Πανεπιστήμιο Πειραιώς
Σχολή Τεχνολογιών Πληροφορικής και Επικοινωνιών
Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ. Ασφάλεια Ψηφιακών Συστημάτων

Μεταπτυχιακή Διπλωματική Εργασία

Εκτίμηση Συμμόρφωσης με το Γενικό Κανονισμό Προστασίας Δεδομένων

Αλτόγλου Δημήτριος
ΜΤΕ1602
Μπότας Σπυρίδων
ΜΤΕ1625

Επιβλέπων:
Καθηγητής, Κωνσταντίνος Λαμπρινουδάκης

Πειραιάς, Σεπτέμβριος 2018

Σελίδα σκόπιμα κενή

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε τις οικογένειες μας για την υποστήριξη που προσέφεραν κατά την διάρκεια της ακαδημαϊκής μας πορείας. Παράλληλα νιώθουμε υπόχρεοι να εκφράσουμε τις θερμές μας ευχαριστίες σε όλους τους καθηγητές του μεταπτυχιακού προγράμματος σπουδών για την αστείρευτη όρεξη που έδειξαν κατά την διάρκεια των διαλέξεων και την συνεχή προσπάθεια διεύρυνσης του γνωσιακού μας επιπέδου. Τέλος, θα θέλαμε να ευχαριστήσουμε τον Καθηγητή του Τμήματος Ψηφιακών Συστημάτων κ. Λαμπρινουδάκη Κωνσταντίνο και τον επιστημονικό συνεργάτη του κ. Νικόλαο Λουκά για την ανάθεση της διπλωματικής εργασίας και για την καθοδήγηση κατά την εκπόνηση της.

Πειραιάς, Σεπτέμβριος 2018

Αλτόγλου Δημήτριος

Μπότας Σπυρίδων

Περίληψη

Στις 25 Μαΐου 2018 τέθηκε σε ισχύ ο Γενικός Κανονισμός Προστασίας Δεδομένων και έφερε ριζικές αλλαγές στον τρόπο διαχείρισης των δεδομένων προσωπικού χαρακτήρα. Οποιαδήποτε οντότητα επεξεργάζεται δεδομένα προσωπικού χαρακτήρα καλείται να συμμορφωθεί με τις απαιτήσεις και να εκτελέσει μια σειρά ενεργειών για την διασφάλιση της ιδιωτικότητας. Δεδομένης της ραγδαίας ανάπτυξης της τεχνολογίας, της πολυπλοκότητας των επιχειρησιακών διαδικασιών και του εύρους των δεδομένων που ενδέχεται να επεξεργάζεται μία επιχείρηση ή ένας οργανισμός, η προστασία των δεδομένων προσωπικού χαρακτήρα και η απόδειξη συμμόρφωσης εξελίσσεται σε ένα περίπλοκο και απαιτητικό εγχείρημα.

Με στόχο την διευκόλυνση του εγχειρήματος αυτού αποφασίστηκε η δημιουργία ενός εργαλείου εκτίμησης της συμμόρφωσης με το Γενικό Κανονισμό Προστασίας Δεδομένων το οποίο θα μπορεί να δώσει στον χρήστη το σύνολο των ενεργειών που απαιτείται να ολοκληρωθούν καθώς και την δυνατότητα αξιολόγησης του επιπέδου συμμόρφωσης. Η παρούσα εργασία αποτελεί συμπληρωματικό έγγραφο το οποίο παρουσιάζει τις απαιτήσεις του κανονισμού που εντοπίστηκαν και τις δυνατότητες του εργαλείου.

Λέξεις κλειδιά: Γενικός Κανονισμός Προστασίας Δεδομένων, απαιτήσεις, ιδιωτικότητα, εκτίμηση συμμόρφωσης

Abstract

The General Data Protection Regulation entered into force on 25 May 2018 and brought radical changes to the way personal data is handled. Any entity processing personal data is required to comply with the requirements and perform a series of actions to ensure privacy. Given the rapid development of technology, the complexity of business processes, and the breadth of data that a business or an organization may process, the protection of personal data the proof of compliance ends up to be a complex and demanding undertaking.

In order to facilitate this task, it was decided to create a tool for assessing compliance with the General Data Protection Regulation, which could give the user all the actions required to be completed and the ability to assess the level of compliance. This paper is a complementary document which presents the identified requirements of the regulation and the tool's capabilities.

