ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΗΛΙΑ Β. ΚΟΥΛΑΚΟΥ

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΦΟΙΤΗΤΗ ΤΟΥ ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟΥ ΜΕΤΑΠΤΥΧΙΑΚΟΥ με αντικείμενο:

«ΤΟΠΙΚΗ ΑΥΤΟΔΙΟΙΚΗΣΗ και ΠΕΡΙΦΕΡΕΙΑΚΗ ΑΝΑΠΤΥΞΗ »

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:ΜΙΧΑΗΛ ΣΦΑΚΙΑΝΑΚΗΣ-

Κοσμήτωρ της Σχολής Διοίκησης Επιχειρήσεων του Πανεπιστημίου Πειραιώς

Θέμα Διπλωματικής:ΤΟ ΝΕΟ ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

THE NEW INSTITUTIONAL FRAMEWORK FOR THE PROTECTION OF PERSONAL DATA(GDPR)

- Αθήνα, ΣΕΠΤΕΜΒΡΙΟΣ 2018

GDPR

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Ένα από τα αποτελέσματα της ταχείας προόδου της τεχνολογίας είναι ότι τα πρότυπα προστασίας δεδομένων γίνονται όλο και πιο αυστηρά, με αποτέλεσμα οι εταιρείες να αντιμετωπίζουν το πολύπλοκο καθήκον της αξιολόγησης τους για το εάν οι δραστηριότητες επεξεργασίας δεδομένων τους, συμμορφώνονται νομικά και πιο ειδικά σε διεθνές πλαίσιο. Τα δεδομένα - από την φύση τους – μπορούν εύκολα να διασχίσουν τα σύνορα και να διαδραματίσουν σημαντικό ρόλο στην παγκόσμια ψηφιακή οικονομία.

Κατά τα τελευταία χρόνια, τα δεδομένα έχουν γίνει πολύτιμο περιουσιακό στοιχείο, καλούνται ακόμα και ως το νόμισμα του μέλλοντος. Η επεξεργασία των προσωπικών δεδομένων πραγματοποιείται σε διάφορους τομείς των οικονομικών και κοινωνικών δραστηριοτήτων, ενώ η πρόοδος στον τομέα της πληροφορικής καθιστά ευκολότερη την επεξεργασία και την ανταλλαγή τέτοιων δεδομένων. Αυτό αποδείχτηκε ιδιαίτερα πρόσφορο για παράνομες δραστηριότητες, όπως για παράδειγμα η πώληση ευαίσθητων προσωπικών δεδομένων ή η επεξεργασία των δεδομένων για διαφορετικό σκοπό από τον οποίο συλλέχθηκαν αρχικά.

Σε αυτό το πλαίσιο, η Ευρωπαϊκή Ένωση (Ε.Ε.) ενέκρινε τον Κανονισμό για την γενική προστασία των δεδομένων (General Data Protection Regulation – GDPR) με σκοπό την περαιτέρω εναρμόνιση των κανόνων για την προστασία των δεδομένων μεταξύ των κρατών – μελών της Ε.Ε. και την αύξηση του επιπέδου προστασίας της ιδιωτικής ζωής για τους κατοίκους της γηραιάς ηπείρου. Το GDPR τέθηκε σε ισχύ στις 25 Μαρτίου 2018. Λόγω του ευρέως διακρατικού πεδίου εφαρμογής του, θα επηρεάσει επίσης πολλές εταιρίες που βρίσκονται εκτός της Ε.Ε. . Οι επιχειρήσεις πρέπει να αξιολογήσουν εάν εμπίπτουν στο πεδίο εφαρμογής του GDPR και να προσπαθήσουν να συμμορφωθούν με τις απαιτήσεις του Κανονισμού εγκαίρως.

Σκοπός της παρούσας εργασίας είναι να γίνει μια σύντομη αναφορά στην Ευρωπαϊκή πορεία προς το GDPR, κάνοντας μια μικρή αναδρομή στην Ελληνική πραγματικότητα και νομοθεσία περί της προστασίας προσωπικών δεδομένων. Το μεγαλύτερο μέρος της εργασίας επικεντρώνεται στην ανάλυση του GDPR, στα δικαιώματα των ατόμων που αφορούν τα δεδομένα και κυρίως στις αλλαγές που επιφέρει στις επιχειρήσεις αναφορικά με την διαχείριση των δεδομένων και την αλληλεπίδραση τους με τις εποπτικές αρχές.

ΚΕΦΑΛΑΙΟ 1 – ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

1.1 Ιστορική αναδρομή προστασίας δεδομένων στην Ευρώπη

Η Ευρωπαϊκή ένωση είχε αναγνωρίσει από τα μέσα του 20ού αιώνα την προστασία των προσωπικών δεδομένων ως ένα από τα θεμελιώδη δικαιώματα των πληθυσμών της. Αξίζει να σημειωθεί ότι οι πρώτες προσπάθειες προστασίας αυτών των δεδομένων έγιναν σε διεθνές επίπεδο και όχι σε επίπεδο κράτους. Αυτό συνέβη γιατί η τεχνολογική πρόοδος καθιστούσε εύκολη την ροή πληροφοριών πέρα από τα σύνορα των κρατών. Από εκείνη την εποχή και μέχρι σήμερα, η τεχνολογία έχει κάνει τεράστια άλματα προόδου και οι νόμοι της Ε.Ε. για την προστασία των δεδομένων έχουν προσαρμοστεί με τέτοιο τρόπο ώστε εδώ και πολλά χρόνια να θεωρούνται ως πρότυπο για την παγκόσμια κοινότητα.

Από τα τέλη της δεκαετίας του '60 έως τη δεκαετία του 1980, πολλές χώρες, κυρίως στην Ευρώπη, πήραν το πρωτοβουλία θέσπισης νομοθεσίας με στόχο τον έλεγχο της χρήσης των προσωπικών πληροφοριών από κυβερνητικούς οργανισμούς και μεγάλες εταιρείες. Αυτές περιλαμβάνουν την Αυστρία, τη Δανία, τη Γαλλία, την Ομοσπονδιακή Δημοκρατία της Γερμανίας, το Λουξεμβούργο, τη Νορβηγία και τη Σουηδία. Σε τρεις ευρωπαϊκές χώρες, την Ισπανία, την Πορτογαλία και την Αυστρία, η προστασία των δεδομένων είχε επίσης ενσωματωθεί στο Σύνταγμα ως θεμελιώδες δικαίωμα. Υπό το πρίσμα αυτής της τάσης, το Συμβούλιο της Ευρώπης αποφάσισε να θεσπίσει ένα ειδικό πλαίσιο αρχών και προτύπων για την πρόληψη της αθέμιτης συλλογής και επεξεργασίας προσωπικών δεδομένων. Αυτό υπήρξε το αποτέλεσμα της ανησυχίας ότι, στο πλαίσιο της ανάπτυξης της τεχνολογίας, οι εθνικές νομοθεσίες δεν προστάτευαν επαρκώς το δικαίωμα στην ιδιωτικότητα. Η ανησυχία αυτή οδήγησε το 1968 στη δημοσίευση της Σύστασης 509 για τα Ανθρώπινα Δικαιώματα και τις Σύγχρονες και Επιστημονικές Τεχνολογικές Εξελίξεις (Recommendation 509 on Human Rights and Modern and Scientific Technological Developments). Το 1973 και το 1974 το Συμβούλιο της Ευρώπης βασίστηκε σε αυτή τη Σύσταση για να καταλήξει στα Ψηφίσματα 73/22 και 74/29, τα οποία θέσπισαν αρχές για την προστασία των προσωπικών δεδομένων σε αυτοματοποιημένες βάσεις δεδομένων στον ιδιωτικό και στον δημόσιο τομέα, αντίστοιχα, με στόχο να αναπτυχθούν εθνικές νομοθεσίες με βάση αυτά τα ψηφίσματα.

Επόμενη σημαντική ημερομηνία αναφορικά με τα δικαιώματα της προστασίας των προσωπικών δεδομένων των Ευρωπαίων πολιτών αποτελεί η 28η Ιανουαρίου 1981. Εκείνη την ημέρα η συνθήκη για την προστασία των ατόμων όσον αφορά την αυτοματοποιημένη επεξεργασία των προσωπικών τους δεδομένων υπογράφηκε ως σύμβαση 108 του Συμβουλίου της Ευρώπης και τέθηκε σε ισχύ από την 1η Οκτωβρίου 1985. Και τα 47 μέλη του Συμβουλίου της Ευρώπης επικύρωσαν τη συνθήκη εκτός από την Τουρκία. Παρά το γεγονός, όμως ότι ο στόχος της σύμβασης 108 ήταν να υπάρξει μια συντονισμένη προσέγγιση για την προστασία των δεδομένων, αναπτύχθηκε ένα διαφορετικό σύνολο καθεστώτων προστασίας των δεδομένων ακόμη και μεταξύ του μικρού αριθμού χωρών που υιοθέτησαν εθνικούς

νόμους με βάση αυτήν. Αυτό συνέβη γιατί η Σύμβαση 108 δεν όριζε αυστηρά τα πρότυπα ασφαλείας που περιέχει κάνοντας αντιληπτό ότι η υιοθέτηση αυτών των αρχών θα μπορούσε να έχει σοβαρές επιπτώσεις για τα θεμελιώδη δικαιώματα των ατόμων.

Το αποκορύφωμα του έργου που ανέλαβε η Ευρωπαϊκή Επιτροπή για να διορθώσει τα κακώς κείμενα της σύμβασης 108 ήταν η οδηγία 95/46/ΕΚ σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (γνωστή και ως Data Protection Directive). Όπως υποδηλώνει ο τίτλος, ο στόχος της Οδηγίας είναι να θωρακιστεί περαιτέρω η προστασία των θεμελιωδών δικαιωμάτων των ατόμων με την ελεύθερη ροή δεδομένων από το ένα κράτος μέλος σε κάποιο άλλο. Δυστυχώς, εξακολούθησαν να υπάρχουν σημαντικές διαφορές στους τρόπους με τους οποίους τα κράτη μέλη υλοποίησαν την οδηγία, που σε ορισμένες περιπτώσεις, οφειλόταν σε εσφαλμένη εφαρμογή, που πρακτικά σήμαινε ότι η νομοθεσία του κράτους μέλους απαιτούσε διόρθωση. Από εκείνο το σημείο χρονικά, έχουν υπάρξει βήματα προς σωστή κατεύθυνση όσων αφορά την προστασία των προσωπικών δεδομένων με σημαντικότερα εξ αυτών:

- Την υπογραφή του Χάρτη Θεμελιωδών Δικαιωμάτων από τους προέδρους του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Επιτροπής για λογαριασμό των θεσμικών οργάνων τους στις 7 Δεκεμβρίου του 2000 στη Νίκαια.
- Στις 4 Νοεμβρίου 2010 η Ευρωπαϊκή Επιτροπή καθορίζει στρατηγική για τον τρόπο προστασίας των προσωπικών δεδομένων, μειώνοντας παράλληλα την γραφειοκρατία για τις επιχειρήσεις και διασφαλίζοντας την ελεύθερη κυκλοφορία δεδομένων εντός της Ε.Ε. . Η εν λόγω επανεξέταση της πολιτικής είχε ως τελικό σκοπό να χρησιμοποιηθεί από την Επιτροπή με τα αποτελέσματα της δημόσιας διαβούλευσης για την αναθεώρηση του Data Protection Directive.
- Στις 25 Ιανουαρίου 2012 η Ευρωπαϊκή Επιτροπή πρότεινε μια συνολική μεταρρύθμιση των κανόνων που θεσπίστηκαν το 1995 για την προστασία των δεδομένων, για την ενίσχυση της διαδικτυακής ανωνυμίας και την ενίσχυση της ψηφιακής οικονομίας της Ευρώπης. Η Επιτροπή αναγνώρισε ότι η τεχνολογική πρόοδος και η παγκοσμιοποίηση έχουν αλλάξει βαθιά τον τρόπο συλλογής, πρόσβασης και χρήσης των δεδομένων. Παράλληλα με την πρόταση για τον Κανονισμό General Data Protection Regulation (5853/12), η Επιτροπή εισήγαγε ειδική οδηγία σχετικά με την επεξεργασία δεδομένων για σκοπούς επιβολής του νόμου (Directive on Data Processing for Law Enforcement Purposes - 5833/12).

1.2 Ιστορική αναδρομή προστασίας δεδομένων στην Ελλάδα

Η πρώτη προσπάθεια για την προστασία των προσωπικών δεδομένων στην Ελλάδα έγινε με την επιτροπή Χαλαζωνίτη το 1985, η οποία πρώτη έκανε αναφορά για υπερευαίσθητα δεδομένα. Στην συνέχεια είναι αξιοσημείωτο ότι το Υπουργείο Δικαιοσύνης πρότεινε σχέδια νόμου για τέσσερις συνεχόμενες χρονιές (από το 1989 έως το 1992), όμως κανένα δεν συζητήθηκε προς υιοθέτηση. Στον ίδιο ρυθμό κινήθηκε η χώρα και κατά την αποδοχή της Ευρωπαϊκής σύμβασης 108, η οποία δεν συνοδεύτηκε από την θέσπιση αντίστοιχης διάταξης στο ελληνικό δίκαιο.

Με το Νόμο 2472/97 έγινε προσπάθεια να προσαρμοστεί στα ελληνικά δεδομένα η Οδηγία 95/46/ΕΚ της Ευρωπαϊκής Ένωσης. Μάλιστα ο Έλληνας νομοθέτης εκμεταλλευόμενος τη διακριτική ευχέρεια που του παρείχε η Οδηγία επεδίωξε να υιοθετήσει τις αρχές και τις προβλέψεις της με αρκετά αυστηρό τρόπο επιδιώκοντας ένα όσο το δυνατόν υψηλότερο επίπεδο προστασίας. Ωστόσο οι αποκλίσεις του από την αντίστοιχη Κοινοτική Οδηγία είναι σε αρκετά σημεία ουσιώδεις. Οι ρυθμίσεις αναφέρονται τόσο στον ιδιωτικό όσο και στο δημόσιο τομέα και καταλαμβάνουν όλη τη διάρκεια του κύκλου ζωής μιας πληροφορίας προσωπικού χαρακτήρα. Οι βασικοί άξονες του Νόμου είναι τρεις και αφορούν α) ένα σύστημα προϋποθέσεων νομιμότητας επεξεργασίας, β) παροχή δικαιωμάτων στα άτομα και γ) την οργάνωση ελέγχου προστασίας των δεδομένων. Επόμενο βήμα για αναθεώρηση πραγματοποιήθηκε το 2011 με τον νόμο 3917/2011, καθώς η χώρα έπρεπε να εναρμονιστεί με τις επιταγές του 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου. Η νομοθεσία αυτή περιελάμβανε για πρώτη φορά την υποχρέωση των τηλεπικοινωνιακών παρόχων να παρέχουν απαραίτητες πληροφορίες για την εξακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Περιελάμβανε διατάξεις οι οποίες προστάτευαν τις ηλεκτρονικές επικοινωνίες του ελληνικού πληθυσμού, παρέχοντας όμως εξαιρέσεις, όπως για παράδειγμα η υπό προϋποθέσεις διατήρηση δεδομένων που αφορούν την τοποθεσία φυσικών ή νομικών προσώπων. Η νομοθεσία περιελάμβανε ακόμα τους τρόπους με τους οποίους πρέπει να επεξεργάζονται τα δεδομένα, ορίζοντας ταυτόχρονα τις υποχρεώσεις των παρόχων και τις ποινές στην περίπτωση μη συμμόρφωσης. Τέλος γινόταν αναφορά στις εποπτικές αρχές οι οποίες ήταν υπεύθυνες για την τήρηση των κανονισμών: εκείνη την εποχή η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ήταν υπεύθυνη για την τήρηση του νόμου 2472/97. Σημαντικό ρόλο διατηρούσε και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, η οποία ήταν υπεύθυνη για την τήρηση του νόμου Ν. 3115/2003, ο οποίος αναφέρεται στα δικαιώματα ελεύθερης ανταπόκρισης και επικοινωνίας.

Μεγάλη σημασία έχει και η προστασία των προσωπικών δεδομένων στον ελληνικό χώρο όπως αυτή προβλέπεται στο Σύνταγμα της χώρας. Σύμφωνα με το άρθρο 9Α του Συντάγματος, “Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων

διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει.” Το Σύνταγμα χρησιμοποιεί αυτό τον ευρύ ορισμό ηθελημένα, μην περιορίζοντας την εφαρμογή του για παράδειγμα στην ηλεκτρονική επεξεργασία δεδομένων (αποκλείοντας με αυτό τον τρόπο την δια χειρός επεξεργασία), ή σε ορισμένες κατηγορίες αυτοματοποιημένης επεξεργασίας Σκοπός του νομοθέτη είναι ένας ευρύς ορισμός για να περιλάβει, μεταξύ άλλων, τα δικαιώματα των ιδιωτών, των φορέων δημόσιας εξουσίας και τις σχέσεις μεταξύ ιδιωτών.

ΚΕΦΑΛΑΙΟ 2 – ΕΙΣΑΓΩΓΗ ΣΤΟ GDPR

2.1 Πεδίο εφαρμογής του GDPR

"This Regulation applies to the processing of personal data wholly or partly by auto-mated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."

Σύμφωνα με το κείμενο του Κανονισμού, επομένως, βρίσκεται σε ισχύ σε οποιαδήποτε περίπτωση έχουμε επεξεργασία προσωπικών δεδομένων με αυτόματο ή μη αυτόματο τρόπο, με σκοπό την αρχειοθέτηση τους σε κάποιο σύστημα. Ο όρος "επεξεργασία" περιλαμβάνει μεταξύ άλλων τη συλλογή, την καταγραφή, την οργάνωση, τη δομή, την αποθήκευση και τη διαγραφή των δεδομένων. Περιλαμβάνει ακόμα και μη αυτόματη επεξεργασία, που πραγματοποιείται αποκλειστικά από τον άνθρωπο και χωρίς την χρήση εργαλείων, με την προϋπόθεση ότι τα δεδομένα θα χρησιμοποιηθούν σε κάποιο σύστημα αρχειοθέτησης ή στην περίπτωση που τα δεδομένα πρέπει να δομηθούν με συγκεκριμένο τρόπο. Οι νομοθέτες επέλεξαν να μην διευκρινίσουν τον όρο με σκοπό να αποφύγουν προσπάθειες καταστρατήγησης του Κανονισμού, αλλά και για να καταστήσουν το πεδίο εφαρμογής ανεξάρτητο από τις τεχνολογικές αλλαγές.

Παράλληλα, τα δεδομένα στα όποια αναφερόμαστε θα πρέπει να είναι προσωπικά για να εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού. Τα δεδομένα θεωρούνται προσωπικά εάν σχετίζονται με κάποιο αναγνωρισμένο ή αναγνωρίσιμο άτομο (Άρθρο 4 του GDPR). Με άλλα λόγια τα δεδομένα είναι προσωπικά, στην περίπτωση που κάποιο άτομο μπορεί να εντοπιστεί, άμεσα ή έμμεσα, μέσω αναφοράς σε κάποιο χαρακτηριστικό το οποίο μπορεί να είναι:

- Το όνομα του ατόμου.
- Αριθμοί ταυτοποίησης, όπως ο Αριθμός Κοινωνικής Ασφάλισης, Αριθμός Ταυτότητας ή Διαβατηρίου.
- Δεδομένα τοποθεσίας.
- Online αναγνωριστικά (για παράδειγμα IP addresses ή cookies).

Ο κανονισμός δεν εφαρμόζεται στα προσωπικά δεδομένα ενός αποθανόντος ατόμου. Ωστόσο, τα εν λόγω δεδομένα μπορεί να είναι προσωπικά δεδομένα ενός συγγενή ή ενός απόγονου του αποθανόντα. Για παράδειγμα, τέτοια δεδομένα θα μπορούσαν να δώσουν πληροφορίες για τις κληρονομικές ασθένειες ενός απογόνου.

Στην ενότητα 2 του άρθρου 2 του Κανονισμού, προβλέπονται τέσσερις εξαιρέσεις από το πεδίο εφαρμογής αυτού. Μεταξύ άλλων, ο Κανονισμός δεν εφαρμόζεται στους τομείς των πολιτικών ασφαλείας ή της ποινικής δίωξης. Η σημαντικότερη εξαίρεση από οικονομικής άποψης προβλέπεται στο σημείο γ) της συγκεκριμένης ενότητας, σύμφωνα με το οποίο "Ο Κανονισμός δεν ισχύει για την επεξεργασία προσωπικών δεδομένων από ένα άτομο κατά τη διάρκεια μιας αυστηρά προσωπικής ή οικιακής δραστηριότητας". Σε αυτή την περίπτωση οι νομοθέτες λαμβάνουν υπ' όψιν την γενικότερη κοινή γνώμη και περιλαμβάνουν

δεδομένα τα οποία επεξεργάζονται για ψυχαγωγικές δραστηριότητες, διακοπές ή διασκέδαση, για τη χρήση σε ένα κοινωνικό δίκτυο ή δεδομένα που αποτελούν μέρος μιας προσωπικής συλλογής διευθύνσεων, γενεθλίων ή άλλες σημαντικές ημερομηνίες, όπως οι επέτειοι. Αξίζει να σημειωθεί, όμως, πως η χρήση του όρου "αυστηρά", συνεπάγεται πως η συγκεκριμένη εξαίρεση αίρεται στην οποιαδήποτε περίπτωση επιχειρηματικής δραστηριότητας, που περιλαμβάνει οικονομική δραστηριότητα, ανεξαρτήτως του αν υφίσταται αμοιβή ή όχι.

2.2 Εφαρμογή του κανονισμού

Το GDPR ισχύει για όποιον επεξεργάζεται ή ελέγχει την επεξεργασία προσωπικών δεδομένων. Δεδομένης της οικονομικής σημασίας των δεδομένων, από τον Κανονισμό θα επηρεαστούν ιδιαίτερα οι επιχειρήσεις. Υπάρχει μεγάλη ποικιλία σχετικά με τους αποδέκτες των κανόνων και το GDPR παρέχει διαφορετικούς ρόλους και υποχρεώσεις για την ασφάλεια των δεδομένων. Προκειμένου να καθοριστεί το πεδίο εφαρμογής του GDPR και οι ευθύνες προστασίας δεδομένων που προκύπτουν, πρέπει να καθοριστεί ποιος είναι ο «υπεύθυνος διαχείρισης» (controller), ποιος είναι ένας «υπεύθυνος επεξεργασίας» (processor) και ποιος επωφελείται από την προστασία των δεδομένων στο πλαίσιο του Κανονισμού.

- <u>Υπεύθυνος διαχείρισης δεδομένων:</u>

Σύμφωνα με το άρθρο νούμερο 4 του Κανονισμού, "Υπεύθυνος διαχείρισης (controller) ορίζεται ένα φυσικό ή νομικό πρόσωπο, μια δημόσια αρχή, ένας οργανισμός ή άλλος φορέας, ο οποίος από μόνος του ή από κοινού με άλλους, καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα". Πρέπει να τονιστεί πως ο Κανονισμός ορίζει κάθε επιχείρηση αποκλειστικά υπεύθυνη για την επεξεργασία δεδομένων υπό την εποπτεία της, ανεξάρτητα από το εάν ανήκει σε έναν όμιλο εταιριών. Επιπρόσθετα, μεμονωμένα άτομα μπορούν να θεωρηθούν Υπεύθυνοι διαχείρισης, σε περίπτωση που χρησιμοποιήσουν προσωπικά δεδομένα για δικούς τους σκοπούς, εκτός των δραστηριοτήτων του οργανισμού στον οποίον ανήκουν.

Οι νομοθέτες θέλησαν να ορίσουν απόλυτα διακριτούς ρόλους στον Κανονισμό, καθώς θα μπορούσε να υπάρξει κάποια σύγχυση ανάμεσα στους ρόλους του «υπεύθυνου διαχείρισης», και του «υπεύθυνου επεξεργασίας». Η κύρια διαφορά έγκειται στο γεγονός πως ο Υπεύθυνος Διαχείρισης, έχει την δυνατότητα λήψης αποφάσεων και μπορεί να αναθέσει, έστω και εν μέρει, την τεχνική ή οργανωτική επεξεργασία των δεδομένων σε κάποιο άτομο. Η εξουσία αυτή μπορεί να του έχει ανατεθεί μέσω κάποιας δημόσιας αρχής, με την νομική ευθύνη να απορρέει από κοινές νομικές διατάξεις ή μέσω συμφωνίας μεταξύ συμβαλλόμενων μερών,

αναθέτοντας τον ρόλο και τις ευθύνες του Υπεύθυνου Διαχείρισης σε έναν ή περισσότερα μέρη.

- Υπεύθυνος επεξεργασίας δεδομένων:

Εκτός από τον υπεύθυνο διαχείρισης δεδομένων, ο Κανονισμός επιβάλλει υποχρεώσεις προστασίας δεδομένων και στον «Υπεύθυνο επεξεργασίας» (processor). Ο τελευταίος ορίζεται ως φυσικό ή νομικό πρόσωπο, δημόσια αρχή, οργανισμός ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του Υπεύθυνου Διαχείρισης δεδομένων, σύμφωνα με το άρθρο 4 του GDPR. Έτσι, η ύπαρξη ενός Υπεύθυνου επεξεργασίας εξαρτάται από μια απόφαση που έχει ληφθεί από τον υπεύθυνο διαχείρισης δεδομένων, ο οποίος μπορεί είτε να επεξεργάζεται δεδομένα εντός της οργάνωσής του (μέσω των υπαλλήλων του) ή να εκχωρήσει όλες ή μέρος των δράσεων επεξεργασίας σε έναν εξωτερικό οργανισμό, καθιστώντας τον τελευταίο "Υπεύθυνο επεξεργασίας".

Δυο συνθήκες πρέπει να πληρούνται για να θεωρηθεί κάποιος Υπεύθυνος επεξεργασίας δεδομένων:

1. Να πραγματοποιεί επεξεργασία προσωπικών δεδομένων για λογαριασμό του Υπεύθυνου διαχείρισης.
2. Να είναι ξεχωριστή νομική οντότητα / άτομο από τον Υπεύθυνο διαχείρισης.

Πέρα όμως από τους ρόλους που ορίζει ο Κανονισμός, σύμφωνα με τον τμήμα 1, Άρθρο 1, το GDPR δημιουργήθηκε για να θέσει κανόνες για την προστασία των ατόμων. Και ενώ δεν υπάρχει περαιτέρω εξήγηση του όρου άτομο, σημειώνεται ότι τα παιδιά επωφελούνται από ειδική, ενισχυμένη προστασία στο πλαίσιο του Κανονισμού διότι ενδέχεται να μην γνωρίζουν τους κινδύνους, τις συνέπειες και τα δικαιώματά τους σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Επιπρόσθετα, ο Κανονισμός δεν ωφελεί νομικά πρόσωπα, ανεξάρτητα από την νομική μορφή τους, καθώς κύριος σκοπός είναι η προστασία των βασικών ατομικών δικαιωμάτων. Μοναδική εξαίρεση σε αυτή την περίπτωση είναι οι νομικές οντότητες που ανήκουν σε ένα άτομο (one-man-owned entity), επειδή σε αυτή την περίπτωση δεν υπάρχει η δυνατότητα διαχωρισμού προσωπικών και εταιρικών δεδομένων.

- Κανονισμός αφορά την επεξεργασία προσωπικών δεδομένων στο πλαίσιο των δραστηριοτήτων του Υπεύθυνου διαχείρισης ή του Υπεύθυνου επεξεργασίας με έδρα στην Ευρωπαϊκή Ένωση, αλλά ανεξάρτητα από το εάν η επεξεργασία πραγματοποιείται στην Ένωση ή όχι.
- Ο Κανονισμός αφορά την επεξεργασία προσωπικών δεδομένων ατόμων τα οποία βρίσκονται εντός της Ένωσης, από έναν ή παραπάνω Υπεύθυνο διαχείρισης ή Υπεύθυνο επεξεργασίας χωρίς έδρα στην Ένωση, εάν η επεξεργασία των δεδομένων σχετίζεται με την προσφορά αγαθών ή

υπηρεσιών, ανεξάρτητα από το αν υφίσταται αμοιβή προς το πρόσωπο στο οποίο αναφέρονται τα δεδομένα.

- Ο Κανονισμός αφορά την επεξεργασία προσωπικών δεδομένων από έναν Υπεύθυνο διαχείρισης, χωρίς έδρα στην Ευρωπαϊκή Ένωση, αλλά σε τοποθεσία η οποία υπάγεται στο Δίκαιο των κρατών μελών , σύμφωνα με το Διεθνές Δίκαιο.

Το άρθρο 3 επεξηγεί τους λόγους για τους οποίους, ενώ το GDPR είναι ένας Ευρωπαϊκός κανονισμός, η εφαρμογή του, δεν σταματά στα σύνορα της Ευρωπαϊκής Ένωσης. Πτυχές της παγκόσμιας οικονομίας με τις πολυεθνικές εταιρίες και την διασυνοριακή μεταφορά δεδομένων, ελήφθησαν σοβαρά υπόψη κατά τη δημιουργία του GDPR. Η διεθνής εφαρμογή εγγυάται την πλήρη προστασία της ιδιωτικής ζωής των ατόμων και τις θεμιτές συνθήκες ανταγωνισμού στην εσωτερική αγορά της ΕΕ. Επίσης, αποφεύγεται το φαινόμενο του forum shopping: λόγω του ότι διαφορετικά πρότυπα προστασίας δεδομένων ίσχυαν μέχρι στιγμής στα κράτη μέλη της Ευρωπαϊκή Ένωσης, οι εταιρίες μπορούσαν να επιλέγουν τον τόπο δραστηριότητάς τους σύμφωνα με το χαμηλότερο εθνικό επίπεδο πρότυπων ασφαλείας (μεταξύ άλλων παραγόντων).

