφαρμογής

Η παρούσα οδηγία είναι εφαρμοστέα και ισχυρή, όχι μόνο όταν ο "διαχειριστής δεδομένων" ή "υπεύθυνος επεξεργασίας δεδομένων" βρίσκεται εντός της Ευρωπαϊκής Ένωσης με φυσικό τρόπο αλλά και όταν χρησιμοποιεί εξοπλισμό ο οποίος βρίσκεται εντός της Ευρωπαϊκής Ένωσης με σκοπό την επεξεργασία προσωπικών δεδομένων. Δηλαδή, για παράδειγμα η οδηγία έχει ισχύ και σε οργανισμούς με έδρα εκτός Ευρωπαϊκής Ένωσης οι οποίοι απευθύνονται σε πολίτες της Ευρωπαϊκής Ένωσης καθώς η έννοια της επεξεργασίας περιλαμβάνει τον ηλεκτρονικό υπολογιστή του τελικού χρήστη.

Έχοντας ορίσει τα παραπάνω, η οδηγία καθορίζει βασικές αρχές όπως η αρχή της διαφάνειας, του νόμιμου σκοπού και της αναλογικότητας τις οποίες και θα αναλύσουμε παρακάτω.

Αρχή της Διαφάνειας

Ορίζεται το ατομικό δικαίωμα στην ενημέρωση για το πότε τα προσωπικά δεδομένα του ατόμου υπόκεινται επεξεργασία. Ο διαχειριστής δεδομένων ή υπεύθυνος επεξεργασίας οφείλει να ενημερώσει για το όνομα, τη διεύθυνση, τον λόγο επεξεργασίας και τους παραλήπτες των προσωπικών δεδομένων καθώς και ό,τι άλλη πληροφορία κρίνεται αναγκαία ώστε η επεξεργασία των προσωπικών δεδομένων να καθίσταται δίκαιη.

Τα δεδομένα μπορούν να υπόκεινται επεξεργασία μόνο εάν τουλάχιστον κάποια από τις βασικές συνθήκες είναι αληθής:

- το άτομο (υποκείμενο των δεδομένων) συναινεί ρητά,
- η επεξεργασία είναι αναγκαία για την απόδοση ή δημιουργία συμβολαίου,
- η επεξεργασία είναι αναγκαία για τη συμμόρφωση με νομική υποχρέωση,
- η επεξεργασία είναι αναγκαία για λόγους προστασίας των συμφερόντων του ίδιου του ατόμου,
- η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημοσίου συμφέροντος ή εξάσκησης επίσημης κυριαρχίας του διαχειριστή ή τρίτου στον οποίο τα δεδομένα αποστέλλονται,
- η επεξεργασία είναι αναγκαία για λόγους προστασίας έννομου συμφέροντος του διαχειριστή ή ενός τρίτου στον οποίο τα δεδομένα προσκομίζονται, με εξαίρεση των περιπτώσεων όπου τα συμφέροντα αυτά καταπατώνται από τα συμφέροντα του ατόμου.

Αρχή του Νόμιμου Σκοπού

Τα προσωπικά δεδομένα μπορούν να υπόκεινται επεξεργασία μόνο για τους σαφής και έννομους σκοπούς και δεν μπορούν να επεξεργάζονται περαιτέρω με τρόπο που δεν καλύπτεται από τις παραπάνω αρχές διαφάνειας. Τα προσωπικά δεδομένα χρήζουν προστασίας από κακή

χρήση σχετικά με τα δικαιώματα και τις ελευθερίες των ατόμων, όπως αυτές προστατεύονται από την Ευρωπαϊκή Ένωση.

Αρχή της Αναλογικότητας

Τα προσωπικά δεδομένα μπορούν να υποβάλλονται σε επεξεργασία μόνο εφόσον η επεξεργασία είναι επαρκής, σχετική και όχι υπερβολική σε σύγκριση με τους σκοπούς για τους οποίους συλλέγονται.

Τα δεδομένα οφείλουν να είναι ακριβή και πρόσφατα όπου κρίνεται απαραίτητο. Ο διαχειριστής των δεδομένων οφείλει να λάβει κάθε εύλογο βήμα για να διασφαλίσει ότι τα δεδομένα που είναι ανακριβή, ελλιπή ή απαρχαιωμένα θα διαγράφονται, διορθώνονται ή ενημερώνονται αναλόγως.

Τα δεδομένα δεν πρέπει να τηρούνται σε μορφή που επιτρέπει την αναγνώριση των υποκειμένων (ατόμων) ανάμεσα σε αυτά για μεγαλύτερο χρονικό διάστημα από ό,τι είναι απαραίτητο, για τους σκοπούς που αρχικά συλλέχθηκαν ή για τους σκοπούς που υποβάλλονται σε περαιτέρω επεξεργασία.

Τα κράτη - μέλη της Ευρωπαϊκής Ένωσης θεσπίζουν κατάλληλες εγγυήσεις για τα προσωπικά δεδομένα που αποθηκεύονται για μεγαλύτερες περιόδους για ιστορική, στατιστική ή επιστημονική χρήση.

Κατά τη χρήση των ευαίσθητων προσωπικών δεδομένων (π.χ. θρησκευτικές ή πολιτικές πεποιθήσεις) ισχύουν επιπλέον περιορισμοί.

Το υποκείμενο των δεδομένων μπορεί να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία προσωπικών δεδομένων για λόγους προώθησης προϊόντων ή υπηρεσιών (marketing).

Δεν επιτρέπεται να λαμβάνονται αποφάσεις που παρήχθησαν αποκλειστικά αλγοριθμικά ή αυτοματοποιημένα και φέρουν νομικές συνέπειες ή επηρεάζουν το υποκείμενο των δεδομένων. Ο διαχειριστής δεδομένων πρέπει να παρέχει τρόπο έφεσης όπου χρησιμοποιούνται αυτοματοποιημένες μέθοδοι λήψεως αποφάσεων.

Μεταφορά προσωπικών δεδομένων σε τρίτες χώρες

Ως "τρίτες χώρες" ορίζονται οι χώρες εκτός της Ευρωπαϊκής Ένωσης. Επιτρέπεται η μεταφορά δεδομένων σε τρίτες χώρες μόνο εάν η χώρα υπό εξέταση παρέχει επαρκή επίπεδα προστασίας.

Σε αυτό το πλαίσιο προβλέφθηκε η σύσταση επιτροπής που μπορεί να συμβουλεύσει και καθοδηγήσει τρίτες χώρες σχετικά με τη παρούσα οδηγία. (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 1995)

Οδηγία 2002/58/ΕΚ και οι τροποποιήσεις 2006/24/ΕΚ και 2009/136/ΕΚ

Την 12η Ιουλίου 2002 η Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο εξέδωσε την οδηγία 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Η οδηγία του 2002 έχει ως σκοπό να αντικαταστήσει την προηγούμενη οδηγία του 1995 με σκοπό τον εκσυγχρονισμό της νομοθεσίας, ώστε να αντικατοπτρίζονται οι τρέχουσες τεχνολογικές εξελίξεις και να αντιμετωπιστούν οι κίνδυνοι που διατρέχουν τα υποκείμενα των δεδομένων.

Η νέα οδηγία του 2002, η οποία είναι ακόμη σήμερα σε ισχύ με τις τροποποιήσεις που έγιναν στο ενδιάμεσο το 2006 και 2009, ασχολείται με τη ρύθμιση ορισμένων ζητημάτων όπως η εμπιστευτικότητα των πληροφοριών (confidentiality), η επεξεργασία των δεδομένων κίνησης στο δίκτυο (traffic data), η αντιμετώπιση της ανεπιθύμητης αλληλογραφίας (spam email) και οι πολιτικές σχετικά με τη χρήση των cookies. (Ευρωπαϊκό Κοινοβούλιο και Ευρωπαϊκό Συμβούλιο, 2002)

Η οδηγία του 2002 τροποποιήθηκε από την οδηγία 2006/24/ΕΚ όπως και από την οδηγία 2009/136 η οποία έφερε περισσότερες αλλαγές κυρίως γύρω από τα cookies, καθιστώντας τη χρήση τους να προαπαιτεί τη συγκατάθεση του χρήστη. (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2009)

Κάποιοι νομοθέτες ήλπιζαν ότι ο Κανονισμός ePrivacy (ePR) που κατά το γράψιμο αυτής της μεταπτυχιακής εργασίας είναι ακόμη σε διαβούλευση και που θα μελετήσουμε στη συνέχεια, θα μπορούσε να είχε εκδοθεί χρονικά μαζί με τον Γενικό Κανονισμό Προστασίας Δεδομένων του

2016 (εφαρμοστέο το 2018) και αντικαθιστώντας την οδηγία του 2002 (2002/58/ΕΚ), αλλά αυτό δεν κατέστη εφικτό τότε. (Lomas, 2018)

Αντικείμενο και Πεδίο Εφαρμογής

Η οδηγία του 2002 για την ηλεκτρονική προστασία της ιδιωτικής ζωής έχει συνταχθεί ειδικά για να καλύψει τις απαιτήσεις των νέων ψηφιακών τεχνολογιών που προέκυψαν από το 1995 έως το 2002 και μετά, και επίσης να διευκολύνει την προώθηση των υπηρεσιών ηλεκτρονικών επικοινωνιών.

Η οδηγία του 2002 πρακτικά συμπληρώνει την προηγούμενη οδηγία του 1995 για την προστασία δεδομένων και εφαρμόζεται σε όλα τα θέματα που δεν καλύπτονταν συγκεκριμένα από την εν λόγω οδηγία. (Ευρωπαϊκό Κοινοβούλιο και Ευρωπαϊκό Συμβούλιο, 2002, Άρθρο 1)

Ειδικότερα, το αντικείμενο της οδηγίας είναι το "δικαίωμα στην ιδιωτική ζωή στον τομέα των ηλεκτρονικών επικοινωνιών" και η ελεύθερη κυκλοφορία δεδομένων, εξοπλισμού και υπηρεσιών επικοινωνίας. (Ευρωπαϊκό Κοινοβούλιο και Ευρωπαϊκό Συμβούλιο, 2002)

Βασικές Διατάξεις

Η πρώτη γενική υποχρέωση σε αυτή την οδηγία είναι η παροχή ασφάλειας των υπηρεσιών, βάσει του άρθρου 4. Οι παραλήπτες είναι όλοι οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών. Αυτή η υποχρέωση περιλαμβάνει επίσης την υποχρέωση ενημέρωσης των συνδρομητών όποτε υπάρχει ιδιαίτερος κίνδυνος, όπως για παράδειγμα σε μία επίθεση από ιό ή άλλου είδους κακόβουλο λογισμικό. (Ευρωπαϊκό Κοινοβούλιο και Ευρωπαϊκό Συμβούλιο, 2002, Άρθρο 4)

Η δεύτερη γενική υποχρέωση σε αυτή την οδηγία είναι η διατήρηση της εμπιστευτικότητας των πληροφοριών, βάσει του άρθρου 5. Οι παραλήπτες είναι τα κράτη - μέλη της Ευρωπαϊκής Ένωσης τα οποία θα πρέπει να απαγορεύουν την ακρόαση, την αποθήκευση και άλλα είδη υποκλοπής ή παρακολούθησης της επικοινωνίας και της σχετικής κυκλοφορίας των δεδομένων στο διαδίκτυο. Μοναδική εξαίρεση σε αυτό το κανόνα είναι οι περιπτώσεις που

δίνεται η ρητή συγκατάθεση του χρήστη όπως περιγράφεται στο άρθρο 15. (Ευρωπαϊκό Κοινοβούλιο και Ευρωπαϊκό Συμβούλιο, 2002, Άρθρο 5)

Διατήρηση Δεδομένων

Βάσει των παραπάνω διατάξεων, η οδηγία υποχρεώνει τους παρόχους υπηρεσιών να διαγράψουν ή να ανωνυμοποιήσουν τα δεδομένα κίνησης που υποβάλλονται σε επεξεργασία όταν αυτά δεν είναι πλέον απαραίτητα, εκτός αν πληρούνται οι προϋποθέσεις του άρθρου 15.

Η διατήρηση των δεδομένων επιτρέπεται για σκοπούς χρέωση,ς αλλά μόνο εφόσον το καταστατικό των περιορισμών επιτρέπει τη νόμιμη παρακολούθηση της πληρωμής. Τα δεδομένα μπορούν να διατηρηθούν κατόπιν συγκατάθεσης ενός χρήστη για υπηρεσίες προώθησης (marketing) και άλλες υπηρεσίες προστιθέμενης αξίας. Και για τις δύο προηγούμενες χρήσεις, το υποκείμενο των δεδομένων πρέπει να ενημερώνεται τον λόγο για τον οποίο γίνεται η επεξεργασία των δεδομένων καθώς και για το αντίστοιχο χρονικό διάστημα.

Οι συνδρομητές έχουν το δικαίωμα για μη αναλυτική χρέωση. Ομοίως, οι χρήστες πρέπει να μπορούν να εξαιρεθούν από την αναγνώριση της τηλεφωνικής γραμμής.