Keywords: General Data Protection Regulation, requirements, privacy, compliance assessment

Περιεχόμενα

Λίστα εικόνων

Λίστα πινάκων

1. Εισαγωγή

Ξεκινώντας το 1995, για την προστασία της ιδιωτικής ζωής, οι Ευρωπαίοι πολίτες καλύπτονταν με τις εθνικές νομοθετικές διατάξεις της χώρας τους η οποίες βασίζονταν σε οδηγία – πλαίσιο της Ευρωπαϊκής Ένωσης, στην οδηγία 95/ 46/ ΕΚ και η οποία συμπληρώθηκε με την οδηγία 2002/ 58/ ΕΚ που πρόσθεσε και την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Η ραγδαία αύξηση της τεχνολογίας, η χρήση ολοένα και περισσότερο των δεδομένων προσωπικού χαρακτήρα και το γεγονός ότι κάθε χώρα της Ευρωπαϊκής Ένωσης εφάρμοζε διαφορετικά και στα δικά της πλαίσια τις οδηγίες οδήγησαν, το 2012, στην μεταρρύθμιση της οδηγίας του ‘95 μιας και δεν αρκούσε πλέον για την προστασία της ιδιωτικής ζωής. Ύστερα από πολλά χρόνια επεξεργασίας και διαπραγματεύσεων, το 2016, η Ευρωπαϊκή Επιτροπή ενέκρινε τελικά το Γενικό Κανονισμό Προστασίας Δεδομένων, εφεξής «ΓΚΠΔ» ή «Κανονισμός».

Οι κανονισμοί της Ευρωπαϊκής Ένωσης υπόσχονται μεγαλύτερη ομοιομορφία στα πρότυπα και τις ερμηνείες από ό,τι μπορεί να παράγει μια οδηγία - πλαίσιο, η οποία γενικά θεωρείται ως όφελος για τις επιχειρήσεις που δραστηριοποιούνται σε πολλές ευρωπαϊκές χώρες. Ως κανονισμός, ο ΓΚΠΔ έχει σχεδιαστεί για μια ενιαία ψηφιακή αγορά στην οποία οι οργανισμοί που επεξεργάζονται προσωπικά δεδομένα γνωρίζουν τι επιτρέπεται να κάνουν και τι όχι με τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται. Ο ΓΚΠΔ προσφέρει ένα ρυθμιστικό πλαίσιο που προσαρμόζεται στην πραγματικότητα του σημερινού ψηφιακού κόσμου και ταυτόχρονα θέτει το υποκείμενο των δεδομένων ως το κέντρο όλων των επιμέρους διαδικασιών.

Εικόνα 1 - General Data Protection Regulation

2. Βασικές έννοιες

Ο ΓΚΠΔ επιφέρει μία πληθώρα αλλαγών τόσο σε ρόλους, αρμοδιότητες και υποχρεώσεις, όσο και στην σημασιολογία βασικών όρων όπως η «επεξεργασία» και τα «δεδομένα προσωπικού χαρακτήρα». Στόχος των αλλαγών είναι η ενίσχυση του κύρους και της σημασίας των όρων και των ρόλων ώστε να δοθεί μεγαλύτερη βαρύτητα στην διασφάλιση της ιδιωτικότητας.

Ακολουθεί ανάλυση κάποιων βασικών όρων όπως παρουσιάζονται από τον Κανονισμό. Οι απαιτήσεις, αρμοδιότητες και υποχρεώσεις παρουσιάζονται σε επόμενο κεφάλαιο.

2.1 Δεδομένα προσωπικού χαρακτήρα

Τα δεδομένα προσωπικού χαρακτήρα είναι οποιαδήποτε πληροφορία μπορεί να συσχετιστεί με ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, ή όπως ορίζεται από τον Κανονισμό ως «υποκείμενο των δεδομένων». Ένα ταυτοποιημένο φυσικό πρόσωπο είναι ένα άτομο που είναι ξεχωριστό και υπάρχει σαφής προσδιορισμός του χωρίς την ανάγκη για περαιτέρω στοιχεία ή άλλα αναγνωριστικά στοιχεία. Ένα ταυτοποιήσιμο φυσικό πρόσωπο, από την άλλη, είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου. Επίσης τα δεδομένα προσωπικού χαρακτήρα περιλαμβάνουν επίσης και άλλα λιγότερα προφανή δεδομένα τα οποία συμμετέχουν στην ψηφιακή οικονομία. Αυτά μπορεί να είναι ένα ηλεκτρονικό αναγνωριστικό όπως μια διεύθυνση IP, δεδομένα θέσης, δεδομένα συμπεριφοράς που αποκτώνται πλέον ευκολότερα χάρη στη χρήση των κοινωνικών δικτύων, της τεχνολογίας RFID, των αναγνωριστικών φωνής και προσώπου, των cookies, του Διαδικτύου των Πραγμάτων (IoT) κ.α.. Διάφορα στοιχεία δηλαδή τα οποία συλλέγονται μαζί και μπορεί να οδηγήσουν στην αναγνώριση ενός συγκεκριμένου προσώπου, συνιστούν επίσης δεδομένα προσωπικού χαρακτήρα.