ΚΕΦΑΛΑΙΟ 3 – ΝΟΜΙΚΗ ΒΑΣΗ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

3.1 Βασικές αρχές επεξεργασίας προσωπικών δεδομένων

Η επεξεργασία των προσωπικών δεδομένων πρέπει να πραγματοποιείται με νόμιμη βάση, να έχει δίκαιο και διαφανή χαρακτήρα για το άτομο το οποίο αφορούν τα προσωπικά δεδομένα, σύμφωνα με το άρθρο 5 παράγραφο 1 του Κανονισμού. Έτσι, η επεξεργασία δεδομένων μπορεί μόνο να πραγματοποιηθεί μόνο εφόσον καλύπτεται από νόμιμη άδεια ή από τη συγκατάθεση του ατόμου αυτού. Τα άτομα πρέπει να έχουν τη δυνατότητα να κατανοήσουν τι συμβαίνει με τα προσωπικά τους δεδομένα. Ως εκ τούτου, θα πρέπει να είναι ξεκάθαρο σε αυτά ότι τα προσωπικά τους δεδομένα συλλέγονται, χρησιμοποιούνται, ή υποβάλλονται σε άλλη επεξεργασία και σε ποιο βαθμό τα δεδομένα αυτά χρησιμοποιούνται ή πρόκειται να χρησιμοποιηθούν. Η αρχή της διαφάνειας απαιτεί, ειδικότερα:

- Τα άτομα να έχουν πρόσβαση σε πληροφορίες σχετικά με την ταυτότητα του Υπεύθυνου διαχείρισης.
- Τα άτομα να έχουν πρόσβαση σε πληροφορίες σχετικά με τους σκοπούς της επεξεργασίας.
- Την ευαισθητοποίηση των ατόμων σχετικά με τους κινδύνους, τους κανόνες και τα δικαιώματα τους σε σχέση με την επεξεργασία των προσωπικών δεδομένων τους και τον τρόπο άσκησής αυτής.

Τα προσωπικά δεδομένα πρέπει να συλλέγονται μόνο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να μην υφίστανται περαιτέρω επεξεργασία κατά τρόπο που δεν συνάδει με τους σκοπούς αυτούς. Ο σκοπός της επεξεργασίας δεδομένων διαδραματίζει βασικό ρόλο για τη νομιμότητα των δραστηριοτήτων των Υπεύθυνων διαχείρισης / επεξεργασίας, καθώς επιτρέπει τον προσδιορισμό του εάν οι βασικές αρχές της ελαχιστοποίησης των δεδομένων (data minimisation), της ακρίβειας (accuracy) και του περιορισμού της αποθήκευσης (storage limitation) γίνονται σεβαστές. Κατά την άσκηση περαιτέρω δραστηριοτήτων επεξεργασίας, οι εταιρίες θα πρέπει να επαληθεύουν ότι αυτές οι δραστηριότητες είναι συμβατές με τον αρχικό σκοπό. Διαφορετικά, η νέα επεξεργασία προσωπικών δεδομένων θα είναι νόμιμη μόνο μέσω ανανεωμένης συγκατάθεσης του ατόμου ή μέσω νόμιμης αιτιολόγηση στο δίκαιο των κρατών μελών της Ευρωπαϊκής Ένωσης που επιτρέπει την αλλαγή του σκοπού της επεξεργασίας των δεδομένων. Το επίπεδο λεπτομέρειας του σκοπού που παρουσιάζεται στα άτομα που αφορά η επεξεργασία μπορεί να ποικίλλει κατά περίπτωση, καθώς προσαρμόζεται με βάση την συγκεκριμένη λειτουργία επεξεργασίας. Μερικές βασικές αρχές σε σχέση με την λεπτομέρεια του σκοπού επεξεργασίας προσωπικών δεδομένων αποτελούν:

- Όσο μεγαλύτερος είναι ο αριθμός των ατόμων και όσο μεγαλύτερη η γεωγραφική περιοχή που επηρεάζεται, τόσο σαφέστερα πρέπει να

προσδιοριστούν οι σκοποί καθώς είναι ιδιαίτερα πιθανό ότι αφορούν άτομα από διαφορετικές ηλικιακές ομάδες ή διαφορετικά πολιτιστικά υπόβαθρα.

- Η ανάλυση του σκοπού επεξεργασίας σε μικρότερους υπό σκοπούς, μπορεί να αποδειχθεί ευεργετική για την σαφήνεια προς τα άτομα που αφορούν τα δεδομένα.
- Επιπλέον, οι διαβαθμισμένες ενημερώσεις απορρήτου μπορεί να είναι πολύ χρήσιμες για την αύξηση του επιπέδου διαφάνειας της επεξεργασίας πληροφοριών για τα άτομα στα οποία αναφέρονται τα δεδομένα. Αυτό σημαίνει ότι για παράδειγμα βασικές πληροφορίες παρέχονται στα άτομα με πολύ συνοπτικό τρόπο, ενώ πρόσθετες πληροφορίες παρέχονται σε όσους χρειάζονται περαιτέρω διευκρινίσεις μέσω συνδέσμου προς μια πιο λεπτομερή περιγραφή της επεξεργασίας σε άλλη ιστοσελίδα.

Αναφέρθηκε νωρίτερα ότι ο σκοπός της επεξεργασίας δεδομένων είναι ιδιαίτερα σημαντικός, διότι προσδιορίζει εάν οι βασικές αρχές της ελαχιστοποίησης των δεδομένων (data minimisation), της ακρίβειας (accuracy) και του περιορισμού της αποθήκευσης (storage limitation) γίνονται σεβαστές. Η πρώτη από αυτές τις αρχές αναφέρεται στην ανάγκη ώστε τα προσωπικά δεδομένα να είναι σχετικά, επαρκή και να περιορίζονται στους σκοπούς για τους οποίους πραγματοποιείται η επεξεργασία. Αφορά περισσότερο στην ελαχιστοποίηση της συλλογής δεδομένων σε ένα κατάλληλο επίπεδο σύμφωνα με τον σκοπό της επεξεργασίας και λιγότερο στην ελαχιστοποίηση της επεξεργασίας αυτών. Οι επιχειρήσεις θα πρέπει να αναρωτηθούν αν τα δεδομένα που συλλέγονται είναι απαραίτητα για την επιτυχία των σκοπών της επεξεργασίας. Τεχνικά και οργανωτικά μέτρα θα πρέπει να διασφαλίζουν την τήρηση αυτής της αρχής και τα προσωπικά δεδομένα τα οποία δεν έπρεπε να είχαν συλλεχθεί ή καθίστανται άσχετα με τους σκοπούς της επεξεργασίας, θα πρέπει να διαγραφούν το συντομότερο δυνατόν.

Σύμφωνα με το άρθρο 5 του Κανονισμού, παράγραφος 1, τα προσωπικά δεδομένα πρέπει να είναι ακριβή και, όπου κρίνεται απαραίτητο, ενημερωμένα. Πρέπει να λαμβάνεται κάθε απαραίτητο μέτρο για την εξασφάλιση ότι δεδομένα τα οποία είναι ανακριβή, σύμφωνα με τους σκοπούς της επεξεργασίας, διαγράφονται ή διορθώνονται χωρίς καθυστέρηση. Δεδομένου ότι τα δεδομένα επιτρέπουν την παρουσίαση μιας κατάστασης ή των χαρακτηριστικών ενός ατόμου, πρέπει να είναι ακριβή ώστε να επιτρέπουν αυτή την παρουσίαση καθώς η χρήση τους ενδέχεται να έχει νομικές συνέπειες. Σε κάθε στιγμή, τα δεδομένα αυτά θα πρέπει να αντανακλούν την πραγματικότητα.

Τέλος, αναφορικά με την τρίτη από τις αναφερόμενες αρχές, τον περιορισμό αποθήκευσης (storage limitation), τα προσωπικά δεδομένα πρέπει να διατηρούνται σε μορφή που επιτρέπει τον προσδιορισμό των ατόμων στα οποία αναφέρονται τα δεδομένα όχι περισσότερο από ό, τι είναι απαραίτητο για τους σκοπούς της επεξεργασίας. Αυτός ο χρονικός περιορισμός αποθήκευσης πρέπει να επιτυγχάνεται με τον καθορισμό προθεσμιών επεξεργασίας των δεδομένων από τον Υπεύθυνο

διαχείρισης. Η υποχρέωση του υπεύθυνου της επεξεργασίας να διαγράψει τα προσωπικά δεδομένα τεκμηριώνεται από την διάταξη του άρθρου 17 του GDPR.

3.2 Νομική βάση για την επεξεργασία προσωπικών δεδομένων

Οι δραστηριότητες επεξεργασίας δεδομένων μπορούν να είναι νόμιμες μόνο εάν καλύπτονται από την συγκατάθεση που αφορούν του ατόμου που αφορούν τα δεδομένα ή με νόμιμη άδεια. Οποιαδήποτε επεξεργασία προσωπικών δεδομένων, ανεξάρτητα από το αν γίνεται εντός της Ευρωπαϊκής Ένωσης ή εκτός της Ευρωπαϊκής Ένωσης, απαγορεύεται, εκτός εάν καλύπτεται με συγκεκριμένη νομική βάση. Επιπλέον, επεξεργασία προσωπικών δεδομένων η οποία αναφέρεται σε παιδιά ή/και άλλες ευαίσθητες κοινωνικά ομάδες, αντιμετωπίζεται με ακόμα περισσότερους περιορισμούς για να διασφαλίσει την ιδιωτικότητα.

3.2.1 Επεξεργασία δεδομένων με βάση την συγκατάθεση του ατόμου

Ο Κανονισμός ορίζει αυστηρές απαιτήσεις για τη λήψη έγκυρης συγκατάθεσης από τα άτομα που αφορούν τα δεδομένα, ειδικά εάν πραγματοποιηθεί κάποια σύγκριση με το παλαιότερο Data Protection Directive το οποίο είχε θεσπιστεί το 1995. Σύμφωνα με το άρθρο 4 παράγραφο 11 του GDPR, συγκατάθεση σημαίνει οποιαδήποτε ελεύθερη, συγκεκριμένη, ενημερωμένη και αδιαμφισβήτητη ένδειξη των επιθυμιών του ατόμου που αφορούν τα δεδομένα σύμφωνα με την οποία, ή με άλλη σαφή καταφατική ενέργεια, δηλώνει συμφωνία για την επεξεργασία των προσωπικών του δεδομένων. Όταν η επεξεργασία βασίζεται σε αυτή την συγκατάθεση, ο Υπεύθυνος διαχείρισης πρέπει να είναι σε θέση να αποδείξει ότι το άτομο στο οποίο αναφέρονται τα δεδομένα έχει συναινέσει στην επεξεργασία. Φέρει επομένως την ευθύνη να αποδείξει το αντίθετο, για παράδειγμα, εάν ένα άτομο ισχυρίζεται ότι δεν έχει δώσει ή δεν υπάρχει έγκυρη συναίνεση για την επεξεργασία των προσωπικών του δεδομένων. Το βάρος του να αποδειχθεί η συγκατάθεση μπορεί να είναι ιδιαίτερα σημαντικό όταν αυτή αποκτήθηκε στο διαδίκτυο, καθώς ο Κανονισμός δεν ορίζει τις τυπικές απαιτήσεις για την απόκτηση του. Δεδομένης της πρακτικότητας, πολλές επιχειρήσεις θα μπορούσαν να επιλέξουν τη λήψη συγκατάθεσης με ηλεκτρονικά μέσα στο μέλλον. Ωστόσο, αν η συγκατάθεση δίνεται στο πλαίσιο γραπτής δήλωσης που αφορά και άλλα θέματα, η αίτηση συγκατάθεσης πρέπει να παρουσιάζεται κατά τρόπο που είναι σαφώς διακριτή από τα άλλα θέματα, με κατανοητή μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα. Είναι σκόπιμο επίσης η αίτηση συγκατάθεσης να επισημαίνεται με γραφικά μέσα στην γραπτή δήλωση και να χρησιμοποιεί ρητά τη λέξη «συγκατάθεση».

Οι προαναφερόμενες διασφαλίσεις πρέπει να διασφαλίζουν ότι το άτομο το οποίο αφορούν τα δεδομένα γνωρίζει το γεγονός και το βαθμό στον οποίο δίνεται

τη συγκατάθεση του και επιτρέπουν τη διασφάλιση της απαραίτητης σαφήνειας. Στην πράξη απαιτείται σαφής καταφατική πράξη του ατόμου, που θα μπορούσε να είναι:

- Τικάροντας ένα μη τικαρισμένο κουτί σε μια ιστοσελίδα στο διαδίκτυο.

- Επιλογή τεχνικών ρυθμίσεων για τις υπηρεσίες της Πληροφορικής (όπως π.χ. ρυθμίσεις ενός προγράμματος περιήγησης στο Internet που επιτρέπει την χρήση cookies).
- Οποιαδήποτε άλλη δήλωση ή συμπεριφορά που υποδηλώνει σαφώς την αποδοχή της προτεινόμενης επεξεργασίας.

Κατά την αξιολόγηση της εθελοντικής συγκατάθεσης των ατόμων, πρέπει να λαμβάνεται υπόψη κατά πόσον, η εκτέλεση μιας σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, εξαρτάται από αυτή την συγκατάθεση για την εκτέλεση της εν λόγω σύμβασης. Έτσι, ο κανονισμός απαγορεύει να εξαρτάται η δράση μιας σύμβασης από τη συγκατάθεσή ατόμων για επεξεργασία των προσωπικών τους δεδομένων, παρόλο που η συναίνεση αυτή δεν είναι απαραίτητη για να πραγματοποιηθεί η δράση. Η έκταση αυτής της απαγόρευσης παραμένει ασαφής. Ενδεχομένως, αυτό θα μπορούσε να απαγορεύσει την πρακτική αυτή μόνο από παρόχους που κατέχουν μονοπωλιακή θέση στην αγορά. Ωστόσο, η διατύπωση του άρθρου 7 δεν προβλέπει μια τέτοια αυστηρή ερμηνεία. Παρόλα αυτά η συγκεκριμένη απαγόρευση θα επηρεάσει σε μεγάλο βαθμό τις online υπηρεσίες που προσφέρονται και βασίζονται στην παροχή προσωπικών δεδομένων από την πλευρά του χρήστη. Φαίνεται ότι ο νομοθέτης θέλει να προστατεύσει τα άτομα από την εκμετάλλευση των προσωπικών τους δεδομένων, καθώς τα τελευταία χρόνια, τα δεδομένα αυτά έχουν καταστεί πολύτιμο περιουσιακό στοιχείο γι' αυτές. Οι εταιρίες θα πρέπει να περιορίσουν τη συλλογή των «περιττών» δεδομένων στο μέλλον καθώς η παραβίαση θα αντιμετωπίζεται με ιδιαίτερα αυστηρά πρόστιμα. Οι εταιρίες μπορεί να έρθουν αντιμέτωπες με την υποχρέωση να προσφέρουν τις υπηρεσίες τους στους χρήστες, χωρίς οι τελευταίοι να μοιράζονται τα προσωπικά δεδομένα τους.

Επιπρόσθετα, το GDPR προβλέπει ρητά το δικαίωμα των ατόμων που αφορούν τα δεδομένα να αποσύρουν τη συγκατάθεσή τους σε σχέση με την επεξεργασία των προσωπικών τους δεδομένων ανά πάσα στιγμή. Η απόσυρση δεν θίγει τη νομιμότητα της επεξεργασίας με βάση τη συναίνεση πριν από την απόσυρσή της. Έτσι, η απόσυρση της συγκατάθεσης έχει αποτελέσματα τα οποία επηρεάζουν μόνο το μέλλον της επεξεργασίας των δεδομένων. Ο Υπεύθυνων διαχείρισης πρέπει να ενημερώσει τα άτομα που αφορούν τα δεδομένα σχετικά με το δικαίωμά τους να αποσυρθούν προτού να δώσουν την συγκατάθεση τους.

Καθώς τα παιδιά χρειάζονται ιδιαίτερη προστασία, η συγκατάθεσή τους πρέπει να πληρεί αυστηρότερες προϋποθέσεις για να θεωρηθεί νόμιμη. Ειδική προστασία πρέπει, ιδίως, να ισχύει σε περιπτώσεις που αφορούν το marketing, την δημιουργία προφίλ χρηστών και τη συλλογή των προσωπικών δεδομένων κατά τη χρήση

υπηρεσιών που προσφέρονται απευθείας σε παιδιά. Ανεξάρτητα από την προσωπική ανάπτυξη του παιδιού, το άρθρο 8 ορίζει ως ελάχιστη ηλικία τα 16 έτη για να λαμβάνεται η απαραίτητη συναίνεση απευθείας από τον ανήλικο. Για τα παιδιά ηλικίας κάτω των 16 ετών, η επεξεργασία των προσωπικών δεδομένων είναι νόμιμη μόνον εάν η συγκατάθεση χορηγείται ή επιτρέπεται από τον κάτοχο γονικής μέριμνας. Ωστόσο, η νομοθεσία των κρατών μελών της Ευρωπαϊκής Ένωσης μπορεί να επιτρέψει μικρότερη ηλικία για τους σκοπούς αυτούς, υπό την προϋπόθεση ότι δεν είναι κατώτερη από τα 13 χρόνια. Ως εκ τούτου, οι όροι για τη συγκατάθεση των παιδιών μεταξύ των ηλικίας 13 και 16 ετών μπορεί να παραμείνουν σε μεγάλο βαθμό ασυνεπείς σε ολόκληρη την Κοινότητα.

3.2.2 Επεξεργασία δεδομένων με βάση Νόμιμη Άδεια ή Σύμβαση

Εάν η δραστηριότητα επεξεργασίας δεδομένων δεν βασίζεται στην συγκατάθεση των ατόμων σύμφωνα με το άρθρο 6 του Κανονισμού, η νομιμότητα μπορεί να προκύψει από άλλη νομική βάση σύμφωνα με το ίδιο άρθρο. Μέχρι την εφαρμογή του Κανονισμού, στην πράξη, οι επιχειρήσεις βάσιζαν σε διάφορες νομικές βάσεις την επεξεργασία των προσωπικών δεδομένων. Για παράδειγμα, όταν μια επιχείρηση επεξεργαζόταν προσωπικά δεδομένα με βάση την αναγκαιότητα για την εκτέλεση μιας σύμβασης/εργασίας, η εν λόγω επιχείρηση θα αποκτούσε συχνά επίσης τη συγκατάθεση των ατόμων. Αυτή η προληπτική προσέγγιση αποσκοπούσε στην εξασφάλιση της νομιμότητας της επεξεργασίας σε περίπτωση που μία ή περισσότερες από τις χρησιμοποιούμενες νομικές βάσεις έχαναν τη νομιμότητά τους. Αυτή η προσέγγιση μπορεί να συνεχισθεί στο πλαίσιο του GDPR, ωστόσο, οι επιχειρήσεις είναι υποχρεωμένες να επιλέξουν μια κύρια νομική βάση μεταξύ των διαθέσιμων επιλογών. Επομένως, θα πρέπει - πριν από την οποιαδήποτε επεξεργασία δεδομένων - να αξιολογήσουν ποια νομική βάση μπορεί να είναι η πλέον κατάλληλη για τις δραστηριότητες τους. Σύμφωνα με την αρχή της Λογοδοσίας, οι επιχειρήσεις πρέπει να είναι σε θέση να αποδείξουν ότι οι νομικές βάσεις τους δικαιολογούνται, να αποδείξουν τα συμφέροντά τους, καθώς και τη νομιμότητα των τελευταίων.
Η επεξεργασία είναι νόμιμη, μόνο εάν και στον βαθμό που ισχύει τουλάχιστον ένα από τα παρακάτω:

1. Το άτομο που αφορούν τα δεδομένων έχει δώσει τη συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων για έναν ή περισσότερους συγκεκριμένους σκοπούς.
2. Η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης στην οποία το άτομο το οποίο αφορούν τα δεδομένα είναι συμβαλλόμενο μέρος ή προκειμένου να πραγματοποιηθούν δράσεις έπειτα από εντολή του ατόμου αυτού με σκοπό τη σύναψη μιας σύμβασης.
3. Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με μια νομική υποχρέωση του Υπεύθυνου διαχείρισης.

4. Η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του ατόμου που αφορούν τα δεδομένα ή άλλο φυσικό πρόσωπο.
5. Η επεξεργασία είναι απαραίτητη για την εκτέλεση μιας εργασίας που εκτελείται στο πλαίσιο του δημοσίου συμφέροντος ή κατά την άσκηση δημόσιας εξουσίας που έχει παραχωρηθεί στον Υπεύθυνο διαχείρισης.
6. Η επεξεργασία είναι απαραίτητη για τους σκοπούς των νόμιμων συμφερόντων του Υπεύθυνου διαχείρισης ή τρίτου ατόμου, εκτός εάν υπερισχύουν τα συμφέροντα ή τα θεμελιώδη δικαιώματα και οι ελευθερίες των ατόμων που απαιτούν ειδικότερα την προστασία των προσωπικών δεδομένων, ειδικά στις περιπτώσεις όπου αφορούν τα δεδομένα ενός παιδιού.

3.3 Επεξεργασία ιδιαίτερα ευαίσθητων προσωπικών δεδομένων

Τα προσωπικά δεδομένα, τα οποία, λόγω της φύσης τους, είναι ιδιαίτερα ευαίσθητα καθώς αφορούν τα θεμελιώδη δικαιώματα και τις ελευθερίες των ατόμων, χρήζουν ειδικής προστασίας. Σύμφωνα με τον Κανονισμό, η επεξεργασία αυτών των ειδών δεδομένων γενικότερα απαγορεύεται, όμως, υπάρχουν ορισμένες εξαιρέσεις από την απαγόρευση αυτή. Ειδικές κατηγορίες προσωπικών δεδομένων είναι προσωπικά δεδομένα που αποκαλύπτουν φυλετική ή εθνική καταγωγή, πολιτικές πεποιθήσεις, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστικές οργανώσεις, δεδομένα σχετικά με την υγεία, δεδομένα σχετικά με τη σεξουαλική ζωή του ατόμου ή τις σεξουαλικές προτιμήσεις, καθώς και τα γενετικά/βιομετρικά δεδομένα για σκοπούς της μοναδικής αναγνώρισης ενός ατόμου (Άρθρο 9 Παράγραφος 1). Τα γενετικά και τα βιομετρικά δεδομένα δεν αναφέρονταν ρητά ως ευαίσθητες κατηγορίες προσωπικών δεδομένων στο πλαίσιο του Data Protection Directive, αλλά έχουν πλέον περιληφθεί επίσημα στον Κανονισμό. Αυτές οι κατηγορίες δεδομένων προσωπικού χαρακτήρα χρήζουν ειδικής προστασίας, δεδομένου ότι επιτρέπουν συμπεράσματα σχετικά με ένα άτομο που συνδέονται, με τα θεμελιώδη δικαιώματά του και τις ελευθερίες του και η επεξεργασία τους ενδέχεται να συνεπάγεται υψηλό κίνδυνο για τα άτομα.

- Τα δεδομένα που αποκαλύπτουν τη φυλετική ή εθνική καταγωγή είναι εξαιρετικά ευαίσθητα, καθώς μπορεί να οδηγήσουν σε διακρίσεις κατά του ατόμου. Αυτά τα δεδομένα περιλαμβάνουν το όνομα και το επώνυμο του ατόμου, το επώνυμό του, τον τόπο γέννησής του, τη μητρική του γλώσσα ή τα ονόματα των γονέων του, τα οποία, όταν συνδυαστούν, μπορούν να οδηγήσουν σε συμπεράσματα ως προς την καταγωγή του.
- Τα δεδομένα που αποκαλύπτουν πολιτικές απόψεις περιλαμβάνουν, μεταξύ άλλων, πληροφορίες σχετικά με την ένταξη του ατόμου σε ένα πολιτικό κόμμα, την συμμετοχή του σε διαδήλωση, πολιτική επανένωση ή παρόμοια εκδήλωση. Αυτή η κατηγορία περιλαμβάνει δεδομένα σχετικά με την

υποστήριξη μιας συγκεκριμένης πολιτικής ιδέας, καθώς και την απόρριψή της.

- Τα δεδομένα που αποκαλύπτουν θρησκευτικές ή φιλοσοφικές πεποιθήσεις σχετίζονται με πληροφορίες που επιτρέπουν συμπεράσματα σχετικά με τους δεσμούς των ατόμων με θρησκευτικούς οργανισμούς ή την έλλειψη αυτών, ενώ η διάταξη γενικά αποσκοπεί στην προστασία των θρησκευτικών πεποιθήσεων, καθώς και των θρησκευτικών πράξεων.
- Τα δεδομένα που αποκαλύπτουν την ιδιότητα συμμετοχής σε κάποιο συνδικαλιστικό όργανο αξίζουν ιδιαίτερη προστασία για να διασφαλίσει την ελευθερία του ατόμου για συλλογική διαπραγμάτευση και δράση στο πλαίσιο του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Στόχος είναι η πρόληψη πάνω απ' όλα της διάκρισης των ατόμων στην αγορά εργασίας βάσει των συνδικαλιστικών δραστηριοτήτων τους.
- Τα δεδομένα σχετικά με την υγεία καλύπτουν προσωπικά δεδομένα που σχετίζονται με τη σωματική ή την πνευματική υγεία ενός ατόμου, συμπεριλαμβανομένης της παροχής υπηρεσιών υγειονομικής περίθαλψης, η οποία αποκαλύπτει πληροφορίες σχετικά με την κατάσταση υγείας του ατόμου.
- Τα δεδομένα σχετικά με τη σεξουαλική ζωή ενός ατόμου ή τον σεξουαλικό προσανατολισμό θεωρούνται ιδιαίτερα ευαίσθητα. Αυτό περιλαμβάνει και τα προσωπικά δεδομένα σχετικά με την ακριβή ταυτότητα των συντρόφων του ατόμου.
- Τα γενετικά δεδομένα είναι προσωπικά δεδομένα σχετικά με τα κληρονομούμενα ή αποκτώμενα γενετικά χαρακτηριστικά ενός ατόμου που παρέχουν μοναδικές πληροφορίες σχετικά με τη φυσιολογία ή την υγεία του συγκεκριμένου ατόμου και τα οποία προκύπτουν, ιδίως, από μια ανάλυση ενός βιολογικού δείγματος από το συγκεκριμένο άτομο.
- Τα βιομετρικά δεδομένα συνεπάγονται προσωπικά δεδομένα που προκύπτουν από ειδική τεχνική επεξεργασία που σχετίζονται με τα φυσικά, ψυχολογικά ή χαρακτηριστικά συμπεριφοράς ενός ατόμου, τα οποία επιτρέπουν ή επιβεβαιώνουν τη μοναδική αναγνώριση αυτού του ατόμου, όπως εικόνες προσώπου ή δακτυλικά αποτυπώματα. Το Άρθρο 9 του Κανονισμού παρουσιάζει αρκετές εξαιρέσεις από την απαγόρευση επεξεργασίας των ειδικών κατηγοριών προσωπικών δεδομένων:

Συγκατάθεση του προσώπου στο οποίο αναφέρονται τα δεδομένα: το άτομο αυτό μπορεί να συναινέσει ρητά στην επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων για έναν ή περισσότερους προκαθορισμένους σκοπούς. Τέτοια πράξη επιβεβαίωσης, όχι μόνο πρέπει να πληρεί τις γενικές προϋποθέσεις για έγκυρη συγκατάθεση βάσει των άρθρων 7 και 8, αλλά πρέπει επίσης να αναφέρεται ρητά στις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που αφορά η συγκατάθεση αλλά και την προβλεπόμενη επεξεργασία. Αξίζει να σημειωθεί, ότι το κρατικό δίκαιο Κρατών μελών μπορεί να προβλέπει ότι η

απαγόρευση επεξεργασίας ειδικών κατηγοριών προσωπικών δεδομένων δεν μπορεί να αρθεί με τη συναίνεση του ατόμου που αφορούν τα δεδομένα.