Όπου μπορούν να υποβληθούν σε επεξεργασία δεδομένα σχετικά με την τοποθεσία των χρηστών ή άλλη κυκλοφορία, το άρθρο 9 προβλέπει ότι αυτό θα επιτρέπεται μόνο εάν *(ι)* τα δεδομένα αυτά είναι ανώνυμα, *(ιι)* οι χρήστες έχουν δώσει τη συγκατάθεσή τους ή *(ιιι)* για τη παροχή υπηρεσιών προστιθέμενης αξίας. Όπως και στη προηγούμενη περίπτωση, οι χρήστες πρέπει να ενημερώνονται εκ των προτέρων για τον χαρακτήρα των πληροφοριών που συλλέγονται και να έχουν την επιλογή να εξαιρεθούν από αυτή τη διαδικασία. (Ευρωπαϊκό Κοινοβούλιο και Ευρωπαϊκό Συμβούλιο, 2002, Άρθρο 15)

Ανεπιθύμητη αλληλογραφία, ηλεκτρονικό ταχυδρομείο ή άλλα μηνύματα

Βάσει του άρθρου 13, απαγορεύεται η χρήση διευθύνσεων ηλεκτρονικού ταχυδρομείου για σκοπούς προώθησης (marketing). Η οδηγία καθορίζει το καθεστώς επιλογής, όπου τα ανεπιθύμητα ηλεκτρονικά μηνύματα μπορούν να αποστέλλονται μόνο με προηγούμενη συμφωνία του παραλήπτη.

Ένα φυσικό ή νομικό πρόσωπο που αρχικά συλλέγει δεδομένα διευθύνσεων στο πλαίσιο της πώλησης ενός προϊόντος ή μιας υπηρεσίας, έχει το δικαίωμα να τα χρησιμοποιεί για εμπορικούς σκοπούς, υπό τη προϋπόθεση ότι οι πελάτες έχουν προηγουμένως την ευκαιρία να απορρίψουν μια τέτοια επικοινωνία.

Η ευκαιρία απόρριψης τέτοιας επικοινωνίας οφείλει να παρέχεται όχι μόνο στην αρχή αλλά και στη συνέχεια. Τα κράτη - μέλη έχουν την υποχρέωση να διασφαλίζουν ότι θα απαγορεύεται η ανεπιθύμητη επικοινωνία εκτός από τις περιπτώσεις που αναφέρονται στο άρθρο 13. (Ευρωπαϊκό Κοινοβούλιο και Ευρωπαϊκό Συμβούλιο, 2002, Άρθρο 13)

Cookies

Η οδηγία αναγνωρίζει τη σημασία και τη χρησιμότητα των cookies για τη λειτουργία του σύγχρονου διαδικτύου, αλλά προειδοποιεί επίσης για τον κίνδυνο που ενδέχεται να παρουσιάσουν τέτοια μέσα στην ιδιωτική ζωή.

Η αλλαγή της οδηγίας δεν επηρεάζει όλους τους τύπους cookie. Εξαιρούνται εκείνα που θεωρούνται "απολύτως απαραίτητα για την παροχή μιας υπηρεσίας που ζητά ο χρήστης", όπως για παράδειγμα τα cookies που παρακολουθούν τα περιεχόμενα του ηλεκτρονικού καλαθιού αγορών του χρήστη σε μία ηλεκτρονική αγορά.

Το άρθρο παραμένει τεχνολογικά ουδέτερο, δηλαδή δεν αναφέρει συγκεκριμένα τεχνολογικά μέσα που μπορούν να χρησιμοποιηθούν για την αποθήκευση δεδομένων, αλλά εφαρμόζεται για οποιεσδήποτε πληροφορίες αναγκάζεται να αποθηκεύσει ο περιηγητής του χρήστη από κάποια ιστοσελίδα. Αυτό αντικατοπτρίζει την επιθυμία των νομοθετών της Ευρωπαϊκής Ένωσης να επιτρέπει μελλοντικές τεχνολογικές εξελίξεις στα πλαίσια της οδηγίας.

Αποδέκτες της υποχρέωσης είναι όλα τα κράτη - μέλη τα οποία και υποχρεούνται να διασφαλίσουν ότι η χρήση δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών στο πρόγραμμα περιηγητή ενός χρήστη, επιτρέπεται μόνο εάν ο χρήστης *(ι)* διαθέτει σαφείς και περιεκτικές πληροφορίες για τους σκοπούς της αποθήκευσης και πρόσβασης των δεδομένων και *(ιι)* έχει δώσει τη συγκατάθεση του για αυτό.

Το καθεστώς είναι τέτοιο ώστε η ρύθμιση να γίνεται με τη μορφή opt-in δηλαδή ο χρήστης πρέπει να δώσει τη συγκατάθεση του προτού αποθηκευτούν cookies ή άλλα δεδομένα

στο πρόγραμμα περιήγησής του. Η αρχική συγκατάθεση του χρήστη για έναν ιστότοπο μπορεί να μεταφερθεί σε επαναλαμβανόμενα αιτήματα περιεχομένου για τον ίδιο ιστότοπο.

Η οδηγία δεν παρέχει κατευθυντήριες γραμμές σχετικά με τι μπορεί να αποτελεί εξαίρεση αλλά απαιτεί να μην τοποθετούνται cookies χωρίς τη συγκατάθεση του χρήστη εκτός από αυτά που είναι "απολύτως απαραίτητα για την παροχή μιας υπηρεσίας που ζητά ο χρήστης". (Ευρωπαϊκό Κοινοβούλιο και Ευρωπαϊκό Συμβούλιο, 2002)

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) ή General Data Protection Regulation (GDPR) αποτελεί το νομοθετικό πλαίσιο που εκδόθηκε το 2016 και τέθηκε σε ισχύ από την Ευρωπαϊκή Ένωση με υποχρεωτική εφαρμογή από την 25η Μαΐου 2018 με σκοπό τη προστασία των πολιτών της Ευρωπαϊκής Ένωσης (ΕΕ) από την επεξεργασία των δεδομένων τους.

Καταργεί προηγούμενη οδηγία του 1995 και φέρνει αυστηρότερες συνθήκες για τη συναίνεση του χρήστη, πιο ευρύ ορισμό των προσωπικών και ευαίσθητων δεδομένων, προβλέψεις για τη προστασία της ιδιωτικότητας των παιδιών καθώς και το δικαίωμα στη λήθη. (Ευρωπαϊκό Κοινοβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016)

Υπόχρεοι συμμόρφωσης

Η έννοια "χρήστες της Ευρωπαϊκής Ένωσης" ή "υποκείμενο των δεδομένων" είναι αρκετά ευρεία καθώς δεν περιορίζεται ούτε στους πολίτες κρατών - μελών της Ευρωπαϊκής Ένωσης, ούτε και στους μόνιμους κατοίκους της Ευρωπαϊκής Ένωσης, αλλά περιλαμβάνει ακόμη και επισκέπτες ή τουρίστες της Ευρωπαϊκής Ένωσης καθ' όλη τη διάρκεια παραμονής τους.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) αφορά άμεσα οργανισμούς με περισσότερους από 250 εργαζόμενους που κατέχουν, διαχειρίζονται ή επεξεργάζονται δεδομένα χρηστών της Ευρωπαϊκής Ένωσης (ΕΕ).

Γενικά, ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) εφαρμόζεται εάν τουλάχιστον κάποιο από τα εξής τρία μέρη εδρεύει στην Ευρωπαϊκή Ένωση:

- ο "χειριστής δεδομένων" ή ο "υπεύθυνος επεξεργασίας" δηλαδή ο οργανισμός που συλλέγει τα δεδομένα πολιτών Ευρωπαϊκής Ένωσης,
- ο "επεξεργαστής δεδομένων" δηλαδή ο οργανισμός που επεξεργάζεται δεδομένα εκ μέρους του χειριστή δεδομένων π.χ. πάροχοι υπηρεσιών cloud,
- το "υποκείμενο των δεδομένων", δηλαδή ο πολίτης της Ευρωπαϊκής Ένωσης τον οποίο φωτογραφίζουν τα ίδια τα δεδομένα.

Ακόμη, υπό συγκεκριμένες συνθήκες ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) εφαρμόζεται ακόμη και σε οργανισμούς που δεν εδρεύουν στην Ευρωπαϊκή Ένωση

αρκεί να συλλέγουν ή να επεξεργάζονται δεδομένα πολιτών που βρίσκονται εντός της Ευρωπαϊκής Ένωσης. Δηλαδή, αυτός ο Ευρωπαϊκός κανονισμός δεν απευθύνεται μόνο σε οργανισμούς που βρίσκονται εντός Ευρωπαϊκής Ένωσης, αλλά εφαρμόζεται και σε οργανισμούς που επιθυμούν να συναλλάσσονται με χρήστες της Ευρωπαϊκής Ένωσης και συνεπώς κατέχουν και επεξεργάζονται δεδομένα αυτών.

Με αυτό το τρόπο ενισχύεται η προστασία των πολιτών κρατών - μελών της Ευρωπαϊκής Ένωσης, καθώς δε χρειάζεται οι ίδιοι οι πολίτες να κάνουν διάκριση των υπηρεσιών που βρίσκουν στο διαδίκτυο σε Ευρωπαϊκές και μη, διότι όσοι οργανισμοί επιτρέπουν πρόσβαση στις υπηρεσίες τους από υπολογιστές της Ευρωπαϊκής Ένωσης οφείλουν να συμμορφώνονται με την ισχύουσα νομοθεσία. (Ευρωπαϊκό Κοινοβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016)

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) ή European Data Protection Board (EDPC) συστάθηκε μαζί με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) ως ανεξάρτητο Ευρωπαϊκό σώμα με στόχο την συνεπή εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) αλλά και της προώθησης της συνεργασίας μεταξύ των εθνικών αρχών προστασίας δεδομένων. (Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 119, 4 Μαΐου 2016, 2016, 14)

Τα καθήκοντα του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων μεταξύ άλλων περιλαμβάνουν:

- την έκδοση κατευθυντήριων γραμμών, συστάσεων και αναγνώρισης των καλών πρακτικών σχετικά με την ερμηνεία και τις εφαρμογές του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ),
- τη συμβουλευτική δράση προς για την Ευρωπαϊκή Επιτροπή ως προς τα ζητήματα σχετικά με τη προστασία των προσωπικών δεδομένων εντός του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ),

- την υιοθεσία απόψεων προκειμένου να διασφαλιστεί η συνεπής εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) από τις εθνικές αρχές σε κάθε χώρα, ιδιαίτερα σε ότι αφορά αποφάσεις που έχουν διασυνοριακές συνέπειες ή αποτελέσματα,
- την λειτουργία ως όργανο επίλυσης διαφορών σε περιπτώσεις που προκύπτουν διαφορές μεταξύ εθνικών αρχών που συνεργάζονται για την εκτέλεση του κανονισμού στο πλαίσιο διασυνοριακών υποθέσεων,
- την ενθάρρυνση της ανάπτυξης κώδικα δεοντολογίας και καθιέρωσης μηχανισμών πιστοποίησης στο πεδίο της προστασίας δεδομένων,
- τη προώθηση της συνεργασίας και αποτελεσματικής ανταλλαγής πληροφοριών και καλών πρακτικών μεταξύ των εθνικών αρχών. (Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 119, 4 Μαΐου 2016, 2016, 70)

Διευκρίνιση Ορισμού Προσωπικών Δεδομένων

Η Ευρωπαϊκή Επιτροπή ορίζει ότι προσωπικά δεδομένα είναι όλα τα δεδομένα που σχετίζονται με αναγνωρισμένο ή αναγνωρίσιμο άτομο. Δηλαδή, ακόμη και εάν δεν μπορεί κανείς να αναγνωρίσει άμεσα το άτομο που αφορούν τα υπό μελέτη δεδομένα, τότε θα πρέπει να ελεγχθεί και διασαφηνιστεί κατά πόσο το άτομο που βρίσκεται πίσω από τα δεδομένα μπορεί να ταυτοποιηθεί από αυτά με άλλους τρόπους. (Information Commissioner's Office, 2021)

Στόχος

Ο κύριος στόχος του Γενικού Κανονισμού Προστασίας Δεδομένων είναι να δώσει στους τελικούς χρήστες τον έλεγχο επί των προσωπικών τους δεδομένων και να απλοποιήσει το νομοθετικό πλαίσιο με σκοπό τη διευκόλυνση παγκόσμιων επιχειρήσεων, ενοποιώντας τη νομοθεσία σε όλη την Ευρωπαϊκή Ένωση. (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2016)

Νόμιμες Συνθήκες Επεξεργασίας

Τα δεδομένα μπορούν να υπόκεινται επεξεργασία μόνο εάν τουλάχιστον κάποια από τις εξής βασικές συνθήκες είναι αληθής:

- το άτομο ή υποκείμενο των δεδομένων συναινεί ρητά,

- η επεξεργασία είναι αναγκαία για την απόδοση ή για τη δημιουργία συμβολαίου,
- η επεξεργασία είναι αναγκαία για τη συμμόρφωση με νομική υποχρέωση,
- η επεξεργασία είναι αναγκαία για λόγους προστασίας των συμφερόντων του ίδιου του ατόμου - υποκειμένου,
- η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημοσίου συμφέροντος,
- η επεξεργασία είναι αναγκαία για λόγους προστασίας έννομου συμφέροντος του διαχειριστή ή ενός τρίτου στον οποίο τα δεδομένα προσκομίζονται, με εξαίρεση των περιπτώσεων όπου τα συμφέροντα αυτά καταπατώνται από τα συμφέροντα του ατόμου ειδικά όταν αυτό αφορά τα θεμελιώδη δικαιώματα παιδιών στην Ευρωπαϊκή Ένωση. (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2016)

Διευκρινίσεις για τη συναίνεση χρήστη

Σε περίπτωση που δίνεται ρητή άδεια από το υποκείμενο των δεδομένων, τότε η επεξεργασία είναι νόμιμη μόνο για το σκοπό που έχουν συλλεχθεί, όπως αυτός αναγράφεται κατά τη συναίνεση.