Δεδομένα προσωπικού χαρακτήρα τα οποία είναι εκ φύσεως ιδιαίτερα ευαίσθητα σε σχέση με θεμελιώδη δικαιώματα και ελευθερίες χρήζουν ειδικής προστασίας, καθότι το πλαίσιο της επεξεργασίας τους θα μπορούσε να δημιουργήσει σημαντικούς κινδύνους για τα θεμελιώδη δικαιώματα και τις ελευθερίες. Υπάρχει λοιπόν μια ειδική κατηγορία δεδομένων που θεωρούνται ιδιαίτερα ευαίσθητα και αφορούν τη

φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές και φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και τα γενετικά δεδομένα, τα βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένα που αφορούν την υγεία ή δεδομένα που αφορούν τη σεξουαλική ζωή του φυσικού προσώπου. Για τέτοιου είδους δεδομένα απαιτείται η ρητή συγκατάθεση ή νομική υποχρέωση για τη συλλογή ή επεξεργασία τους και απαιτούν αυξημένη ασφάλεια και προσοχή στα όρια αποθήκευσης τους.

Στην περίπτωση που τα δεδομένα προσωπικού χαρακτήρα, έχουν καταστεί ανώνυμα με έναν μη αναστρέψιμο τρόπο καθιστώντας έτσι το άτομο μη ταυτοποιήσιμο τότε παύουν να αναγνωρίζονται πλέον και ως δεδομένα προσωπικού χαρακτήρα. Ο νόμος προστατεύει τα δεδομένα προσωπικού χαρακτήρα ανεξαρτήτου τεχνολογίας που χρησιμοποιείται για την επεξεργασία και είναι τεχνολογικά ουδέτερος τόσο για αυτοματοποιημένες όσο και για χειροκίνητες επεξεργασίες. Επίσης, δεν επηρεάζεται από τον τρόπο αποθήκευσης των δεδομένων σε ένα σύστημα πληροφορικής κι αν αυτή πραγματοποιείται μέσω κάποιας βιντεοσκόπησης ή ακόμη και από έντυπα έγγραφα. Σε κάθε περίπτωση η προστασία όλων αυτών έγκειται κάτω από τον ΓΚΠΔ και για τα ταυτοποιημένα και για ταυτοποιήσιμα υποκείμενα των δεδομένων.

2.2 Επεξεργασία δεδομένων προσωπικού χαρακτήρα

Η έννοια της επεξεργασίας στον Κανονισμό διαφέρει από την καθιερωμένη της επιστήμης της πληροφορικής όπου παρουσιάζεται ως το σύνολο των ενεργειών που μετασχηματίζουν αδόμητα δεδομένα σε πληροφορία.

Ο ΓΚΠΔ ορίζει την επεξεργασία ως το σύνολο πάσης φύσεως ενεργειών που εκτελείται επί των δεδομένων προσωπικού χαρακτήρα. Ενδεικτικά παραδείγματα επεξεργασίας δεδομένων προσωπικού χαρακτήρα είναι η συλλογή, η διαγραφή, μεταβολή, αποθήκευση και κοινολόγηση με διαβίβαση.

Μέσα από αυτή την ευρύτερη έννοια της επεξεργασίας διαφαίνεται πληρέστερα και το επίπεδο δυσκολίας συμμόρφωσης με τον Κανονισμό καθώς έμμεσα εισάγει την ανάγκη διασφάλισης της ιδιωτικότητας σε ένα μεγάλο ποσοστό των επιχειρησιακών λειτουργιών ενός οργανισμού ή μιας επιχείρησης.

2.3 Υπεύθυνος επεξεργασίας

Ως υπεύθυνος επεξεργασίας ορίζεται από το ΓΚΠΔ η οντότητα εκείνη που μόνη ή από κοινού με άλλες αποφασίζει ποιος είναι ο σκοπός και ο τρόπος με τον οποίο εκτελείται η επεξεργασία.

Ο υπεύθυνος επεξεργασίας, φυσικό ή νομικό πρόσωπο, καλείται να εφαρμόζει τεχνικά και οργανωτικά μέτρα προς διασφάλιση των δεδομένων προσωπικού χαρακτήρα, να εξυπηρετεί την άσκηση των δικαιωμάτων των υποκειμένων, όπως αυτά παρουσιάζονται στην συνέχεια, και να αποδεικνύει συνεχώς την πλήρη συμμόρφωσή του με τον Κανονισμό.

2.4 Εκτελών την επεξεργασία

Ως εκτελών την επεξεργασία ορίζεται η οντότητα που εκτελεί μια επεξεργασία δεδομένων προσωπικού χαρακτήρα εκ μέρους ενός υπευθύνου επεξεργασίας σύμφωνα με τον τρόπο και για τον σκοπό που του έχει ορίσει.

Αν και οι ευθύνες του εκτελούντος είναι περιορισμένες σε σχέση με τον υπεύθυνο επεξεργασίας, καλείται να επιδεικνύει τη δέουσα προσοχή κατά την εκτέλεση της επεξεργασίας, ώστε να προστατεύει τα δεδομένα προσωπικού χαρακτήρα και να συμμορφώνεται με το ΓΚΠΔ.