- Απασχόληση και κοινωνική ασφάλιση: η επεξεργασία είναι απαραίτητη για τη εκπλήρωση των υποχρεώσεων και την άσκηση των συγκεκριμένων δικαιωμάτων του Υπεύθυνου διαχείρισης ή του ατόμου που αφορούν τα δεδομένα, στον τομέα της απασχόλησης, και της κοινωνικής ασφάλισης. Η επεξεργασία σε αυτή την περίπτωση πρέπει να τελείται στο βαθμό που έχει εγκριθεί από το δίκαιο των κρατών μελών της Ευρωπαϊκής Ένωσης, ή από μια συλλογική σύμβαση σύμφωνα με την Νομοθεσία της Ευρωπαϊκής Ένωσης που προβλέπει κατάλληλες διασφαλίσεις για τα θεμελιώδη δικαιώματα και συμφέροντα των ατόμων. Η διάταξη αυτή λαμβάνει υπόψη ότι, πάνω απ' όλα, οι εργοδότες πρέπει τακτικά να επεξεργάζονται ειδικές κατηγορίες προσωπικών δεδομένων, όπως τα δεδομένα υγείας, στο πλαίσιο της εργασιακής σχέσης.
- Προστασία ζωτικών συμφερόντων: η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφέροντα του ατόμου στο οποίο αναφέρονται τα δεδομένα ή άλλου ατόμου στο οποίο ανήκουν τα δεδομένα, στην περίπτωση που το άτομο που αφορούν τα δεδομένα είναι φυσικά ή νομικά ανίκανο να δώσει την συγκατάθεση του. Τα ζωτικά συμφέροντα είναι όλες οι υπαρξιακές ανάγκες και συμφέροντα, ιδίως η προστασία της ζωής και της σωματικής ακεραιότητας.
- Μη κερδοσκοπικοί οργανισμοί και φορείς: η επεξεργασία πραγματοποιείται στο πλαίσιο των νόμιμων δραστηριοτήτων με κατάλληλες διασφαλίσεις από έναν μη κερδοσκοπική οργανισμό με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό σκοπό και με την επεξεργασία να αφορά αποκλειστικά τα (πρώην) μέλη του ή σε πρόσωπα τα οποία έχουν τακτική επαφή με αυτό. Για να εμπίπτει στην εξαίρεση αυτή, ο στόχος της οντότητας είναι ο μόνος αποφασιστικός παράγοντας, ενώ η νομική μορφή ή η δομή της είναι άσχετη. Δεδομένων των στόχων αυτών των οργανώσεων, η λειτουργικότητά τους εξαρτάται συνήθως από τέτοια νόμιμη άδεια για επεξεργασία ευαίσθητων προσωπικών δεδομένων. Σημειώνεται ότι τα δεδομένα δεν μπορούν να αποκαλυφθούν εκτός του οργανισμού χωρίς τη συγκατάθεση των (πρώην) μελών που αφορούν τα δεδομένα.
- Ηθελημένα δημοσιευμένα δεδομένα: η επεξεργασία αφορά προσωπικά δεδομένα που είναι ηθελημένα δημοσιευμένα από το άτομο το οποίο αφορούν τα δεδομένα. Η δημοσίευση πρέπει να προκύπτει από ελεύθερη απόφαση του ατόμου και μπορεί να αφορά δεδομένα από δημόσια μητρώα, ιστότοπους, λίστες, φόρουμ ή ακόμη και από ένα προφίλ σε ένα κοινωνικό δίκτυο που είναι προσβάσιμο χωρίς λογαριασμό χρήστη.
- Η ύπαρξη κατάλληλων νομικών αιτημάτων: η επεξεργασία είναι απαραίτητη για την άσκηση ή την υπεράσπιση νομικών αιτημάτων ή όταν τα δικαστήρια ενεργούν εντός της δικαστικής τους δικαιοδοσίας. Το GDPR

απαιτεί μια ιδιαίτερα εμπεριστατωμένη εξισορρόπηση των συμφερόντων σύμφωνα με αυτή τη νόμιμη εξαίρεση.

- Λόγοι δημόσιου συμφέροντος: η επεξεργασία είναι απαραίτητη για λόγους σημαντικού δημόσιου συμφέροντος και πραγματοποιείται με βάση την νομοθεσία του κράτους μέλους της Ευρωπαϊκής Ένωσης ή της ίδιας της Ένωσης. Η νομοθεσία αυτή πρέπει να προβλέπει και να διασφαλίζει την προστασία των δεδομένων. Δεδομένου ότι η προστασία του δημοσίου συμφέροντος είναι απαραίτητη, οι λόγοι που την καθιστούν απαραίτητη θα πρέπει να ικανοποιούν αυστηρές απαιτήσεις ως προς τη σημασία τους. Θα έπρεπε να αφορούν θεμελιώδη δικαιώματα, καθώς και την προστασία της ζωής, της υγείας και της ελευθερίας των ατόμων.
- Υγειονομική περίθαλψη: η επεξεργασία είναι απαραίτητη για ατομικούς σκοπούς υγειονομικής περίθαλψης (την αξιολόγηση της εργασιακής ικανότητας των εργαζομένων, την ιατρική διάγνωση, την παροχή υγειονομικής φροντίδας ή περίθαλψης, την διαχείριση του συστήματος υγειονομικής περίθαλψης και των υπηρεσιών αυτού) με βάση την νομοθεσία των κρατών μελών της Ευρωπαϊκής Ένωσης ή της ίδιας της Ένωσης ή σύμφωνα με μια σύμβαση με έναν επαγγελματία υγείας. Σε περίπτωση επεξεργασίας η οποία διενεργείται με βάση αυτή τη σύμβαση, πρέπει να πραγματοποιείται από ή υπό την ευθύνη ενός επαγγελματία που υπόκειται στην υποχρέωση τήρησης του επαγγελματικού απορρήτου σύμφωνα με το δίκαιο της Ευρωπαϊκής Ένωσης ή των κρατών μελών.
- Ζητήματα δημόσιας υγείας: η επεξεργασία είναι απαραίτητη για λόγους δημόσιου ενδιαφέροντος στον τομέα της δημόσιας υγείας και πραγματοποιείται βάσει νομοθεσίας κράτους μέλους της Ευρωπαϊκής Ένωσης ή της ίδιας της Ένωσης. Βιώσιμοι λόγοι θα μπορούσαν να είναι η προστασία από σοβαρές διασυνοριακές απειλές στην υγεία ή στην εξασφάλιση του υψηλού επιπέδου και της ασφάλειας της υγειονομικής περίθαλψης, των ιατρικών προϊόντων και υπηρεσιών.
- Ερευνητικοί σκοποί: η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης δημοσίου συμφέροντος, για επιστημονικούς, ιστορικούς ή στατιστικούς σκοπούς και λαμβάνει χώρα βάσει του δικαίου των κρατών μελών της Ευρωπαϊκής Ένωσης ή της ίδιας της Ένωσης. Αυτές οι δραστηριότητες είναι υπέρ του δημοσίου συμφέροντος και, επομένως, θα υπάρξει γενικό όφελος από την εξαίρεση αυτή. Παρ 'όλα αυτά, η επεξεργασία που πραγματοποιείται βάσει της παρούσας διάταξης πρέπει να υπόκειται στις κατάλληλες εγγυήσεις που εγγυώνται την ύπαρξη τεχνικών και οργανωτικών μέτρων για την εξασφάλιση, ιδίως, της αρχής της ελαχιστοποίησης των δεδομένων. Αυτές οι διασφαλίσεις πρέπει να αντιστοιχούν στον ευαίσθητο χαρακτήρα των προσωπικών δεδομένων. Επεξεργασία προσωπικών δεδομένων σχετικά με ποινικές καταδίκες και αδικήματα πραγματοποιείται μόνο σε μία από τις ακόλουθες περιπτώσεις:

3.4 Μεταφορά δεδομένων σε τρίτες χώρες

3.4.1 Νομικές απαιτήσεις για μεταφορά δεδομένων σε τρίτες χώρες

Για τους πολυεθνικούς οργανισμούς και τις εταιρείες, οι διασυνοριακές μεταφορές δεδομένων είναι απαραίτητες στο πλαίσιο των επιχειρηματικών δραστηριοτήτων τους. Αυτό συχνά συνεπάγεται μεταφορά σε τρίτες χώρες, με το τελευταίο να σημαίνει οποιαδήποτε χώρα που δεν είναι μέλος της ΕΕ. Η εξασφάλιση επαρκούς επιπέδου προστασίας σε αυτές τις περιπτώσεις επεξεργασίας είναι ένα από τα πιο σύνθετα ζητήματα του νόμου περί προστασίας δεδομένων.

Οι διασυνοριακές διαβιβάσεις δεδομένων υπόκεινται σε πολυάριθμες διασφαλίσεις στο πλαίσιο του Κανονισμού προκειμένου να εξασφαλιστεί υψηλό επίπεδο ασφάλειας. Οποιαδήποτε μεταβίβαση προσωπικών δεδομένων που υποβάλλονται σε επεξεργασία ή προορίζονται για επεξεργασία μετά τη μεταβίβαση σε τρίτη χώρα ή διεθνή οργανισμό, πρέπει να συμμορφώνεται με την προϋποθέσεις που καθορίζονται στο άρθρο 44 του GDPR. Αυτό περιλαμβάνει συμμόρφωση με περαιτέρω προϋποθέσεις μεταφορών προσωπικών δεδομένων από την τρίτη χώρα / διεθνή οργανισμό σε άλλη εταιρία/οργανισμό. Οι νομικές απαιτήσεις για διασυνοριακές μεταφορές δεδομένων βάσει του κανονισμού είναι παρόμοιες με εκείνες τις υπάρχουσας νομοθεσίας, αλλά οι νομικές διατάξεις του GDPR χαρακτηρίζονται από μεγαλύτερο επίπεδο λεπτομέρειας. Η υπάρχουσα προσέγγιση σε δύο στάδια για τη δικαιολόγηση της μεταφοράς δεδομένων σε τρίτες χώρες σύμφωνα με την οδηγία για την προστασία των δεδομένων δεν έχει τροποποιηθεί στο πλαίσιο του GDPR:

1. Σε ένα πρώτο στάδιο, η μεταφορά πρέπει να ανταποκρίνεται στις απαιτήσεις για την επεξεργασία δεδομένων εντός της Ευρωπαϊκής Ένωσης και, συνεπώς, να βασίζεται στην συγκατάθεση του ατόμου που αφορούν τα δεδομένα ή άλλη νόμιμη άδεια.
2. Σε μια δεύτερη φάση, η μεταφορά πρέπει να συμμορφώνεται επιπλέον με τους όρους που του άρθρου 44 του GDPR, προκειμένου να διασφαλιστεί ένα κατάλληλο επίπεδο προστασίας των δεδομένων. Σε περίπτωση που δεν προβλέπονται τέτοιες διασφαλίσεις, η μεταφορά δεν μπορεί να γίνει ανεξάρτητα από το αν υπάρχει νομική βάση για τη μεταποίηση στο στάδιο 1.

Μόνο αν ληφθούν και τα δύο βήματα, τα δεδομένα μπορούν να μεταφερθούν σε παραλήπτες από τρίτες χώρες. Στην πράξη, τα προσωπικά δεδομένα μεταφέρονται συχνά από Υπεύθυνους διαχείρισης σε Υπεύθυνους επεξεργασίας που βρίσκονται εκτός Ευρωπαϊκής Ένωσης, για παράδειγμα, που βρίσκονται στις ΗΠΑ. Σε αυτές τις περιπτώσεις, οι νομικές απαιτήσεις που ορίζονται στο άρθρο 44 GDPR θα πρέπει να εκπληρωθούν.

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή σε διεθνή οργανισμό μπορεί να πραγματοποιηθεί όταν η Ευρωπαϊκή Επιτροπή έχει αποφασίσει ότι η τρίτη χώρα, ή ο εν λόγω οργανισμός εντός της τρίτης χώρας

εξασφαλίζει επαρκές επίπεδο προστασίας των δεδομένων. Σε αυτές τις περιπτώσεις μπορούν να πραγματοποιηθούν μεταφορές δεδομένων σε «ασφαλείς» τρίτες χώρες χωρίς την ανάγκη περαιτέρω εξουσιοδότησης από την εποπτική Αρχή. Η Ευρωπαϊκή Επιτροπή μέχρι στιγμής έχει αναγνωρίσει την Ανδόρα, την Αργεντινή, τον Καναδά, τις Νήσους Φερόες, το Γκέρνσεϋ, το Ισραήλ, τη Νήσο του Μαν, το Τζέρσεϋ, τη Νέα Ζηλανδία, την Ελβετία, τις Η.Π.Α. σε σχέση με την πιστοποίηση Privacy Shield και την Ουρουγουάη ως πάροχο επαρκούς επιπέδου προστασίας των δεδομένων.

Υπάρχει η περίπτωση, ακόμη και αν μια τρίτη χώρα δεν μπορεί να εξασφαλίσει ένα κατάλληλο επίπεδο προστασίας δεδομένων όσον αφορά τα πρότυπα του GDPR, οι επιχειρήσεις να εξακολουθούν να ενδιαφέρονται για τη μεταφορά δεδομένων στη χώρα αυτή. Προκειμένου να αντισταθμιστεί η έλλειψη προστασίας των δεδομένων, το συμβαλλόμενο μέρος που διαβιβάζει δεδομένα και το μέρος που τα λαμβάνει μπορούν να χρησιμοποιήσουν ένα είδος ρήτρας της Ευρωπαϊκής Κοινότητας που ονομάζεται Standard Contractual Clause και το οποίο χρησιμοποιείται επιτυχώς, έπειτα από την εισαγωγή του υπό το Data Protection Directive. Όταν τα συμβαλλόμενα μέρη χρησιμοποιούν το SCC, υφίσταται επάρκεια προστασίας των προσωπικών δεδομένων, αποκλειστικά για τον εισαγωγέα δεδομένων/ συμβαλλόμενο μέρος, ο οποίος βρίσκεται σε τρίτη χώρα, αλλά δεν χαρακτηρίζεται ολόκληρη η τρίτη χώρα ως ασφαλής χώρα για μεταφορές ευαίσθητων δεδομένων από την Ευρωπαϊκή Ένωση. Αυτό οφείλεται στο γεγονός ότι η SCC δεσμεύει με συμβόλαιο μόνο ένα συγκεκριμένο οργανισμό εκτός Ευρωπαϊκής Ένωσης, ώστε αυτός να διασφαλίζει το επίπεδο προστασίας δεδομένων, το οποίο πρέπει να βρίσκεται σε παρόμοιο επίπεδο με αυτό της προστασίας δεδομένων εντός της Ένωσης.

Σε σύγκριση με το Data Protection Directive, το GDPR εισάγει ορισμένες καινοτόμες διαδικασίες, σχετικά με την μεταφορά δεδομένων σε τρίτες χώρες:

- Μέχρι στιγμής, ορισμένα κράτη μέλη της Ευρωπαϊκής Ένωσης επέβαλαν εκτεταμένες νομικές απαιτήσεις σχετικά με τις διεθνείς μεταφορές δεδομένων: Εκτός από τη χρήση των SCC, σύμφωνα με την νομοθεσία κρατών μελών της Ευρωπαϊκής Ένωσης, οι επιχειρήσεις έπρεπε να υποβληθούν σε μια πρόσθετη διαδικασία αδειοδότησης, η οποία και πραγματοποιούνταν από τις αντίστοιχες Εποπτικές Αρχές. Δεδομένης της διατύπωσης του άρθρου 46 παράγραφος 2 του GDPR, αυτό δεν επιτρέπεται πλέον στο πλαίσιο του GDPR. Εάν μια μεταφορά δεδομένων πληρεί τους όρους του άρθρου 44 δεν πρέπει να υποβληθεί σε καμία άλλη διαδικασία χορήγησης άδειας. Στην πράξη, η χρήση των SCC συνεπάγεται πλεονεκτήματα, καθώς και μειονεκτήματα, που πρέπει να ληφθούν υπόψη πριν από την επιλογή αυτής της νομικής βάσης.

Τα πλεονεκτήματα περιλαμβάνουν:

- Η χρήση τους είναι ταχύτερη και απαιτεί μικρότερες διαδικασίες από τη διαπραγμάτευση μεμονωμένης σύμβασης ή από την υιοθέτηση δεσμευτικών εταιρικών κανόνων.
- Η χρήση SCC περιέχει κανόνες προστασίας δεδομένων που συμμορφώνονται με το νόμο και, καθώς πρέπει να χρησιμοποιηθεί αυτούσια και αμετάβλητη, το νόμιμο πρότυπο προστασίας δεδομένων δεν μπορεί να επηρεαστεί αρνητικά κατά τις διαπραγματεύσεις μεταξύ των συμβαλλομένων μερών.
- Μπορούν να χρησιμεύσουν ως συμβατική βάση για μεταφορές δεδομένων μεταξύ εξαγωγέων Υπεύθυνων διαχείρισης και εισαγωγέων Υπεύθυνων διαχείρισης/επεξεργασίας, ανεξάρτητα από την μεταξύ τους σχέση. Επομένως, δεν υπάρχει περιορισμός, για παράδειγμα, για επεξεργασία δεδομένων εντός της ίδιας ομάδας.
- Οι ρήτρες SCC μπορούν να χρησιμοποιηθούν σε περιπτώσεις όπου εμπλέκονται περισσότερα από δύο μέρη.

Μειονεκτήματα της χρήσης των SCC αποτελούν:

- Η έλλειψη εξατομίκευσης και ευελιξίας για τις συγκεκριμένες ανάγκες των διαφορετικών επιχειρήσεων, γεγονός που είναι εγγενές σε οποιαδήποτε μορφή μοντέλου συμβολαίων.

- Η χρήση τους για περιπτώσεις επεξεργασίας δεδομένων εντός ενός ομίλου ενδέχεται να απαιτεί αυξημένη διοικητική επιβάρυνση καθώς πρέπει να συμφωνηθούν ξεχωριστά μεταξύ όλων των ομάδων - μελών του ομίλου.

3.4.2 Εξαιρέσεις από τις νομικές απαιτήσεις

Το Άρθρο 49 του GDPR εισάγει εξαιρέσεις που επιτρέπουν μεταφορές δεδομένων σε τρίτες χώρες σε περιορισμένες περιπτώσεις, ακόμη και αν δεν εκπληρωθεί καμία από τις προαναφερόμενες νομικές απαιτήσεις. Το άρθρο στην ουσία ανταποκρίνεται στο Data Protection Directive, αλλά εισάγει ένα νέο τύπο εξαίρεσης. Η πρώτη περίπτωση εξαίρεσης αφορά στην ύπαρξη σύμβασης με το άτομο που αφορούν τα προσωπικά δεδομένα. Η συγκεκριμένη περίπτωση καλυπτόταν και από το προηγούμενο νομοθετικό πλαίσιο. Πρέπει να ερμηνεύεται με αυστηρό τρόπο, ορίζοντας της μεταφορά των δεδομένων αναγκαία μόνο εάν

υπάρχει στενή και ουσιαστική σχέση μεταξύ του ατόμου και των σκοπών της σύμβασης. Εάν οι σκοποί της σύμβασης μπορούν να εκπληρωθούν χωρίς την μεταφορά των δεδομένων σε τρίτες χώρες, η μεταφορά αυτή είναι περιττή και συνεπώς δεν κρίνεται νόμιμη σύμφωνα με το άρθρο. Αξίζει να σημειωθεί πως αυτή η εξαίρεση δεν μπορεί να χρησιμοποιηθεί προκειμένου να συγκεντρωθούν οι λειτουργίες πληρωμές και η διαχείριση του ανθρώπινου δυναμικού ενός ομίλου εταιριών σε μια συμφέρουσα, για τον όμιλο, τοποθεσία.

Μια δεύτερη εξαίρεση, που επιτρέπει τη μεταφορά δεδομένων σε τρίτες χώρες, είναι όταν αυτό κρίνεται απαραίτητο για σημαντικούς λόγους δημοσίου συμφέροντος. Σύμφωνα με το άρθρο 49, μόνο σημαντικές περιπτώσεις δημοσίου συμφέροντος, οι οποίες προσδιορίζονται ως τέτοιες από τα κράτη μέλη της Ευρωπαϊκής Ένωσης, οι οποίες έχουν δικαιοδοσία στον συγκεκριμένο Υπεύθυνο διαχείρισης ή την ίδια την Ένωση. Τέτοιες περιπτώσεις μπορούν να θεωρηθούν, για παράδειγμα, η διεθνής ανταλλαγή δεδομένων μεταξύ των αρχών ανταγωνισμού, φορολογικών ή τελωνειακών αρχών, μεταξύ των αρχών χρηματοπιστωτικής εποπτείας, μεταξύ υπηρεσιών αρμόδιων για θέματα κοινωνικής ασφάλισης ή για τη δημόσια υγεία.

Ένας καινούριος τύπος εξαίρεσης εισάγεται στην παράγραφο 1, υποπαράγραφο 2 του άρθρου 49 του Κανονισμού. Σύμφωνα με την εν λόγω διάταξη, μπορεί να γίνει μεταφορά δεδομένων σε τρίτες χώρες σε περιορισμένες περιπτώσεις που έχουν να κάνουν με τα νόμιμα συμφέροντα του Υπεύθυνου Διαχείρισης. Δεδομένης της σαφής διατύπωσης της διάταξης, δεν μπορεί να χρησιμεύσει ως νόμιμη βάση για τους Υπεύθυνους επεξεργασίας προκειμένου να μεταφέρουν προσωπικά δεδομένα σε υπο-επεξεργαστές εκτός Ευρωπαϊκής Ένωσης. Αυτή η γενική ρήτρα ισχύει μόνο εάν δεν μπορεί να χρησιμοποιηθεί άλλη νόμιμη άδεια για τη διεθνή μεταφορά των δεδομένων και μόνο στην περίπτωση που ο Υπεύθυνος Διαχείρισης συμμορφώνεται με συγκεκριμένους νομικούς όρους:

- Η μεταφορά δεν είναι επαναλαμβανόμενη.
- Η μεταφορά αφορά μόνο περιορισμένο αριθμό προσώπων στα οποία αναφέρονται τα δεδομένα .
- Η μεταφορά είναι απαραίτητη για την προστασία των έννομων συμφερόντων του Υπεύθυνου διαχείρισης.
- Αυτά τα έννομα συμφέροντα δεν βρίσκονται σε σύγκρουση με τα συμφέροντα ή τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα.
- Ο Υπεύθυνος Διαχείρισης / εξαγωγέας δεδομένων αξιολόγησε όλες τις περιστάσεις και παρείχε κατάλληλες διασφαλίσεις για τη μεταφορά βάσει αυτής της εκτίμησης.

Μια τέτοια αξιολόγηση θα πρέπει να δίνει ιδιαίτερη προσοχή στην φύση των προσωπικών δεδομένων, τον σκοπό και τη διάρκεια της προτεινόμενης επεξεργασίας, την κατάσταση στην χώρα καταγωγής, την τρίτη χώρα και τη χώρα του τελικού προορισμού. Η ερμηνεία των απαιτήσεων αυτής της εξαίρεσης παραμένει ασαφής καθώς η διατύπωση είναι πολύ αόριστη. Οι έννοιες του «μη

επαναλαμβανόμενου» ή του «περιορισμένου αριθμού» δεν διευκρινίζονται περαιτέρω. Για παράδειγμα, μια μεταφορά μπορεί να θεωρηθεί «επαναλαμβανόμενη» εάν χρειαστεί να πραγματοποιηθεί περισσότερες από μία φορές ή εάν πραγματοποιείται τακτικά. Οι μεταφορές στο πλαίσιο αυτής της εξαίρεσης πραγματοποιούνται μόνο όταν δεν ισχύουν άλλοι λόγοι μεταφοράς και συνεπάγονται πρόσθετες υποχρεώσεις του Υπεύθυνου διαχείρισης:

- Να ενημερώσει την Εποπτική αρχή για τη μεταφορά αυτή.
- Να Ενημερώσει το άτομο που αφορούν τα δεδομένα σχετικά με τη αναγκαιότητα υπεράσπισης των νόμιμων συμφερόντων του στην συγκεκριμένη περίπτωση και
- Να τεκμηριώνει την εκτίμηση του για την συγκεκριμένη περίπτωση, καθώς και τις κατάλληλα μέτρα ασφαλείας που λαμβάνονται στο πλαίσιο των Data Processing Records. Δεδομένων των πολυάριθμων προϋποθέσεων για νόμιμη διαβίβαση δεδομένων σύμφωνα με αυτό το άρθρο του GDPR, θα πρέπει σπάνια να χρησιμεύσει ως νομική βάση για τέτοιου είδους μεταφορές.

3.4.3 Μεταφορά δεδομένων προς τις Ηνωμένες Πολιτείες της Αμερικής

Σύμφωνα με την Οδηγία Προστασίας Προσωπικών Δεδομένων (Data Protection Directive) και την Ασπίδα Προστασίας Προσωπικών Δεδομένων μεταξύ Ευρωπαϊκής Ένωσης και ΗΠΑ (EU–U.S. Privacy Shield) οι επιχειρήσεις των ΗΠΑ μπορούν να πιστοποιούνται ως ασφαλείς παραλήπτες προσωπικών δεδομένων. Σύμφωνα με το άρθρο 45 παράγραφος 9 του GDPR, κατά πάσα πιθανότητα αυτό θα παραμείνει σε ισχύ και σταδιακά θα τροποποιηθεί ώστε μεσοπρόθεσμα να συμμορφωθεί με τις διατάξεις του Κανονισμού. Η πρακτική εφαρμογή αυτών είναι υποχρεωτικό να εξετάζεται σε ετήσια βάση.

Η Ασπίδα Προστασίας Προσωπικών Δεδομένων περιέχει επτά αρχές προστασίας της ιδιωτικής ζωής οι οποίες συνάδουν με τις απαιτήσεις του Ευρωπαϊκού Δικαστηρίου για επάρκεια. Η Ευρωπαϊκή Ένωση και οι ΗΠΑ προσπάθησαν να βελτιωθεί η προστασία των θεμελιωδών δικαιωμάτων και να υπάρξει αποτελεσματική νομική προστασία των ατόμων που αφορούν τα δεδομένα. Ως μέρος της αυτο-πιστοποίησης τους στο πλαίσιο της Ασπίδας Προστασίας Προσωπικών Δεδομένων, οι επιχειρήσεις πρέπει να δεσμευτούν να συμμορφωθούν με αυτές τις αρχές:

1. Αρχή της ενημέρωσης: Οι επιχειρήσεις είναι υποχρεωμένες να παρέχουν πληροφορίες για βασικά στοιχεία των δραστηριοτήτων τους που αφορούν την επεξεργασία δεδομένων (πχ τύπος δεδομένων που συλλέγονται, σκοπός επεξεργασίας, δικαίωμα πρόσβασης, προϋποθέσεις για μεταγενέστερες μεταφορές και ευθύνη).

2. Αρχή της ακεραιότητας των δεδομένων και του περιορισμού του σκοπού: τα επεξεργασμένα προσωπικά δεδομένα πρέπει να περιορίζονται σε ό, τι αφορά τον σκοπό της επεξεργασίας, να είναι αξιόπιστα για την προβλεπόμενη χρήση, ακριβή, πλήρη και πρόσφατα. Αυτό πρέπει να διασφαλίζεται για όσο διάστημα η επιχείρηση διατηρεί τα προσωπικά δεδομένα, ανεξάρτητα από το αν έχει λήξει η πιστοποίησή της επιχείρησης από την Ασπίδα Προστασίας Δεδομένων.
3. Αρχή της επιλογής: Οι επιχειρήσεις πρέπει να προσφέρουν στα πρόσωπα στα οποία αναφέρονται τα δεδομένα την δυνατότητα του να αρνηθούν την γνωστοποίηση σε τρίτους ή τη χρήση για διαφορετικό ή νέο σκοπό από εκείνο για το οποίο συλλέχθηκαν αρχικά. Όσον αφορά ειδικές κατηγορίες προσωπικών δεδομένων, αυτή η μεταφορά ή χρήση μπορεί να πραγματοποιηθεί μόνο κατόπιν ρητής ρητής συγκατάθεσης (opt-in) του ατόμου αυτού.
4. Αρχή της λογοδοσίας για περαιτέρω μεταφορά: σύμφωνα με την αρχή αυτή, οι επιχειρήσεις πρέπει να συνάπτουν συμβάσεις για τη διαβίβαση δεδομένων σε τρίτους παραλήπτες, υποχρεώνοντας αυτούς τους τρίτους παραλήπτες να εξασφαλίσουν ένα επίπεδο προστασίας δεδομένων επαρκές σε σχέση με αυτό που εγγυάται η Ασπίδα Προστασίας Προσωπικών Δεδομένων και να επεξεργαστούν τα λαμβανόμενα δεδομένα μόνο για περιορισμένους και συγκεκριμένους σκοπούς.
5. Αρχή ασφάλειας: οι πιστοποιημένοι φορείς πρέπει να λαμβάνουν εύλογα και κατάλληλα μέτρα για την προστασία των προσωπικών δεδομένων από απώλεια, κατάχρηση, μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη, τροποποίηση και καταστροφή, λαμβάνοντας δεόντως υπόψη τους σχετικούς κινδύνους στην επεξεργασία και τη φύση των προσωπικών δεδομένων.
6. Αρχή της πρόσβασης: τα άτομα στα οποία αναφέρονται τα δεδομένα πρέπει να έχουν πρόσβαση στα προσωπικά δεδομένα τους που κατέχει μια επιχείρηση/ ένας οργανισμός και να είναι σε θέση να τα διορθώσουν, να τα τροποποιήσουν ή να τα διαγράψουν εάν είναι ανακριβή ή έχουν υποβληθεί σε επεξεργασία κατά παράβαση των αρχών περί απορρήτου, με εξαίρεση τις περιπτώσεις όπου το κόστος παροχής πρόσβασης θα ήταν δυσανάλογο της παραβίασης.
7. Προσφυγή, εκτέλεση και ευθύνη: Τα άτομα πρέπει να έχουν εύκολη πρόσβαση σε διαθέσιμους ανεξάρτητους μηχανισμούς προσφυγής, οι οποίοι θα διερευνούν και θα επιλύουν τις καταγγελίες και τις ενστάσεις χωρίς καθυστέρηση και χωρίς κόστος για το άτομο.