Η συναίνεση πρέπει να είναι συγκεκριμένη, να δίνεται ελεύθερα, να περιγράφεται με απλά λόγια και με ξεκάθαρο τρόπο επιβεβαίωσης από το χρήστη. Παραδείγματα παραβίασης του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) είναι:

- μία διαδικτυακή φόρμα που έχει προεπιλεγμένη την θετική απάντηση στις ρυθμίσεις συναίνεσης,
- διαφορετικά είδη δεδομένων που είναι ομαδοποιημένα σε μία προτροπή επιβεβαίωσης συγκατάθεσης.

Τα υποκείμενα δεδομένων πρέπει να έχουν δικαίωμα υπαναχώρησης και η διαδικασία αυτή απαγορεύεται να είναι δυσκολότερη από ότι η διαδικασία συναίνεσης. (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2016)

Δικαιώματα των υποκειμένων

Διαφάνεια και τυπικότητα

Το άρθρο 12 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) απαιτεί ότι ο διαχειριστής των δεδομένων ή ο υπεύθυνος επεξεργασίας πρέπει να παρέχει πληροφορίες στο υποκείμενο των δεδομένων σε μια συνοπτική, διαφανή, κατανοητή και σε εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα. Αυτό είναι ιδιαίτερα σημαντικό και αυστηρό για οποιεσδήποτε πληροφορίες αφορούν ή απευθύνονται σε παιδιά. (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2016)

Δεδομένα, Πρόσβαση και Φορητότητα

Το άρθρο 15 καθορίζει ότι τα υποκείμενα των δεδομένων έχουν δικαίωμα πρόσβασης στα δεδομένα τους. Ο υπεύθυνος επεξεργασίας οφείλει να παρέχει πληροφορίες σχετικά με τον τρόπο επεξεργασίας αυτών των προσωπικών δεδομένων. Ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να παρέχει, κατόπιν αιτήματος του υποκειμένου, επισκόπηση των κατηγοριών δεδομένων που υποβάλλονται σε επεξεργασία όπως και αντίγραφο των πραγματικών δεδομένων. Επιπλέον, ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να ενημερώνει το υποκείμενο των δεδομένων σχετικά με λεπτομέρειες επί της επεξεργασίας των δεδομένων, όπως οι σκοποί της επεξεργασίας, σε ποιους τρίτους κοινοποιούνται τα δεδομένα και πως απέκτησε τα δεδομένα που κατέχει.

Το υποκείμενο των δεδομένων θα πρέπει να μπορεί να μεταφέρει τα προσωπικά του δεδομένα από ένα ηλεκτρονικό σύστημα σε κάποιο άλλο (export - import), χωρίς την όποια παρεμπόδιση από τον διαχειριστή δεδομένων. Δεδομένα που έχουν περάσει από διαδικασία επαρκής ανωνυμοποίησης εξαιρούνται από αυτό τον όρο, όσο η έννοια "επαρκής" εξασφαλίζει ότι είναι πρακτικά και τεχνικά ανέφικτο να αναγνωρίσουμε το υποκείμενο των δεδομένων. Όμως τα δεδομένα που είναι εφικτό να ξανασυνδεθούν με το υποκείμενο των δεδομένων, για παράδειγμα μέσω ενός πίνακα αντιστοιχίας, πρέπει να είναι ανακτήσιμα από το σύστημα. (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2016)

Η παραπάνω παράγραφος περί ανάκτησης ή και μεταφοράς προσωπικών δεδομένων, όπως η ανάκτηση ελαφρώς ανωνυμοποιημένων ή αποσυνδεδεμένων προσωπικών δεδομένων φέρνει

τεχνικές δυσκολίες στην υλοποίηση που θα μελετήσουμε ακολούθως. (Veale et al., 2018, 111-112)

Όσον αφορά τα δεδομένα που δίνονται στο υποκείμενο των δεδομένων κατόπιν αιτήματος του, περιλαμβάνει όχι μόνο τα δεδομένα που το ίδιο το υποκείμενο υπέβαλε αλλά και ότι άλλα δεδομένα ή γεγονότα παρατηρήθηκαν από το σύστημα, όπως για παράδειγμα η συμπεριφορά του υποκειμένου κατά τη χρήση της εν λόγω υπηρεσίας, διαδικτυακής ιστοσελίδας ή ηλεκτρονικού προϊόντος. Δηλαδή περιλαμβάνει όλα τα δεδομένα που το σύστημα δημιούργησε και αφορούν το συγκεκριμένο χρήστη. (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2016)

Βάσει του άρθρου 20, όλα τα δεδομένα πρέπει να δίνονται στον χρήστη με δομημένη μορφή και να χρησιμοποιούνται κοινά ηλεκτρονικά πρότυπα, σεβόμενοι το δικαίωμα των χρηστών στη φορητότητα δεδομένων. (European Commission, 2017)

Διόρθωση και Διαγραφή

Το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση. 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. (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2018)

Βάσει το άρθρου 30 του Γενικού Κανονισμού Προστασίας Δεδομένων, το προηγούμενο δικαίωμα στη λήθη καταργείται και αντικαθίσταται από ένα πιο περιορισμένο δικαίωμα του υποκειμένου των δεδομένων για τη διαγραφή προσωπικών του δεδομένων βασισμένο σε έναν από τους προβλεπόμενους λόγους. (Ευρωπαϊκό Κοινοβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016)

Δικαίωμα εναντίωσης στην αυτοματοποιημένη επεξεργασία

Βάσει του άρθρου 21 του Γενικού Κανονισμού Προστασίας Δεδομένων, κάθε υποκείμενο έχει τη δυνατότητα εναντίωσης στην επεξεργασία των προσωπικών του δεδομένων για λόγους προώθησης, πωλήσεων ή άλλους μη-υπηρεσιακούς λόγους. Αυτό συνεπάγεται ότι ο διαχειριστής

των δεδομένων οφείλει να δίνει την επιλογή στο χρήστη για να σταματήσει την επεξεργασία. (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2016)

Ακόμη, πρέπει να καθορίζεται σαφώς πού χρησιμοποιούνται αυτοματοποιημένες μέθοδοι λήψης αποφάσεων και αυτόματης δημιουργίας προφίλ για τον χρήστη βάσει των δεδομένων του. Επίσης, οι διαχειριστές δεδομένων οφείλουν να ενημερώνουν τα υποκείμενα δεδομένων, να έχουν απλές μεθόδους ανθρώπινης παρέμβασης σχετικά με τις αποφάσεις που λαμβάνονται αυτόματα και να ελέγχουν σε τακτά χρονικά διαστήματα ότι τα εν λόγω συστήματα λειτουργούν όπως σχεδιάστηκαν. (Rights related to automated decision making including profiling, 2021)

Ψευδο-ανωνυμοποίηση

Βάσει του άρθρου 25, ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) απαιτεί τη χρήση μεθόδων ψευδοανωνυμοποίησης, όπως περιγράφονται παραπάνω στο κεφάλαιο τεχνικών ορισμών και ορολογίας. Δηλαδή, τα αποθηκευμένα δεδομένα οφείλουν να μην μπορούν να απεικονίζουν συγκεκριμένο υποκείμενο χωρίς τη χρήση επιπρόσθετων πληροφοριών.

Ένα παράδειγμα που ικανοποιεί τη συνθήκη της ψευδοανωνυμοποίησης είναι η χρήση της κρυπτογράφησης μέσω της οποίας κάθε απεικόνιση των δεδομένων ως έχουν καθιστά το αποτέλεσμα μη αναγνώσιμο χωρίς τη χρήση του κλειδιού αποκρυπτογράφησης. Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) απαιτεί ότι το κλειδί αποκρυπτογράφησης θα πρέπει να αποθηκεύεται ξεχωριστά από τα ψευδοανωνυμοποιημένα δεδομένα για σκοπούς ασφάλειας.

Ένας άλλος τρόπος ικανοποίησης της συνθήκης ψευδοανωνυμοποίησης είναι η χρήση συμβολισμών (tokenization) δηλαδή της αντικατάστασης των ευαίσθητων προσωπικών πληροφοριών με υποκατάστατα τα οποία δεν αποτελούν ευαίσθητα προσωπικά δεδομένα. Αυτή η προσέγγιση εξασφαλίζει τόσο την προστασία των υποκειμένων όσο και τη χρηστικότητα των δεδομένων και άμεσης εκμετάλλευσης τους χωρίς μετασχηματισμούς. (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2016)

Ασφάλεια προσωπικών δεδομένων

Βάσει των άρθρων 33 και 34, ο διαχειριστής δεδομένων είναι νομικά υπεύθυνος για να ενημερώσει την εποπτική αρχή, χωρίς καθυστέρηση και εντός 72 ωρών το αργότερο, για κάθε

παραβίαση δεδομένων που ενδέχεται να έχει επιπτώσεις ή να επηρεάζει τα δικαιώματα και τις ελευθερίες των υποκειμένων. Τα υποκείμενα πρέπει επίσης να ειδοποιηθούν, εάν το ρίσκο από τη παραβίαση κρίνεται υψηλό. (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2016)

Υπεύθυνος Προστασίας Δεδομένων

Βάσει του άρθρου 37, απαιτείται ο διορισμός ενός "Υπεύθυνου Προστασίας Δεδομένων" ή Data Protection Officer (D.P.O.) σε κάθε οργανισμό, ο οποίος πρέπει έχει μεγάλη πείρα και γνώση σχετικά με τις καλές πρακτικές και το νόμο και θα παρέχει βοήθεια στο διαχειριστή δεδομένων με σκοπό την επίβλεψη των συστημάτων και την εξασφάλιση της νομικής συμμόρφωσης με τους κανονισμούς.

Ο υπεύθυνος προστασίας δεδομένων δύναται να είναι υπάρχον μέλος του προσωπικού ή εξωτερικός συνεργάτης μέσω συμβολαίου. Σε κάθε περίπτωση τα δεδομένα και στοιχεία του υπεύθυνου επεξεργασίας δεδομένων πρέπει να είναι δημοσιευμένα εντός του οργανισμού αλλά και κοινοποιημένα στην επιβλέπουσα αρχή και να ανανεώνονται με κάθε αλλαγή. (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2016)

Βάσει των οδηγιών που εκδόθηκαν το 2016 και αναθεωρήθηκαν το 2017, αναμένεται ότι ο υπεύθυνος προστασίας δεδομένων να είναι ειδήμων σε θέματα διαχείρισης πληροφοριακών και υπολογιστικών διαδικασιών, στην προστασία δεδομένων περιλαμβανομένου ηλεκτρονικών επιθέσεων και άλλων θεμάτων περί κρίσιμης διαχείρισης της επιχειρησιακής συνέχειας όσον αφορά τη τήρηση και επεξεργασία προσωπικών και ευαίσθητων δεδομένων. Επομένως απαιτούνται περισσότερες δεξιοτεχνίες και γνώσεις αντί απλή γνώση της νομοθεσίας. (European Commission, 2017)

Αποτελέσματα του Γενικού Κανονισμού Προστασίας Δεδομένων

Η πρόταση του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) παρ' όλο το όφελος ως προς την προστασία της ιδιωτικής ζωής προκάλεσε ποικίλες συζητήσεις, αντιδράσεις και αμφισβητήσεις οι οποίες εκτείνονται σε τεχνικό, κοινωνικό αλλά και πολιτικό επίπεδο. (Veale et al., 2018, 111-112) (Politou et al., 2018, 1-20) (Bozdag, 2018, 1-7)

Ακόμη, κόσμος που τον απασχολεί το θέμα της ιδιωτικότητας του ατόμου καθώς και οι πρόσφατες εξελίξεις στους τεχνολογικούς κλάδους φαίνεται να φέρνουν μικτές κριτικές για τα αποτελέσματα του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) σημειώνοντας μεν ότι ο κανονισμός έκανε βήματα προς τη σωστή κατεύθυνση, αλλά τονίζοντας δε ότι οι ερωτήσεις για την επάρκεια αυτής της ρύθμισης δεν έχουν απαντηθεί πλήρως. (Vanberg, 2020, 52-78)

Αυτά τα αποτελέσματα αλλά και τις τρέχουσες επιπτώσεις του Γενικού Κανονισμού Προστασίας Δεδομένων θα τα κατηγοριοποιήσουμε σε αυτό το κεφάλαιο ως ακολούθως:

- Προκλήσεις και προβλήματα που έφερε ο Γενικός Κανονισμός Προστασίας Δεδομένων στη Διοίκηση Οργανισμών Τεχνολογικού ενδιαφέροντος
- Θετικές απόψεις από το χώρο της τεχνολογίας

Προκλήσεις στη Διοίκηση Οργανισμών Τεχνολογίας

Προκλήσεις Κόστους και Ύψους Επένδυσης

Επαγγελματίες του κλάδου της πληροφορικής εκτιμούν ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων χρειάζεται επιπλέον επένδυση χρημάτων. Συγκεκριμένα, σε έρευνα σχετικά με τα έξοδα και επενδύσεις που προκύπτουν από την ανάγκη για συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) 80% των συμμετεχόντων ανέφεραν ότι θα χρειαστούν τουλάχιστον 100 χιλιάδες δολάρια Ηνωμένων Πολιτειών Αμερικής (ΗΠΑ) επιπλέον. (Babel, 2017)