2.5 Εποπτικές Αρχές

Η εποπτική αρχή είναι μια ανεξάρτητη δημόσια αρχή που είναι υπεύθυνη, μέσω ερευνών και διορθωτικών εξουσιών, για την παρακολούθηση της εφαρμογής του ΓΚΠΔ. Οι εποπτικές αρχές, προϋπήρχαν του ΓΚΠΔ σε κάθε μέλος κράτος όμως δεν υπήρχαν τα κοινά πλαίσια που θα επέτρεπαν την ομοιογενή εφαρμογή του.

Ορίζονται λοιπόν οι σχετικοί κανόνες που οριοθετούν το πλαίσιο με τις αρμοδιότητες, τα καθήκοντα και τις εξουσίες του κάθε μηχανισμού και συμβάλουν στην ορθότερη συνεργασία μεταξύ τους, μεταξύ των κρατών μελών που ανήκουν αλλά και συγκεντρωτικά σε όλη την Ευρώπη. Κάθε κράτος μέλος, διασφαλίζει ότι οι εποπτικές αρχές που λειτουργούν στο έδαφος τους επιφορτίζονται με τους απαραίτητους ανθρώπινους, τεχνικούς και οικονομικούς πόρους για την αποτελεσματική εκτέλεση των καθηκόντων και άσκηση των εξουσιών της.

Μέσα στα πλαίσια των καθηκόντων της, η εποπτική αρχή όντας κύριο σημείο επαφής αναφορικά με θέματα προστασίας δεδομένων προσωπικού χαρακτήρα, είναι η παροχή συμβουλών στους πολίτες, στους οργανισμούς όπως και στους εθνικούς φορείς για νομοθετικά και διοικητικά μέτρα, ο χειρισμός των καταγγελιών κατά παραβιάσεων του ΓΚΠΔ και των σχετικών εθνικών νόμων, η συνεργασία με άλλες εποπτικές αρχές παρέχοντας αμοιβαία συνδρομή και η επιβολή επίπληξης ή διοικητικών προστίμων σε περιπτώσεις μη συμμόρφωσης.

Εξίσου σημαντικό είναι η συνεργασία μεταξύ της επικεφαλής εποπτικής αρχής και των άλλων ενδιαφερόμενων εποπτικών αρχών ώστε να υλοποιήσουν και να εφαρμόσουν τον παρόντα Κανονισμό με συνεκτικό τρόπο, και θεσπίζουν μέτρα για την αποτελεσματική συνεργασία τους. Η αμοιβαία συνδρομή καλύπτει, ιδίως, αιτήματα παροχής πληροφοριών και μέτρα ελέγχου, παραδείγματος χάρη αιτήματα για προηγούμενες διαβουλεύσεις και ελέγχους καθώς και από κοινού έρευνες. Προκειμένου επίσης να συμβάλλουν στη συνεκτική εφαρμογή του παρόντος Κανονισμού στο σύνολο της Ένωσης, οι εποπτικές αρχές συνεργάζονται και διασυνοριακά μεταξύ τους αλλά και με το Συμβούλιο Προστασίας Δεδομένων.

Το Συμβούλιο Προστασίας Δεδομένων απαρτίζεται από τον προϊστάμενο μίας εποπτικής αρχής κάθε κράτους μέλους και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων ή τους αντίστοιχους εκπροσώπους τους. Λειτουργεί ανεξάρτητα και είναι υπεύθυνο για την ορθή και συνεκτική εφαρμογή του παρόντος Κανονισμού. Συμβάλει με τη γνώμη της στη θέσπιση μέτρων που αποζητά μια ενδιαφερόμενη εποπτική αρχή και εμπλέκεται στην επίλυση των διαφορών μεταξύ τους, εκδίδοντας δεσμευτικές αποφάσεις.

Επίσης, γνωμοδοτεί και αυτό με τη σειρά του την Επιτροπή για κάθε ζήτημα σχετικό με την προστασία των δεδομένων προσωπικού χαρακτήρα στην Ένωση και εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές σε θέματα με υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων όπως είναι τα κριτήρια και οι προϋποθέσεις σχετικά με τη λήψη αποφάσεων που βασίζονται σε κατάρτιση προφίλ, και οι παραβιάσεις ή οι διαβιβάσεις των δεδομένων προσωπικού χαρακτήρα.

Για την ορθή εφαρμογή, την αποτελεσματικότητα και τη συνεχή εξέλιξη του ΓΚΠΔ χρειάζεται η ατομική αλλά και η ομαδική προσπάθεια όλων των εμπλεκόμενων φορέων όπως είναι τα ίδια τα υποκείμενα, οι εποπτικές αρχές κάθε κράτους μέλους, οι υπεύθυνοι και εκτελών την επεξεργασία, και το Ευρωπαϊκό Συμβουλίου Προστασίας Δεδομένων.