ΚΕΦΑΛΑΙΟ 4 – ΟΡΓΑΝΩΤΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

Η εφαρμογή του GDPR συνεπάγεται εκτεταμένες ευθύνες και αυξημένες ποινές, προς την κατεύθυνση των εταιριών και των οργανισμών. Σε αυτό το κλίμα οι εταιρείες πρέπει να είναι ιδιαίτερα προσεκτικές κατά την προσαρμογή των μέτρων προστασίας δεδομένων για την τήρηση των αυξημένων προτύπων προστασίας. Πολλές επιχειρήσεις θα πρέπει να καταβάλουν σημαντικές προσπάθειες για την υλοποίηση ενός συστήματος Data Protection Management (Data Protection Management System - DPMS) που συμμορφώνεται με τον Κανονισμό. Ωστόσο, η εναρμόνιση με τον Κανονισμό σε ολόκληρη την Ευρωπαϊκής Ένωσης διευκολύνει παράλληλα την οργάνωση της προστασίας των δεδομένων για τις διεθνείς εταιρείες.

4.1 Λογοδοσία (Accountability)

Ενώ η Ευρωπαϊκή Οδηγία Προστασίας Δεδομένων (Data Protection Directive) δεν είχε δώσει κατά το παρελθόν έμφαση στην λογοδοσία, το GDPR εισαγάγει την αρχή της Λογοδοσίας, η οποία επιβάλλει την ευθύνη για τη συμμόρφωση με τον Κανονισμό αλλά και το βάρος της απόδειξης για την εν λόγω συμμόρφωση στον Υπεύθυνο διαχείρισης δεδομένων. Έτσι, η αρχή της λογοδοσίας αποτελείται από δύο στοιχεία:

1. Την ευθύνη του Υπεύθυνου διαχείρισης για τη διασφάλιση της συμμόρφωσης με το GDPR και
2. Την ικανότητα του Υπεύθυνου διαχείρισης να αποδείξει τη συμμόρφωσή του με τον Κανονισμό στις εποπτικές αρχές.

Τα πρόστιμα για μη συμμόρφωση με το συγκεκριμένο κομμάτι του Κανονισμού μπορεί να ανέλθουν στα 20 εκατομμύρια ευρώ ή μέχρι και στο 4% του συνολικού ετήσιου κύκλου εργασιών παγκοσμίως για έναν οργανισμό (Άρθρο 83, τομέας 5). Αυτό το γεγονός, δίνει ισχυρό κίνητρο στους Υπεύθυνους διαχείρισης ώστε να εφαρμόσουν τα απαραίτητα μέτρα για την προστασία των δεδομένων. Τα κατάλληλα μέτρα περιλαμβάνουν την υιοθέτηση εσωτερικών πολιτικών, την χρήση προγραμμάτων για την εφαρμογή των αρχών προστασίας των δεδομένων και άλλα μέτρα που πληρούν, κυρίως, τις αρχές του σχεδιασμού της προστασίας των δεδομένων. Παράλληλα, τα αρχεία του Υπεύθυνου διαχείρισης, που περιλαμβάνουν λεπτομέρειες σχετικά με τις ροές δεδομένων της οικονομικής οντότητας, είναι πιθανό να αποδεικνύονται πολύ χρήσιμα. Σε περίπτωση ελέγχου των Εποπτικών Αρχών, οι Υπεύθυνοι διαχείρισης / επεξεργασίας είναι υποχρεωμένοι να τα θέτουν στη διάθεση της αιτούσας εποπτικής αρχής, ώστε να

χρησιμεύσουν στην παρακολούθηση των διαδικασιών επεξεργασίας δεδομένων της οντότητας.

Ιδιαίτερα σημαντικό για τον Κανονισμό είναι το ζήτημα της Προστασίας των προσωπικών δεδομένων στην περίπτωση που επεξεργάζονται από μια πληθώρα οντοτήτων. Οι υπεύθυνοι διαχείρισης έχουν την δυνατότητα να καθορίσουν τους σκοπούς της επεξεργασίας δεδομένων και να είναι εξίσου υπεύθυνοι ή μπορούν να χωρίσουν την διαδικασία επεξεργασίας και να αναλάβουν την ευθύνη για τα αντίστοιχα βήματα της επεξεργασίας που τους αναλογούν. Σε κάθε περίπτωση, πρέπει να υπάρχει συμφωνία, αναφορικά με το ποιος υπεύθυνος διαχείρισης είναι υπεύθυνος για κάθε υποχρέωση ως προς τον Κανονισμό, πριν πραγματοποιηθεί η οποιαδήποτε επεξεργασία δεδομένων. Σύμφωνα με το τομέα 2 του Άρθρου 26, η ουσία της συμφωνίας αυτής θα πρέπει να είναι διαθέσιμη στα άτομα τα οποία αφορούν τα δεδομένα. Ο κανονισμός δεν ορίζει απαραίτητα την μορφή παρουσίασης αυτής της συμφωνίας (για παράδειγμα ένα κείμενο), αλλά στην περίπτωση που αφορά παιδιά, πρέπει να παρουσιαστεί με κατανοητό τρόπο για αυτά.

Σύμφωνα με το άρθρο 31 του GDPR, η συνεργασία των επιχειρήσεων πραγματοποιείται κατόπιν «αιτήματος» της Εποπτικής αρχής, κάτι που σημαίνει ότι οι Υπεύθυνοι διαχείρισης/ επεξεργασίας δεν χρειάζεται να απευθύνονται στις αρχές με δική τους πρωτοβουλία. Παρ 'όλα αυτά, μια τέτοια κίνηση θα μπορούσε να είναι χρήσιμη καθώς η εθελοντική επικοινωνία και συνεργασία ίσως αποτελέσει ευεργετικό παράγοντα σε περίπτωση που οι οργανισμοί είναι αντιμέτωποι με πρόστιμα ή άλλες αξιώσεις σύμφωνα με το GDPR.

4.2 Τεχνικά και οργανωτικά μέτρα για τις επιχειρήσεις

Τα τεχνικά και οργανωτικά μέτρα εγγυώνται την προστασία των προσωπικών δεδομένων. Το άρθρο 32 του GDPR υποχρεώνει τον Υπεύθυνο διαχείρισης και τον Υπεύθυνο επεξεργασίας να αναλάβουν τα απαραίτητα μέτρα, στοιχείο που αποτελεί μία από τις πιο θεμελιώδεις υποχρεώσεις του GDPR. Η τεχνολογία δύναται να επιβάλλει την ασφάλεια δεδομένων πριν από την επεξεργασία αυτών, όμως τα τεχνικά και τα οργανωτικά μέτρα που πρέπει να ληφθούν, είναι αυτά που θα διασφαλίσουν την διαδικασία της επεξεργασίας.

4.2.1 Απαραίτητο επίπεδο Προστασίας δεδομένων

Τα κατάλληλα μέτρα περιλαμβάνουν κάθε ενέργεια που σχετίζεται με τη συλλογή, επεξεργασία ή χρήση προσωπικών δεδομένων που παρέχει επαρκές επίπεδο προστασίας στο πλαίσιο του GDPR. Το άρθρο 32 του GDPR δεν περιορίζει το πεδίο των κατάλληλων μέτρων με αποτέλεσμα μια μεγάλη ποικιλία μέτρων να είναι διαθέσιμη. Παραδείγματα περιλαμβάνουν τα ακόλουθα:

- Ελαχιστοποίηση της επεξεργασίας προσωπικών δεδομένων.
- Χρήση ψευδωνύμων.
- Παροχή δυνατότητας παρακολούθησης της επεξεργασία δεδομένων στο άτομο
- Δημιουργία και βελτίωση των χαρακτηριστικών ασφαλείας, οποίο αφορούν τα δεδομένα.
- Μέτρα για την αποφυγή μη εξουσιοδοτημένης φυσικής πρόσβασης σε προσωπικά.
- Δεδομένα, όπως χώροι πρόσβασης με εξουσιοδότηση , φορείς ελέγχου, πρόσβαση μέσω κωδικού πρόσβασης ή μέσω ταυτοποίησης, κ.λπ. .
- Τακτική εκπαίδευση των εργαζομένων σχετικά με την ασφάλεια δεδομένων.
- Κωδικοποιημένη μεταφορά δεδομένων.
- Τακτικοί έλεγχοι του επιπέδου ασφάλειας των δεδομένων και άλλα.

Στο ελάχιστο τα μέτρα τα οποία θα πρέπει να εφαρμοστούν αφορούν την εμπιστευτικότητα (confidentiality) , την ακεραιότητα (integrity), τη διαθεσιμότητα (availability) και την ανθεκτικότητα (resilience) της επεξεργασίας δεδομένων, τα οποία αποτελούν την βάση της ασφάλειας δεδομένων.

4.2.2 Ασφάλεια δεδομένων με βάση τον ενδεχόμενο κίνδυνο

Το GDPR εισαγάγει μια προσέγγιση βασισμένη στους ενδεχόμενους κινδύνους, για να προσδιορίσει τα τεχνικά και οργανωτικά μέτρα τα οποία είναι κατάλληλα σε κάθε περίπτωση. Το απαιτούμενο επίπεδο της ασφάλειας των δεδομένων πρέπει να αναγνωρίζεται διαφορετικά σε κάθε περίπτωση, με μια αξιολόγηση των αντικειμενικών κινδύνων. Η αξιολόγηση θα πρέπει να επικεντρώνεται κατά κύριο λόγο σε πιθανούς κινδύνους για το άτομο, αλλά οι κίνδυνοι για τρίτα άτομα και τους Υπεύθυνους διαχείρισης ή τους Υπεύθυνους επεξεργασίας θα πρέπει επίσης να ληφθούν υπόψη.

Δεδομένου ότι η επεξεργασία προσωπικών δεδομένων θέτει σε κίνδυνο τα θεμελιώδη δικαιώματα των ατόμων, πρέπει να ληφθεί υπόψη το νόμιμο ενδιαφέρον τους για την ασφάλεια των δεδομένων. Συγκεκριμένα, πρέπει να λαμβάνονται υπόψη οι κίνδυνοι που προκύπτουν από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση ή μη εξουσιοδοτημένη πρόσβαση σε δεδομένα προσωπικού χαρακτήρα. Ως μεγαλύτεροι κίνδυνοι για το άτομο αναγνωρίζονται εκείνοι, οι οποίοι μπορεί να προκαλέσουν:

- Κλοπή ταυτότητας ή απάτη, οικονομική ζημία, βλάβη της φήμης ή οποιοδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα.
- Στέρηση ή περιορισμό από τα δικαιώματα και τις ελευθερίες ή εμπόδια στην άσκηση ελέγχου της επεξεργασίας των προσωπικών δεδομένων τους.
- Επικίνδυνα αποτελέσματα λόγω χρήσης ειδικών κατηγοριών προσωπικών δεδομένων (βλέπε άρθρο 9 παράγραφος 1 του GDPR).
- Την επεξεργασία προσωπικών δεδομένων παιδιών ή άλλων ευαίσθητα κοινωνικά ομάδων.
- Την επεξεργασία μεγάλου όγκου προσωπικών δεδομένων ή προσωπικών δεδομένων πολλών ατόμων.
- Επιπρόσθετα, οι επικείμενοι κίνδυνοι για τους Υπεύθυνους διαχείρισης/ επεξεργασίας προσωπικών δεδομένων πρέπει να ληφθούν σοβαρά υπ’ όψιν. Οι παράγοντες για την ανάπτυξη κατάλληλων μέτρων είναι το κόστος εφαρμογής και η φύση, το πεδίο εφαρμογής, το πλαίσιο και οι σκοποί της επεξεργασίας προσωπικών δεδομένων. Οι κίνδυνοι για τους Υπεύθυνους διαχείρισης/ επεξεργασίας συχνά ταυτίζονται με τους κινδύνους των ατόμων τα οποία αφορούν τα δεδομένα. Μερικοί από τους κινδύνους που ενδιαφέρουν κυρίως τις επιχειρήσεις και τους Υπεύθυνους διαχείρισης/ επεξεργασίας προσωπικών δεδομένων είναι:
- Νομικοί κίνδυνοι που προκύπτουν από τη μη συμμόρφωση με τις υποχρεώσεις προστασίας δεδομένων όπως τις ορίζει ο Κανονισμός (π.χ. πρόστιμα, ποινές).
- Χρηματοοικονομικοί κίνδυνοι (π.χ. απαιτήσεις για αποζημιώσεις, δαπάνες για τη βελτίωση της DPMS).

- Επιχειρηματικοί κίνδυνοι (π.χ. κίνδυνοι για τη φήμη των επιχειρήσεων, αποτυχία επίτευξης επιχειρηματικών στόχων, μεγάλος φόρτος εργασίας για τη διοίκηση).

4.2.3 Ευρωπαϊκή Οδηγία NIS

Σημαντικό ρόλο στα τεχνικά μέτρα του GDPR έχει η Ευρωπαϊκή Οδηγία δικτυακών και πληροφοριακών συστημάτων (NIS - Network and Information System Directive), η οποία εγκρίθηκε τον Ιούλιο του 2016 και προσπάθησε να θέσει κοινά πρότυπα ασφάλειας στον κυβερνοχώρο για όλες τις χώρες της κοινότητας. Ένα υψηλό επίπεδο ασφάλειας των δεδομένων και ένα υψηλό επίπεδο ασφάλειας σε ένα σύστημα πληροφορικής είναι αλληλοεξαρτώμενα: το πιο περίπλοκο σύστημα προστασίας δεδομένων δεν μπορεί να προστατεύσει τα προσωπικά δεδομένα εάν το σύστημα πληροφορικής που τα επεξεργάζεται μπορεί εύκολα να παραβιαστεί.

Καθώς πρόκειται για Ευρωπαϊκή Οδηγία, τα κράτη μέλη δεν την εφάρμοσαν άμεσα, αλλά την μετέφεραν στα εθνικό δίκαιο τους, διαδικασία που ολοκληρώθηκε στις 9 Μαΐου 2018. Επιπρόσθετα, η Ευρωπαϊκή Οδηγία NIS έχει περιορισμένο πεδίο εφαρμογής σε σχέση με το GDPR και υποχρεώνει τους παρόχους ψηφιακών υπηρεσιών να εφαρμόσουν, με βάση τα διαθέσιμα πρότυπα τεχνολογίας, κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων που τίθενται για την ασφάλεια των πληροφοριακών συστημάτων και των δικτύων τους. Η Οδηγία εξασφαλίζει υψηλό επίπεδο ασφάλειας δικτύων και συστημάτων, καθώς και μέγιστη διαθεσιμότητα υπηρεσιών για τους χρήστες ψηφιακών υπηρεσιών. Επιπλέον, οι πάροχοι ψηφιακών υπηρεσιών πρέπει να κοινοποιούν περιστατικά με σημαντική επίπτωση στην σταθερότητα των υπηρεσιών στις αρμόδιες (εθνικές) αρχές. Τέλος, τα κράτη μέλη της Ευρωπαϊκής Ένωσης εφαρμόζουν κανόνες σχετικά με τις κυρώσεις που επιβάλλονται στις παραβιάσεις των υποχρεώσεων ασφάλειας βάσει της Οδηγίας, ώστε αυτές οι κυρώσεις να έχουν χαρακτήρα αποτελεσματικό, αναλογικό και αποτρεπτικό.

4.2.4 Αρχείο δραστηριοτήτων επεξεργασίας δεδομένων

Οι απαιτήσεις ως προς το περιεχόμενο των απαραίτητων εγγραφών διαφέρουν ελαφρώς μεταξύ των Υπεύθυνων διαχείρισης και Υπεύθυνων επεξεργασίας προσωπικών δεδομένων. Συγκεκριμένα, οι Υπεύθυνοι διαχείρισης υποχρεούνται να διατηρούν πιο εκτεταμένα αρχεία των δραστηριοτήτων επεξεργασίας δεδομένων , δεδομένου ότι το μεγαλύτερο μέρος της προστασίας των δεδομένων επιβαρύνει του ίδιους. Τα αρχεία διατηρούνται γραπτώς, συμπεριλαμβανομένης της ηλεκτρονικής μορφής και αυξάνουν τη διαφάνεια των δραστηριοτήτων επεξεργασίας δεδομένων. Η επιμελής διατήρηση τους συνίσταται καθώς:

- Πρέπει να τίθενται στη διάθεση των εποπτικών αρχών, κατόπιν αιτήματος, για να επιτρέπουν την παρακολούθηση της επεξεργασίας προσωπικών δεδομένων.

- Επιτρέπουν την απόδειξη της συμμόρφωσης με το GDPR.

- Συμβάλλουν στην πληροφόρηση των ατόμων που αφορούν τα δεδομένα κατά την άσκηση των δικαιωμάτων τους βάσει του GDPR (παράγραφος 5.3) και

- Μη τήρηση τους επιφέρει πρόστιμα σύμφωνα με το άρθρο 83, παράγραφος 4

Δεδομένου ότι τα αρχεία που τηρεί ο Υπεύθυνος διαχείρισης περιέχουν τους σκοπούς της επεξεργασίας δεδομένων, πρέπει να εξεταστεί πόσο λεπτομερώς θα περιγράφουν/τεκμηριωθούν αυτοί. Από τη μία πλευρά, τα αρχεία πρέπει να επιτρέπουν μια συνοπτική αξιολόγηση της νομιμότητας της επεξεργασίας κατά τρόπο που επιτρέπει την αξιολόγηση αυτής. Από την άλλη, ο σκοπός δεν πρέπει να είναι υπερβολικά συγκεκριμένος, καθώς θα περιορίσει το φάσμα της νόμιμης επεξεργασίας δεδομένων. Καθώς το επίπεδο λεπτομέρειας αναφορικά με τα αρχεία δραστηριοτήτων επεξεργασίας δεδομένων παραμένει ασαφές, θα απαιτηθεί περαιτέρω διευκρίνιση από τα δικαστήρια και τις Εποπτικές Αρχές στο μέλλον. Δεδομένου ότι η διατήρηση των αρχείων θα είναι χρονοβόρα και (ενδεχομένως) δαπανηρή, δεν είναι υποχρεωμένες όλες οι οντότητες να το πράξουν. Το GDPR παρέχει μια απαλλαγή για κάθε επιχείρηση ή οργανισμό που απασχολεί λιγότερα από 250 άτομα, με την λογική ότι κατά πάσα πιθανότητα, δεν διαθέτουν επαρκείς οικονομικούς και ανθρώπινους πόρους για την εκπλήρωση της υποχρέωσης. Στην περίπτωση, όμως, που οι επιχειρήσεις έχουν ετήσιο κύκλο εργασιών άνω των 50 εκατ. ευρώ ή συνολικό ετήσιο ισολογισμό που υπερβαίνει τα 43 εκατομμύρια ευρώ δεν επωφελούνται από αυτή την απαλλαγή. Ακόμα, όμως και σε αυτή την περίπτωση οι επιχειρήσεις που απασχολούν λιγότερα από 250 άτομα είναι υποχρεωμένες να διατηρούν αρχεία επεξεργασίας προσωπικών δεδομένων στις περιπτώσεις που:

1. Η επεξεργασία των δεδομένων είναι πιθανό να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων.

2. Η επεξεργασία συμβαίνει περιστασιακά, για μικρό χρονικό διάστημα ή για μια μόνο φορά και αποτελεί μικρό κομμάτι των υποχρεώσεων των Υπεύθυνων διαχείρισης και επεξεργασίας.

3. Η επεξεργασία αφορά ειδικές κατηγορίες προσωπικών δεδομένων (άρθρο 9 παρ. 1 του GDPR) ή προσωπικά δεδομένα σχετικά με ποινικές καταδίκες και αδικήματα.

4.2.5 Data Protection Impact Assessment

Καθώς η επεξεργασία προσωπικών δεδομένων, ιδίως με τη χρήση νέων τεχνολογιών, επιφέρει κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων, ο Υπεύθυνος διαχείρισης οφείλει να πραγματοποιήσει μια εκτίμηση των επιπτώσεων αυτής της επεξεργασίας στην προστασία των δεδομένων. Αυτό επιτυγχάνεται με το Data Protection Impact Assessment, το οποίο εξασφαλίζει την προστασία των προσωπικών δεδομένων και την απόδειξη της συμμόρφωσης με το GDPR, όντας ένα προληπτικό μέσο προστασίας δεδομένων. Η συγκεκριμένη αξιολόγηση πραγματοποιείται σε δυο στάδια:

1. Ο Υπεύθυνος διαχείρισης διεξάγει μια εσωτερική αξιολόγηση και
2. Εάν εντοπιστεί υψηλός κίνδυνος, η Εποπτική αρχή θα ήταν θεμιτό να συμμετάσχει στην διαδικασία

Η αξιολόγηση Data Protection Impact Assessment οφείλει να καλύπτει όλες τις διαδικασίες επεξεργασίας δεδομένων, από την προετοιμασία τους μέχρι και τις συνέπειες τους. Σύμφωνα με το άρθρο 35, παράγραφος 7 στο ελάχιστο το Data Protection Impact Assessment πρέπει να περιλαμβάνει:

- Συστηματική περιγραφή των στόχων και προβλεπόμενων εργασιών επεξεργασίας και, κατά περίπτωση, το έννομο συμφέρον που επιδιώκει ο υπεύθυνος διαχείρισης.
- Εκτίμηση της αναγκαιότητας της επεξεργασίας σε σχέση με τον αντίστοιχο στόχο.
- Αξιολόγηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των ατόμων που αφορούν τα δεδομένα.
- Τα μέτρα που προβλέπονται για την αντιμετώπιση των κινδύνων.

Κατά την αξιολόγηση των μέτρων που έχουν υλοποιηθεί σε μια επιχείρηση ή έναν οργανισμό, ο Υπεύθυνος διαχείρισης θα πρέπει να αναφέρει μέτρα ασφαλείας και μηχανισμούς ασφαλείας για την προστασία των προσωπικών δεδομένων αλλά και για να αποδείξει τη συμμόρφωση με τον κανονισμό GDPR. Με τον τρόπο αυτό, ο ελεγκτής πρέπει να λάβει υπόψη τα δικαιώματα και τα έννομα συμφέροντα των ατόμων που αφορούν τα δεδομένα και άλλων ενδιαφερομένων. Ο Κανονισμός δεν περιέχει άλλα κριτήρια για το εύρος της αξιολόγησης, αφήνοντας με αυτό τον τρόπο ασαφείς τις νομικές απαιτήσεις σε σχέση με αυτή την διαδικασία.

Εάν κριθεί απαραίτητο από τον Υπεύθυνο διαχείρισης, αυτός μπορεί να ζητήσει τη συμβολή ενός Αξιωματικού Προστασίας Δεδομένων (Data Protection Officer), οποίος θα δράσει σε συμβουλευτικό ρόλο. Η ευθύνη της αξιολόγησης παραμένει με

τον Υπεύθυνο διαχείρισης, οποίος όμως μπορεί να λάβει πολύτιμες συμβουλές στα παρακάτω θέματα:

- Εάν θα πρέπει να πραγματοποιηθεί αξιολόγηση Data Protection Impact ή όχι.
- Ποια μεθοδολογία πρέπει να ακολουθείται κατά την εκτέλεση της αξιολόγησης.
- Ποια τεχνικά και οργανωτικά μέτρα πρέπει να ληφθούν για να αποφευχθούν πιθανοί κίνδυνοι για τα δικαιώματα των ατόμων τα όποια αφορούν τα δεδομένα.
- Εάν η αξιολόγηση έχει πραγματοποιηθεί με τον σωστό τρόπο και κατά πόσο τα συμπεράσματά της συμμορφώνονται με το GDPR.

Εξαιρέσεις από την υποχρέωση να πραγματοποιηθεί η αξιολόγηση Data Protection Impact Assessment προβλέπει το άρθρο 35, παράγραφος 10 του κανονισμού, σε περίπτωση που ισχύουν τρεις προϋποθέσεις:

1. Ο Υπεύθυνος διαχείρισης υπόκειται σε νομοθεσία Κράτους μέλους ή στη νομοθεσία της Ένωσης που καθιστά την επεξεργασία προσωπικών δεδομένων απαραίτητη για τη συμμόρφωση με μια νομική υποχρέωση ή για την εκπλήρωση μιας εργασίας που εκτελείται προς το δημόσιο συμφέρον ή στην άσκηση δημόσιας εξουσίας που έχει ανατεθεί σε αυτόν.
2. Η εν λόγω νομοθεσία καθορίζει τις συγκεκριμένες διαδικασίας επεξεργασίας δεδομένων και
3. Έχει ήδη πραγματοποιηθεί μια γενική αξιολόγηση Data Protection Impact Assessment για τον οργανισμό στα πλαίσια της έγκρισης της νομικής βάσης της επεξεργασίας δεδομένων.

4.2.6 Data Protection Officer

Μέχρι την παρουσίαση του όρου Data Protection Officer (DPO στην συνέχεια) στο GDPR, τα Κράτη μέλη ως επί το πλείστον δεν είχαν γνώση για την υποχρέωση διορισμού του συγκεκριμένου ρόλου. Ωστόσο, υποχρεωτικό διορισμό του DPO έχει προβλέψει ο γερμανικός νόμος για την προστασία δεδομένων για περισσότερα από 30 χρόνια, ο οποίος και έχει στεφθεί με επιτυχία. Σύμφωνα με τον Κανονισμό, ο DPO θα διαδραματίσει βασικό ρόλο στην επίτευξη της συμμόρφωσης με το GDPR.

Το άρθρο 37 αναλύει την διαδικασία διορισμού του DPO, η οποία μπορεί να είναι υποχρέωση του Υπεύθυνου διαχείρισης ή του Υπευθύνου επεξεργασίας. Ταυτόχρονα στην παράγραφο 4 αναφέρεται πως τα κράτη μέλη έχουν την δυνατότητα να εισαγάγουν νομοθεσία η οποία επιτρέπει στις επιχειρήσεις να ορίσουν νόμιμους εκπροσώπους τους, οι οποίοι και είναι υπεύθυνοι για τον καθορισμό του DPO. Σε κάθε περίπτωση, μόλις ολοκληρωθεί ο καθορισμός του

DPO, ο Υπεύθυνου διαχείρισης οφείλει να κοινοποιήσει τα στοιχεία αυτού στην Εποπτική Αρχή. Δεδομένου ότι ο DPO λειτουργεί ως ο βασικός τρόπος επικοινωνίας με τα άτομα τα οποία αφορούν τα προσωπικά δεδομένα, θα ήταν θεμιτό τα στοιχεία του να είναι μονίμως διαθέσιμα πχ π.χ. μέσω της ιστοσελίδας της εταιρείας / οργανισμού. Επιπρόσθετα, μια ομάδα επιχειρήσεων ή και διαφορετικές ομάδες εντός του ίδιου οργανισμού, έχουν το δικαίωμα να ορίσουν κοινό DPO, αρκεί να υφίσταται αυστηρά καθορισμένη πρόσβαση σε αυτόν για όλα τα συμβαλλόμενα μέρη. Γνώμονα προς αυτή την κατεύθυνση, αποτέλεσε η θέληση των νομοθετών να διευκολύνουν ως ένα βαθμό την επεξεργασία προσωπικών δεδομένων εντός μιας ομάδας, με τον ορισμό ενός κοινού DPO για όλους, χωρίς να πραγματοποιηθούν διακριτοί ορισμοί για κάθε στέλεχος.

Στην παράγραφο 5 του άρθρου 37 αναφέρεται πως ένας DPO θα πρέπει ορίζεται με βάση:

- Την επαγγελματική ποιότητα.
- Την εξειδικευμένη γνώση στην Νομοθεσία και στις πρακτικές προστασίας προσωπικών δεδομένων.
- Την ικανότητα εκπλήρωσης των υποχρεώσεων που απορρέουν από το νόμο.

Καθώς τα προσόντα του DPO συνδέονται με την ικανότητα εκπλήρωσης των υποχρεώσεων που απορρέουν από το νόμο, ο υποψήφιος κρίνεται σε σχέση με τις διαδικασίες επεξεργασίες προσωπικών δεδομένων μιας εταιρίας. Το αναγκαίο επίπεδο εξειδικευμένων γνώσεων καθορίζεται με βάση τις διαδικασίας επεξεργασίας δεδομένων που υλοποιεί η επιχείρηση και την απαιτούμενη προστασία αυτών. Σύμφωνα με την Γερμανική νομοθεσία, η οποία είναι ιδιαίτερα πιθανό να αποτελέσει πρότυπο για πολλές χώρες στο μέλλον, η αλληλεπίδραση των νομικών, οργανωτικών και τεχνικών γνώσεων καθορίζουν την επαγγελματική ποιότητα του υποψηφίου. Αξίζει ακόμα να σημειωθεί πως ο Κανονισμός δεν καθορίζει εάν ένα νομικό πρόσωπο μπορεί να οριστεί ως DPO στην περίπτωση της Γερμανίας, το συγκεκριμένο γεγονός απασχόλησε ιδιαίτερα την νομολογία της χώρας.

Οι Υπεύθυνοι διαχείρισης και Επεξεργασίας έχουν την επιλογή να ορίσουν εσωτερικούς ή εξωτερικούς DPO και να ορίσουν το εάν η θέση αυτών είναι μόνιμη ή προσωρινή. Παράγοντες που μπορεί να επηρεάσουν αυτές τις αποφάσεις είναι το μέγεθος και ο προϋπολογισμός μιας εταιρίας. Ειδικά για την μονιμότητα των DPO η αρχική πρόταση του GDPR προέβλεπε μια ελάχιστη περίοδο διορισμού τουλάχιστον 2 ετών, προκειμένου να διασφαλιστεί η ανεξαρτησία του ρόλου και να καθιερωθεί η συνεχής παρακολούθηση της επεξεργασίας δεδομένων, αλλά τελικά αποφασίστηκε το στοιχείο αυτό να μην περιλαμβάνεται στο νομικό κείμενο του Κανονισμού.