Οι ανησυχίες επαναλήφθηκαν σε μία έκθεση που ανέθεσε η δικηγορική εταιρεία Baker & McKenzie η οποία διαπίστωσε ότι "περίπου το 70% των ερωτηθέντων πιστεύουν ότι οι οργανισμοί θα πρέπει να επενδύσουν επιπλέον προϋπολογισμό και ανθρωπο-ώρες ώστε οι

αντίστοιχοι οργανισμοί να συμμορφωθούν με τις νομικές απαιτήσεις για τη συγκατάθεση χρηστών, τη χαρτογράφηση των δεδομένων που συλλέγουν ήδη και τις απαιτήσεις της διασυνοριακής μεταφοράς δεδομένων". (Baker & McKenzie, 2016)

Το συνολικό κόστος συμμόρφωσης από όλες τις εταιρείες και τους οργανισμούς που εδρεύουν στην Ευρωπαϊκή Ένωση εκτιμάται περίπου σε 200 δισεκατομμύρια ευρώ, ενώ το αντίστοιχο συνολικό κόστος για οργανισμούς και εταιρείες που εδρεύουν στις Ηνωμένες Πολιτείες Αμερικής (ΗΠΑ) εκτιμάται γύρω στα 41.7 δισεκατομμύρια δολάρια Ηνωμένων Πολιτειών Αμερικής. (Georgi, 2018)

Υποστηρίζεται ότι οι μικρότερου μεγέθους επιχειρήσεις και οι νεοσύστατες εταιρείες ενδέχεται να μην έχουν τους απαραίτητους οικονομικούς πόρους που χρειάζεται για να συμμορφωθούν επαρκώς με τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ), σε αντίθεση με τους μεγαλύτερους κολοσσούς της τεχνολογίας ανά το παγκόσμιο, όπως η Google και το Facebook. (The Guardian, 2018)

Προκλήσεις Διοίκησης, Κατεύθυνσης και Συμμόρφωσης

Ακόμη μία ανησυχία των επαγγελματιών της πληροφορικής και το τεχνολογικών εταιρειών είναι η ενδεχόμενη έλλειψη γνώσης ή και κατανόησης των κανονισμών σε βάθος και τα προβλήματα που αυτό θα έφερνε κατά την υιοθέτηση του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ). (McGrath, 2014)

Παρουσιάζεται κυρίως ως ένας κίνδυνος για τον κλάδο παρότι υπάρχει το αντεπιχείρημα ότι οι εταιρείες και οι οργανισμοί εν γένει είχαν τουλάχιστον δύο ημερολογιακά έτη (δηλαδή από το 2016 που ανακοινώθηκε επίσημα έως το 2018 που τέθηκε σε ισχύ), προτού εφαρμόστηκε ο κανονισμός, χρόνος που θεωρείται ως ικανοποιητικός για εναρμόνιση με νέα νομοθεσία. (Jeong, 2018)

Οι κανονισμοί, συμπεριλαμβανομένου του εάν μια επιχείρηση πρέπει να διαθέτει υπεύθυνο προστασίας δεδομένων, έχουν επικριθεί για πιθανή διοικητική επιβάρυνση αλλά και ασαφείς απαιτήσεις συμμόρφωσης. (Edwards, 2018)

Παρόλο που ο κανονισμός απαιτεί την ελαχιστοποίηση των δεδομένων που συλλέγονται με αναφορές στη χρήση ψευδώνυμων ή τεχνικών ψευδο-ανωνυμοποίησης , ο Γενικός Κανονισμός

Προστασίας Δεδομένων (ΓΚΠΔ) όπως προτάθηκε και εγκρίθηκε δεν παρείχε κάποια υπόδειξη ή καθοδήγηση σχετικά με τον τρόπο που αυτό πρέπει να εκτελείται ούτε κάποιο τεχνικό παράδειγμα αποτελεσματικού σχήματος αποσύνδεσης των δεδομένων από τα υποκείμενα που περιγράφουν. Αυτό δίνει την αντίληψη στον κλάδο της πληροφορικής ότι ο κανονισμός εμπεριέχει γκρίζες ζώνες σχετικά με το τι θεωρείται επαρκής ή ανεπαρκής ψευδοανωνυμοποίηση. (Chassang, 2017) (Wes, 2017)

Προβλήματα Τεχνικής Υλοποίησης

Σε συνέχεια των γκρίζων ζωνών που δημιουργούνται, ένα πραγματικό παράδειγμα που τελικά όντως εξελίχθηκε τελικά σε δύσκολο πρόβλημα υλοποίησης είναι η περίπτωση της Apple και των δεδομένων φωνής Siri.

Υπενθυμίζουμε ότι βάσει του άρθρου 15, το υποκείμενο των δεδομένων έχει το δικαίωμα να μεταφέρει τα δεδομένα του από μία ηλεκτρονική πλατφόρμα σε μία άλλη. Εάν τα δεδομένα έχουν ανωνυμοποιηθεί επαρκώς τότε εξαιρούνται από τον κανονισμό αλλά εάν υπάρχει στη θεωρία ένας τρόπος ανάκτησης αυτών, τότε νομικά ο διαχειριστής των δεδομένων είναι υποχρεωμένος να τα επανασυνδέει προκειμένου να τα διαθέσει στο υποκείμενο ώστε να ικανοποιεί τις απαιτήσεις φορητότητας δεδομένων.

Στην πράξη όμως στο παράδειγμα της Apple και των δεδομένων της Siri, η παροχή και η προσπέλαση ψευδοαναγνωριστικών μπορεί να είναι πρακτικά πολύ δύσκολη καθώς:

(ι) τα δεδομένα φωνής και μεταγραφής αποθηκεύονται μαζί με ένα προσωπικό αναγνωριστικό του υποκειμένου στο οποίο ο κατασκευαστής περιορίζει τη πρόσβαση σε επίπεδο υλικού με σκοπό την ασφάλεια (Veale et al., 2018, 111-112), ή και

(ιι) τα δεδομένα δύναται να αφορούν συμπεριφορική στόχευση η οποία βασίζεται σε μεγάλο βαθμό στα δακτυλικά αποτυπώματα συσκευών τα οποία δεν αποθηκεύονται στον εξυπηρετητή - διακομιστή αλλά μόνο στην ίδια τη συσκευή του χρήστη και άρα είναι πολύ δύσκολο να τα ανακτήσουμε από αυτήν προκειμένου να τα μεταδώσουμε και επιβεβαιώσουμε. (Zuiderveen Borgesius, 2016)

Το παραπάνω παράδειγμα μας δείχνει ότι η απαίτηση για συμμόρφωση με το γράμμα του νόμου με μεγαλύτερη ευκολία θα μπορούσε να οδηγήσει κάποιες εταιρείες σε διαφορετικές

πρακτικές υλοποίησης των συστημάτων τους, οι οποίες τελικά δεν έχουν τον απαιτούμενο βαθμό προστασίας και εξασφάλισης του απορρήτου, κάτι που αντιτίθεται στον σκοπό εφαρμογής του κανονισμού.

Υπάρχει, επίσης, ανησυχία σχετικά με την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) σε συστήματα μπλοκ αλυσίδας (blockchain), καθώς το διαφανές και σταθερό αρχείο συναλλαγών blockchain στο οποίο προστίθενται συνεχώς δεδομένα και το οποίο αποτελεί δημόσια πληροφορία έρχεται σε αντίθεση με την ίδια τη φύση του Γενικού Κανονισμού Προστασίας Δεδομένων. (Gorey, 2017)

Οφέλη των Φυσικών Προσώπων και Κλάδου

Αδιαμφισβήτητα, για όλους τους λόγους που εξετάσαμε παραπάνω, ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ), έφερε οφέλη στα φυσικά πρόσωπα αλλά και στους κλάδους της πληροφορικής, τηλεπικοινωνιών και άλλων τεχνολογιών διαδικτύου.

Κυρίως, ο κανονισμός είχε ως αποτέλεσμα μεγαλύτερη διαφάνεια μεταξύ των οργανισμών που συλλέγουν και επεξεργάζονται δεδομένα και των χρηστών αυτών των υπηρεσιών ή προϊόντων σχετικά με τους λόγους επεξεργασίας. Έδωσε την επιλογή στο χρήστη να εξαιρεθεί από συγκεκριμένες λειτουργίες επεξεργασίας χωρίς απαραίτητα να στερηθεί τη χρήση της υπηρεσίας, όπως για παράδειγμα την άρνηση της χρήσης των cookie για σκοπούς marketing παρότι συνεχίζουν να υπάρχουν και να χρησιμοποιούνται άλλα cookie που θεωρούνται απαραίτητα.

Ακόμη, η ψήφιση και εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων αναζωπύρωσε τις συζητήσεις σε κοινωνικό επίπεδο για τη συλλογή και επεξεργασία δεδομένων, δημιουργώντας την ευαισθησία των πολιτών γύρω από τα θέματα των προσωπικών δεδομένων.

Κατά την στρατηγική εφαρμογή και εισαγωγή αλλαγών σε όλα τα συστήματα με σκοπό την νομική συμμόρφωση των οργανισμών, παρατηρήθηκε συνάμα και βελτίωση της κυβερνοασφάλειας στο σύνολο καθώς αυτό αποτελεί και μεγάλη ευκαιρία προώθησης του εταιρικού σήματος σε ευαισθητοποιημένο κοινό.

Περαιτέρω, οφείλουμε να παραδεχτούμε ότι ο κανονισμός έθεσε κάποια πρότυπα στο χώρο της προστασίας δεδομένων, ακόμη και εάν αυτά δεν είναι είναι πλήρως αποτελεσματικά ή εάν δεν επαρκούν για την ουσιαστική προστασία της ιδιωτικής ζωής.

Θετικές απόψεις από τον κλάδο πληροφορικής

Παρά τις όλες προκλήσεις που έφερε ο κανονισμός στο κλάδο της πληροφορικής, της τεχνολογίας και των υπηρεσιών διαδικτύου, συγκεντρώθηκαν και υποστηρικτικές απόψεις από τη κοινότητα περιγράφοντας τον κανονισμό ως μια ευκαιρία για τις επιχειρήσεις να βελτιώσουν τη διαχείριση των δεδομένων τους. (Fimin, 2018)

Ακόμη, υψηλά στελέχη τεχνολογικών κολοσσών των Ηνωμένων Πολιτειών Αμερικής όπως ο Mark Zuckerberg, ιδρυτής της εταιρείας Facebook, ανέφερε ότι "ο Γενικός Κανονισμός Προστασίας Δεδομένων θα είναι εν γένει ένα θετικό βήμα για το διαδίκτυο". (Jaffe & Hautala, 2018)

Αρθρογράφοι Αμερικανών ειδησεογραφικών ιστοσελίδων παρουσιάζουν ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) θα πρέπει να αποτελέσει ένα μοντέλο - πρότυπο για τους φορείς χάραξης πολιτικής των Ηνωμένων Πολιτειών Αμερικής. (Butterworth, 2018) (Schulze, 2019) (Cage, 2018)

Ο Richard Stallman, που είναι υποστηρικτής του ελεύθερου και ανοικτού λογισμικού, επαίνεσε ορισμένες πτυχές του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) και ζήτησε για επιπλέον διασφαλίσεις με σκοπό να αποτρέπονται οι τεχνολογικές εταιρείες από το να "κατασκευάζουν τη συγκατάθεση του χρήστη". (Stallman, 2018)

Τρέχουσα Κατάσταση

Την πρόταση για τον κανονισμό ePrivacy Regulation συνοδεύουν κάποια έγγραφα εργασίας των υπηρεσιών της επιτροπής, ανάμεσά τους *(ι)* μία εκ των υστέρων αξιολόγηση της οδηγίας 2002/58/ΕΚ που είναι σε ισχύ (European Commission, 2017), όπως και *(ιι)* μια μελέτη εκτίμησης επιπτώσεων των διαφορετικών επιλογών που μελετήθηκαν για την πρόταση για το νέο κανονισμό. (European Commission, 2017)

Ο συνδυασμός αυτών απεικονίζει τα ανοιχτά προβλήματα που παρατηρούνται, τα οποία καθορίζουν και την ανάγκη για δράση, τους στόχους που πρέπει να φτάσουμε για να τα επιλύσουμε, τις διάφορες επιλογές που έχει η επιτροπή στη διάθεσή της, τα οφέλη αλλά και επιπτώσεις της κάθε επιλογής. (European Commission, 2017)

Ανάγκη για δράση

Ανοιχτά προβλήματα και η πηγή τους

Η εκ των υστέρων αξιολόγηση της οδηγίας 2002/58/ΕΚ σε συνδυασμό με την μελέτη εκτίμησης επιπτώσεων της πρότασης οδήγησε στον εντοπισμό τριών κύριων συνόλων προβλημάτων:

1. Η ιδιωτική ζωή των πολιτών κατά την επικοινωνία τους στο διαδίκτυο δεν προστατεύεται επαρκώς και αποτελεσματικά.
2. Οι πολίτες δεν προστατεύονται αποτελεσματικά από το ανεπιθύμητο μάρκετινγκ.
3. Οι επιχειρηματίες αντιμετωπίζουν εμπόδια που δημιουργούνται από τη κατακερματισμένη νομοθεσία και τις διαφορετικές ερμηνείες των οδηγιών σε διαφορετικά κράτη - μέλη, καθώς και ασαφείς και ξεπερασμένες διατάξεις.

Η εκ των υστέρων αξιολόγηση της οδηγίας 2002/58/ΕΚ κατέληξε επίσης στο συμπέρασμα ότι υπάρχει περιθώριο απλούστευσης της νομοθεσίας, ειδικά όσον αφορά την ύπαρξη ορισμένων ξεπερασμένων ή περιττών διατάξεων και των κανόνων εκτέλεσης.