2.6 Αυξημένο εδαφικό πεδίο εφαρμογής

Η μεγαλύτερη αλλαγή, σε σύγκριση με την ισχύουσα οδηγία, στο ρυθμιστικό περιβάλλον της ιδιωτικότητας των δεδομένων έρχεται με την εκτεταμένη αρμοδιότητα του ΓΚΠΔ. Ο Κανονισμός αφορά όλες τις εταιρείες που προσφέρουν αγαθά και υπηρεσίες (έναντι πληρωμής ή όχι) και επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα των υποκειμένων των δεδομένων των πολιτών που διαμένουν στην ΕΕ ανεξάρτητα από την τοποθεσία της. Εφαρμόζεται επίσης στην επεξεργασία των δεδομένων ακόμη και αν πραγματοποιείται σε χώρα εκτός ΕΕ. Οι επιχειρήσεις εκείνες, για λόγους συμμόρφωσης, θα πρέπει να διορίσουν έναν εκπρόσωπο στην ΕΕ.

3. Υποχρέωση συμμόρφωσης

Ο Κανονισμός έχει καθολική ισχύ και από 25 Μαΐου 2018 η απόδειξη συμμόρφωσης με τις απαιτήσεις του θεωρείται υποχρεωτική για κάθε οντότητα που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα.

3.1 Κυρώσεις

Σε περίπτωση μη συμμόρφωσης με τον Κανονισμό ή παραβίασης δεδομένων προσωπικού χαρακτήρα, ο ΓΚΠΔ προβλέπει την εφαρμογή ποινικών και διοικητικών κυρώσεων τόσο μέσω των εποπτικών αρχών όσο και μέσω των δικαστηρίων κάθε κράτους μέλος.

Το υποκείμενο των δεδομένων, έχει το δικαίωμα της υποβολής καταγγελίας στην εποπτική αρχή όταν οι επεξεργασίες των δεδομένων προσωπικού χαρακτήρα που το αφορούν, παραβαίνουν τον Κανονισμό και φέρουν σε κίνδυνο τα δεδομένα του ή περιορίζουν τα δικαιώματα του και σύμφωνα με τον παρόντα Κανονισμό, δικαιούται αποζημίωση από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία για την υλική ή μη υλική ζημία που υπέστη.

Κάθε υπεύθυνος ή εκτελών την επεξεργασία που εμπλέκεται στην επεξεργασία και φέρει ευθύνες για τις ζημιές που υπέστη το υποκείμενο των δεδομένων, έρχεται αντιμέτωπος με τις κυρώσεις και τα πρόστιμα που του επιβάλει η εποπτική αρχή. Ο ΓΚΠΔ διαχωρίζει το μέγεθος των ποινών αξιολογώντας τη φύση, τη βαρύτητα και τη διάρκεια της παράβασης, τον αντίκτυπο, το ιστορικό παραβατικότητας και τη λήψη τυχών αντίμετρων και ενεργειών που προέβη ο υπεύθυνος σε περίπτωση παραβίασης των δεδομένων. Οι οργανισμοί που οι παραβάσεις τους αφορούν υποχρεώσεις του υπεύθυνου και εκτελούντος την επεξεργασία μπορούν να δεχθούν από σοβαρές επιπλήξεις έως και πρόστιμα των 10.000.000€ ή 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού τους έτους. Σημαντικότερες θα είναι οι κυρώσεις όταν παραβιάζονται τα δικαιώματα των υποκειμένων, οι βασικές αρχές που διέπουν τις επεξεργασίες των δεδομένων, οποιεσδήποτε υποχρεώσεις που ορίζει το δίκαιο κράτους μέλους ή διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτους και άλλα υψίστης σημασίας θέματα στα οποία ο οργανισμός εκμεταλλεύεται ή θέτει σε κίνδυνο άμεσα ή έμμεσα το υποκείμενο των δεδομένων. Σε αυτές τις περιπτώσεις, όταν ο οργανισμός δεν συμμορφώνεται με τον Κανονισμό και με εντολές της εποπτικής αρχής, μπορεί να του δοθεί πρόστιμο της τάξης των 20.000.000€ ή 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου έτους. Ο ΓΚΠΔ επιβάλει λοιπόν, μια σειρά από διοικητικά πρόστιμα με οικονομικά μεγέθη και ποσοστά

ικανά να συμμορφώσουν από μικρομεσαίους οργανισμούς μέχρι πολυεθνικές εταιρείες, αποτελεσματικά και αποτρεπτικά.

4. Δικαιώματά του υποκειμένου των δεδομένων

Ο ΓΚΠΔ παρέχει στους πολίτες και στους καταναλωτές ένα ευρύ φάσμα συγκεκριμένων δικαιωμάτων των υποκειμένων των δεδομένων που μπορούν να ασκήσουν κάτω υπό συγκεκριμένες συνθήκες και πάντα με μερικές εξαιρέσεις. Τα δικαιώματα των υποκειμένων εξάλλου δεν είναι ποτέ απόλυτα. Οι οργανισμοί έχουν νομικές υποχρεώσεις και μπορεί να υπάρχουν και συμβατικές διατάξεις που να υπερισχύουν τα δικαιώματα των υποκειμένων των δεδομένων.