Εσωτερικός DPO

- Καλύτερη αντίληψη της επιχειρηματικής δραστηριότητας της εταιρίας και των διεργασιών επεξεργασίας δεδομένων (σημαντικό σε εταιρίες με πολύπλοκες δομές)
- Η προϋπάρχουσα εμπειρογνωμοσύνη και ο επαγγελματισμός.
- Η αντίληψη αυτή απλοποιεί την διενέργεια του Data Protection Impact Assessment, σύμφωνα με τις ανάγκες του οργανισμού.
- Έχει συνήθως επαρκή ασφαλιστική κάλυψη, η οποία καλύπτει τις συνέπειες των παραβάσεων των υποχρεώσεών του
- Όσο μεγαλύτερος είναι ο οργανισμός, τόσο περισσότερος χρόνος απαιτείται για τον έλεγχο των διαδικασιών επεξεργασίας δεδομένων
- Δεν υπάρχει σύμβαση εργασίας, επομένως ο οργανισμός δεν έχει συμβατικές υποχρεώσεις ενός εργοδότη προς τον εξωτερικό DPO.
- Μπορεί εύκολα να χρησιμοποιηθεί ως εσωτερικό σημείο επαφής για κάθε επιχειρηματική μονάδα του ομίλου.

Προτεινόμενο για:
-Μεγάλες επιχειρήσεις.
-Μικρές και Μεσαίου μεγέθους επιχειρήσεις.
-Όμιλο εταιριών.
-Οργανισμούς που πραγματοποιούν επεξεργασία δεδομένων υψηλού κίνδυνο.

Σε κάθε περίπτωση, για να μπορέσει ο DPO να διατελέσει επιτυχώς το έργο του, θα πρέπει ο Υπεύθυνος διαχείρισης ή ο Υπεύθυνος επεξεργασίας:

- Να διασφαλίσουν ότι ο DPO λαμβάνει τις κατάλληλες δράσεις, έγκαιρα και σύμφωνα με τον Κανονισμό, σε όλα τα θέματα αναφορικά με την προστασία προσωπικών δεδομένων
- Να παρέχουν τους απαραίτητους πόρους ώστε ο DPO να εκτελεί τα καθήκοντά του, πρόσβαση στα προσωπικά δεδομένα και στις διαδικασίες επεξεργασίας αυτών και χορήγηση κατάλληλου χώρου εργασίας, υποστήριξης πληροφορικής, οικονομικούς πόρους, εξειδικευμένη βιβλιογραφία, προσωπικό υποστήριξης και επαρκή χρόνο για να εκπληρώσει τα καθήκοντά του.

Εξωτερικός DPO

Ο Data Protection Officer λειτουργεί ως σημείο επαφής για τα άτομα τα οποία αφορούν τα προσωπικά δεδομένα, για οποιαδήποτε πληροφορία σε σχέση με την επεξεργασία αυτών. Αυτό υποχρεώνει τον DPO να διατηρεί μια ουδέτερη θέση με τον Υπεύθυνο διαχείρισης και τον Υπεύθυνο Επεξεργασίας, καθώς συμβουλεύει και τους οργανισμούς που επεξεργάζονται τα δεδομένα αλλά και τα άτομα που αφορούν τα δεδομένα. Γι’ αυτό το λόγο ο DPO προστατεύεται από τον Κανονισμό, ο

οποίος ορίζει ότι δεν μπορεί να δεχθεί ποινές ή να απολυθεί αναφορικά με τα καθήκοντα του από τον Υπεύθυνο διαχείρισης ή τον Υπεύθυνος επεξεργασίας, εκτός των περιπτώσεων όπου υφίσταται παραβίαση του συμβολαίου ή οικονομικοί λόγοι. Ταυτόχρονα, ο DPO αποτελεί το σημείο επαφής των Εποπτικών αρχών και τα καθήκοντα του δεσμεύονται από το απόρρητο ή την εμπιστευτικότητα σύμφωνα με το δίκαιο των κρατών μελών της Ευρωπαϊκής Ένωσης, σύμφωνα με το άρθρο 38 παράγραφος 5 του GDPR. Έτσι, το GDPR δεν θεσπίζει τους δικούς του κανόνες περί εμπιστευτικότητας, αλλά βασίζεται στην υπάρχουσα νομοθεσία και, κατά συνέπεια, το καθήκον εμπιστευτικότητας μπορεί να περιορίζεται από το δίκαιο των κρατών μελών της Ευρωπαϊκής Ένωσης.

Όπως είναι αντιληπτό, ο ρόλος του DPO είναι ιδιαίτερα πολύπλοκος, αλλά στο ελάχιστο θα πρέπει να περιλαμβάνει:

- Ενημερωτικό και συμβουλευτικό ρόλο προς τους Υπεύθυνους διαχείρισης, τους Υπεύθυνους Επεξεργασίας και τους υπαλλήλους αυτών σχετικά με τις υποχρεώσεις προστασίας των προσωπικών δεδομένων τα οποία επεξεργάζονται
- Παρακολούθηση της συμμόρφωσης με τη νομοθεσία περί προστασίας προσωπικών δεδομένων, συμπεριλαμβανομένης της διεξαγωγής των σχετικών ελέγχων
- Τον επιμερισμό εργασιών, την ευαισθητοποίηση και την κατάρτιση του προσωπικού το οποίο έχει αναλάβει την επεξεργασία δεδομένων.
- Παροχή συμβουλών, εφόσον ζητηθεί, σχετικά με την επίπτωση διεργασιών επεξεργασίας δεδομένων στην προστασία αυτών
- Αξιολόγηση και παρακολούθηση της απόδοσής του
- Συνεργασία με την εποπτική αρχή (δεν περιλαμβάνεται η υποχρέωση να κοινοποιεί παραβιάσεις δεδομένων και
- Ενεργώντας ως σημείο επαφής της Εποπτικής αρχής

Τέλος, το GDPR δεν προβλέπει κανόνες σχετικά με κυρώσεις κατά του DPO, κυρίως λόγω του συμβουλευτικού του ρόλου, καθιστώντας ασαφές εάν αυτός μπορεί να υπόκειται σε ποινικές, διοικητικές ή εταιρικές συνέπειες για τις πράξεις του. Ωστόσο, η νομοθεσία της Ευρωπαϊκής Ένωσης μπορεί να προβλέπει τέτοια ευθύνη. Βάσει της νομοθεσίας των κρατών μελών της Ένωσης, τα άτομα τα οποία αφορά η επεξεργασία δεδομένων ή οι Υπεύθυνοι διαχείρισης/Επεξεργασίας μπορούν να απαιτήσουν αποζημίωση που προκύπτει από παραβίαση των υποχρεώσεων του DPO. Παρ' όλα αυτά, τα κράτη μέλη της Ευρωπαϊκής Ένωσης ενδέχεται να περιορίσουν την έκταση των εν λόγω απαιτήσεων με νέους κανονισμούς του εργατικού δικαίου τους.

4.2.7 Παραβιάσεις ασφαλείας δεδομένων

Το GDPR προβλέπει για πρώτη φορά, για τις περισσότερες Ευρωπαϊκές χώρες, την υποχρέωση του Υπεύθυνου διαχείρισης να αναφέρει την οποιαδήποτε περίπτωση παραβίασης προσωπικών δεδομένων. Αυτή η υποχρέωση προστατεύει τα δικαιώματα και τις ελευθερίες των ατόμων τα οποία αφορούν τα δεδομένα μέσω ενός συστήματος με μεγαλύτερο βαθμό διαφάνειας. Μοναδική προϋπόθεση για την υποχρέωση αναφοράς είναι η ύπαρξη της παραβίασης των προσωπικών δεδομένων, χωρίς όμως αυτό να σημαίνει πως οποιαδήποτε παραβίαση συνεπάγεται την αναγκαιότητα αναφοράς. Σύμφωνα με το άρθρο 4 παράγραφος 12 του GDPR, μια «παραβίαση προσωπικών δεδομένων» αποτελεί παραβίαση της ασφάλειας οδηγώντας σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη πρόσβαση σε προσωπικά δεδομένα που έχουν μεταδοθεί, αποθηκευτεί ή επεξεργαστεί με οποιοδήποτε τρόπο. Η παραβίαση προσωπικών δεδομένων μπορεί να συμβεί με τεχνικό ή φυσικό τρόπο. Ο ορισμός δεν απαιτεί πρόθεση ή αμέλεια και συνεπώς, ισχύει ανεξάρτητα από το πώς και γιατί συνέβη και περιλαμβάνει ακόμη και τυχαίες παραβιάσεις.

Σε περίπτωση παραβίασης προσωπικών δεδομένων, ο Υπεύθυνος διαχείρισης ενημερώνει χωρίς καθυστέρηση την αρμόδια Εποπτική Αρχή και, ει δυνατόν, το αργότερο εντός 72 ωρών από τη στιγμή που θα λάβει γνώση της παραβίασης των δεδομένων. Αντίθετα, ο Υπεύθυνος επεξεργασίας δεν έχει υποχρέωση να ενημερώσει τις εποπτικές αρχές αλλά μόνο τον Υπεύθυνο διαχείρισης, σύμφωνα με το συμβόλαιο μεταξύ τους, το οποίο πρέπει να αναφέρει ότι ο πρώτος υποστηρίζει τον δεύτερο στις υποχρεώσεις του σε περιπτώσεις παραβίασης. Η οργανωτική δομή της επιχείρησης δεν έχει σημασία για τον προσδιορισμό της έναρξη της περιόδου ενημέρωσης. Η ενημέρωση του Υπεύθυνου διαχείρισης είναι μείζονος σημασίας: μόλις μπορέσει να προβεί σε επαρκή κοινοποίηση σύμφωνα με το άρθρο 33 του Κανονισμού, η περίοδος ενημέρωσης αρχίζει. Έτσι, πιθανότατα δεν θα είναι σε θέση να προβεί σε ολοκληρωμένη νομική ανάλυση της παραβίασης των δεδομένων πριν από την ενημέρωση των αρμόδιων Αρχών. Κατά συνέπεια, πολλές επιχειρήσεις θα μπορούσαν δυνητικά να κοινοποιήσουν παραβιάσεις δεδομένων πριν να μπορέσουν να αξιολογήσουν συνολικά την κατάσταση.

Στο άρθρο 33, παράγραφος 3 του GDPR καθορίζονται οι ελάχιστες απαιτήσεις για το περιεχόμενο μιας ειδοποίησης για παραβίαση προσωπικών δεδομένων:

- Η φύση της παραβίασης των προσωπικών δεδομένων (εάν είναι εφικτό, ο αριθμός και οι κατηγορίες σχετικών εγγραφών δεδομένων, οι οποίες επηρεάστηκαν).
- Το όνομα και τα στοιχεία επικοινωνίας του DPO(Data Protection Officer).
- Τις πιθανές συνέπειες της παραβίασης των προσωπικών δεδομένων και
- Τα μέτρα (που προτείνονται) για την αντιμετώπιση της παραβίασης των δεδομένων.

Εξαίρεση από την υποχρέωση της αναφοράς στις Εποπτικές Αρχές, υφίσταται μόνο στην περίπτωση που η παραβίαση των προσωπικών δεδομένων είναι απίθανο να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων που αφορούν τα δεδομένα. Στην περίπτωση που ο Υπεύθυνος διαχείρισης διαπιστώσει, σύμφωνα με την εκτίμηση του για μια συγκεκριμένη παραβίαση, μόνο ένα μικρό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων που αφορούν οι πληροφορίες, δεν έχει καθήκον να κοινοποιεί την παραβίαση των δεδομένων στις Εποπτικές Αρχές. Παρόλα αυτά, δεν αρκεί να εκτιμηθεί ο πιθανός κίνδυνος την στιγμή της παραβίασης' αντίθετα θα πρέπει να εκτιμηθεί πιθανός μελλοντικός κίνδυνος από την παραβίαση των δεδομένων. Σε αυτές τις περιπτώσεις ο Υπεύθυνος διαχείρισης αντιμετωπίζει τον κίνδυνο του να μην συμφωνούν με τις προβλέψεις του οι Εποπτικές Αρχές, θεωρώντας τις πράξεις του ως παραβίαση της υποχρέωσης ενημέρωσης που τιμωρείται με σημαντικά πρόστιμα. Λαμβάνοντας αυτό υπόψη, οι Υπεύθυνοι διαχείρισης πρέπει να υιοθετήσουν μια πολιτική αναφοράς ακόμα και των λιγότερο σημαντικών παραβιάσεων ασφαλείας.

Στην περίπτωση του εντοπισμού παραβίασης προσωπικών δεδομένων που επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων στα οποία αναφέρονται τα δεδομένα, ο Υπεύθυνος διαχείρισης είναι υποχρεωμένος να κοινοποιεί την παραβίαση προς τα εμπλεκόμενα άτομα χωρίς αδικαιολόγητη καθυστέρηση. Η κοινοποίηση αυτή θα πρέπει να περιγράψει στον πληθυσμό οποίος επηρεάστηκε, τη φύση της παραβίασης των προσωπικών δεδομένων, να δώσει συστάσεις για τον μετριασμό πιθανών δυσμενών επιπτώσεων και έχει σκοπό να δώσει την ευκαιρία στα άτομα αυτά να λάβουν τις απαραίτητες προφυλάξεις. Εάν, μετά την ενημέρωση της, η Εποπτεύουσα Αρχή επιβεβαιώσει την πιθανότητα υψηλού κινδύνου, δύναται να απαιτήσει από τον Υπεύθυνο διαχείρισης να ενημερώσει τα άτομα τα οποία αφορούν τα συγκεκριμένα δεδομένα. Σύμφωνα με το άρθρο 34, παράγραφος 3 η ενημέρωση αυτή δεν απαιτείται εάν πληρείται τουλάχιστον μια από τις ακόλουθες προϋποθέσεις:

- Υπεύθυνος διαχείρισης έχει εφαρμόσει σχεδιάσει τεχνικά και οργανωτικά μέτρα, τα οποία και εφαρμόστηκαν στα προσβεβλημένα προσωπικά δεδομένα.
- Ο Υπεύθυνος διαχείρισης έλαβε τα απαραίτητα, μεταγενέστερα της παραβίασης, μέτρα, ώστε να εξασφαλίσει ότι ο υψηλός κίνδυνος των δικαιωμάτων και ελευθεριών που είχε προκύψει δεν είναι πλέον υλοποιήσιμος.
- Η επικοινωνία με όλα τα άτομα με τα οποία επηρεάστηκαν, θα συνεπαγόταν τεράστια προσπάθεια (θα υπάρξει αντίθετα μια δημόσια ανακοίνωση ή αντίστοιχο ενημερωτικό μέτρο.).

ΚΕΦΑΛΑΙΟ 5 – ΤΕΧΝΙΚΕΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

5.1 Κώδικες δεοντολογίας και Πιστοποιήσεις

Με την κατάλληλη εφαρμογή οι κώδικες δεοντολογίας και οι πιστοποιήσεις παρέχουν μια ταχύτερη και ευέλικτη απάντηση στις προκλήσεις της προστασίας δεδομένων, αυξάνοντας την εμπιστοσύνη των ατόμων στην επεξεργασία των προσωπικών τους δεδομένων. Και τα δύο μέσα μπορούν να συνδυαστούν ή να χρησιμοποιηθούν ξεχωριστά για να αποδειχθεί η συμμόρφωσή με το GDPR. Ενώ, όμως, παρέχουν έναν τρόπο στις επιχειρήσεις να αποδείξουν στους πελάτες τους ότι λαμβάνουν σοβαρά τη συμμόρφωσή τους για την προστασία των προσωπικών δεδομένων, εξυπηρετούν διαφορετικούς σκοπούς στα πλαίσια της συμμόρφωσης με τον Κανονισμό.

Οι κώδικες δεοντολογίας καθορίζουν τις οργανωτικές και υλικές απαιτήσεις για μια συγκεκριμένη διαδικασία επεξεργασίας προσωπικών δεδομένων. Έτσι, επιτρέπουν στις επιχειρήσεις να αυτοπροσδιορίζουν εάν και πώς οι δραστηριότητές τους συμμορφώνονται με το GDPR αλλά δεν μπορούν να χρησιμοποιηθούν ως απόδειξη συμμόρφωσης με τον Κανονισμό. Από την άλλη πλευρά, οι Πιστοποιήσεις δεν καθορίζουν τις νομικές απαιτήσεις, αλλά αποδεικνύουν τη συμμόρφωση συγκεκριμένων διαδικασιών επεξεργασίας δεδομένων με τον Κανονισμό. Θα μπορούσε να αναφερθεί με αυτή τη λογική, ότι η σχέση των δυο μέσων είναι συμπληρωματική. Οι επιχειρήσεις πρέπει να αποφασίζουν κατά περίπτωση αν και ποια προσέγγιση ανταποκρίνεται καλύτερα στις ανάγκες τους.

Κώδικες δεοντολογίας

Πιστοποιήσεις

Η επιχείρηση θέλει μια πρακτική ερμηνεία των υποχρεώσεων της έναντι στο GDPR σε σχέση με:

- Μια συγκεκριμένη τεχνολογία
- Ένα συγκεκριμένο προϊόν
- Μια συγκεκριμένη διαδικασία επεξεργασίας δεδομένων

Η επιχείρηση θέλει μια απόδειξη την συμμόρφωση με το GDPR σε σχέση με:

- Μια συγκεκριμένη διαδικασία επεξεργασίας δεδομένων
- Συγκεκριμένες διαδικασίες

Διαδικασία

- Μετά την συμμόρφωση με έναν Κώδικα δεοντολογίας, η επιχείρηση αυτο-επιτηρείται διαρκώς για να επιβεβαιώσει την συμμόρφωση με αυτόν

- Εποπτικές αρχές πραγματοποιούν έκτακτους ελέγχους για τον προσδιορισμό της συμμόρφωσης με τον Κώδικα δεοντολογίας.
- Πριν από την απόκτηση μιας Πιστοποίησης, απαιτείται ένας ενδελεχής έλεγχος των διαδικασιών επεξεργασίας δεδομένων, ο οποίος πραγματοποιείται από ένα φορέα Πιστοποίησης και επιφέρει κόστος στην επιχείρηση.
- Στην περίπτωση θετικής έκβασης του ελέγχου , η επιχείρηση πιστοποιείται για την συγκεκριμένη διαδικασία.

Προτεινόμενο για

- Επιχειρήσεις που θέλουν έναν μηχανισμό αυτο-ελέγχου να καθορίσει τη συμμόρφωση όλων/ της πλειοψηφία των δραστηριοτήτων τους με το GDPR
- Μεγάλες εταιρείες που θέλουν έναν μηχανισμό αυτοελέγχου που να ανταποκρίνεται στις ιδιαιτερότητές του τομέα ή του προϊόντος τους.
- Εταιρίες που θέλουν ένα γρήγορο και αποτελεσματικό αυτοέλεγχο που μπορούν να χρησιμοποιήσουν ως κατευθυντήρια γραμμή για την συμμόρφωση με το GDPR.
- Επιχειρήσεις που θέλουν αποδείξεις συμμόρφωσης με το GDPR για επιλεγμένες δραστηριότητες επεξεργασίας δεδομένων.
- Επιχειρήσεις που αναζητούν νομικές βεβαιώσεις, σχετικά με την συμμόρφωση τους με τον Κανονισμό.

Η χρήση των κωδικών δεοντολογίας, ενώ δεν αποτελεί ένα καινούριο μέσο, ορίζεται με πολύ αυστηρούς όρους υπό το πρίσμα του GDPR, αναφορικά με το πότε πρέπει να χρησιμοποιηθούν και πως θα ελέγχονται. Η κύρια σκοπιμότητα τους είναι να προσδιορίσουν απροσδιόριστες νομικά έννοιες, και γενικές απαιτήσεις συμμόρφωσης ως προς το επίπεδο προστασίας των δεδομένων. Στο άρθρο 40 παράγραφος 2 δίνονται μερικές περιπτώσεις όπου επιτρέπεται να προσδιοριστεί η εφαρμογή του Κανονισμού:

- Οι διαδικασίες συλλογής δεδομένων προσωπικού χαρακτήρα
- Η χρήση ψευδώνυμων προσωπικών δεδομένων
- Η διαφάνεια στην επεξεργασία των δεδομένων
- Οι πληροφορίες που πρέπει να παρέχονται στα υποκείμενα που επηρεάζονται από μια παραβίαση προσωπικών δεδομένων
- Η άσκηση των δικαιωμάτων των ατόμων που αφορούν τα προσωπικά δεδομένα
- Ο τρόπος ενημέρωσης και προστασίας των παιδιών
- Εξωδικαστικές διαδικασίες και άλλες διαδικασίες επίλυσης διαφορών
- Μεταφορά προσωπικών δεδομένων σε τρίτες χώρες / διεθνείς οργανισμούς: Η διαδικασία έγκρισης του Κώδικα Δεοντολογίας διαφέρει στην περίπτωση της έγκρισης για ένα Κράτος μέλος ή για περισσότερα.

Στην πρώτη περίπτωση, μετά την επιτυχή κατάρτιση ενός Κώδικα Δεοντολογίας, η επιχείρηση οφείλει να τον καταθέσει στην αρμόδια εθνική εποπτική αρχή, η οποία γνωμοδοτεί κατά πόσον το σχέδιο είναι σύμφωνο με το GDPR και το κατά πόσον περιέχει επαρκείς διασφαλίσεις. Εάν τελικά εγκριθεί, καταχωρείται και δημοσιεύεται από την εποπτική αρχή και ο Υπεύθυνος διαχείρισης μπορεί να τον ακολουθεί για να αποδείξει την συμμόρφωσή του με ορισμένες πτυχές του GDPR. Σημειώνεται ότι η συμμόρφωση με τον Κώδικα Δεοντολογίας είναι βάσιμη και αφορά μόνο την χώρα μέλος, η οποία τον ενέκρινε.

Στην δεύτερη περίπτωση, που ο Κώδικάς Δεοντολογίας πρέπει να εγκριθεί για περισσότερα από ένα Κράτη μέλη, η διαδικασία έγκρισης απαιτεί περισσότερα βήματα. Πρώτον, η αρμόδια Εθνική Εποπτική Αρχή θα λάβει τη γνώμη του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων για το σχέδιο. Το Συμβούλιο αυτό μπορεί, με εκτελεστικές διατάξεις, να αποφασίσει ότι το σχέδιο έχει γενική εγκυρότητα εντός της Ευρωπαϊκής Ένωσης και να το δημοσιεύσει επίσημα.

Θα πρέπει να υπάρξουν ειδικοί φορείς που είναι υπεύθυνοι για τον έλεγχο της ορθή λειτουργίας και υιοθέτησης των Κωδικών Δεοντολογίας. Μέρος των υποχρεώσεων των φορέων αυτών είναι η λήψη κατάλληλων ενεργειών σε περίπτωση παράβασης της Κωδικών, συμπεριλαμβανομένης της αναστολής ή του αποκλεισμού του σχετικού Υπεύθυνου διαχείρισης / επεξεργασίας και η σχετική ενημέρωση στην αρμόδια εποπτική αρχή για τέτοιες ενέργειες. Για να οριστεί ένας τέτοιος ελεγκτικός φορέας πρέπει να πληρεί κάποια συγκεκριμένα κριτήρια:

- Θα πρέπει να διαθέτει ανεξαρτησία και εμπειρογνωμοσύνη σε σχέση με το αντικείμενο του Κώδικα Δεοντολογίας. Πιθανότατα, αυτό απαιτεί τεχνογνωσία στον τομέα στον οποίο αναφέρεται ο Κώδικας
- Ο ελεγκτικός φορέας πρέπει να θεσπίσει διαδικασίες που του επιτρέπουν να αξιολογεί την ικανότητα των Υπεύθυνων διαχείρισης / επεξεργασίας να εφαρμόζουν τον Κώδικα και να παρακολουθούν τη συμμόρφωσή τους σε αυτόν. Το εν λόγω όργανο ενδέχεται να υποχρεωθεί να υποβάλει συγκεκριμένο σχέδιο για την διαδικασία ελέγχου πριν από τη διαπίστευση, η οποία θα εγγυάται έναν συστηματικό τρόπο για να αποδείξει ότι πληρεί αυτή την προϋπόθεση.
- Οφείλει να έχει καθιερώσει διαδικασίες για τη διεκπεραίωση καταγγελιών σχετικά με παραβάσεις του Κώδικα Δεοντολογίας.
- Τα καθήκοντα της επιχείρησης και τα καθήκοντα του φορέα ελέγχου δεν θα οδηγήσουν σε σύγκρουση συμφερόντων. Μια τέτοια σύγκρουση μπορεί να συμβεί εάν ο ελεγκτικός φορέας διεξάγει άμεσα ή έμμεσα επιχειρησιακή δραστηριότητα στον τομέα που αναφέρεται στον Κώδικα Δεοντολογίας.

Συνοψίζοντας οι Κώδικες δεοντολογίας δεν έχουν δεσμευτική νομική υπόσταση και δεν μπορούν να χρησιμεύσουν ως απόδειξη συμμόρφωσης με το

GDPR προς τις αρμόδιες εποπτικές Αρχές. Ταυτόχρονα, όμως, οι επιχειρήσεις που αυτό-παρακολουθούν την συμμόρφωση τους με έναν Κώδικα δεοντολογίας καθορίζουν ένα ορισμένο επίπεδο προστασίας των δεδομένων τους και κατά συνέπεια, χρειάζεται να καταβάλουν λιγότερες προσπάθειες για την επίτευξη της συμμόρφωσης με το GDPR.

Αντιθέτως, ο σκοπός των Πιστοποιήσεων είναι να αποδείξουν ότι ορισμένες δραστηριότητες επεξεργασίας συμμορφώνονται με τα πρότυπα προστασίας δεδομένων βάσει του GDPR, γεγονός που μπορούν να ενισχύσουν το ανταγωνιστικό πλεονέκτημα ενός Υπεύθυνου διαχείρισης / επεξεργασίας στην αγορά. Έτσι, αποκτώντας μια Πιστοποίηση η εταιρία μπορεί να αποκτήσει μια θετική δημόσια εικόνα, καθώς αυξάνει την εμπιστοσύνη των ατόμων στην επεξεργασία προσωπικών δεδομένων που υλοποιεί. Μεγαλύτερη σημασία, έχει το γεγονός πως οι πιστοποιημένες εταιρίες έχουν την αυτοπεποίθηση, ότι οι διαδικασίες τους έχουν εγκριθεί για συμμόρφωση με το GDPR. Το GDPR δεν καθορίζει λεπτομερείς κανόνες για τη διαδικασία πιστοποίησης, προβλέπει μόνο βασικές αρχές και τα κριτήρια πιστοποίησης θα ορίζονται από τις αρμόδιες εθνικές εποπτικές αρχές.

Σύμφωνα με το άρθρο 42 Παράγραφος 3 του GDPR, η πιστοποίηση είναι εθελοντική και πραγματοποιείται μέσω διαφανούς διαδικασίας. Για την απόκτηση της Πιστοποίησης, οι Υπεύθυνοι διαχείρισης / επεξεργασίας πρέπει να παρέχουν στην αρμόδια Εποπτική Αρχή όλες τις πληροφορίες και πρόσβαση στις δραστηριότητες επεξεργασίας που κρίνονται απαραίτητες για τη διεξαγωγή της διαδικασίας πιστοποίησης. Η πιστοποίηση χορηγείται για ένα ανώτατο όριο των 3 ετών και μπορεί να ανανεωθεί, υπό την προϋπόθεση ότι πληρούνται τα σχετικά κριτήρια. Τα κριτήρια της πιστοποίησης εξακολουθούν να ικανοποιούνται από τους υπεύθυνους και μετά την διαδικασία πιστοποίησης. Οι πιστοποιήσεις ενδέχεται να αποτελέσουν σημαντικό εργαλείο για την προστασία δεδομένων από την πλευρά των Υπεύθυνων διαχείρισης / επεξεργασίας. Ωστόσο, η επιτυχία τους θα κριθεί σε μεγάλο βαθμό από τη δημιουργία κοινών μηχανισμών πιστοποίησης για αρκετά κράτη μέλη της Ευρωπαϊκής Ένωσης, καθώς οι διασυνοριακές ή πανευρωπαϊκές δραστηριότητες επεξεργασίας δεδομένων αποτελούν τη νόρμα στις μέρες μας.

Οι οργανισμοί πιστοποίησης οφείλουν να είναι διαπιστευμένοι και για να το πετύχουν αυτό πρέπει να πληρούν έναν αριθμό προϋποθέσεων, οι οποίες συμπίπτουν με τις προϋποθέσεις των ελεγκτικών φορέων για τους Κώδικες Δεοντολογίας: ανεξαρτησία, εμπειρογνωμοσύνη, θέσπιση διαδικασιών και η απουσία σύγκρουσης συμφερόντων. Λεπτομερή κριτήρια διαπίστευσης θα καθορίζονται από την αρμόδια εποπτική αρχή. Η διαπίστευση αυτή ανακαλείται από τον τελευταίο εάν ένας οργανισμός δεν πληρεί πλέον τους όρους διαπίστευσης ή οι δράσεις που αναλαμβάνει ο οργανισμός πιστοποίησης παραβιάζουν το GDPR. Οι οργανισμοί πιστοποίησης, αφού ενημερώσουν την Εποπτική Αρχή, εκδίδουν και ανανεώνουν Πιστοποιήσεις και είναι υπεύθυνοι για τη σωστή αξιολόγηση που οδηγεί σε μια Πιστοποίηση ή την ανάκληση της.