Αυτό υποστηρίζεται επίσης από τη γνώμη της πλατφόρμας REFIT που συνιστά *(ι)* την ενίσχυση της προστασίας της ιδιωτικής ζωής των πολιτών μέσω της ευθυγράμμισης της οδηγίας για την ηλεκτρονική ιδιωτικότητα του 2002 με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ), *(ιι)* την προσθήκη εξαίρεσης στο κανόνα συγκατάθεσης για τα cookie, και ότι *(ιιι)* η Ευρωπαϊκή επιτροπή θα αντιμετωπίσει τα εθνικά προβλήματα υλοποίησης. (European Commission, 2017)

Αντικειμενικοί Στόχοι

Οι συγκεκριμένοι στόχοι της αναθεώρησης είναι η διασφάλιση αποτελεσματικού απορρήτου των ηλεκτρονικών επικοινωνιών, η εξασφάλιση αποτελεσματικής προστασίας από ανεπιθύμητες εμπορικές επικοινωνίες, η ενίσχυση της εναρμόνισης και η απλούστευση ή ενημέρωση του νομικού πλαισίου αντίστοιχα. (European Commission, 2017)

Προστιθέμενη αξία της δράσης σε επίπεδο Ευρωπαϊκής Ένωσης

Καθώς οι ηλεκτρονικές επικοινωνίες και ειδικά αυτές που βασίζονται σε πρωτόκολλα διαδικτύου έχουν παγκόσμια εμβέλεια, η διάσταση του προβλήματος υπερβαίνει κατά πολύ το έδαφος των μεμονωμένων κρατών - μελών.

Οι εθνικοί κανόνες για την εμπιστευτικότητα των επικοινωνιών ποικίλουν πολύ σε πεδίο εφαρμογής και περιεχόμενο. Ενώ, είναι εφικτό για τα κράτη - μέλη να θεσπίσουν πολιτικές που να διασφαλίζουν ότι αυτό το δικαίωμα δεν παραβιάζεται, αυτό δεν μπορεί να επιτευχθεί με ομοιόμορφο τρόπο, ελλείψει κοινών κανόνων της Ευρωπαϊκής Ένωσης. Ελλείψη κοινού νομοθετικού πλαισίου, θα δημιουργούνταν περιορισμοί στις διασυνοριακές ροές προσωπικών δεδομένων που σχετίζονται με τη χρήση υπηρεσιών ηλεκτρονικών επικοινωνιών σε άλλα κράτη - μέλη που δεν πληρούν ακριβώς τα ίδια πρότυπα προστασίας δεδομένων.

Έτσι, η επικείμενη αναθεώρηση της οδηγίας για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών θεωρείται ότι συμμορφώνεται τόσο με την επικουρικότητα όσο και με την αναλογικότητα διατηρώντας την προσέγγιση εναρμόνισης και ενισχύοντας τον μηχανισμό συνεργασίας μεταξύ κρατών - μελών, ενώ επιτρέπει στα κράτη - μέλη

να λαμβάνουν εθνικά μέτρα για συγκεκριμένους νόμιμους σκοπούς. (European Commission, 2017)

Πιθανές Λύσεις

Οι πιθανές λύσεις ομαδοποιούνται ακολούθως σύμφωνα με το επίπεδο αυξανόμενης φιλοδοξίας τους σχετικά με την ικανοποίηση των παραπάνω αντικειμενικών στόχων και αναγκών για ιδιωτικότητα αλλά και απλοποίηση.

Επιλογή 1 - Μη νομοθετικά μέτρα ("soft law")

Περιλαμβάνει αποκλειστικά οδηγίες που θα παρέχονται από την Ευρωπαϊκή Επιτροπή σχετικά με την ενθάρρυνση των πρωτοβουλιών αυτορρύθμισης και άλλων απαλών μέτρων σε εθνικό επίπεδο. Δηλαδή δεν περιλαμβάνει κανονισμούς ή άλλες εφαρμοστέες νομοθεσίες παρά μόνο προτάσεις, οδηγίες και προδιαγραφές καλών πρακτικών για κάθε χώρα - μέλος της Ευρωπαϊκής Ένωσης.

Επιλογή 2 - Περιορισμένη ενίσχυση του απορρήτου, εμπιστευτικότητας και εναρμόνισης

Προβλέπει την ελάχιστη ενίσχυση *(ι)* των δικαιωμάτων απορρήτου ή εμπιστευτικότητας μέσω διευκρίνησης του πεδίου εφαρμογής του κανονισμού ePrivacy Regulation ώστε να καλύπτει τους Κορυφαίους Παρόχους (Over-the-Top providers ή OTT), τα δημόσια δίκτυα Wi-Fi και συσκευές διαδικτύου πραγμάτων (Internet of Things ή IoT), *(ιι)* της προστασίας έναντι ανεπιθύμητων κλήσεων μέσω αποσαφήνισης των ισχυόντων κανόνων και επιβολής προτύπου προθέματος στις κλήσεις μάρκετινγκ και *(ιιι)* την απλοποίηση μέσω κατάργησης των διατάξεων ασφαλείας, ενίσχυσης της συνεργασίας σε διασυνοριακές υποθέσεις.

Επιλογή 3 - Μέτρια ενίσχυση του απορρήτου, εμπιστευτικότητας και εναρμόνισης

Προβλέπει μια πιο σημαντική ενίσχυση των δικαιωμάτων απορρήτου ή εμπιστευτικότητας *(ι)* μέσω επέκτασης του πεδίου εφαρμογής, βελτιωμένης διαφάνειας ρυθμίσεων απορρήτου, μεγαλύτερης διαφάνειας, ενίσχυσης της εξουσίας επιβολής, *(ιι)* προστασίας από ανεπιθύμητες επικοινωνίες μέσω εισαγωγής της opt-in επιλογής κλήσεων μάρκετινγκ και *(ιιι)* απλοποίησης μέσω διεύρυνσης των εξαιρέσεων, περαιτέρω κατάργησης των περιττών διατάξεων, εξορθολογισμό της επιβολής με την ανάθεση εξουσιών στις εθνικές αρμόδιες αρχές για την επιβολή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) και επέκτασης του μηχανισμού συνέπειας του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ).

Επιλογή 4 - Εκτεταμένη ενίσχυση του απορρήτου, εμπιστευτικότητας και εναρμόνισης

Περιλαμβάνει πιο εκτεταμένα μέτρα επιπλέον της επιλογής 3, όπως μία γενική απαγόρευση των "τειχών cookie", την κατάργηση της εξαίρεσης προηγούμενης επιχειρηματικής σχέσης για μάρκετινγκ μέσω ηλεκτρονικού ταχυδρομείου ή γραπτού μηνύματος, επιπλέον κατάργηση εδαφίων της οδηγίας 2002/58/ΕΚ και πρόβλεψη εκτελεστικών αρμοδιοτήτων της Ευρωπαϊκής Επιτροπής.

Επιλογή 5 - Ανάκληση της οδηγίας 2002/58/ΕΚ

Αυτή η επιλογή προβλέπει την πλήρη κατάργηση της οδηγίας 2002/58/ΕΚ και την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ), συμπεριλαμβανομένου ενός συστήματος επιβολής για την προστασία του απορρήτου των προσωπικών δεδομένων, της γενικευμένης εφαρμογής ενός συστήματος καθολικής εξαίρεσης από ανεπιθύμητες επικοινωνίες και εφαρμογή μηχανισμού συνέπειας του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ).

Ενδιαφερόμενα μέρη και οι προτιμήσεις τους

Πολίτες

Τα δικαιώματα των πολιτών επηρεάζονται από το επίπεδο προστασίας του απορρήτου των επικοινωνιών τους. Θα προτιμούσαν τις επιλογές - λύσεις που ενισχύουν τα δικαιώματά τους, όπως οι επιλογές 2, 3 και 4.

Εθνικές αρχές

Οι εθνικές αρχές αναμένεται να υποστηρίξουν τις επιλογές που οδηγούν σε όλο και περισσότερο συνεπή προστασία της ιδιωτικής ζωής, όπως οι επιλογές 2, 3 και 4.

Πάροχοι Ηλεκτρονικών Επικοινωνιών

Οι πάροχοι ηλεκτρονικών επικοινωνιών είναι οι κύριοι παραλήπτες των υποχρεώσεων της οδηγίας ή κανονισμού περί προστασίας της ιδιωτικής ζωής. Συνεπώς, θα τους ευνοούσε έντονα η επιλογή 5. Ως δεύτερη καλύτερη επιλογή, θα ήταν δυνατό να αποδεχθούν τις επιλογές 2 και 3 που διασφαλίζουν ότι οι ανταγωνιστικοί κορυφαίοι πάροχοι (Over-the-Top providers ή OTT) υπόκεινται στους ίδιους κανόνες.

Κορυφαίοι Πάροχοι (Over-the-Top providers ή OTT)

Οι κορυφαίοι πάροχοι θα προτιμούσαν τις επιλογές 1 και 5, καθώς θα προτιμούσαν να μη υπόκεινται σε αυστηρότερες κανονιστικές απαιτήσεις. Ως δεύτερη καλύτερη επιλογή για αυτούς θα ήταν η επιλογή 3 δεδομένου του περιθωρίου ευελιξίας που εξασφαλίζει.

Δημιουργοί Ιστοτόπων ή προϊόντων διαδικτυακής συμπεριφορικής διαφήμισης

Οι δημιουργοί ιστοτόπων ή προϊόντων διαδικτυακής συμπεριφορικής διαφήμισης θα προτιμούσαν σαφώς την επιλογή 5 για τους ίδιους λόγους με τους κορυφαίους παρόχους και τους παρόχους ηλεκτρονικών επικοινωνιών.

Πάροχοι λογισμικού περιηγητών

Οι πάροχοι προγραμμάτων περιήγησης υπόκεινται σε συγκεκριμένες ευθύνες σύμφωνα με την επιλογή 3, επομένως, δεν θα υποστηρίξουν τις επιλογές 3 και 4.

Μικρές και μεσαίες επιχειρήσεις (ΜΜΕ)

Οι μικρές και μεσαίες επιχειρήσεις (Μ.Μ.Ε.) θα υποστήριζαν γενικά τις επιλογές 1 και 5. Εάν αυτές οι μικρές και μεσαίες επιχειρήσεις είναι πάροχοι ηλεκτρονικών επικοινωνιών, τότε θα υποστήριζαν την επιλογή 2 ή 3 για ίσους όρους ανταγωνισμού με τους κορυφαίους παρόχους. Εάν είναι κορυφαίοι πάροχοι (ΟΤΤ) τότε θα προτιμούσαν τις επιλογές 1 και 5, με την επιλογή 3 να είναι η δεύτερη καλύτερη αποδεκτή λύση.

Επιλογή Λύσης, Αναμενόμενο Όφελος και Επιπτώσεις

Από τη παραπάνω ανάλυση προκύπτει ότι η βέλτιστη λύση είναι η επιλογή 3.

Τα κύρια οφέλη είναι *(ι)* η ενίσχυση της προστασίας της εμπιστευτικότητας μέσω ενός τεχνολογικά ουδέτερου ορισμού, οι βελτιωμένες απαιτήσεις ελέγχου και διαφάνειας του χρήστη και αποτελεσματικότερη επιβολή, *(ιι)* η ενίσχυση της προστασίας από ανεπιθύμητες επικοινωνίες, χάρη στην εισαγωγή του opt-in για κλήσεις μάρκετινγκ, την εισαγωγή προθέματος και την επακόλουθη απαγόρευση ανώνυμων κλήσεων μάρκετινγκ και τις βελτιωμένες δυνατότητες αποκλεισμού κλήσεων από ανεπιθύμητους αριθμούς, και *(ιιι)* η απλοποίηση μέσω εναρμόνισης και αποσαφήνισης του ρυθμιστικού περιβάλλοντος, χάρη στη μείωση του περιθωρίου ελιγμών που αφήνεται στα κράτη μέλη, την κατάργηση ξεπερασμένων διατάξεων και η διεύρυνση των εξαιρέσεων στους κανόνες συγκατάθεσης.

Η προτιμώμενη επιλογή αναμένεται να αποφέρει εξοικονόμηση ως αποτέλεσμα πρόσθετης εναρμόνισης και απλοποίηση. Για παράδειγμα, έχουν υπολογιστεί εξοικονομήσεις έως και 70% του κόστους που σχετίζεται με την ιδιωτικότητα μέσω μιας κεντρικής διαχείρισης των επιλογών απορρήτου μία φορά για όλους τους ιστότοπους και τις εφαρμογές.

Στο επίπεδο συγκεκριμένων κατηγοριών ενδιαφερομένων, οι φορείς Κορυφαίοι Πάροχοι OTT θα πρέπει να επιβαρυνθούν με κάποιο κόστος για την αποκατάσταση της νομιμότητα των επιχειρηματικών τους μοντέλων. Ωστόσο, το κόστος αυτό δεν αναμένεται να είναι σημαντικό. Οι εκδότες ιστότοπων ενδέχεται να επιβαρύνονται με μικρό κόστος προσαρμογής. Οι πάροχοι λογισμικού περιήγησης διαδικτύου και πάροχοι παρόμοιων εφαρμογών που επιτρέπουν την πρόσβαση στο διαδίκτυο θα πρέπει να επιβαρυνθούν με σημαντικό κόστος για να διασφαλίσουν ότι οι χρήστες έχουν τις κατάλληλες επιλογές σχετικά με τις ρυθμίσεις απορρήτου τους. Οι έμποροι (marketers) θα επιβαρύνονται με κάποιο κόστος μετά την εισαγωγή του opt-in για κλήσεις μάρκετινγκ.