4.1 Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων

Δίνεται το δικαίωμα στο υποκείμενο των δεδομένων να λαμβάνει γνώση το κατά πόσον τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υπόκεινται σε επεξεργασία και συγκεκριμένα το δικαίωμα πρόσβασης σε διάφορες πληροφορίες που ο υπεύθυνος επεξεργασίας υποχρεούται να διαθέσει.

Το υποκείμενο μπορεί να πληροφορηθεί για τους σκοπούς, τις κατηγορίες και το χρονικό διάστημα για τα οποία γίνεται η επεξεργασία και η αποθήκευση των δεδομένων του. Επίσης, του δίνεται το δικαίωμα να του γνωστοποιηθεί κάθε διαθέσιμη πληροφορία για την προέλευση των δεομένων προσωπικού χαρακτήρα όταν αυτά δε συλλέγονται από το ίδιο το υποκείμενο των δεδομένων και να ζητήσει πληροφορίες για την ύπαρξη αυτοματοποιημένων λήψεων αποφάσεων και τις προβλεπόμενες συνέπειες αυτών. Εξίσου σημαντικό είναι η πρόσβαση στους αποδέκτες ή στις κατηγορίες αποδεκτών στους οποίους κοινολογούνται (ή πρόκειται να κοινολογηθούν) τα δεδομένα προσωπικού χαρακτήρα και ειδικότερα όταν αυτά διαβιβάζονται σε μια Τρίτη χώρα ή σε ένα διεθνή οργανισμό όπου τότε θα πρέπει να παρέχονται και όλες οι απαραίτητες εγγυήσεις που συνοδεύουν τη σχετική διαβίβαση. Τέλος, για όλα τα προαναφερθέντα ορίζεται το δικαίωμα λήψης αντίγραφου χωρίς όμως αυτό να επηρεάζει τις ελευθερίες και τα δικαιώματα των άλλων.

4.2 Δικαίωμα διόρθωσης

Το υποκείμενο των δεδομένων δικαιούται να ζητήσει από τον υπεύθυνο επεξεργασίας τη διόρθωση ή την συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα που το αφορούν.

4.3 Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)

Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από την υπεύθυνο επεξεργασίας τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν όταν τα δεδομένα αυτά δεν είναι πλέον απαραίτητα για τους σκοπούς για του οποίους συλλέχθηκαν. Επίσης δίνεται η ελευθερία στο υποκείμενο να ανακαλέσει την συγκατάθεση του ή να αντιτεθεί στην επεξεργασία των δεδομένων του όταν αυτό το θελήσει ή όταν αυτή έγινε παράνομα. Στις περιπτώσεις αυτές, ο υπεύθυνος επεξεργασίας λαμβάνοντας υπόψιν το κόστος και τη διαθέσιμη τεχνολογία, χρησιμοποιεί όλα τα εύλογα μέτρα (και τεχνικά) για να προβεί στην εκτέλεση των απαραίτητων διαγραφών. Υπάρχουν όμως και περιπτώσεις στις οποίες η επεξεργασία είναι απαραίτητη όπως η επιβολή της επεξεργασίας βάσει δικαίου της Ένωσης ή του δικαίου κράτους μέλους στο οποίο εδρεύει ο υπεύθυνος επεξεργασίας, για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, επιστημονικής ή ιστορικής έρευνας καθώς επίσης και τη θεμελίωση, άσκηση ή υποστήριξη των νομικών αξιώσεων. Σε τέτοιες περιπτώσεις δε μπορεί να ασκηθεί το παρών δικαίωμα.

4.4 Δικαίωμα περιορισμού της επεξεργασίας

Εφόσον κριθεί ότι υπάρχει ανακρίβεια στα δεδομένα προσωπικού χαρακτήρα, δίνεται η δυνατότητα στο υποκείμενο των δεδομένων να ζητήσει τον περιορισμό της επεξεργασίας τους. Επιπρόσθετα, όταν ολοκληρωθεί ο σκοπός της επεξεργασίας των δεδομένων από τον υπεύθυνο επεξεργασίας αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο για τη θεμελίωση ή άσκηση νομικών αξιώσεων τότε μπορεί να εφαρμοστεί το δικαίωμα του περιορισμού της επεξεργασίας. Επίσης, στην περίπτωση που το υποκείμενο κρίνει ότι είναι παράνομη ή έχει αντιρρήσεις για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα τότε δύναται η άσκηση του δικαιώματος του περιορισμού εν αναμονή της επαλήθευσης του κατά πόσον υπερισχύουν οι νόμιμοι λόγοι του υπευθύνου της επεξεργασίας έναντι των λόγων του υποκειμένων των δεδομένων. Τέλος, όταν έχει γίνει περιορισμός της επεξεργασίας, οποιαδήποτε περεταίρω επεξεργασία γίνεται μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων εκτός κι αν χρειάζονται σε υποστήριξη/ άσκηση νομικών αξιώσεων, προστασία δικαιωμάτων φυσικών προσώπων ή δημόσιου συμφέροντος.