Οι Πιστοποιήσεις επιτρέπουν στις επιχειρήσεις να βεβαιώνουν (τον εαυτό τους) ότι έχουν εγκριθεί επισήμως οι δραστηριότητες επεξεργασίας προσωπικών

δεδομένων για συμμόρφωση με το GDPR. Αν και η έγκριση αυτή δεν έχει νομική ισχύ και δεν περιορίζει τις αρμοδιότητες των εποπτικών αρχών για ελέγχους, διευκολύνει σε μεγάλο βαθμό το βάρος της απόδειξης συμμόρφωσης με το GDPR. Πιστοποιήσεις μπορούν να χρησιμοποιηθούν για να αποδείξουν την τήρηση των απαιτήσεων του Κανονισμού για την προστασία των δεδομένων μέσω της τεχνολογίας. Επιπλέον, όταν μια εποπτική αρχή πραγματοποιεί έλεγχο σχετικά με την ορθή εφαρμογή του GDPR σε μια πιστοποιημένη επιχείρηση, ο έλεγχος θα είναι λιγότερο διεξοδικός, καθώς η πιστοποίηση εξ ορισμού αποδεικνύει ένα ορισμένο επίπεδο συμμόρφωσης. Εντός της επιχείρησης, οι πιστοποιήσεις μπορούν να χρησιμοποιηθούν για να επιβεβαιώσουν στους υπαλλήλους, στα όργανα εκπροσώπησης τους και, όπου προβλέπεται από το νόμο των κρατών μελών της Ευρωπαϊκής Ένωσης, ότι η επεξεργασία δεδομένων του τμήματος HR είναι πιστοποιημένη και συνεπώς συμβατή με το υψηλό επίπεδο προστασίας δεδομένων στο πλαίσιο του GDPR. Εκτός της επιχείρησης, οι Πιστοποιήσεις μπορούν να δημιουργήσουν μια θετική δημόσια εικόνα και, συνεπώς, να ενισχύσουν ανταγωνιστικό πλεονέκτημα μιας επιχείρησης στην αγορά. Οι πιστοποιήσεις ενδέχεται να συμβάλλουν στην προσέλκυση επιχειρηματικών εταίρων. Για παράδειγμα, ένας Υπεύθυνος διαχείρισης είναι πιθανό να επιλέξει έναν Υπεύθυνο επεξεργασίας του οποίου οι δραστηριότητες επεξεργασίας πιστοποιούνται για συμμόρφωση με το GDPR και όχι κάποιον ο οποίος δεν έχει ελεγχθεί για συμμόρφωση με τον κανονισμό.

5.2 Ανωνυμοποίηση και Χρήση Ψευδωνύμων

Η Ανωνυμοποίηση είναι μια μέθοδος τροποποίησης των προσωπικών δεδομένων που έχει ως αποτέλεσμα την μη ύπαρξη σύνδεσης αυτών με κάποιο άτομο. Τα δεδομένα έπειτα από αυτή την διαδικασία καθίστανται ανώνυμα με την έννοια πως δεν σχετίζονται με κάποιο άτομο που μπορεί να αναγνωριστεί. Η Ανωνυμοποίηση μπορεί να επιτευχθεί μέσω ενός αριθμού τεχνικών που κατά κανόνα εμπίπτουν σε δύο κατηγορίες:

1. Η ψευδοτυχαία μεταβολή της ακρίβειας των δεδομένων, προκειμένου να διασπαστεί η ισχυρή σχέση μεταξύ των προσωπικών δεδομένων και του ατόμου. Εάν τα δεδομένα γίνουν επαρκώς αβέβαια, δεν μπορεί πλέον να αναφέρεται σε ένα συγκεκριμένο άτομο.
2. Γενίκευση: συνίσταται στη γενίκευση των χαρακτηριστικών των υποκειμένων των δεδομένων με τροποποίηση της αντίστοιχης κλίμακας ή της σειράς των δεδομένων (δηλ. παρουσίαση των δεδομένων ανά μια περιοχή και όχι μια πόλη, ανά ένα μήνα και όχι μια εβδομάδα κτλ).

Η χρήση ψευδωνύμων ορίζεται ως η επεξεργασία προσωπικών δεδομένων κατά τρόπο ώστε τα προσωπικά δεδομένα να μην μπορούν πλέον να αποδίδονται σε συγκεκριμένα δεδομένα χωρίς τη χρήση πρόσθετων πληροφοριών. Αυτό θα μπορούσε να επιτευχθεί με την αντικατάσταση του ονόματος ή άλλων χαρακτηριστικών με ορισμένους δείκτες. Οι πρόσθετες πληροφορίες που επιτρέπουν την ταυτοποίηση πρέπει να τηρούνται ξεχωριστά. Ταυτόχρονα η συγκεκριμένη τεχνική θα μπορούσε να ισχυροποιηθεί παραπάνω μέσω της ισχυρής κωδικοποίησης των πληροφοριών, περιορίζοντας ταυτόχρονα των αριθμό των ατόμων που έχουν πρόσβαση στα αντίστοιχα κλειδιά. Αξίζει να σημειωθεί πως, αντίθετα με την ανωνυμοποίηση, η χρήση ψευδωνύμων εμπίπτει στα πλαίσια εφαρμογής του GDPR, καθώς ο κίνδυνος προσδιορισμού του ατόμου είναι υψηλότερος με ψευδώνυμα δεδομένων παρά με ανώνυμα δεδομένα.

ΚΕΦΑΛΑΙΟ 6 – ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΑΤΟΜΩΝ

6.1 Ενημέρωση των ατόμων για την επεξεργασία των δεδομένων τους

Οι πληροφορίες που παρέχονται στο άτομο που αφορούν τα δεδομένα αυξάνουν τη διαφάνεια των δραστηριοτήτων επεξεργασίας και επιτρέπουν την αποτελεσματική άσκηση των Δικαιωμάτων τους. Μόνο ένα ενημερωμένο άτομο θα είναι σε θέση να ασκεί έλεγχο ή να επηρεάσει τη μεταχείριση των προσωπικών του δεδομένων. Έτσι, τα δικαιώματα ενημέρωσης και οι αντίστοιχες υποχρεώσεις του Υπεύθυνου Διαχείρισης διαδραματίζουν καθοριστικό ρόλο στην προστασία των προσωπικών δεδομένων. Οποιαδήποτε επικοινωνία με το άτομο που αφορούν τα δεδομένα πρέπει να διέπεται από την αρχή της διαφάνειας σύμφωνα με το άρθρο 5 παράγραφος 1 του GDPR. Σε σύγκριση με την Οδηγία για την Προστασία των Δεδομένων (Data Protection Directive), οι υποχρεώσεις πληροφόρησης του Υπεύθυνου Διαχείρισης προς τα πρόσωπα στα οποία αναφέρονται τα δεδομένα έχουν αυξηθεί σε μεγάλο βαθμό, όπως επίσης και τα αντίστοιχα πρόστιμα για την μη τήρηση αυτών των υποχρεώσεων. Προκειμένου να είναι σε θέση να επικοινωνεί με τα άτομα στα οποία αναφέρονται τα δεδομένα, ο Υπεύθυνος Διαχείρισης υποχρεούται να δημιουργήσει κατάλληλα μέτρα πληροφόρησης. Αυτά τα μέτρα πρέπει να χαρακτηρίζονται από συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα, για μια συγκεκριμένη λειτουργία ή για το σύνολο των λειτουργιών επεξεργασίας στα προσωπικά δεδομένα. Αυτές οι αρχές πρέπει να τηρούνται για κάθε επικοινωνία με τα άτομα που αφορούν τα δεδομένα. Ο τρόπος και η μορφή παροχής πληροφοριών είναι ιδιαίτερα σημαντικά όταν οι πληροφορίες απευθύνονται στα παιδιά. Αυτό οφείλεται στο γεγονός ότι τα παιδιά χρειάζονται ειδική προστασία, έτσι ώστε κάθε ενημέρωση και επικοινωνία, αναφορικά με την επεξεργασία των προσωπικών τους δεδομένων, να παρέχεται με τόσο απλή και σαφή γλώσσα, που το παιδί να την καταλαβαίνει εύκολα. Οι διαφορετικές απαιτήσεις διέπουν τον τρόπο παροχής των πληροφοριών με σκοπό πάντα την αύξηση της διαφάνειας και την κατανόηση από την πλευρά των ατόμων που αφορούν τα δεδομένα. Ωστόσο, η οριοθέτηση του οφέλους από τα διαφορετικά κριτήρια παραμένει ασαφής καθώς επικαλύπτονται μερικώς:

- Η συνοπτικότητα απαιτεί την ορθή και περιεκτική πληροφόρηση όσον αφορά το περιεχόμενό. Ωστόσο, καθώς το περιεχόμενο παρουσιάζεται με ευανάγνωστο τρόπο πρέπει να αποφεύγονται οι άσκοπες πληροφορίες. Για να δοθούν περισσότερες πληροφορίες σχετικά με ορισμένες πτυχές της επεξεργασίας, ο Υπεύθυνος Διαχείρισης μπορεί να χρησιμοποιεί διαβαθμισμένες ειδοποιήσεις απορρήτου.
- Η προσβασιμότητα απαιτεί προσαρμογή των πληροφοριών στις ανάγκες και περιστάσεις που αφορούν τα εν λόγω άτομα. Ωστόσο, το επίπεδο προσαρμογής πρέπει να είναι ανάλογο της προσπάθειας που απαιτείται στη συγκεκριμένη περίπτωση. Ο υπεύθυνος διαχείρισης θα πρέπει να

προσαρμόσει τα μέτρα πληροφόρησης του ως προς το μέσο όρο των ατόμων που σχετίζονται με τα δεδομένα.

Η επικοινωνία με το άτομο που αφορούν τα δεδομένα δεν υπόκειται σε αυστηρούς κανόνες. Ωστόσο, οι πληροφορίες πρέπει να παρέχονται στα άτομα που αφορούν τα δεδομένα σε μια εύκολη και προσιτή μορφή. Αυτό θα μπορούσε να συνεπάγεται γραπτή μορφή ή με άλλα μέσα, συμπεριλαμβανομένων, ενδεχομένως και ηλεκτρονικά μέσα, σύμφωνα με το άρθρο 12 του GDPR. Η επικοινωνία μέσω ηλεκτρονικών μέσων είναι ιδιαίτερα κατάλληλη όταν τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία με ηλεκτρονικά μέσα ή αποκτώνται ηλεκτρονικά. Στην τελευταία περίπτωση, ο Υπεύθυνος διαχείρισης μπορεί να παρέχει γενικές πληροφορίες σχετικά με την επεξεργασία δεδομένων μέσω δημοσίευσης στον δικτυακό του τόπο. Από την άποψη αυτή, η δημοσίευση στο δικτυακό τόπο μπορεί να αποδειχθεί ιδιαίτερα σημαντική σε καταστάσεις όπου η τεχνολογική πολυπλοκότητα της επεξεργασίας καθιστούν δυσχερή την κατανόηση για το άτομο, αναφορικά με το ποιος και για ποιο σκοπό συλλέγει τα προσωπικά δεδομένα του, όπως στην περίπτωση της διαδικτυακής διαφήμισης. Γενικές πληροφορίες σχετικά με την επεξεργασία ενδέχεται να παρέχονται σε συνδυασμό με τυποποιημένες εικόνες (που θα μπορούσαν να αναπτυχθούν από την Ευρωπαϊκή Επιτροπή στο μέλλον), προκειμένου να δοθεί μια εικόνα των σκοπών της επεξεργασίας με ευδιάκριτο και κατανοητό τρόπο. Ωστόσο, η χρήση μόνο εικονιδίων για την παροχή πληροφοριών είναι παράνομη.

Η επικοινωνία με το άτομο που αφορούν τα δεδομένα, αναφορικά με μια συγκεκριμένη ενέργεια επεξεργασίας προσωπικών του δεδομένων, πρέπει να πραγματοποιείται κατά τον χρόνο συλλογής τους (άρθρο 13, παράγραφος 1). Εάν τα δεδομένα δεν λαμβάνονται απευθείας από το άτομο, αλλά από άλλη πηγή, οι αντίστοιχη ενημέρωση πρέπει να παρέχεται στο άτομο εντός ενός εύλογου χρονικού διαστήματος, ανάλογα με την υπόθεση, αλλά το αργότερο εντός ένα μήνα. Αντίθετα, εάν τα προσωπικά δεδομένα συλλέγονται απ ευθείας από το άτομο το οποίο αφορούν, ο Υπεύθυνος διαχείρισης πρέπει να παρέχει τις ακόλουθες πληροφορίες:

- Την ταυτότητα και τα στοιχεία επικοινωνίας του Υπεύθυνος διαχείρισης και, ενδεχομένως, του αντιπρόσωπου του
- Τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων (Data Protection Officer)
- Τους σκοπούς και τη νομική βάση για την επεξεργασία των προσωπικών δεδομένων. Σύμφωνα με αυτό, και η περίπτωση που η επεξεργασία βασίζεται στα νόμιμα συμφέροντα του Υπεύθυνου διαχείρισης, πρέπει να δηλωθεί στο ενδιαφερόμενο άτομο.
- Τους παραλήπτες / τις κατηγορίες παραληπτών των προσωπικών δεδομένων, εάν υπάρχουν.
- κατά περίπτωση, την πρόθεση του Υπεύθυνου διαχείρισης να μεταφέρει τα προσωπικά δεδομένα σε τρίτες χώρες και τις προβλεπόμενες δικλείδες ασφαλείας για τη μεταφορά αυτή.

- Την διάρκεια της περιόδου για την οποία θα αποθηκεύονται τα προσωπικά δεδομένα
- Πληροφορίες σχετικά με τα δικαιώματα του ατόμου και τα δεδομένα αυτά βάσει των άρθρων 15-23 του GDPR.
- Πληροφορίες σχετικά με το δικαίωμα απόσυρσης της συγκατάθεσης όταν η επεξεργασία βασίζεται στην συγκατάθεση του ατόμου.
- Το δικαίωμα υποβολής καταγγελίας στην εποπτική αρχή

Επιπλέον, όταν ο Υπεύθυνος διαχείρισης ανταποκρίνεται στις αιτήσεις των ατόμων που αφορούν τα προσωπικά δεδομένα πρέπει να πληρούνται οι γενικές απαιτήσεις επικοινωνίας βάσει του άρθρου 12 του GDPR. Όταν το αίτημα γίνεται με ηλεκτρονικά μέσα, οι πληροφορίες, πρέπει να παρέχονται, εάν είναι δυνατόν, με ηλεκτρονικά μέσα. Εάν το άτομο ζητήσει να ενημερωθεί προφορικά, γεγονός που συνήθως συμβαίνει στις περιπτώσεις όπου επιδιώκεται επιβεβαίωση της συμμόρφωσης του Υπεύθυνου διαχείρισης με ήδη υπάρχον αίτημα, είναι απαραίτητη αρχικά η ταυτοποίηση του ατόμου. Η ενημέρωση του ατόμου, ασχέτως του τρόπου επικοινωνίας είναι απολύτως δωρεάν, εκτός των περιπτώσεων που τα αιτήματα του ατόμου είναι προφανώς αβάσιμα ή υπερβολικά, στις οποίες περιπτώσεις, είναι δυνατή η άρνηση εκπλήρωσης του αιτήματος ή η χρέωση του ατόμου.

Ο Υπεύθυνος διαχείρισης οφείλει παρέχει στο άτομο στο οποίο αναφέρονται τα δεδομένα, πληροφορίες σχετικά με τις ενέργειες που έχουν ακολουθηθεί ύστερα από αίτημα του δεύτερου, χωρίς αδικαιολόγητη καθυστέρηση και, σε κάθε περίπτωση, εντός ενός μήνα από την παραλαβή του αιτήματος. Η περίοδος ενημέρωσης μπορεί να παραταθεί κατά δύο περαιτέρω μήνες, όταν αυτό είναι απαραίτητο, με βάση την πολυπλοκότητα του αιτήματος ή τον αριθμό των αιτήσεων. Στην περίπτωση αυτή, το πρόσωπο στο οποίο αναφέρονται τα δεδομένα πρέπει να ενημερώνεται για οποιαδήποτε καθυστέρηση, εντός ενός μήνα από την παραλαβή του αιτήματος, μαζί με ενδείξεις για τους λόγους της καθυστέρησης. Ωστόσο, οι νομοθέτες δεν καθιστούν σαφές σε ποιες περιπτώσεις μια αίτηση θεωρείται αρκετά «πολύπλοκη», για να δικαιολογηθεί παράταση της περιόδου ενημέρωσης. Η νομική αυτή αβεβαιότητα είναι προβληματική δεδομένης των υψηλών προστίμων σε περιπτώσεις παράβασης.

6.2 Δικαίωμα ατόμου στην πρόσβαση

Εκτός από τα δικαιώματα ενημέρωσης των ατόμων στα οποία αναφέρονται τα δεδομένα και των αντίστοιχων υποχρεώσεων των υπευθύνων διαχείρισης, το GDPR έχει αυξήσει τα δικαιώματα των ατόμων, τα οποία αφορούν την πρόσβαση στα προσωπικά τους δεδομένα. Το δικαίωμα πρόσβασης αυξάνει την αμεροληψία και της διαφάνεια στην επεξεργασία δεδομένων, δεδομένου ότι επιτρέπει στα άτομα να επαληθεύουν τη νομιμότητα των δραστηριοτήτων επεξεργασίας που πραγματοποιούνται στα προσωπικά τους δεδομένα και, ως εκ τούτου, τα άτομα συμβάλλουν τελικά στην αποτελεσματική επιβολή των δικαιωμάτων τους. Σε αντίθεση με τα δικαιώματα πληροφόρησης που αναφέρονται στα άρθρα 13 και 14 του GDPR, το δικαίωμα πρόσβασης υπερβαίνει την απλή παροχή γενικών πληροφοριών. Παρέχεται η δυνατότητα να ζητηθούν περισσότερο λεπτομερείς πληροφορίες σχετικά με την επεξεργασία των προσωπικών δεδομένων, προκειμένου να μπορέσει να εκτιμηθεί περαιτέρω η νομιμότητα αυτής. Το δικαίωμα πρόσβασης σύμφωνα με το GDPR οργανώνεται (νομικά) σε δύο στάδια. Σε ένα πρώτο στάδιο το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει το δικαίωμα να λάβει επιβεβαίωση από τον υπεύθυνο διαχείρισης για το αν τα προσωπικά δεδομένα του υποβάλλονται σε επεξεργασία ή όχι. Εάν υφίσταται τέτοια επεξεργασία, σε δεύτερο στάδιο, το πρόσωπο στο οποίο αναφέρονται τα δεδομένα θα έχει πρόσβαση στα επεξεργασμένα προσωπικά του δεδομένα και τις ακόλουθες πληροφορίες:

- Τους σκοπούς της επεξεργασίας.
- Τις κατηγορίες προσωπικών δεδομένων.
- Οι παραλήπτες στους οποίους τα δεδομένα έχουν αποκαλυφθεί ή θα αποκαλυφθούν, ιδίως εάν αυτοί βρίσκονται σε τρίτες χώρες ή σε διεθνείς οργανισμούς
- Εάν είναι δυνατόν, την προβλεπόμενη διάρκεια της αποθήκευσης των δεδομένων, ή εάν δεν είναι δυνατόν, τα κριτήρια που θα καθορίσουν την περίοδο αυτή.
- Την ύπαρξη δικαιωμάτων διαγραφής, διόρθωσης, περιορισμού της επεξεργασίας ή του δικαιώματος της ένστασης.
- Το δικαίωμα υποβολής καταγγελίας στην εποπτική αρχή.
- Πληροφορίες σχετικά με την πηγή των δεδομένων, εάν δεν τα παρείχε το ίδιο το άτομο.
- Όταν τα προσωπικά δεδομένα μεταφέρονται σε τρίτες χώρες, πληροφορίες σχετικά με τις δικλίδες ασφαλείας που έχουν ληφθεί για τη μεταφορά αυτή.
- Προκειμένου να δοθεί στο άτομο στο οποίο αναφέρονται τα δεδομένα πρόσβαση σε αυτά, ο υπεύθυνος διαχείρισης πρέπει να του παράσχει αντίγραφο των δεδομένων αυτών που υποβάλλονται σε επεξεργασία.

Επιπλέον, η παροχή πρόσβασης στα δεδομένα προσωπικού χαρακτήρα πρέπει να πληρεί τις γενικές αρχές και τις απαιτήσεις του άρθρου 12. Αυτό συνεπάγεται,

μεταξύ άλλων, ότι το πρώτο αντίγραφο παρέχεται δωρεάν στο άτομο. Στην περίπτωση που ο υπεύθυνος διαχείρισης επεξεργάζεται μια μεγάλη ποσότητα πληροφοριών σχετικά με το συγκεκριμένο άτομο, πρέπει να ζητηθεί από το άτομο να προσδιορίσει με ποιες πληροφορίες σχετίζεται το αίτημα του, πριν από την παροχή πληροφοριών. Εαν το άτομο επιθυμεί να λάβει πληροφορίες για κάθε επεξεργασία ή δραστηριότητα που διεξάγονται από τον Υπεύθυνο διαχείρισης στα προσωπικά του δεδομένα και η αίτηση αυτή δεν θεωρείται υπερβολική, ο υπεύθυνος διαχείρισης πρέπει να παρέχει εκτεταμένες πληροφορίες στο άτομο το οποίο κατέθεσε το αίτημα.

Όταν το άτομο στο οποίο αναφέρονται τα δεδομένα υποβάλλει την αίτηση πρόσβασης με ηλεκτρονικά μέσα και δεν έχει ορίσει κάτι διαφορετικό σε αυτή, οι πληροφορίες πρέπει να παρέχονται σε ηλεκτρονική μορφή. Τέτοιου είδους ηλεκτρονική παροχή πρέπει να περιλαμβάνει την παροχή πληροφοριών μέσω ηλεκτρονικού ταχυδρομείου, ωστόσο, τα μηνύματα θα πρέπει να κρυπτογραφούνται για την προστασία των εν λόγω πληροφοριών. Ο Υπεύθυνος διαχείρισης θα μπορούσε να δώσει εναλλακτικά απομακρυσμένη πρόσβαση σε μια ηλεκτρονική πλατφόρμα που θα παρέχει άμεση πρόσβαση στα προσωπικά δεδομένα του ατόμου, υπηρεσία η οποία κρίνεται προαιρετική για τους Υπεύθυνους διαχείρισης. Όποια και να είναι η μορφή της ηλεκτρονικής επικοινωνίας, έχει μεγάλη σημασία η ταυτοποίηση του ατόμου που ζητεί πρόσβαση σε προσωπικά δεδομένα προκειμένου να αποτραπεί η κατάχρηση. Έτσι, ο ελεγκτής θα πρέπει να χρησιμοποιήσει όλα τα εύλογα μέτρα για να πραγματοποιήσει την ταυτοποίηση, ιδίως στο πλαίσιο των ηλεκτρονικών υπηρεσιών και του διαδικτύου.

6.3 Δικαίωμα διόρθωσης, το δικαίωμα διαγραφής και το δικαίωμα περιορισμού της επεξεργασίας

Δεδομένου ότι η επεξεργασία δεδομένων μπορεί να βλάψει αρνητικά τα δικαιώματα και τις ελευθερίες των ατόμων, ιδίως όταν είναι παράνομη ή όταν περιλαμβάνει ανακριβή ή ελλιπή δεδομένα, το GDPR προβλέπει διαφορετικά δικαιώματα που επιτρέπουν περιορισμούς στις επεξεργασίες αυτές Τα δικαιώματα αυτά είναι το δικαίωμα διόρθωσης, το δικαίωμα διαγραφής και το δικαίωμα περιορισμού της επεξεργασίας. Αυτά τα δικαιώματα είναι σε ισχύ όταν τα ανακριβή ή ελλιπή προσωπικά τους δεδομένα παραβιάζουν το GDPR ή νομοθεσία άλλου νόμου κράτους μέλους της Ευρωπαϊκής Ένωσης ή της ίδιας της Ένωσης στην οποία υπόκειται ο Υπεύθυνος διαχείρισης. Έτσι, τα δικαιώματα αυτά εξυπηρετούν κατά κύριο λόγο την εξάλειψη των παραβιάσεων του νόμου. Το ποιο δικαίωμα είναι το πιο χρήσιμο εξαρτάται από τις συγκεκριμένες περιστάσεις της υπόθεσης. Ωστόσο, εναπόκειται στη διακριτική ευχέρεια του ενδιαφερομένου να επιλέξει ποιο δικαίωμα επιθυμεί να ασκήσει.

Το δικαίωμα της διόρθωσης μπορεί να συμβάλει στην αποτροπή αρνητικών επιπτώσεων στα δικαιώματα και τις ελευθερίες των ατόμων στα οποία αναφέρονται τα δεδομένα. Ορίζει την αρχή της ακρίβειας σύμφωνα με την οποία, τα επεξεργασμένα δεδομένα, σε κάθε δεδομένη στιγμή, πρέπει να αντανακλούν την πραγματικότητα. Μια παραπλανητική παρουσίαση της πραγματικότητας μπορεί, για παράδειγμα, να συμβεί όταν τα δεδομένα πιστοληπτικής ικανότητας ενός ατόμου αποθηκεύονται λανθασμένα και ως αποτέλεσμα, υπάρχει η περίπτωση της άρνησης πίστωσης για το εν λόγω άτομο ή όταν τα αποτελέσματα των ιατρικών θεραπειών είναι καταγεγραμμένα λάθος. Καθώς το δικαίωμα διόρθωσης πρέπει (εκ νέου) να δημιουργήσει μια νόμιμη κατάσταση επεξεργασίας, τα άτομα δεν χρειάζεται να αιτιολογούν τα αιτήματά τους βάσει της παρούσας διάταξης. Ωστόσο, το άτομο έχει την ευθύνη να αποδείξει την ανακρίβεια ή την έλλειψη πληρότητας των προσωπικών δεδομένων που τους αφορούν και, ως εκ τούτου, πρέπει να επισυνάπτει τα απαραίτητα έγγραφα για να βασίσει το αίτημα του βάσει του άρθρου 16 του GDPR.

Η απόφαση εναντίον της Google στην Ισπανία το 2014, αναφορικά με το αίτημα του να διαγραφούν μόνιμα τα προσωπικά δεδομένα ενός ατόμου, έπαιξε σημαντικό ρόλο για τον νομοθέτη, όταν στοιχειοθέτησε το δικαίωμα της διαγραφής. Στο άρθρο 17 του GDPR ορίζονται ευθύνες του Υπεύθυνου διαχείρισης σχετικά με το δικαίωμα της διαγραφής, που περιλαμβάνουν και τις μεταφορές σε τρίτους οργανισμούς. Το άτομο έχει δικαίωμα να ζητήσει την διαγραφή των προσωπικών του δεδομένων, εάν ισχύει ένας από τους ακόλουθους λόγους:

- Τα προσωπικά δεδομένα δεν είναι πλέον απαραίτητα αναφορικά με τους σκοπούς για τους οποίους συλλέχθηκαν και επεξεργάστηκαν: η διάταξη αυτή εφαρμόζεται στα δεδομένα που συλλέχθηκαν αρχικά και υποβλήθηκαν σε νόμιμη επεξεργασία. Ωστόσο, σε περίπτωση που τα σχετικά δεδομένα

είναι απαραίτητα για σκοπό διαφορετικό από τον αρχικό, αλλά που σε κάποια σημεία ταυτίζονται, η διαγραφή δεν χρειάζεται να πραγματοποιηθεί.

- Το άτομο αποσύρει τη συγκατάθεση στην οποία βασίζεται η επεξεργασία των δεδομένων και δεν υπάρχει άλλη νομική βάση για αυτή: κάθε άτομο έχει το δικαίωμα να αποσύρει τη συναίνεσή του οποιαδήποτε στιγμή, με άμεσο αποτέλεσμα η επεξεργασία που δεν μπορεί να βασιστεί σε άλλη νομική βάση να καθίσταται παράνομη. Έτσι, κατά την απόσυρση της συγκατάθεσης, προκύπτει το δικαίωμα της διαγραφής.
- Το άτομο που αφορούν τα δεδομένα αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 του GDPR και δεν υπάρχουν επιτακτικοί λόγοι επεξεργασίας. Ο ελεγκτής έχει το δικαίωμα να επανεκτιμήσει την κατάσταση ως προς την προστασία των δικών του συμφερόντων και ίσως να μην χρειαστεί να υπάρξει διαγραφή. Αυτή η αξιολόγηση μπορεί να απαιτεί κάποιο χρονικό διάστημα και έτσι το άτομο μπορεί να ασκήσει το δικαίωμά του περιορισμού της επεξεργασίας των δεδομένων του εν τω μεταξύ.
- Τα προσωπικά δεδομένα έχουν υποστεί παράνομη επεξεργασία: η διάταξη αυτή παρέχει το δικαίωμα διαγραφής όταν η επεξεργασία είναι παράνομη, είτε σε περίπτωση έλλειψης νομικής άδειας για επεξεργασία είτε στην περίπτωση μη συμμόρφωσης με τον κανονισμό.
- Τα προσωπικά δεδομένα πρέπει να διαγραφούν για συμμόρφωση με νομοθεσία του κράτους μέλους της Ευρωπαϊκής Ένωσης ή της ίδιας της Ένωσης, στο οποίο υπάγεται ο Υπεύθυνος διαχείρισης: βάσει αυτού είναι ασαφές αν ο Κανονισμός περιέχει ένα παράθυρο που επιτρέπει στα κράτη μέλη της Ευρωπαϊκής Ένωσης να εισάγουν εθνικές νομικές υποχρεώσεις για την διαγραφή των δεδομένων.
- Τα προσωπικά δεδομένα συλλέχθηκαν με βάση τη συναίνεση ενός παιδιού σε σχέση με την προσφορά υπηρεσιών ασφάλειας πληροφοριών: η διάταξη αυτή επιβάλλει την προστασία των προσωπικών δεδομένων των παιδιών, δεδομένου ότι παρέχει το δικαίωμα της διαγραφής των δεδομένων σε σχέση με υπηρεσίες ασφάλειας πληροφοριών βασισμένες στην συγκατάθεση ενός παιδιού . Αυτό έχει να κάνει με το γεγονός ότι το παιδί μπορεί να μην έχει πλήρη επίγνωση των κινδύνων που συνεπάγεται η επεξεργασία των δεδομένων του και αργότερα να θέλει να τα διαγράψει, ειδικά από το Διαδίκτυο. Αυτό το δικαίωμα είναι δυνατόν να ασκείται ανεξάρτητα από το γεγονός ότι το άτομο που αφορούν τα δεδομένα δεν είναι πλέον παιδί.