Οι κύριες επιπτώσεις στους εθνικούς προϋπολογισμούς των κρατών - μελών της Ευρωπαϊκής Ένωσης και της διοίκησης θα προέρχονται από την εφαρμογή του μηχανισμού συνέπειας και την πιθανή ανάγκη εκ νέου κατανομής των αρμοδιοτήτων επιβολής των αρχών προστασίας δεδομένων μόνο. Ο αντίκτυπος δεν θεωρείται σημαντικός, καθώς θα μπορούσαν να αξιοποιηθούν οι συνέργειες με ήδη υπάρχοντες φορείς συντονισμού της Ευρωπαϊκής Ένωσης (π.χ. στον τομέα της προστασίας δεδομένων).

Δεν αναμένονται άλλες σημαντικές επιπτώσεις από την ψήφιση αυτού του κανονισμού. Όσον αφορά την αναλογικότητα, η προτιμώμενη επιλογή περιλαμβάνει ισορροπημένα μέτρα, όλα τα οποία κρίνονται απαραίτητα για την επίτευξη των στόχων χωρίς να επιβάλλεται υπερβολική επιβάρυνση στους ενδιαφερόμενους.

Επιπλέον, τα μέτρα είναι σχεδιασμένα με ευελιξία, ώστε να επιτρέπονται οι απαραίτητες εξαιρέσεις και να ελαχιστοποιούνται τυχόν στρεβλώσεις του ανταγωνισμού με διασφάλιση ίσων όρων ανταγωνισμού.

Η συνεχής παρακολούθηση θα διασφαλιστεί, μεταξύ άλλων, μέσω αναφορών από τα κράτη - μέλη προς στην Ευρωπαϊκή Επιτροπή και από την Επιτροπή προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Οικονομική και Κοινωνική Επιτροπή.

Επόμενο βήμα

Μετά από τη παραπάνω μελέτη, ανάλυση και επιλογή της βέλτιστης λύσης 3 ανάμεσα στις 5 πιθανές λύσεις, η Ευρωπαϊκή Επιτροπή κατέθεσε πρόταση για κανονισμό η οποία είναι προς διαβούλευση τη στιγμή που γράφεται η παρούσα μελέτη.

Πρόταση 2017/003: Κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες (ePrivacy Regulation)

Ο κανονισμός ePrivacy Regulation (ePR) είναι προς το παρόν μία πρόταση υπό διαβούλευση για την νομοθέτηση μιας σειράς από θέματα που αφορούν την ιδιωτικότητα του ατόμου, κυρίως σχετικά με τις ηλεκτρονικές επικοινωνίες, εντός ή δια της Ευρωπαϊκής Ένωσης. (European Parliament Legislative Observatory, 2017)

Η ολοκληρωμένη ονομασία του επερχόμενου κανονισμού είναι "*Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ*" και σε πιο σύντομη ονομασία: "*Κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες*". (Ευρωπαϊκή Επιτροπή, 2017)

Όπως υποδηλώνει και η ίδια ονομασία του επερχόμενου κανονισμού, ο νέος κανονισμός πρόκειται να *(ι)* καταργήσει την τελευταία οδηγία του 2002 αλλά και να *(ιι)* λειτουργήσει συμπληρωματικά με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) που μπήκε σε ισχύ τον Μάιο του 2018. Θα εξειδικεύσει και θα συμπληρώσει τον τελευταίο σε σχέση με θέματα που αφορούν την προστασία της ιδιωτικής ζωής. (European Commission, 2017)

Είναι σημαντικό να σημειωθεί όταν αυτός ο κανονισμός ψηφιστεί και τεθεί σε ισχύ θα μετασχηματίσει τη φύση της νομοθετικής ρύθμισης από οδηγία σε κανονισμό, δηλαδή από τον καθορισμό στόχων που πρέπει να επιτύχουν τα κράτη-μέλη της Ευρωπαϊκής Ένωσης προχωράμε σε δεσμευτικές πράξεις για όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης τα οποία είναι και υποχρεωμένα να τις εφαρμόσουν.

Οι πρόσφατες αλλαγές

Όπως αναφέραμε και νωρίτερα, υπήρξε προσπάθεια ώστε ο Γενικός Κανονισμός Προστασίας Δεδομένων που τέθηκε σε ισχύ το 2018 να είχε συγχρονιστεί με τον κανονισμό εξετάζουμε τώρα αλλά αυτό δεν κατέστει εφικτό τότε. (Ευρωπαϊκή Επιτροπή, 2017)

Ένα χρόνο μετά, δηλαδή το Μάιο του 2019 δεν είχε ακόμη επιτευχθεί συμφωνία για το τελικό κείμενο. Ένας λόγος για την καθυστέρηση ήταν η έλλειψη συμφωνίας μεταξύ των κρατών - μελών της Ευρωπαϊκής Ένωσης υπό διάφορες προεδρίες του Ευρωπαϊκού Συμβουλίου σχετικά με τις βασικές διατάξεις της νομοθεσίας.

Η Ευρωπαϊκή Επιτροπή ενέκρινε την πρόταση ePrivacy Regulation στις αρχές Ιανουαρίου 2017 και η Επιτροπή Πολιτικών Ελευθεριών, Δικαιοσύνης και Εσωτερικών Υποθέσεων στο Ευρωπαϊκό Κοινοβούλιο ενέκρινε την έκθεσή της στα τέλη Οκτωβρίου του ίδιου έτους.

Η εξέταση της πρότασης από το Συμβούλιο, η οποία διεξήχθη από την "Ομάδα Εργασίας για τις Τηλεπικοινωνίες και την Κοινωνία της Πληροφορίας", ήταν το πιο χρονοβόρο βήμα στη διαδικασία, η οποία διήρκεσε περισσότερο από ενάμιση χρόνο υπό τις προεδρίες διάφορων χωρών όπως η Μάλτα, η Εσθονία, η Βουλγαρία, η Αυστρία και η Ρουμανία. Ενώ οι αποκλίνουσες απόψεις μεταξύ των αντιπροσωπειών είχαν οδηγήσει σε σημαντικές διευκρινίσεις στο κείμενο της πρότασης, η επίλυση αυτών των αποκλίσεων έχει επίσης καθυστερήσει την πρόοδο του κανονισμού ePrivacy Regulation.

Η έκθεση προόδου της ρουμανικής προεδρίας κυκλοφόρησε στις 21 Μαΐου 2019 σχετικά με την τρέχουσα "κατάσταση" στο Ευρωπαϊκό Συμβούλιο και για παράδειγμα σημειώνει ότι έχουν γίνει διευκρινίσεις σε αρκετές αιτιολογικές σκέψεις, δεδομένου ότι υπάρχουν ανησυχίες μεταξύ των αντιπροσωπειών σχετικά με τον τρόπο αλληλεπίδρασης του ePrivacy Regulation με νέες τεχνολογίες, όπως το διαδίκτυο των πραγμάτων (internet of things ή IoT) και την τεχνητή νοημοσύνη.

Ειδικότερα, στην αναθεωρημένη συμβιβαστική πρόταση που δημοσίευσε το συμβούλιο τον Φεβρουάριο του 2019, έγιναν τροποποιήσεις στην αιτιολογική σκέψη 21 για την εξαίρεση συσκευών IoT, όπως π.χ. οι συνδεδεμένοι θερμοστάτες, από τις απαιτήσεις συναίνεσης, καθώς οι

τύποι αποθήκευσης και πρόσβασης που σχετίζονται με αυτές είναι "απαραίτητοι και αναλογικό για τον σκοπό παροχής συγκεκριμένης υπηρεσίας (...) που ζητείται από τον τελικό χρήστη".

Σύμφωνα με την έκθεση προόδου, ζητήματα σχετικά με την "πρόληψη ή ανίχνευση ή αναφορά εικόνων κακοποίησης παιδιών" έχουν επίσης αποτελέσει αντικείμενο διαφωνίας μεταξύ των αντιπροσωπειών σχετικά με το πώς και εάν πρέπει να αντιμετωπιστούν από τον κανονισμό ePrivacy Regulation. Ενώ ορισμένα κράτη - μέλη προτείνουν να αντιμετωπιστούν αυτά τα ζητήματα προσθέτοντας μια διάταξη στο άρθρο 6 σχετικά με την επιτρεπόμενη επεξεργασία δεδομένων ηλεκτρονικών επικοινωνιών, άλλα κράτη - μέλη υποστηρίζουν ότι το ζήτημα θα αντιμετωπιστεί καλύτερα με μια ξεχωριστή νομική πράξη έναντι του άρθρου 11 σχετικά με τους περιορισμούς.

Συγκεκριμένα, το άρθρο 11 του ePrivacy Regulation επιτρέπει στα κράτη - μέλη να περιορίσουν το πεδίο εφαρμογής των υποχρεώσεων και δικαιωμάτων που αναφέρονται στο άρθρο 5-8 σχετικά με την εμπιστευτικότητα των δεδομένων ηλεκτρονικών επικοινωνιών (άρθρο 5), την επιτρεπόμενη επεξεργασία δεδομένων ηλεκτρονικών επικοινωνιών (άρθρο 6), την αποθήκευση και τη διαγραφή δεδομένων ηλεκτρονικών επικοινωνιών (άρθρο 7) και προστασία των πληροφοριών τερματικού εξοπλισμού τελικών χρηστών (άρθρο 8).

Όπως και με τους περιορισμούς που επιβάλλονται από τα κράτη - μέλη στα άρθρα 12 - 22, 34 και 5 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ), ένας περιορισμός που επιβάλλεται από ένα κράτος μέλος στα άρθρα 5 - 8 του κανονισμού ePrivacy Regulation θα επιτρέπεται μόνο εφόσον "σέβεται την ουσία των θεμελιωδών δικαιωμάτων και ελευθερίες και είναι ένα αναγκαίο, κατάλληλο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση ενός ή περισσοτέρων από τα γενικά συμφέροντα του κοινού που αναφέρονται στο άρθρο 23 παράγραφος 1 στοιχεία γ) έως ε), όπως και ι) και κ) του κανονισμού (ΕΕ) 2016/679".

Συγκεκριμένα, αυτά περιλαμβάνουν τη δημόσια ασφάλεια, την "πρόληψη, διερεύνηση, εντοπισμό ή δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινικών κυρώσεων", καθώς και "άλλους σημαντικούς στόχους γενικού δημόσιου συμφέροντος της Ένωσης ή ενός κράτους μέλους", όπως "νομισματικά, δημοσιονομικά και φορολογικά θέματα, δημόσια υγεία και κοινωνική ασφάλιση". (Fazlioglu, 2019)

Βασικοί πυλώνες και πεδίο εφαρμογής

Τα βασικά πεδία του προτεινόμενου κανονισμού είναι η εμπιστευτικότητα των επικοινωνιών, η ηλεκτρονική συγκατάθεση και τα στοιχεία ελέγχου απορρήτου μέσω προγραμμάτων περιήγησης και η χρήση των cookies.

Το πεδίο εφαρμογής του κανονισμού για την ηλεκτρονική ιδιωτικότητα εξακολουθεί να συζητείται. Σύμφωνα με ορισμένες προτάσεις, θα ισχύει για κάθε επιχείρηση που επεξεργάζεται δεδομένα σε σχέση με οποιαδήποτε μορφή διαδικτυακής υπηρεσίας ή επικοινωνίας, για κάθε οργανισμό που χρησιμοποιεί που διαδικτυακές τεχνολογίες παρακολούθησης ή συμμετέχει σε ηλεκτρονικό άμεσο μάρκετινγκ. (Ευρωπαϊκή Επιτροπή, 2017)

Σημαντικά Σημεία στη πρόταση της Ευρωπαϊκής Επιτροπής

Με αυτή τη πρόταση η Ευρωπαϊκή Επιτροπή περιλαμβάνει σημαντικές αλλαγές όπως τις ακόλουθες.