4.5 Υποχρέωση γνωστοποίησης σχετικά με την διόρθωση, τη διαγραφή και τον περιορισμό της επεξεργασίας

Γίνεται η γνωστοποίηση της διόρθωσης ή διαγραφής των δεδομένων προσωπικού χαρακτήρα ή περιορισμού της επεξεργασίας τους, σε κάθε αποδέκτη στον οποίο γνωστοποιήθηκαν από τον υπεύθυνο επεξεργασίας εκτός κι αν αυτό αποδεικνύεται ανέφικτο και γίνεται η ενημέρωση του υποκειμένου εφόσον αυτό ζητηθεί από εκείνο.

4.6 Δικαίωμα στη φορητότητα των δεδομένων

Το υποκείμενο των δεδομένων έχει την δυνατότητα να λάβει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν και που έχουν επέλθει στην κατοχή του υπεύθυνου επεξεργασίας σε ένα μια κοινώς χρησιμοποιούμενη και αναγνωρίσιμη μορφή, αλλά όχι όταν η συλλογή τους εξυπηρετεί το δημόσιο συμφέρον ή την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο. Επίσης, υφίσταται η φορητότητα των δεδομένων από τον έναν υπεύθυνο επεξεργασίας στον άλλον όταν αυτό είναι τεχνικά εφικτό.

4.7 Δικαίωμα εναντίωσης

Το υποκείμενο των δεδομένων, ανά πάσα στιγμή, έχει τη δικαίωμα να αντιτεθεί στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν καθώς και στην κατάρτιση προφίλ, στην περίπτωση που αυτή γίνεται. Η ενημέρωση του υποκειμένου για το δικαίωμα αυτό γίνεται κατά την πρώτη κιόλας επικοινωνία του υπεύθυνου επεξεργασίας με αυτό. Το δικαίωμα παύει να ισχύει στις περιπτώσεις στις οποίες οι νομικοί λόγοι για την επεξεργασία υπερισχύουν των συμφερόντων και ελευθεριών του υποκειμένου.

4.8 Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ

Δίνεται το δικαίωμα στο υποκείμενο των δεδομένων να αντιτάσσεται σε αποφάσεις που λαμβάνονται αποκλειστικά βάσει μιας αυτοματοποιημένης διαδικασίας και η οποία παράγει έννομα αποτελέσματα που το αφορούν. Όταν όμως η επεξεργασία είναι απαραίτητη για το δημόσιο συμφέρον και ειδικότερα για την προστασία της δημόσιας και διασυνοριακής υγείας βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους τότε παύει να ισχύει το παρών δικαίωμα. Το ίδιο ισχύει και στην περίπτωση που η αυτοματοποιημένη λήψη αποφάσεων είναι υποχρεωτική για την

εκτέλεση της σύμβασης μεταξύ του υπεύθυνου επεξεργασίας και του υποκειμένου των δεδομένων

5. Προσδιορισμός απαιτήσεων ανά άρθρο

Κατόπιν εκτενής μελέτης του ΓΚΠΔ προσδιορίστηκαν τα άρθρα που υπαγορεύουν τις βασικές υποχρεώσεις που φέρουν οι υπεύθυνοι επεξεργασίας, όπως οργανισμοί και εταιρείες, κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

5.1 Αρχές που διέπουν την επεξεργασία (Άρθρο 5)

Ορίζονται οι βασικές αρχές σύμφωνα με τις οποίες οφείλει ο υπεύθυνος να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα.

«νομιμότητα, αντικειμενικότητα και διαφάνεια» : Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα θα πρέπει να γίνεται κατόπιν ενημέρωσης του υποκειμένου και να είναι σύννομη.

«περιορισμός του σκοπού» : Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πραγματοποιείται σύμφωνα με τον σκοπό ή τους σκοπούς συλλογής.

«ελαχιστοποίηση των δεδομένων» : Τα δεδομένα προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία περιορίζονται σε αυτά που ορίζει ο σκοπός της επεξεργασίας.

«ακρίβεια» : Τα δεδομένα προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία σύμφωνα με ένα σκοπό πρέπει να ακριβή και σε αντίθετη περίπτωση να επικαιροποιούνται.

«περιορισμός της περιόδου αποθήκευσης» : Η περίοδος τήρησης των δεδομένων προσωπικού χαρακτήρα πρέπει να είναι περιορισμένη και να προσδιορίζεται από τον υπεύθυνο, σύμφωνα με τον σκοπό επεξεργασίας.

«ακεραιότητα και εμπιστευτικότητα» : Θα πρέπει να διασφαλίζεται η ασφάλεια των δεδομένων προσωπικού χαρακτήρα κατά την επεξεργασία.

«λογοδοσία» : Ευθύνη συμμόρφωσης με αυτές τις αρχές φέρει ο υπεύθυνος επεξεργασίας.