Τελευταίο από τα δικαιώματα προς ανάλυση είναι το δικαίωμα περιορισμού της επεξεργασίας. Το συγκεκριμένο δικαίωμα πιθανότατα θα φανεί πολύ χρήσιμο στις περιπτώσεις που το άτομο θέλει να προχωρήσει στην διαγραφή των προσωπικών του δεδομένων ενώ ο Υπεύθυνος διαχείρισης, θέλει να συνεχίσει την επεξεργασία αυτών. Το άρθρο 18 παράγραφος 1 προβλέπει τέσσερις λόγους που δικαιολογούν το δικαίωμα περιορισμού της επεξεργασίας:

- Η ακρίβεια των προσωπικών δεδομένων αμφισβητείται από το άτομο στο οποίο αναφέρονται και ο περιορισμός της επεξεργασίας πραγματοποιείται

για χρονικό διάστημα που επιτρέπει στον υπεύθυνο διαχείρισης να επαληθεύσει την ακρίβεια των εν λόγω δεδομένων. Το άτομο παράλληλα είναι υποχρεωμένο να προσδιορίσει και να συμπεριλάβει αποδεικτικά στοιχεία σχετικά με τα συγκεκριμένα δεδομένα που σχετίζονται με το αίτημα του. Ωστόσο, στην πράξη, μια τυχαία αμφισβήτηση της ακρίβειας των δεδομένων ενδέχεται να οδηγήσει σε προσωρινό περιορισμό της επεξεργασίας καθώς ο υπεύθυνος διαχείρισης δεν μπορεί να ελέγξει, τουλάχιστον σε αρχικό στάδιο, αν οι ισχυρισμοί του ατόμου ανταποκρίνονται στην πραγματικότητα.

- Η επεξεργασία είναι παράνομη και το άτομο αντιτίθεται στη διαγραφή των προσωπικών δεδομένων και ζητεί τον περιορισμό της επεξεργασίας τους. Αυτό μπορεί να συμβεί στην περίπτωση που το άτομο θέλει να αποδείξει την ύπαρξη των δεδομένων στον Υπεύθυνο διαχείρισης.
- Ο υπεύθυνος διαχείρισης δεν χρειάζεται πλέον τα δεδομένα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα είναι χρήσιμα στο άτομο στο οποίο αναφέρονται για την άσκηση των δικαιωμάτων του. Τα προσωπικά δεδομένα διατηρούνται και σε αυτή την περίπτωση ως αποδεικτικά στοιχεία.
- Το άτομο που αφορούν τα δεδομένα έχει αρνηθεί την επεξεργασία αυτών και βρίσκεται εν αναμονή της επαλήθευσης κατά πόσον τα νόμιμα συμφέροντα του υπεύθυνου διαχείρισης υπερισχύουν των δικών του νόμιμων συμφερόντων . Κατά τη διάρκεια αυτής της αξιολόγησης, η επεξεργασία αυτή περιορίζεται βάσει του δικαιώματος του περιορισμού της επεξεργασίας.

Ξεχωριστή αναφορά πρέπει να γίνει στο δικαίωμα της ένστασης. Υπό ειδικές περιστάσεις που ορίζονται στο άρθρο. 21 GDPR, το υποκείμενο των δεδομένων έχει το δικαίωμα να αντιταχθεί στην επεξεργασία που θα υποχρεώσει τον ελεγκτή να αποφύγει περαιτέρω επεξεργασία των προσωπικών δεδομένων του συγκεκριμένου ατόμου. Σε σύγκριση με την Οδηγία για την Προστασία των Δεδομένων, το δικαίωμα υποβολής αντιρρήσεων ενισχύεται σημαντικά στα πλαίσια του GDPR. Το άρθρο 21 παρέχει τρεις περιπτώσεις, οι οποίες μπορούν να αποτελέσουν δικαίωμα ένστασης για κάποιον.

Η πρώτη περίπτωση έχει να κάνει με το δικαίωμα στην ένσταση εάν το άτομο βρίσκεται σε μια ιδιαίτερη κατάσταση και η επεξεργασία βασίζεται στα νομικά συμφέροντα του Υπευθύνου διαχείρισης ή την εκτέλεση των καθηκόντων/ άσκηση δημόσιας εξουσίας από τον τελευταίο. Αυτό συνεπάγεται ότι έχουν προκύψει νέα δεδομένα τα οποία επηρεάζουν άμεσα την εξισορρόπηση των συμφερόντων. Ο κανονισμός παρ όλα αυτά προβλέπει δυο αντί-εξαιρέσεις από το δικαίωμα της ένστασης, εάν ο Υπεύθυνος διαχείρισης:

- Παρουσιάσει επιτακτικούς νομικούς λόγους που υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του ατόμου ή

- ότι η επεξεργασία εξυπηρετεί τη σύσταση, την άσκηση ή την υπεράσπιση νομικών απαιτήσεων.

Η δεύτερη περίπτωση έχει να κάνει με την επεξεργασία προσωπικών δεδομένων για σκοπούς Άμεσου Μάρκετινγκ. Άμεσο μάρκετινγκ αποτελεί η άμεση (ειδικά εξατομικευμένη) επικοινωνία με τα άτομα για σκοπούς μάρκετινγκ, για παράδειγμα μέσω ηλεκτρονικού ταχυδρομείου ή μέσω διαφημίσεων σε ιστότοπους ή σε εφαρμογές. Το άτομο έχει το δικαίωμα να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία των προσωπικών του δεδομένων για την εν λόγω εμπορική προώθηση, η οποία περιλαμβάνει τη δημιουργία προφίλ, στο βαθμό τον οποίο το τελευταίο σχετίζεται με το άμεσο Μάρκετινγκ.

Η τελευταία περίπτωση αναφέρεται στο δικαίωμα ένστασης, όταν η επεξεργασία δεδομένων πραγματοποιείται για σκοπούς επιστημονικής/ ιστορικής έρευνας ή για στατιστικούς λόγους. Η εφαρμογή του δικαιώματος σε αυτή την περίπτωση έχει νόημα, καθώς συνήθως αναφέρεται στην μαζική επεξεργασία δεδομένων, η οποία μπορεί να αποδώσει μια τεράστια ποσότητα γνώσης, αλλά, ταυτόχρονα, θέτει τα δικαιώματα και τις ελευθερίες των ατόμων σε κίνδυνο. Σύμφωνα με το GDPR, ως «στατιστικοί σκοποί» νοείται η επεξεργασία προσωπικών δεδομένων αναγκαία για στατιστικές έρευνες ή για την παραγωγή στατιστικών αποτελεσμάτων που ενδέχεται να χρησιμοποιηθούν περαιτέρω για διάφορους σκοπούς. Η εισαγωγή ειδικών κανόνων για στατιστικούς σκοπούς στον Κανονισμό αμφισβητήθηκε έντονα καθ' όλη τη διάρκεια της νομοθετικής διαδικασίας δεδομένου ότι οι «στατιστικοί στόχοι» δεν πρέπει απαραίτητα να εξυπηρετούν επιστημονικά συμφέροντα ή άλλα συμφέροντα κοινής ωφέλειας, αλλά μπορούν να πραγματοποιηθούν από διάφορους φορείς με σκοπό την δημιουργία στατιστικές επιχειρήσεων ή πελατών. Το δικαίωμα ένστασης για την επεξεργασία δεδομένων για ερευνητικούς ή στατιστικούς σκοπούς περιορίζεται δεδομένου ότι εξαιρείται εάν η επεξεργασία είναι απαραίτητη για την εκτέλεση μιας εργασίας που πραγματοποιείται υπέρ του δημόσιου συμφέροντος. Ο υπεύθυνος της διαχείρισης θα είναι υποχρεωμένος να το αποδείξει αυτό, ωστόσο, αρκετά συχνά οι ερευνητικοί ή στατιστικοί στόχοι συμβαδίζουν με το δημόσιο συμφέρον, καθώς η απόκτηση γνώσεων είναι συνήθως προς το συμφέρον της κοινωνίας.

Πρέπει να σημειωθεί ότι, σύμφωνα με το άρθρο 23 του GDPR, η νομοθεσία της Ευρωπαϊκής Ένωσης ή των κρατών μελών της μπορεί να περιορίσει το πεδίο εφαρμογής των δικαιωμάτων των ατόμων που αφορούν τα δεδομένα και των αντίστοιχων υποχρεώσεων, όταν ένας τέτοιος περιορισμός σέβεται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών και είναι ένα απαραίτητο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διαφύλαξη ορισμένων από τους στόχους που απαριθμούνται παρακάτω. Το GDPR επιτρέπει όχι μόνο την θέσπιση νέας νομοθεσίας αλλά και την τήρηση της προϋπάρχουσας νομοθεσίας, αρκεί να είναι σύμφωνη με τον Κανονισμό.

Σύμφωνα με το άρθρο 23, μια τέτοια νομοθεσία μπορεί να θεσπιστεί ή να διατηρηθεί αρκεί να εξυπηρετεί ενός από τους παρακάτω στόχους:

1. Εθνική ασφάλεια

2. Άμυνα
3. Δημόσια ασφάλεια ·
4. Την πρόληψη, διερεύνηση ή δίωξη αξιόποινων πράξεων ή την εκτέλεση ποινικών κυρώσεων
5. Άλλους σημαντικούς στόχους γενικού δημόσιου συμφέροντος της ΕΕ ή ενός Κράτους μέλους
6. Την προστασία της δικαστικής ανεξαρτησίας και των διαδικασιών της
7. Την πρόληψη, διερεύνηση, ανίχνευση και δίωξη παραβιάσεων δεοντολογίας για νομοθετικά κατοχυρωμένα επαγγέλματα.
8. Παρακολούθηση, επιθεώρηση ή ρυθμιστική λειτουργία συνδεδεμένη, έστω και περιστασιακά, στην άσκηση δημόσιας εξουσίας στις προαναφερθείσες περιπτώσεις (εκτός από την προστασία της δικαστικής ανεξαρτησίας και των διαδικασιών της)
9. Την επιβολή των αξιώσεων του αστικού δικαίου

ΚΕΦΑΛΑΙΟ 7 – ΕΠΙΒΟΛΗ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ ΚΑΙ ΕΛΕΓΧΟΣ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

7.1 Επικοινωνία των επιχειρήσεων με τις Εποπτικές Αρχές

Σε σύγκριση με την Οδηγία για την Προστασία των Δεδομένων, το GDPR εισάγει εκτεταμένες αλλαγές όσον αφορά την αρμοδιότητα και τη συνεργασία των εθνικών εποπτικών αρχών. Κάθε κράτος μέλος της Ευρωπαϊκής Ένωσης διαθέτει δική του Εποπτική Αρχή, η οποία ως ανεξάρτητη δημόσια αρχή είναι υπεύθυνη για την παρακολούθηση της εφαρμογής του GDPR, σύμφωνα με το άρθρο 4. Περαιτέρω στην αποστολή τους περιλαμβάνεται η προστασία των θεμελιωδών δικαιωμάτων και οι ελευθεριών των ατόμων σε σχέση με την επεξεργασία των προσωπικών τους δεδομένων και η διευκόλυνση της νόμιμης ροής προσωπικών δεδομένων εντός της Ένωσης. Συχνά, η επεξεργασία των προσωπικών δεδομένων πραγματοποιείται σε παραπάνω από μια χώρες μέλη ή επηρεάζει άτομα τα οποία βρίσκονται σε διαφορετικές χώρες. Έτσι, παραπάνω από μια Εποπτικές Αρχές ενδέχεται να ασχοληθούν με μια μεμονωμένη περίπτωση. Για να επιλύσετε πιθανά προβλήματα, το GDPR εισάγει ένα μηχανισμό ενιαίας αρμοδιότητας που ορίζει μόνο μια εποπτική αρχή ως αρμόδια για μια συγκεκριμένη υπόθεση.

Σύμφωνα με το άρθρο 56 του GDPR, μία Εποπτική αρχή (Lead Supervisory Authority) ενεργεί ως μοναδικό σημείο επαφής για τον Υπεύθυνο διαχείρισης / Υπεύθυνο επεξεργασίας των οποίων οι δραστηριότητες επεξεργασίας επηρεάζουν πολλά κράτη μέλη της Ευρωπαϊκής Ένωσης. Θα αποτελεί τον οργανισμό οποίος αναλαμβάνει την ευθύνη για την αλληλεπίδραση με το Υπεύθυνο διαχείρισης / Υπεύθυνο επεξεργασίας εξ ονόματος όλων των εμπλεκομένων Εθνικών εποπτικών Αρχών Η επιλογή αυτής της ενιαίας Εποπτικής Αρχής συνοδεύεται από μηχανισμούς συνεργασίας και συνέπειας που θα απλοποιήσει περαιτέρω την κατάσταση για τις υπόλοιπες εθνικές αρχές. Επίσης αποτελεί μεγάλο πλεονέκτημα για τις επιχειρήσεις, οι οποίες γενικά θα αλληλεπιδρούν μόνο με μια ενιαία εποπτική αρχή, γεγονός που θα εξαλείψει τις προσπάθειές τους για αλληλεπίδραση με διαφορετικές αρχές. Έτσι, οι επιχειρήσεις θα πρέπει να προσπαθήσουν να προσδιορίσουν εγκαίρως ποια εποπτική αρχή είναι πιθανόν να αποτελέσουν το ενιαίο σημείο επαφής τους. Δυστυχώς, η θετική δράση του μηχανισμού της Lead Supervisory Authority μειώνεται με διαφορετικές εξαιρέσεις και παράλληλες απαιτήσεις. Σε ορισμένες περιπτώσεις, η τοπική αρμοδιότητα των εθνικών εποπτικών αρχών παραμένει σε ισχύ. Ακόμη και όταν έχει ορισθεί Εποπτική αρχή (Lead Supervisory Authority) , οι συνεργαζόμενες εθνικές εποπτικές αρχές ενδέχεται να μην είναι σε θέση να καταλήξουν σε συμφωνία ως προς την τελική τους απόφαση για μια συγκεκριμένη περίσταση. Σε μια τέτοια περίπτωση, τα άτομα ενδέχεται να αντιμετωπίσουν νομικές αβεβαιότητες έως ότου ληφθεί τελική απόφαση από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων.

Από την πλευρά των επιχειρήσεων είναι ιδιαίτερα σημαντικό, μέσω των Υπευθύνων Διαχείρισης/επεξεργασίας να προσδιορίσουν το συντομότερο δυνατό την αρμόδια Εποπτική αρχή τους, με σκοπό την εμπρόθεσμη εκπλήρωση διαφόρων οργανωτικών απαιτήσεων στο πλαίσιο του GDPR. Στην περίπτωση που μιλάμε για πολυεθνικές επιχειρήσεις, με βάσεις σε διαφορετικές χώρες, θα πρέπει αρχικά να επιλεχθεί η κύρια έδρα τους, προτού οριστεί μία Άρχουσα Εποπτική αρχή (Lead Supervisory Authority). Αυτό, ίσως παρουσιάσει κάποιες δυσκολίες αν αναλογιστούμε τον μη αυστηρό ορισμό της έννοιας "έδρα" στη νομοθεσία της Ευρωπαϊκής Ένωσης. Η ύπαρξη αυτής της έδρας, σε μια συγκεκριμένη χώρα, πρέπει να προσδιοριστεί με βάση τις συγκεκριμένες συνθήκες και χρησιμοποιώντας συγκεκριμένα κριτήρια Σύμφωνα με το άρθρο 4, ως Κύρια Βάση μιας εταιρίας μπορεί να οριστεί:

- Η τοποθεσία της κεντρικής διοίκησής της στην Ευρωπαϊκής Ένωσης, εκτός εάν οι αποφάσεις σχετικά με τους σκοπούς και τα μέσα επεξεργασίας προσωπικών δεδομένων για τον Υπεύθυνο διαχείρισης λαμβάνονται σε άλλο κράτος μέλος, και εάν η τελευταία αυτή τοποθεσία έχει την εξουσία να λάβει τέτοιες αποφάσεις, αυτή θα θεωρείται ως η κύρια εγκατάσταση.
- Η τοποθεσία της κεντρικής διαχείρισης ενός Υπευθύνου επεξεργασίας και σε περίπτωση που ο Υπεύθυνος επεξεργασίας, δεν έχει ορίσει μια τέτοια τοποθεσία, ορίζεται εκείνη όπου πραγματοποιούνται οι κύριες δραστηριότητες επεξεργασίας δεδομένων που υπάγονται στον GDPR.

Για να επιβεβαιωθεί η εύκολη πρόσβαση των εταιριών στις εποπτικές αρχές και για να αποφευχθεί το φαινόμενο του forum shopping, έχουν υλοποιηθεί διάφοροι μηχανισμοί που ορίζουν την επικοινωνία των εποπτικών αρχών με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Το Συμβούλιο αυτό αποτελεί ένα νέο ανεξάρτητο φορέα ελέγχου για την νομική προστασία προσωπικών δεδομένων σε επίπεδο Ευρωπαϊκής Ένωσης. Οι κανόνες σχετικά με τα καθήκοντα και την οργάνωση του Συμβουλίου καθορίζονται στα άρθρα 68-76 του Κανονισμού. Σύμφωνα με αυτά, το Συμβούλιο αποτελείται από τους επικεφαλείς της Εποπτικής Αρχής κάθε κράτους μέλους της Ευρωπαϊκής Ένωσης και τον Προϊστάμενο Προστασίας Ευρωπαϊκών Δεδομένων. Κύριος ρόλος του οργάνου είναι η λήψη τελικών αποφάσεων στο πλαίσιο των μηχανισμών συνεργασίας και συνέπειας του GDPR. Ο στόχος των μηχανισμών συνεργασίας είναι η αποτελεσματική ανταλλαγή πληροφοριών και την αμοιβαία συνδρομή από τις εθνικές εποπτικές αρχές προκειμένου να επιτευχθεί συναίνεση ως προς την απόφαση σε μια συγκεκριμένη περίπτωση. Αντίστοιχα, ο μηχανισμός συνέπειας θα ενεργοποιείται μόνο σε περίπτωση που η συνεργασία των εποπτικών αρχών δεν μπορεί να οδηγήσει σε συναίνεση. Τέλος, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων θα είναι το τελικό σημείο έκδοσης γνωμοδοτήσεων και δεσμευτικών αποφάσεων για την επίλυση διαφωνιών μεταξύ των ενδιαφερόμενων εποπτικών αρχών.

7.2 Επιβολή του κανονισμού και πρόστιμα

Για να μπορέσουν οι εποπτικές αρχές να εκπληρώσουν τα νέα εκτεταμένα καθήκοντά τους, η εξουσία ελέγχου που τους παραχωρείται έχει περιγραφεί λεπτομερώς στο άρθρο 58 παράγραφος 1 του GDPR. Καθώς ο Κανονισμός είναι άμεσα εφαρμόσιμος σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης, η εξουσία αυτή θα είναι ευρέως συνεπής σε ολόκληρη την Ένωση. Η εν λόγω συνέπεια θα επιφέρει πλεονεκτήματα για την επεξεργασία προσωπικών δεδομένων, λόγω του ότι οι επιχειρήσεις γνωρίζουν εκ των προτέρων το εύρος των ελέγχων και την δικαιοδοσία των Αρχών. Ωστόσο, στο άρθρο 58 περιέχεται ρήτρα που επιτρέπει σε κάθε κράτος μέλος της Ένωσης να εισαγάγει πρόσθετες εξουσίες στην εθνική του νομοθεσία. Σύμφωνα με το άρθρο 58 η εξουσία ελέγχου που έχει κάθε εθνική Εποπτική αρχή περιλαμβάνει:

- Το δικαίωμα να απαιτήσει από τον Υπεύθυνο διαχείρισης, τον Υπεύθυνο επεξεργασίας, ή τον αντίστοιχο εκπρόσωπο στην Ευρωπαϊκή Ένωση, την παροχή των πληροφοριών που απαιτούνται για την εκτέλεση των καθηκόντων της Εποπτικής Αρχής. Αυτό συμβαδίζει με το άρθρο 31 και την γενικότερη απαίτηση προς τις επιχειρήσεις για συνεργασία.
- Το δικαίωμα της διεξαγωγής ερευνών με τη μορφή ελέγχων για την προστασία των προσωπικών δεδομένων. Οι Εποπτικές αρχές θα καθορίσουν το πεδίο εφαρμογής και τον λόγο για τον έλεγχο, δεδομένου ότι και τα δύο δεν προβλέπονται από το νόμο. Τέτοιοι έλεγχοι δύναται να διεξαχθεί στις εγκαταστάσεις του υπεύθυνου Διαχείρισης/ επεξεργασίας, μέσω της πρόσβασης στα συστήματα πληροφορικής της αντίστοιχης επιχείρησης ή μέσω συνολικών αιτήσεων για πληροφορίες.
- Το δικαίωμα να πραγματοποιήσει επιθεώρηση σχετικά με μια συγκεκριμένη Πιστοποίηση.
- Την υποχρέωση να κοινοποιεί στον Υπεύθυνο Διαχείρισης/ επεξεργασίας μια εικαζόμενη παράβαση του GDPR. Εάν κατά τον έλεγχο από τις εποπτικές αρχές, βρεθεί ένα συγκεκριμένου περιστατικό που έχει χαρακτηριστεί ως πιθανή παράβαση του GDPR, η επιχείρηση πρέπει να ειδοποιηθεί το συντομότερο δυνατόν.
- Την πρόσβαση σε όλα τα προσωπικά δεδομένα και σε όλες τις απαραίτητες πληροφορίες για την εκτέλεση των καθηκόντων της.
- Την πρόσβαση σε οποιαδήποτε εγκατάσταση του υπεύθυνο Διαχείρισης / επεξεργασίας, συμπεριλαμβανομένων όλων των εξοπλισμών και μέσων επεξεργασίας δεδομένων, σε συμφωνία με το δίκαιο των κρατών μελών. Η διάταξη αυτή παρέχει στις Εποπτικές Αρχές την εξουσία να διεξάγουν αιφνιδιαστικές επιτόπιες επιθεωρήσεις. Καθώς όμως, τα μέτρα της έρευνας πρέπει να είναι κατάλληλα, αναγκαία και αναλογικά των πιθανών παραβιάσεων, σε ορισμένες περιπτώσεις, μια ειδοποίηση θα πρέπει να υπάρξει πριν από την επιθεώρηση.

Ο Κανονισμός στο άρθρο 82 του περιλαμβάνει το δικαίωμα αποζημίωσης των ατόμων για οποιαδήποτε ζημιά, υλική ή μη, την οποία υπέστησαν ως παράβαση του GDPR. Το δικαίωμα αυτό δεν περιορίζεται σε ορισμένες φάσεις επεξεργασίας δεδομένων ή ορισμένες διαδικασίες. Επιπλέον, η έννοια της παραβίασης του GDPR πρέπει να ερμηνεύεται με ένα ευρύ τρόπο και, συνεπώς, περιλαμβάνει επεξεργασία που παραβιάζει τον Κανονισμό αλλά και την νομοθεσία των κρατών μελών. Υπό αυτό το πρίσμα, οι εταιρίες πρέπει να είναι σε εγρήγορση όσον αφορά την ύπαρξη εθνικών ιδιαιτεροτήτων στην επεξεργασία προσωπικών δεδομένων.

Μια σημαντική καινοτομία του GDPR αποτελεί ότι ο Υπεύθυνος διαχείρισης μπορεί να θεωρηθεί άμεσα υπεύθυνος για παραβιάσεις των υποχρεώσεών του βάσει του GDPR. Στην πραγματικότητα, και ο Υπεύθυνος διαχείρισης και ο Υπεύθυνος επεξεργασίας είναι υπόχρεοι σύμφωνα με το άρθρο 82. Διευκρινίζεται όμως ότι ο υπεύθυνος της Διαχείρισης φέρει την ευθύνη για την παράνομη επεξεργασία και, ως εκ τούτου, πρέπει να αποζημιώσει τυχόν ζημίες που προκύπτουν από αυτή ανεξάρτητα από το αν προκάλεσε άμεσα τη ζημία ή όχι.

Η συνολική του ευθύνη προκύπτει από τον προσδιορισμό των σκοπών και των μέσων επεξεργασίας, καθώς και την εξουσία του να δίνει εντολές στους Υπεύθυνους επεξεργασίας ως προς την διεξαγωγή της επεξεργασίας. Λαμβάνοντας υπόψη το γεγονός ότι ο Υπεύθυνος επεξεργασίας ενεργεί για λογαριασμό του Υπεύθυνου διαχείρισης, η ευθύνη του πρώτου περιορίζεται στις ζημίες που απορρέουν από τις παραβιάσεις των δικών του υποχρεώσεων στο πλαίσιο του Κανονισμού ή όπου αυτός ενήργησε εκτός ή σε αντίθεση με τις νόμιμες οδηγίες του Υπεύθυνου διαχείρισης. Έτσι, ο Υπεύθυνος επεξεργασίας είναι προνομιούχος, καθώς είναι υπεύθυνος μόνο σε περιορισμένες περιπτώσεις.

Με βάση τις ευθύνες αυτές ο Κανονισμός προβλέπει αυστηρά πρόστιμα τα οποία μπορεί να φτάσουν τα 20 εκατ. Ευρώ ή το 4% του συνολικού ετήσιου κύκλου εργασιών παγκοσμίως για το προηγούμενο οικονομικό έτους, όποιο είναι υψηλότερο. Κατά κύριο λόγο οι εποπτικές αρχές πριν από την επιβολή ενός προστίμου θα πρέπει να λαμβάνουν υπ’ όψιν τους:

- Τη φύση, τη σοβαρότητα και τη διάρκεια της παράβασης.
- Τον εκ προθέσεως χαρακτήρα της παράβασης.
- Τα μέτρα που ελήφθησαν για τον μετριασμό της ζημίας που υπέστη.
- Βαθμός ευθύνης ή τυχόν σχετικές προηγούμενες παραβάσεις.
- Τον τρόπο με τον οποίο έγινε γνωστή η παράβαση στον εποπτικό φορέα.
- Συμμόρφωση με τα μέτρα που διατάχθηκαν κατά του Υπεύθυνου διαχείρισης επεξεργασίας.
- Τήρηση ενός Κώδικα δεοντολογίας.

ΚΕΦΑΛΑΙΟ 8 – ΕΙΔΙΚΕΣ ΠΕΡΙΠΤΩΣΕΙΣ

8.1 Εθνικές ιδιαιτερότητες και GDPR

Το GDPR δεν απαιτεί κάποια αναθεώρηση στην εθνική νομοθεσία των κρατών μελών της Ευρωπαϊκής Ένωσης, δεδομένου ότι θεωρείται άμεσα εφαρμόσιμη ως νομοθεσία σε αυτά. Ωστόσο, διατηρεί έναν χαρακτήρα γενικού Κανονισμού ο οποίος επιτρέπει στα κράτη μέλη της Ένωσης να θεσπίσουν εθνική νομοθεσία για συγκεκριμένους τομείς της προστασίας προσωπικών δεδομένων. Ορισμένοι από αυτούς τους τομείς έχουν πολύ μεγάλη πρακτική σημασία καθώς αποτελούν μέρος της καθημερινής επιχειρηματικής δραστηριότητας πολλών επιχειρήσεων. Δεδομένου ότι οι αντίστοιχοι εθνικοί νόμοι των κρατών μελών της Ευρωπαϊκής Ένωσης είναι πιθανόν να έχουν μεγάλες διαφορές στον βαθμό προστασίας των δεδομένων, θα πρέπει οι επιχειρήσεις να είναι πολύ προσεκτικές όσον αφορά την ύπαρξη εθνικών ιδιαιτεροτήτων. Μερικά άρθρα του Κανονισμού, τα οποία έχουν ρήτρες σχετικά με το δικαίωμα των κρατών να θεσπίσουν νομοθεσίες για περαιτέρω διασαφήνιση του GDPR είναι τα παρακάτω:

Όρος του Κανονισμού

Αντικείμενο θέματος

Περιεχόμενο ρήτρας

Άρθρο 4 Σημείο 7

<u>Ορισμός του Υπεύθυνου Διαχείρισης:</u>

Αναφορικά με τους σκοπούς και τα μέσα ορισμένων δραστηριοτήτων επεξεργασίας δεδομένων, ο Υπεύθυνος Διαχείρισης ή τα κριτήρια για το διορισμό του μπορούν να οριστούν από τη νομοθεσία του κράτους μέλους της ΕΕ.