Νέοι παίκτες

Οι κανόνες απορρήτου θα εφαρμόζονται επίσης και για νέους παίκτες που παρέχουν υπηρεσίες ηλεκτρονικών επικοινωνιών όπως για παράδειγμα το WhatsApp, το Facebook Messenger και το Skype. Αυτό θα διασφαλίσει ότι οι δημοφιλείς υπηρεσίες εγγυώνται το ίδιο επίπεδο εμπιστευτικότητας των επικοινωνιών με τους παραδοσιακούς φορείς τηλεπικοινωνιών. (Ευρωπαϊκή Επιτροπή, 2017)

Ισχυρότερες διατάξεις

Όλοι οι άνθρωποι και επιχειρήσεις στην Ευρωπαϊκή Ένωση θα απολαμβάνουν το ίδιο επίπεδο προστασίας ηλεκτρονικών επικοινωνιών μέσω αυτού του άμεσα εφαρμόσιμου κανονισμού. Οι επιχειρήσεις θα επωφεληθούν επίσης από ένα ενιαίο σύνολο κανόνων σε ολόκληρη την Ευρωπαϊκή Ένωση. (Ευρωπαϊκή Επιτροπή, 2017)

Περιεχόμενο και μεταδεδομένα επικοινωνιών

Το απόρρητο είναι εγγυημένο για επικοινωνίες όπως η ακριβής ημερομηνία, η ώρα και η γεωγραφική τοποθεσία μιας κλήσης. Τα μεταδεδομένα έχουν υψηλό στοιχείο απορρήτου και πρέπει να ανωνυμοποιούνται ή να διαγράφονται εάν οι χρήστες δεν έδωσαν τη συγκατάθεσή τους ή εκτός εάν τα δεδομένα είναι απολύτως απαραίτητα για τον καθορισμό της χρέωση της αντίστοιχης υπηρεσίας. (Ευρωπαϊκή Επιτροπή, 2017)

Νέες επιχειρηματικές ευκαιρίες

Μόλις δοθεί η συγκατάθεση για επεξεργασία δεδομένων (περιεχομένου ή και μεταδεδομένων), οι παραδοσιακοί φορείς τηλεπικοινωνιών θα έχουν περισσότερες ευκαιρίες να παρέχουν πρόσθετες υπηρεσίες και να αναπτύξουν τις επιχειρήσεις τους. Για παράδειγμα, οι φορείς τηλεπικοινωνιών θα μπορούσαν να παράγουν γεωγραφικούς χάρτες θερμότητας (heatmaps) που να δείχνουν την παρουσία ατόμων ή πλήθους, οι οποίοι θα μπορούσαν να βοηθήσουν τις δημόσιες αρχές και τις εταιρείες μεταφορών κατά την ανάπτυξη νέων έργων υποδομής. (Ευρωπαϊκή Επιτροπή, 2017)

Απλούστεροι κανόνες για τα cookies

Θα απλοποιηθεί η διάταξη των cookies, η οποία είχε ως αποτέλεσμα την υπερφόρτωση των χρηστών διαδικτύου με αιτήματα συναίνεσης. Ο νέος κανόνας θα είναι πιο φιλικός προς τον χρήστη, καθώς οι ρυθμίσεις του ίδιου του προγράμματος περιήγησης θα παρέχουν έναν εύκολο τρόπο αποδοχής ή άρνησης των cookie παρακολούθησης και άλλων αναγνωριστικών.

Η πρόταση του κανονισμού διευκρινίζει επίσης ότι δεν απαιτείται η συγκατάθεση του χρήστη για μη εμπιστευτικά cookie που βελτιώνουν την εμπειρία του χρήστη στο Διαδίκτυο (όπως για παράδειγμα το cookie που είναι απαραίτητο για να κρατάει το ιστορικό καλαθιού αγορών) ή cookie που χρησιμοποιούνται από έναν ιστότοπο για τον υπολογισμό του αριθμού των επισκεπτών. (Ευρωπαϊκή Επιτροπή, 2017)

Προστασία από ανεπιθύμητα μηνύματα

Η πρόταση απαγορεύει τις ανεπιθύμητες ηλεκτρονικές επικοινωνίες μέσω ηλεκτρονικού ταχυδρομείου (email), γραπτού μηνύματος (sms) και αυτοματοποιημένων τηλεφωνικών μηχανών.

Ανάλογα με την εθνική νομοθεσία της κάθε χώρας, τα άτομα είτε θα προστατεύονται από προεπιλογή, είτε θα μπορούν να χρησιμοποιούν μια λίστα απαγορευμένων κλήσεων για να αποφύγουν τη λήψη τηλεφωνικών κλήσεων μάρκετινγκ.

Οι καλούντες μάρκετινγκ θα πρέπει να εμφανίσουν τον αριθμό τηλεφώνου τους ή να χρησιμοποιήσουν μια ειδική προκαθορισμένη ρύθμιση που υποδεικνύει μια κλήση μάρκετινγκ. (Ευρωπαϊκή Επιτροπή, 2017)

Συμπεράσματα και Απόψεις

Γενικά

Παρ' όλη τη κόπωση και προσπάθεια των θεσμών, αλλά κυρίως και των εταιρειών τεχνολογίας και επικοινωνιών με τους κανονισμούς που μπήκαν πρόσφατα σε ισχύ, τα δεδομένα δείχνουν πως η πρόσφατη νομοθεσία και ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) αποτελούν μόνο ένα κομμάτι ενός μεγαλύτερου παζλ που ακόμα λύνουμε.

Ενώ ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) υπήρξε ένα σημαντικό βήμα προς τη σωστή κατεύθυνση για τη προστασία του δικαιώματος στην ιδιωτική ζωή, πρέπει ωστόσο να σημειωθεί ότι δεν αποτελεί ούτε την "πλήρη επανάσταση", ούτε την "επανοικοδόμηση της ιδιωτικότητας του ατόμου", όπως παρουσιάζεται από κάποιες εταιρείες τεχνολογικού ενδιαφέροντος. Αυτό συμβαίνει κυρίως διότι βασίζεται στην ισχύουσα νομοθεσία της Ευρωπαϊκής Ένωσης για τη προστασία δεδομένων, όπως αυτή ξεκίνησε το 1995 και εξελίχθηκε το 2002, 2006 και 2009.

Μια πολύ σημαντική πτυχή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) όσο και της πρότασης για τον κανονισμό προστασίας της ιδιωτικής ζωής (ePrivacy Regulation) είναι η ενδυνάμωση των υποκειμένων των δεδομένων κατά της εμπορικής και μη εκμετάλλευσης και της πιθανής κατάχρησης των δεδομένων τους. Από αυτή την άποψη, ο κανονισμός είναι ένα κρίσιμο μέσο για την προστασία της ιδιωτικής ζωής.

Στα πλαίσια της παρούσας μελέτης οφείλουμε να αναγνωρίσουμε πως η μετατροπή των νομοθετικών πράξεων από "οδηγίες" σε "κανονισμούς" τα τελευταία χρόνια, καθώς και η εισαγωγή οικονομικών επιπτώσεων, προστίμων και κυρώσεων στο πλαίσιο του νόμου αποτελούν τα πιο αποδοτικά κίνητρα για τη παρακίνηση της εξέλιξης του κλάδου της τεχνολογίας ως προς το σεβασμό των υποκειμένων των δεδομένων.

Από την άσκηση της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) το 2018, αλλά και από μελέτη της κοινής γνώμης περί της ιδιωτικότητας του ατόμου και

απορρήτου των επικοινωνιών, φαίνεται ότι το μεγαλύτερο όπλο προς τη ρύθμιση αυτού του πεδίου αποτελεί η εναρμονισμένη προσπάθεια όλων των κρατών - μελών ΕΕ για επιβολή ενιαίας νομοθεσίας που θα καλύπτει όλη την Ευρωπαϊκή Ένωση με τον ίδιο τρόπο. Κάθε απόκλιση στις πρακτικές μεταξύ διαφορετικών κρατών - μελών της Ευρωπαϊκής Ένωσης ή αμφισημειών αποτελεί αχίλλειο πτέρνα σε κάθε δικαστική διαμάχη μεταξύ των τεχνολογικών κολοσσών και των θεσμών.

Πάραυτα, έχοντας τα παραπάνω υπόψη, ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) και η πρόταση για το νέο κανονισμό περί προστασίας της ιδιωτικής ζωής (ePrivacy Regulation) είναι απλώς ένα νομικό μέσο και δεν επαρκεί για την ενίσχυση της προστασίας των δεδομένων ή την ενίσχυση του απορρήτου των πληροφοριών στον διαδικτυακό τομέα.

Πρόβλημα Κακόβουλων Επιθέσεων

Όπως συζητήθηκε παραπάνω, ακόμη και οι ισχυρότεροι νόμοι περί απορρήτου, όπως ο Γενικός Κανόνας Προστασίας Δεδομένων (ΓΚΠΔ), δεν μπορούν να σταματήσουν τις παραβιάσεις δεδομένων που προκαλούνται για παράδειγμα από κακόβουλες επιθέσεις ασφάλειας οι οποίες εξελίσσονται στο διαδίκτυο. Η τρέχουσα προσέγγιση του Ευρωπαϊκού Συμβουλίου είναι ο περιορισμός της επεξεργασίας δεδομένων χωρίς τεχνικές προσεγγίσεις για την κυβερνοασφάλεια του δικτύου και αποθήκευσης δεδομένων. Επομένως, υπάρχει ακόμη πολύς δρόμος για την επίτευξη της πληροφοριακής ιδιωτικής ζωής σε ικανοποιητικό βαθμό, όσον αφορά την ασφάλεια.

Πρόταση για ασφάλεια δικτύων και αντιγράφων ασφαλείας

Προτείνεται η εξερεύνηση παράλληλης δράσης με την έκδοση οδηγιών από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) για καλές πρακτικές ασφάλειας δικτύων, αποθήκευσης και διακίνησης δεδομένων. Αυτές οι οδηγίες θα μπορούσαν σε μεταγενέστερο στάδιο να μετατραπούν και αυτές σε κανονισμό, θέτοντας τα πρότυπα για καλές πρακτικές ασφάλειας δεδομένων.

Ένας αποτελεσματικός τρόπος ρύθμισης του πεδίου της αποθήκευσης και διακίνησης δεδομένων είναι η εισαγωγή απαιτήσεων κρυπτογράφησης τόσο στα δεδομένα που "τρέχουν" στο δίκτυο ή τις συσκευές μας, όσο και στα αρχεία ασφαλείας που συχνά αποθηκεύονται αποκλειστικά χωρίς κρυπτογράφηση ή με κρυπτογράφηση χαμηλού επιπέδου για εύκολη πρόσβαση.

Συγκεκριμένα, προτείνεται η ενθάρρυνση της χρήσης κρυπτογράφησης ηλεκτρονικών συσκευών όπως κινητά, tablet και προσωπικοί υπολογιστές από προεπιλογή σε επίπεδο λειτουργικού συστήματος, καθώς και η ενθάρρυνση κρυπτογράφησης των αντιγράφων ασφαλείας δεδομένων υπηρεσιών νέφους διαδικτύου (cloud).

Πρόβλημα ρυθμού ανάπτυξης τεχνολογίας έναντι νομοθέτησης

Παρατηρείται ότι η τεχνολογία εξελίσσεται γρηγορότερα από τη συνηθισμένη νομοθετική δραστηριότητα. Για παράδειγμα, οι αυτόματοι τηλεφωνητές marketing χρησιμοποιούνται εδώ και χρόνια ενώ αναφέρονται ή περιορίζονται από τη νομοθεσία της Ευρωπαϊκής Ένωσης ξεκινώντας από τη πρόταση του νέου κανονισμού το 2017, η οποία δεν αποτελεί ακόμη ισχύοντα κανονισμό.

Εν γένει, η χρήση ορισμένων ορολογιών και ορισμών ενδεχομένως να πρέπει να επανεξετάζεται συχνά (π.χ. κάθε ένα έτος) λόγω του ρυθμού της τεχνολογικής προόδου, ώστε να διασφαλίζεται πως οι διατάξεις δεν θα καθίστανται παρωχημένες σε μικρότερο χρονικό διάστημα από ότι ενεργά προστάτευαν επαρκώς τους πολίτες.

Πρόταση ρυθμού νομοθέτησης

Βάσει των παραπάνω, χρειάζεται να επιταχυνθούν οι κύκλοι των νομοθετικών εργασιών. Προτείνονται συχνότερες τεχνικές μελέτες των τεχνολογικών τάσεων της αγοράς με σκοπό την κάλυψη κενών σημείων από τη νομοθεσία και την πιο άμεση ρύθμιση. Συγκεκριμένα, είναι εύλογο να εκτελείται επισκόπηση της τεχνολογίας σε τακτά χρονικά διαστήματα όπως για παράδειγμα κάθε ένα με δύο έτη το αργότερο.

Οι ομάδες εργασίας που εκτελούν τις τακτικές μελέτες θα ήταν καλό να απαρτίζονται από πρόσφατα στελέχη μεγάλων τεχνολογικών εταιρειών, με έμφαση σε αυτές που

δραστηριοποιούνται έντονα στο πεδίο της έρευνας και ανάπτυξης νέων τεχνολογιών πληροφορικής.

Πρόταση διεθνής συνεργασίας και άξονα παιδείας, εκπαίδευσης, κοινωνίας

Η προστασία της ιδιωτικής ζωής των πληροφοριών δεν είναι ούτε ένα απλό καθήκον που μπορεί να αφεθεί μόνο στην Ευρωπαϊκή Ένωση, ούτε σε ένα συγκεκριμένο, ενιαίο νομοθετικό πλαίσιο. Ως εκ τούτου, όχι μόνο η Ευρωπαϊκή Ένωση, αλλά όλες οι ανεπτυγμένες ή αναπτυσσόμενες χώρες και οι διεθνείς οργανισμοί, συμπεριλαμβανομένου του Ευρωπαϊκού Συμβουλίου και των Ηνωμένων Εθνών, πρέπει να εργαστούν προς την κατεύθυνση μιας ενιαίας και σύμφωνης πολιτικής που αποσκοπεί στη θέσπιση κοινών, βασικών κανόνων για την προστασία της ιδιωτικής ζωής στον διαδικτυακό τομέα.

Κατά την άποψη πολλών, δεν αρκεί μόνο ο αγώνας της νομοθέτησης. Χρειάζεται να υπάρχει και η ανάλογη ευαισθητοποίηση της κοινωνίας προς τη κατανόηση των κινδύνων που εγκυμονεί η φύση της ηλεκτρονικής επικοινωνίας. Σε αυτό το πλαίσιο, προτείνονται παράλληλες δράσεις στον άξονα της παιδείας, της εκπαίδευσης και της κοινωνίας σε τοπικό επίπεδο για δράσεις που θα κάνουν τα παιδιά, τους σπουδαστές και τους πολίτες πιο ώριμους απέναντι στο φαινόμενο της δημοσιοποίησης των προσωπικών δεδομένων τους στο διαδίκτυο αλλά και της κατανόησης των κινδύνων που ελλοχεύουν στη πολιτική απορρήτου κάθε ηλεκτρονικής υπηρεσίας.