Άρθρο 6 Παράγραφος 2

<u>Νομιμότητα επεξεργασίας:</u>

Τα κράτη μέλη της ΕΕ μπορούν να διατηρούν ή να θεσπίσουν πιο συγκεκριμένες διατάξεις όσον αφορά τη νομιμότητα της:

(i) επεξεργασίας βάσει νόμιμων αρμοδιοτήτων του Υπεύθυνου Διαχείρισης ή της

ii) επεξεργασίας που πραγματοποιείται βάσει του δημοσίου συμφέροντος καθορίζοντας με σαφήνεια ειδικές απαιτήσεις για τη διασφάλιση μιας νόμιμης και δίκαιης επεξεργασίας.

Άρθρο 8 Παράγραφος 1

Όροι που ισχύουν για την συγκατάθεση του παιδιού σε σχέση με Υπηρεσίες Πληροφοριών:

Η νομοθεσία των Κρατών Μελών μπορεί να επιτρέψει μικρότερη ηλικία για την συγκατάθεση παιδιών, σχετικά με τα προσωπικά τους δεδομένα, με την προϋπόθεση ότι δεν θα είναι μικρότερη των 13 ετών.

Άρθρο 9 Παράγραφος 2

Επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων:

Τα κράτη μέλη της ΕΕ μπορούν να ορίσουν διαφορετικές διατάξεις σχετικά ειδικές κατηγορίες προσωπικών δεδομένων, πχ για να αποκλείσουν την επεξεργασία χωρίς την συγκατάθεση ή την επεξεργασία στα πλαίσια της εργασιακής σχέσης κ.α. .

Άρθρο 9 Παράγραφος 4

Επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων:

Τα κράτη μέλη της ΕΕ μπορούν να ορίσουν διαφορετικές διατάξεις, συμπεριλαμβανομένων περιορισμών, σχετικά με την επεξεργασία γενετικών, βιομετρικών δεδομένων κ.τ.λ.

Άρθρο 10

Επεξεργασία προσωπικών δεδομένων που αφορούν ποινικά αδικήματα και καταδίκες:

Επεξεργασία προσωπικών δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα μπορεί να διεξαχθεί όταν επιτρέπεται από το δίκαιο των κρατών μελών της ΕΕ.

Άρθρο 14 Παράγραφος 5

Παροχή πληροφοριών όταν τα προσωπικά δεδομένα:

Η υποχρέωση ενημέρωσης του ατόμου από τον Υπεύθυνο δεν συλλέχθηκαν από το άτομο στο οποίο αναφέρονται διαχείρισης, δεν υφίσταται εάν αυτό ορίζεται από το δίκαιο των κρατών μελών της ΕΕ ή όπου τα προσωπικά δεδομένα πρέπει να παραμείνουν απόρρητα βάση επαγγελματικού απορρήτου.

Άρθρο 17 Παράγραφος 1

Δικαίωμα της διαγραφής:

Ο Υπεύθυνος Διαχείρισης είναι υποχρεωμένος να διαγράψει προσωπικά δεδομένα με βάση τις υποχρεώσεις του προς το δίκαιο του κράτους μέλους της ΕΕ στο οποίο υπόκειται. Ταυτόχρονα, το δικαίωμα διαγραφής δεν ισχύει εάν προκύψει ότι απαιτείται επεξεργασία με βάση μια νόμιμη διαδικασία του ίδιου δικαίου.

Άρθρο 22 Παράγραφος 2

Αυτοματοποιημένη λήψη αποφάσεων, αναφορικά με την επεξεργασία:

Η γενική απαγόρευση της Αυτοματοποιημένης λήψης αποφάσεων δεν εφαρμόζεται σε περίπτωση που η τελευταία επιτρέπεται από κράτος μέλος της ΕΕ στο οποία υπόκειται ο Υπεύθυνος Διαχείρισης.

Άρθρο 23

Περιορισμοί:

Το δίκαιο των κρατών μελών της ΕΕ μπορεί να περιορίσει την εφαρμογή των δικαιωμάτων των ατόμων και τις αντίστοιχες υποχρεώσεις επεξεργασίας δεδομένων από τις επιχειρήσεις για διάφορους λόγους που συνδέονται με το δημόσιο συμφέρον.

Άρθρο 26

Πολλαπλοί Υπεύθυνοι Διαχείρισης:

Το δίκαιο των κρατών μελών της ΕΕ μπορεί να ορίσει τις ευθύνες πολλαπλών Υπεύθυνων Διαχείρισης.

Άρθρο 28 Παράγραφος 3

Υπεύθυνος Διαχείρισης:

Το δίκαιο των κρατών μελών της ΕΕ μπορεί να:

- Επιτρέψει στους Υπεύθυνους επεξεργασίας να επεξεργαστούν δεδομένα χωρίς την άδεια του Υπεύθυνου διαχείρισης
- Απαιτήσει την μη διαγραφή των προσωπικών δεδομένων, μετά τις υπηρεσίες τους προς τον Υπεύθυνο Διαχείρισης
- Θεσπίσει κανόνες σχετικά με τις δικαιοδοσίες των υπο-Υπεύθυνων επεξεργασίας

Άρθρο 32 Παράγραφος 4

Ασφάλεια της επεξεργασίας δεδομένων :

Το δίκαιο των κρατών μελών της ΕΕ μπορεί να επιτρέψει σε άτομα τα οποία αναφέρονται στους Υπεύθυνους Διαχείρισης / Επεξεργασίας, να πραγματοποιήσουν επεξεργασία δεδομένων χωρίς την έγκριση αυτών των Υπεύθυνων Διαχείρισης/Επεξεργασίας.

Άρθρο 35 Παράγραφος 10

Data Protection Impact Assessment:

Μια αξιολόγηση DPIA δεν θεωρείται απαραίτητη, εάν έχει πραγματοποιηθεί ήδη μια γενική αξιολόγηση στο πλαίσιο της νομοθεσίας του Κράτους μέλους, αρκεί αυτή να συνάδει με το άρθρο 6, παράγραφο 2 του Κανονισμού.

Άρθρο 36 Παράγραφος 5

Προγενέστερη διαβούλευση:

Το δίκαιο των κρατών μελών της ΕΕ μπορεί να επιβάλει την προγενέστερη διαβούλευση και απόκτηση έγκρισης από την Εποπτική αρχή, πριν πραγματοποιηθεί μια επεξεργασία δεδομένων υπέρ του δημοσίου συμφέροντος.

Άρθρο 37 Παράγραφος 4

Διορισμός του DPO - Data Protection Officer:

Το δίκαιο των κρατών μελών της ΕΕ μπορεί να επιβάλει επιπλέον υποχρεώσεις στους Υπεύθυνους διαχείρισης/Επεξεργασίας για τον διορισμό του DPO.

Άρθρο 39 Παράγραφος 1

Αρμοδιότητες του DPO:
Ο DPO έχει ως αρμοδιότητα την ενημέρωση των επιχειρήσεων για τις υποχρεώσεις τους ως προς την προστασία των δεδομένων υπό την νομοθεσία των κρατών μελών και να επιβλέπει τη συμμόρφωση με αυτές.

Άρθρο 49 Παράγραφος 1

Εξαιρέσεις σε ορισμένες περιπτώσεις:

Μια μεταφορά δεδομένων σε τρίτη χώρα μπορεί να είναι νόμιμη με βάση το δημόσιο συμφέρον του Κράτους μέλους της ΕΕ. Αντίστοιχα το Δίκαιο των κρατών μελών της ΕΕ μπορεί να περιορίσει τις μεταφορές προσωπικών δεδομένων προς τρίτες χώρες για λόγους δημοσίου συμφέροντος.

Άρθρο 58 Παράγραφος 1

Εξουσίες:
Οι επιθεωρήσεις στις εγκαταστάσεις των επιχειρήσεων από τις εποπτικές αρχές πρέπει να είναι σύμφωνες με το Δίκαιο των κρατών μελών .

Άρθρο 84 Παράγραφος 1

Ποινές:

Τα κράτη μέλη της ΕΕ έχουν το δικαίωμα να καθορίσουν μόνα τους τις κυρώσεις για παραβιάσεις του GDPR, ιδίως στις περιπτώσεις που οι παραβάσεις δεν υπόκεινται σε πρόστιμο υπό τον Κανονισμό

8.2 Επεξεργασία ειδικών δεδομένων (Big data, Internet of things, Cloud computing)

Η τεχνολογική πρόοδος φέρνει στο φως νέους τρόπους και δυνατότητες επεξεργασίας δεδομένων. Τεράστιες ποσότητες δεδομένων μπορούν να υποβάλλονται σε επεξεργασία με ολοένα και πιο εύκολο, γρήγορο και οικονομικά αποδοτικό τρόπο. Αυτό ανοίγει νέες επιχειρηματικές ευκαιρίες, αλλά, ταυτόχρονα, θέτει σε κίνδυνο το δικαίωμα στην ιδιωτικότητα. Για την αποτελεσματική προστασία των ατόμων, οι διατάξεις του GDPR διατυπώνονται με έναν γενικά αφηρημένο τρόπο. Σύμφωνα με αυτή την λογική, ορισμένοι φορείς επέκριναν την έλλειψη σαφών και ειδικών διατάξεων για την ηλεκτρονική επεξεργασία Δεδομένων και συγκεκριμένα για αυτές που έχουν μεγάλη εφαρμογή: το cloud computing, τα μέσα κοινωνικής δικτύωσης, το marketing με βάση την συμπεριφορά των ατόμων και άλλα. Όμως, αυτό το επίπεδο μη εξειδίκευσης επιτρέπει στο GDPR να είναι ανεξάρτητο από τις τεχνολογικές αλλαγές και, συνεπώς, να έχει μεγαλύτερη βιωσιμότητα. Οι επιχειρήσεις που εκτελούν ειδικές δραστηριότητες επεξεργασίας δεδομένων θα πρέπει από μόνες τους να προσδιορίσουν σε ποια από τα δεδομένα που επεξεργάζονται έχει αρμοδιότητα το GDPR και πώς μπορούν να εκπληρώσουν τις υποχρεώσεις τους προς αυτό. Αξίζει παρ' όλα αυτά να γίνει αναφορά σε τρεις δημοφιλείς κατηγορίες τεχνολογιών επεξεργασίας δεδομένων, οι οποίες επηρεάζονται άμεσα από τον κανονισμό .

Ο όρος Big Data αναφέρεται σε μια συγκεκριμένη προσέγγιση της επεξεργασίας δεδομένων και όχι σε συγκεκριμένες τεχνικές αυτής. Πολλές επιχειρήσεις διαθέτουν διαφορετικές τεχνολογίες για να συλλέγουν, να επεξεργάζονται, να ταξινομούν και να αναλύουν τεράστιες ποσότητες δεδομένων, με τέτοιο τρόπο ώστε αυτά τα δεδομένα να παράγουν αξία. Τέτοιες μεγάλες εφαρμογές δεδομένων συχνά επεξεργάζονται δεδομένα, όπως οι καιρικές συνθήκες ή διαδικασίες μηχανών, αλλά πρόσφατα, όλο και περισσότερο χρησιμοποιούν τεράστιους όγκους προσωπικών δεδομένων των χρηστών για κατανόηση, πρόβλεψη και ,εν τέλει, την διαμόρφωση της ανθρώπινης συμπεριφοράς. Τυπικές δραστηριότητες Big data που αφορούν τα προσωπικά δεδομένα, αφορούν στην παρακολούθηση ατόμων, όπως για παράδειγμα με στοχευμένες διαφημίσεις, οι προβλέψεις και οι αναλύσεις συμπεριφοράς των χρηστών, που μετατρέπουν αυτά τα προσωπικά δεδομένα σε ένα πολύτιμο περιουσιακό στοιχείο. Οι δραστηριότητες αυτές μπορούν να ταξινομηθούν σε δύο κατηγορίες: ανάλυση συμπεριφοράς σχετικά με ομάδες ατόμων που λαμβάνουν χώρα σε ένα «Μακροοικονομικό επίπεδο» και ανάλυσης της συμπεριφοράς των ατόμων. Ιδιαίτερα, η ύπαρξη profile των χρηστών εν αγνοία τους έχει αναγνωριστεί από τον νομοθέτη της Ευρωπαϊκής Ένωσης, ως εξαιρετικά κρίσιμη επεξεργασία δεδομένων και συνεπώς, υπόκειται στο άρθρο 22 του Κανονισμού. Γενικότερα, εάν κάποιο σύνολο Big Data περιέχει προσωπικά δεδομένα, δηλαδή δεδομένα που μπορούν να ταυτιστούν ή να ταυτίσουν με ένα συγκεκριμένο άτομο, ανήκει στο πεδίο εφαρμογής του GDPR.

Δεδομένου του μεγάλου αριθμού και της ποικιλίας δεδομένων μέσα στα σύνολα Big Data, υπάρχει μεγάλη πιθανότητα να περιέχουν προσωπικά δεδομένα, π.χ. μέσω συνδυασμού των διαθέσιμων πληροφοριών. Εάν συμβαίνει αυτό, ολόκληρο το σύνολο δεδομένων εμπίπτει στο πεδίο εφαρμογής του GDPR.

Το Cloud computing αποτελείται από ένα σύνολο τεχνολογιών και υπηρεσιών που εστιάζουν στην χρήση εφαρμογών πληροφορικής, στην δυνατότητα επεξεργασίας και / ή αποθηκευτικού χώρου. Υπάρχει μια μεγάλη ποικιλία υπηρεσιών cloud που κυμαίνονται από εικονικά επεξεργαστικά συστήματα (virtual processing systems - στην ουσία υποδομή IT με απομακρυσμένη πρόσβαση), σε εφαρμογές διαδικτύου, όπως ημερολόγια, ηλεκτρονικό ταχυδρομείο ή σουίτες εφαρμογών γραφείου. Το Cloud computing προσφέρει τεχνικά και οικονομικά οφέλη στις επιχειρήσεις καθώς τους επιτρέπει να χρησιμοποιούν λύσεις Πληροφορικής υψηλής ποιότητας, που διαφορετικά θα ήταν εκτός του προϋπολογισμού τους και / ή δεν θα ήταν τεχνικά εφικτό γι' αυτές. Οι υπηρεσίες αυτές χρησιμοποιούνται συχνά για την επεξεργασία προσωπικών δεδομένων, όπως δεδομένα HR και επομένως εμπίπτουν στην δικαιοδοσία του GDPR.

Οι εταιρίες , χρησιμοποιώντας τις υπηρεσίες που τους παρέχονται από τις Cloud υπηρεσίες, ορίζουν τους σκοπούς και τα μέσα της επεξεργασίας των προσωπικών δεδομένων, αλλά οι λειτουργίες τελικά εκτελούνται από τους παρόχους των Cloud υπηρεσιών. Έτσι, σαν γενικός κανόνας, οι πελάτες των υπηρεσιών Cloud χαρακτηρίζονται ως Υπεύθυνοι διαχείρισης και οι πάροχοι υπηρεσιών cloud ως Υπεύθυνοι επεξεργασίας στο πλαίσιο του GDPR. Ωστόσο, πρέπει να υπάρχει αυστηρή κατανομή των υποχρεώσεων μεταξύ των διαφόρων φορέων, η οποία και θα καθορίζεται ανά περίπτωση. Όσο μεγαλύτερη επιρροή έχει ο πάροχος υπηρεσιών cloud στα μέσα και τους σκοπούς της επεξεργασίας, τόσο πιο πιθανό είναι να θεωρηθεί ως Υπεύθυνος διαχείρισης σύμφωνα με το GDPR. Για παράδειγμα, εάν ο πάροχος υπηρεσιών Cloud επεξεργάζεται τα προσωπικά δεδομένα για δικούς του σκοπούς, μπορεί να χαρακτηριστεί ως Υπεύθυνος διαχείρισης. Πρέπει να σημειωθεί ότι, παρόλο που οι πελάτες των υπηρεσιών cloud computing ενδέχεται να χρειαστεί να αποδεχθούν τους όρους του παρόχου υπηρεσιών και δεν έχουν περιθώρια διαπραγμάτευσης της σύμβασης, είναι ελεύθεροι να επιλέξουν μεταξύ διαφορετικών παρόχων και, να αποφασίσουν σχετικά με την κατανομή μέρους ή του συνόλου των εργασιών επεξεργασίας σε διαφορετικές υπηρεσίες cloud. Ως εκ τούτου, συνήθως φέρουν και την ευθύνη του Υπεύθυνου διαχείρισης.

Το Internet of Things, αναφέρεται σε μια υποδομή στην οποία υπάρχουν δισεκατομμύρια αισθητήρες ενσωματωμένοι σε κοινές, καθημερινές συσκευές, προσφέροντας συνεχή καταγραφή, επεξεργασία και μεταφορά δεδομένων, μετατρέποντας τις συσκευές αυτές σε «έξυπνες». Με βάση τα δεδομένα που συλλέγονται από τις συσκευές, προσφέρονται εφαρμογές και υπηρεσίες βασισμένες στην ανάλυση των δεδομένων που αντιστοιχούν στις συνήθειες ή τις δραστηριότητες του χρήστη, όπως το fitness tracking. Το IoT βασίζεται στην εκτεταμένη επεξεργασία δεδομένων που αφορούν το περιβάλλον και την

συμπεριφορά του χρήστη. Είναι ευνόητο, επομένως, πως η συγκεκριμένη διαδικασία επεξεργασίας δεδομένων εμπίπτει στην δικαιοδοσία του GDPR. Το πρόβλημα όμως που παρουσιάζεται στην συγκεκριμένη περίπτωση είναι πως οι χρήστες ενδέχεται να μην γνωρίζουν το βαθμό στον οποίο επεξεργάζονται τα δεδομένα τους μέσω κάποιων υπηρεσιών, δυσχεραίνοντας και την δυνατότητα από την πλευρά των εταιριών του να αποδείξουν ότι έχουν την συγκατάθεση των ατόμων. Έτσι, οι οργανισμοί που παρέχουν υπηρεσίες IoT θα πρέπει να αυξήσουν τις προσπάθειές τους για να παρέχουν στους χρήστες τους πληροφορίες σχετικά με τις προβλεπόμενες δραστηριότητες επεξεργασίας και για την απόκτηση έγκυρης συναίνεσης. Από την άποψη αυτή, θα μπορούσαν να εξετάσουν την ανάπτυξη νέων τρόπων απόκτησης συγκατάθεσης, συμπεριλαμβανομένης της εφαρμογής μηχανισμών συναίνεσης μέσω των ίδιων των συσκευών τους.

ΚΕΦΑΛΑΙΟ 9 – ΠΡΑΚΤΙΚΗ ΕΦΑΡΜΟΓΗ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

Όπως είναι ευνόητο οι επιχειρήσεις αντιμετωπίζουν πολλές νέες οργανωτικές υποχρεώσεις στο πλαίσιο του GDPR. Επιπλέον, καθώς ο κανονισμός έχει πολύ μεγάλο γεωγραφικό πλαίσιο εφαρμογής, επιχειρήσεις που βρίσκονται εκτός της Ευρωπαϊκής Ένωσης ενδέχεται να χρειαστεί να συμμορφωθούν με το GDPR. Επομένως, είναι ενδεδειγμένο για τις επιχειρήσεις, εάν δεν το έχουν κάνει ήδη καθώς ο κανονισμός βρίσκεται σε ισχύ από τις 25 Μαΐου 2018, να αναλογιστούν εάν βρίσκονται εντός της δικαιοδοσίας του και να προχωρήσουν στην απαραίτητη αναδιοργάνωση των εσωτερικών διαδικασιών τους. Όσον αφορά τους ομίλους επιχειρήσεων, θα πρέπει να αξιολογούν εάν είναι περισσότερο αποτελεσματικό να υλοποιήσουν μια πολιτική για την προστασία των προσωπικών δεδομένων για όλες τις οντότητες εντός του ομίλου ή αν κάθε οντότητα του ομίλου πρέπει να υλοποιήσει την δική της επιλογή. Αυτό πρέπει να καθορίζεται κατά περίπτωση, αλλά σε πολλές περιπτώσεις είναι σκόπιμο να υλοποιηθεί μια πολιτική για όλες ή πολλές οντότητες του ομίλου προκειμένου να εφαρμόσει μια ομοιόμορφη προσέγγιση για την προστασία των δεδομένων εντός του ομίλου.

Επιπρόσθετα, το GDPR αφήνει ένα σημαντικό περιθώριο στις εθνικές νομοθεσίες για να προσδιορίσουν τους κανόνες για την προστασία των προσωπικών δεδομένων. Έτσι, είναι πιθανό ότι διαφορετικά κράτη μέλη της Ευρωπαϊκής Ένωσης θα εισαγάγουν πρόσθετες απαιτήσεις προστασίας δεδομένων που οι επιχειρήσεις θα είναι υποχρεωμένες να εφαρμόσουν. Εάν οι επιχειρήσεις διεξάγουν δραστηριότητες επεξεργασίας δεδομένων σε διαφορετικά κράτη μέλη της Ευρωπαϊκής Ένωσης ή που επηρεάζουν πολλά κράτη μέλη της Ένωσης, πρέπει να ελέγξουν εάν οι λειτουργίες τους αυτές θα επηρεαστούν από τη νομοθεσία για την προστασία των δεδομένων σε εθνικό επίπεδο. Από την άποψη αυτή, οι κανόνες για την προστασία δεδομένων των παιδιών και των εργαζομένων αξίζουν ιδιαίτερης προσοχής.

Ιδιαίτερο ενδιαφέρον έχουν οι εκτιμήσεις για τον αντίκτυπο που θα έχει το GDPR στην Ευρώπη και στον κόσμο γενικότερα. Υπάρχει η αίσθηση ότι ο Κανονισμός θα δημιουργήσει ένα νέο πρότυπο σε παγκόσμιο επίπεδο για την προστασία των δεδομένων. Από την άλλη, υπάρχει η άποψη ότι οι επιχειρήσεις, αφού πραγματοποιήσουν εκτιμήσεις για το τι είναι πιο οικονομικά αποδοτικό για αυτές είτε θα προσαρμόσουν νέες παγκόσμιες πρακτικές ή θα προσφέρουν διαφορετικές υπηρεσίες σε διαφορετικές αγορές. Όποια και να είναι η αλήθεια, οι Ευρωπαίοι πολίτες βίωσαν τον αντίκτυπο του Κανονισμού, αρκετά νωρίτερα από την πρώτη μέρα εφαρμογής του. Δεκάδες ενημερωτικά emails έχουν σταλθεί από εταιρίες, οι οποίες σπεύδουν να κερδίσουν την συγκατάθεση των ατόμων, σχετικά με την επεξεργασία των προσωπικών τους δεδομένων. Αντίστοιχα, ενημερωτικά μηνύματα εμφανίζονται σε ιστοχώρους και εφαρμογές και σε όλες τις υπηρεσίες της Κοινωνίας της Πληροφορίας Ιδιαίτερα ανησυχητικό αποτελεί το γεγονός ότι στην επικοινωνία τους οι περισσότερες εταιρίες, διατηρούν έναν απειλητικό τόνο για απόλυτη συγκατάθεση αναφορικά με την χρήση των προσωπικών δεδομένων.

Συγκεκριμένα, δεν δίνεται η δυνατότητα στον χρήστη να επιλέξει τμηματικά ή την κατά περίπτωση χρήση των δεδομένων του. Ο χρήστης είναι αναγκασμένος να δώσει την απόλυτη συγκατάθεση του για την επεξεργασία των προσωπικών του δεδομένων ή να σταματήσει την χρήση της υπηρεσίας εντελώς.

Αυτός είναι και ο λόγος που δυο κολοσσοί του παγκόσμιου Internet, η Google και το Facebook, εταιρίες που είχαν προβλήματα με τους νόμους περί ιδιωτικότητας και στο παρελθόν, βρίσκονται ήδη αντιμέτωποι με πρόστιμα τα οποία μπορεί να αγγίξουν συνολικά τα 9.3 δις. Αμφότερες οι εταιρίες, σύμφωνα με δηλώσεις τους έχουν πάρει τα απαραίτητα μέτρα τους τελευταίους 18 μήνες για να συμβαδίσουν με τον Κανονισμό. Σύμφωνα, όμως, με την πρώτη προσφυγή εναντίον τους, οι εταιρείες γνώριζαν εξ αρχής πως τα μέτρα αυτά δεν είναι επαρκή. Ένα ακόμα αποτέλεσμα του Κανονισμού, κατά τις πρώτες ώρες λειτουργίας του, υπήρξε η αδυναμία των Ευρωπαίων χρηστών του διαδικτύου να έχουν πρόσβαση σε αρκετά αμερικανικά πρακτορεία ειδήσεων. Ιστοσελίδες, οι οποίες δεν πληρούσαν τις απαιτήσεις του Κανονισμού, όπως για παράδειγμα αυτές των Chicago Tribune και LA Times ήταν μεταξύ εκείνων που δήλωσαν ότι δεν ήταν διαθέσιμες στις περισσότερες ευρωπαϊκές χώρες.

Η εφαρμογή του Κανονισμού, όμως, δεν θα επηρεάσει μόνο συγκεκριμένες εταιρίες’ σε ορισμένες περιπτώσεις, θα επηρεάσει ολόκληρους κλάδους υπηρεσιών. Ορισμένοι κλάδοι πιθανότατα να ενδυναμώσουν τη θέση τους στην αγορά όπως μεγάλες επιχειρήσεις οι οποίες μπορούν να οργανώσουν το δικό τους σύστημα απόκτησης συγκατάθεσης ή υπηρεσίες που βασίζονται σε συνδρομές, αλλά σε ορισμένες περιπτώσεις τα αποτελέσματα είναι εκ διαμέτρου αντίθετα. Για παράδειγμα, δυο εταιρίες οι οποίες ασχολούνται με την διαδικτυακή διαφήμιση, η Verve και η Drawbridge σταμάτησαν τη λειτουργία τους στην Ευρώπη και ανέφεραν το GDPR, ως τον κύριο λόγο γι’ αυτό. Θα υπάρξουν και άλλοι που αποφασίζουν ότι η επιβάρυνση του κόστους για τη συμμόρφωση με τον Κανονισμό, καθώς και η δυσκολία λήψης της συγκατάθεσης των χρηστών όσων αφορά την επεξεργασία των δεδομένων τους για πολλαπλές χρήσεις, δεν αξίζει τον κόπο, ειδικά εάν τα ευρωπαϊκά έσοδα είναι ένα κλάσμα των αντίστοιχων από τις ΗΠΑ.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Albert J., Privacy on the Internet: Protecting and Empowering Users, EC Conference,

Data Protection Conference on the Implementation of Directive 95/46/EC, Workshop 2:Developments in the Information Society: Internet and Privacy Enhancing

Technologies,

http://europa.eu.int/comm/internal_market/privacy/lawreport/programme_en.htm

[2] Burkert H., Establishing the law applicable to the networks – Standards applicable to theInternet: Benefits and Limitations (general report 1), International Colloqium, Internet law – European and international approaches (Paris 2001),

http://droit-internet-2001.univ-paris1.fr/ve/page004.html

[3] Αλεξανδρής Ν., Γκρίτζαλης Δ., Κιουντούζης Ε., Μια προσέγγιση της κοινωνικά

αποδεκτής αξιοποίησης της Πληροφορικής σε ΕΠΥ, Ασφάλεια Πληροφοριών:

Τεχνικά, Νομικά και Κοινωνικά Θέματα, Αθήνα 1995, σελ. 381 επ.

[4] Ανθίμου Κ., Το δικαίωμα πληροφοριακού αυτοκαθορισμού του ατόμου ως έκφανση του

δικαιώματος επί της προσωπικότητας, ΚριτΕ 1998, σελ. 155 επ.

[5] Αραβαντινός Β., Η προστασία των στοιχείων προσωπικού χαρακτήρα από την αθέμιτη

επεξεργασία τους με ηλεκτρονικό υπολογιστή , Αθήνα – Κομοτηνή 1997.

[6] Αραβαντινός Β., Εισαγωγή στη Νομοπληροφορική και τη Δικαιοκυβερνητική, τόμος 1 ος ,

Νομοπληροφορική, Αθήνα – Κομοτηνή 1994.

[7] Αυγουστιανάκης Μ., Προστασία του ατόμου από την επεξεργασία προσωπικών

δεδομένων. Προβλήματα και αντιμετώπιση από το δίκαιο, σε : ΔτΑ, 2001, σελ. 673 επ.

[8] Γέροντας Απόστολος, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία

προσωπικών δεδομένων, Αθήνα-Κομοτηνή 2002.

[9] Γιαννόπουλος Γ., Προστασία προσωπικών δεδομένων και διασυνοριακή ροή

πληροφοριών. Το πρόβλημα του «ικανοποιητικού επιπέδου προστασίας», ΔτΑ

2001,σελ..733 επ.

[10] International Working Group on Data Protection in Telecommunications, Budapest-Berlin Memorandum",Report and Guidance on Data Protection and Privacy on the Internet (1996)

http://www.datenschutz-berlin.de/doc/int//iwgdpt/

[11]Αντώνιος Π. Χαρακίδας, Διπλωματική Εργασία: Νομιμοποίηση Εσόδων από Εγκληματικές Δραστηριότητες & Προστασία Προσωπικών Δεδομένων

[12]Βασίλειος Νικήτας, Μεταπτυχιακή Διατριβή: Ασφάλεια και Προστασία Προσωπικών Δεδομένων στο Διαδίκτυο.