Υπολογισμός Διοικητικής Επιβάρυνσης Τεχνολογικών Εταιρειών

Από τις πρόσφατες μελέτες αλλά και ειδήσεις, φαίνεται ότι η Ευρωπαϊκή Επιτροπή θα πρέπει να συνυπολογίζει τη διοικητική επιβάρυνση των νέων κανονισμών στις τεχνολογικές εταιρείες, ιδιαίτερα ότι αφορά την τεχνική υλοποίηση διαφορετικών υπηρεσιών.

Προτείνεται η κάθε πρόταση κανονισμού να δέχεται δειγματοληπτικά απόψεις από στελέχη μεγάλων οργανισμών τεχνολογίας αλλά και μικρών νεοϊδρυθέντων εταιρειών με σκοπό την άμεση και γρήγορη ανατροφοδότηση απόψεων ως προς τη δυσκολία εφαρμογής ή και ανίχνευσης σημείων που χρειάζονται επικαιροποίηση ή διευκρίνηση.

Κατακλείδα

Τελικά, πρέπει να σημειωθεί ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) ή και η πρόταση για τον νέο κανονισμό ePrivacy Regulation δεν είναι ο αυτοσκοπός για την προστασία και την προώθηση της ιδιωτικής ζωής, αλλά είναι μόνο η αρχή ενός ταξιδιού προς την θεμελίωση του σεβασμού της προσωπικής ζωής παρά την εξέλιξη της τεχνολογίας.

Πιστεύω πως η προστασία και ο σεβασμός της ιδιωτικής ζωής αφορά όλους μας και αποτελεί θέμα κουλτούρας, συνήθειας και αρχών, σε μεγαλύτερο βαθμό από ότι αποτελεί νομοθετικό πλαίσιο ή οικονομικές ποινές.

Βιβλιογραφικές Αναφορές - Παραπομπές - Πηγές από το διαδίκτυο

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο. (1995, 10 24). *Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών*. EUR-Lex. Retrieved 01 15, 2021, from https://eur-lex.europa.eu/eli/dir/1995/46/oj

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (1997, 11 10). *Άρθρο 2 ν. 2472/1997 Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα*. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. https://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL

Ευρωπαϊκό Κοινοβούλιο και Ευρωπαϊκό Συμβούλιο. (2002, 07 31). *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*. EUR-Lex. Retrieved 01 18, 2021, from https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32002L0058&qid=1610997530977

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο. (2009, 11 25). *Οδηγία 2009/136/ΕΚ του ΕΚ&Σ., της 25/11/09, για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλ. επικοινωνιών, της οδηγίας 2002/58/ΕΚ και του κανονισμού 2006/2004*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32009L0136&qid=1611179763549

Ευρωπαϊκό Κοινοβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης. (2016, 04 27). *Κανονισμός (ΕΕ) 2016/679 του ΕΚ και του Σ., της 27ης Απρ. 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο. (2016, 04 27). *Ενοποιημένο κείμενο: Κανονισμός (ΕΕ) 2016/679 του ΕΚ και ΕΣ της 27ης Απ. 2016 για την προστασία των φυσικών προσώπων*

έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση 95/46/ΕΚ. EUR-Lex. Retrieved 01 19, 2021, from https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A02016R0679-20160504

Ευρωπαϊκή Επιτροπή. (2017, 1 10). *Πρόταση: ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ*. EUR-Lex. Retrieved 1 21, 2021, from https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52017PC0010

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ). (2018, 05 25). Δήλωση ΕΣΠΔ σχετικά με την αναθεώρηση του Κανονισμού για την Προστασία της Ιδιωτικής Ζωής στον Τομέα των Ηλεκτρονικών Επικοινωνιών και τον αντίκτυπό της στην προστασία των φυσικών προσώπων όσον αφορά την ιδιωτικότητα και το απόρρητο των επικοινωνιών τους. *e-Privacy Regulation*. https://edpb.europa.eu/our-work-tools/our-documents/otros/statement-edpb-revision-eprivacy-regulation-and-its-impact_el

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο. (2018, 11 21). *Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης*. EUR-Lex. Retrieved 01 19, 2021, from https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32018R1725&qid=1611071991029

Babel, C. (2017, 07 11). *The High Costs of GDPR Compliance*. InformationWeek IT Network Dark Reading. Retrieved 01 20, 2021, from https://www.darkreading.com/endpoint/the-high-costs-of-gdpr-compliance/a/d-id/1329263

Baker & McKenzie. (2016, 05 04). *Preparing for New Privacy Regimes: Privacy Professionals' Views on the General Data Protection Regulation and Privacy Shield*. Baker & McKenzie. Retrieved 01 20, 2021, from http://f.datasrvr.com/fr1/416/76165/IAPP_GDPR_and_Privacy_Shield_Survey_Report.pdf

Bozdag, E. (2018, 01 28). Data Portability Under GDPR: Technical Challenges. *SSRN*, *SSRN*(01), 1-7. 10.2139/ssrn.3111866

Butterworth, T. (2018, 05 23). Europe's tough new digital privacy law should be a model for US policymakers. *Vox*. https://www.vox.com/the-big-idea/2018/3/26/17164022/gdpr-europe-privacy-rules-facebook-data-protection-eu-cambridge

Cage, M. (2018, 5 25). Today, a new E.U. law transforms privacy rights for everyone. Without Edward Snowden, it might never have happened. *The Washington Post*. https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/25/today-a-new-eu-law-transforms-privacy-rights-for-everyone-without-edward-snowden-it-might-never-have-happened/

Chassang, G. (2017, 01 03). The impact of the EU general data protection regulation on scientific research. *ecancer*, *11*(709). 10.3332/ecancer.2017.709

Edwards, E. (2018, 02 22). *New rules on data protection pose compliance issues for firms*. The Irish Times. Retrieved 01 20, 2021, from https://www.irishtimes.com/business/technology/new-rules-on-data-protection-pose-compliance-issues-for-firms-1.3397742

European Commission. (2017, 1 10). *Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC accompanying the document Proposal for a Regulation on Privacy and Electronic Communications*. EUROPA. Retrieved 01 22, 2021, from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41242

European Commission. (2017, 1 10). *Impact Assessment accompanying the proposal for a regulation on privacy and electronic communications*. EUROPA. Retrieved 1 22, 2021, from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41246

European Commission. (2017, 10 27). *Guidelines on the right to "Data Portability"*. Justice and Consumers. Retrieved 01 19, 2021, from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

European Commission. (2017, 10 30). *Guidelines on Data Protection Officers ('DPOs')*. EUROPA. Retrieved 01 20, 2021, from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

European Parliament Legislative Observatory. (2017, 01 10). *2017/0003(COD) Respect for private life and the protection of personal data in electronic communications*. European Parliament Legislative Observatory. Retrieved 01 21, 2021, from https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD)&l=en

European Union. (2020, 09 29). *Regulations, Directives and other acts*. EUROPA. Retrieved 01 18, 2021, from https://europa.eu/european-union/law/legal-acts_en

Fazlioglu, M. (2019, 5 29). *The GDPR, one year on: What about ePrivacy?* iapp.org. Retrieved 1 22, 2021, from https://iapp.org/news/a/the-gdpr-one-year-on-what-about-eprivacy/

Fimin, M. (2018, 03 29). Five Benefits GDPR Compliance Will Bring To Your Business. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business/

Georgi, G. (2018). *GDPR Compliance Cost Calculator*. GIGAcalculator.com. https://www.gigacalculator.com/calculators/gdpr-compliance-cost-calculator.php

Gorey, C. (2017, 11 23). *Are financial institutions ready for blockchain and GDPR?* siliconrepublic. https://www.siliconrepublic.com/enterprise/blockchain-gdpr-report-bai

The Guardian. (2018, 04 19). How Europe's 'breakthrough' privacy law takes on Facebook and Google. *The Guardian*. https://www.theguardian.com/technology/2018/apr/19/gdpr-facebook-google-amazon-data-privacy-regulation

Information Commissioner's Office. (2021, 01 01). *Guide to the General Data Protection Regulation (GDPR)*. Information Commissioner's Office. Retrieved 01 18, 2021, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

ISO. (2017, 01 01). *ISO 25237:2017 Health informatics — Pseudonymization*. ISO. Retrieved 01 20, 2021, from https://www.iso.org/standard/63553.html

Jaffe, J., & Hautala, L. (2018, 05 25). *What the GDPR means for Facebook, the EU and you*. cnet.com. Retrieved 01 21, 2021, from https://www.cnet.com/how-to/what-gdpr-means-for-facebook-google-the-eu-us-and-you/

Jeong, S. (2018, 05 22). No one's ready for GDPR. *THE VERGE*. https://www.theverge.com/2018/5/22/17378688/gdpr-general-data-protection-regulation-eu

Karras, G. G., Kalnis, P., & Mamoulis, N. (2007, September). Fast Data Anonymization with low information loss. *Proceedings of the 33rd international conference on Very large data bases*, *01*(01), 758-769. http://www.vldb.org/conf/2007/papers/research/p758-ghinita.pdf

Katz, J., & Lindell, Y. (2021). *Introduction to Modern Cryptography* (3rd Edition ed.). Routledge (Taylor & Francis Group). ISBN 9781351133036

Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 119, 4 Μαΐου 2016. (2016, 05 04). *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, *L119*(1), 1-149. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=OJ:L:2016:119:TOC

Lawspot. (2017, 12 26). *Κανονισμοί, Οδηγίες και άλλες νομοθετικές πράξεις της Ευρωπαϊκής Ένψσης*. LAWSPOT. Retrieved 01 18, 2001, from https://www.lawspot.gr/nomikes-plirofories/voithitika-kemena/kanonismoi-odigies-kai-alles-nomothetikes-praxeis-tis

Lomas, N. (2018, 10 7). *ePrivacy: An overview of Europe's other big privacy rule changes*. TechCrunch. Retrieved 01 20, 2021, from https://techcrunch.com/2018/10/07/eprivacy-an-overview-of-europes-other-big-privacy-rule-change/

McGavisk, T. (2018, 6 6). *The Positive and Negative Implications of GDPR*. timedatasecurity.com (tds). Retrieved 2 7, 2021, from https://www.timedatasecurity.com/blogs/the-positive-and-negative-implications-of-gdpr

McGrath, S. (2014, 11 11). *Lack of GDPR knowledge is a danger and an opportunity*. MicroScope UK. Retrieved 01 20, 2021, from https://www.computerweekly.com/microscope/news/2240234469/Lack-of-GDPR-knowledge-is-a-danger-and-an-opportunity

Neubauer, T., & Heurix, J. (2011, 03). A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics*, *80*(3), 190-204. 10.1016/j.ijmedinf.2010.10.016

New Cyber-attack Advice for European Hospitals. (2021, 1 22). Info Security Group. Retrieved 1 25, 2021, from https://www.infosecurity-magazine.com/news/new-cyberattack-advice-for/

Parent, W. A. (1983, 12 01). A new definition of privacy for the law. *Law and Philosophy*, *2*(3), 305-338. 10.1007/BF00144949

Politou, E., Alepis, E., & Patsakis, C. (2018, 03 26). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1), 1-20. 10.1093/cybsec/tyy001

The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. (2012). *Computer Law & Security Review*, *28*(2), 130-142. 10.1016/j.clsr.2012.01.011

Renaud, K., & Gálvez-Cruz, D. (2010). Privacy: Aspects, definitions and a multi-faceted privacy preservation approach. *2010 Information Security for South Africa*, 1-8. 10.1109/ISSA.2010.5588297

Rights related to automated decision making including profiling. (2021, 01 01). Information Commissioner's Office. Retrieved 01 19, 2021, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

Schulze, E. (2019, 4 1). *Mark Zuckerberg says he wants stricter European-style privacy laws — but some experts are questioning his motives*. CNBC. Retrieved 1 21, 2021, from https://www.cnbc.com/2019/04/01/facebook-ceo-zuckerbergs-call-for-gdpr-privacy-laws-raises-questions.html

Scrambox. (2016, 10 30). *How long would it take to brute force AES-256?* scrambox.com. Retrieved 01 20, 2021, from https://scrambox.com/article/brute-force-aes/

Stallman, R. (2018, 4 3). A radical proposal to keep your personal data safe. *The Guardian*. https://www.theguardian.com/commentisfree/2018/apr/03/facebook-abusing-data-law-privacy-big-tech-surveillance

Vanberg, A. D. (2020, 7 9). Informational privacy post GDPR – end of the road or the start of a long journey? *The International Journal of Human Rights*, *25*(1), 52-78. 10.1080/13642987.2020.1789109

Veale, M., Binns, R., & Jef, A. (2018, 05). When data protection by design and data subject rights clash. *International Data Privacy Law*, *8*(2), 105-123. 10.1093/idpl/ipy002

Wes, M. (2017, 04 25). *Looking to comply with GDPR? Here's a primer on anonymization and pseudonymization*. iapp.org. Retrieved 01 20, 2021, from https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/

Westin, A. F. (1968). *Privacy and Freedom* (Vol. 25). Washington and Lee Law Review. https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr

Zuiderveen Borgesius, F. J. (2016, 04). Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer Law & Security Review*, *32*(2), 256-271. 10.1016/j.clsr.2015.12.013