5.2 Νομιμότητα (Άρθρο 6)

Σύμφωνα με τον ΓΚΠΔ ο σκοπός της εκάστοτε επεξεργασίας δεδομένων προσωπικού χαρακτήρα θεωρείται σύννομος εάν συνοδεύεται από κάποια νομική βάση. Συνήθεις νομικές βάσεις τις οποίες θα μπορούσε να επικαλεστεί ο υπεύθυνος της επεξεργασίας αποτελούν η ρητή συγκατάθεση από το υποκείμενο των δεδομένων

(Άρθρο 6.1(α)), η επεξεργασία λόγω έννομου συμφέροντος της εταιρείας (Άρθρο 6.1(στ)), λόγω έννομης υποχρέωσης (Άρθρο 6.1(γ)) ή στο πλαίσιο της συμβατικής σχέσης.

Ειδικές περιπτώσεις αποτελούν η επεξεργασία στο πλαίσιο διαφύλαξης του ζωτικού συμφέροντος (Άρθρο 6.1(δ)) του υποκειμένου και για λόγους δημοσίου συμφέροντος / εξουσίας (Άρθρο 6.1(ε)) τις οποίες θα μπορούσαν να επικαλεστούν οργανισμοί παροχής εξειδικευμένων υπηρεσιών.

5.3 Συγκατάθεση (Άρθρο 7)

Ο υπεύθυνος επεξεργασίας, σε περιπτώσεις που η επεξεργασία δεδομένων προσωπικού χαρακτήρα θεωρείται σύννομη λόγω συγκατάθεσης, έχει την ευθύνη να αποδείξει ότι τα υποκείμενα συγκατατέθηκαν αφού πρώτα ενημερώθηκαν πλήρως και με σαφή τρόπο για όλους τους σκοπούς επεξεργασίας και να διαφυλάσσει το δικαίωμα τους για ανάκληση της συγκατάθεσης.

5.4 Συγκατάθεση ανήλικου (Άρθρο 8)

Ο υπεύθυνος επεξεργασίας, σε περιπτώσεις που η επεξεργασία δεδομένων προσωπικού χαρακτήρα θεωρείται σύννομη λόγω συγκατάθεσης ενώ το υποκείμενο είναι ανήλικο, έχει την ευθύνη να λαμβάνει και να επαληθεύει την συγκατάθεση από το πρόσωπο που έχει τη γονική μέριμνα του υποκειμένου.

5.5 Επεξεργασία Ειδικές κατηγορίες δεδομένων (Άρθρο 9)

Ορίζονται οι ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα όπως τα δεδομένα υγείας, οι σεξουαλικές προτιμήσεις και τα πολιτικά φρονήματα. Σύμφωνα με τον Κανονισμό η επεξεργασία τέτοιων τύπων δεδομένων απαγορεύεται αν δεν γίνεται σύμφωνα με κάποιες ξεχωριστές νομικές βάσεις από αυτές που αναφέρει το Άρθρο 6.

Ενδεικτικά αναφέρονται ορισμένες από αυτές όπως η ρητή συγκατάθεση του υποκειμένου (Άρθρο 9.2(α)), η επεξεργασία λόγω προστασίας των ζωτικών συμφερόντων του υποκειμένου (Άρθρο 9.2(γ)) και στο πλαίσιο άσκησης ή υποστήριξης νομικών αξιώσεων (Άρθρο 9.2(στ)).

5.6 Ποινικές καταδίκες και αδικήματα (Άρθρο 10)

Όταν για την εκπλήρωση ενός σκοπού δύναται να γίνει επεξεργασία δεδομένων που αφορούν ποινικές καταδίκες ή αδικήματα θα πρέπει να γίνεται μόνο αν θεωρείται επιτρεπτό από το δίκαιο της Ένωσης, το δίκαιο κράτους μέλους ή υπό τον έλεγχο που διενεργείται από επίσημη αρχή.

5.7 Διαφανής ενημέρωση και άσκηση των δικαιωμάτων του υποκειμένου (Άρθρα 12, 13, 14)

Ο υπεύθυνος επεξεργασίας οφείλει να παρέχει όλα τα δυνατά μέσα και διαδικασίες για την διευκόλυνση της άσκησης των δικαιωμάτων των υποκειμένων. Επιπλέον ευθύνη του υπεύθυνου αποτελεί η πλήρης ενημέρωση του υποκειμένου των δεδομένων αναφορικά με ένα εύρος πληροφοριών που σχετίζονται με την επεξεργασία. Ενδεικτικά και μεταξύ άλλων, η ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και του υπευθύνου προστασίας, ο σκοπός επεξεργασίας και η περίοδος τήρησης των δεδομένων αποτελούν πληροφορίες για της οποίες το υποκείμενο θα πρέπει να είναι ενήμερο.

5.8 Δικαιώματα των υποκειμένων (Άρθρα 15 έως 22)

Τα υποκείμενα των δεδομένων σύμφωνα με τον ΓΚΠΔ έχουν επαυξημένα δικαιώματα σε σχέση με την επεξεργασία που υφίστανται τα δεδομένα τους. Ο υπεύθυνος κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα οφείλει να σέβεται, διασφαλίζει και να μην καταπατά τα δικαιώματα των υποκειμένων, όπως αυτά περιεγράφηκαν στο Κεφάλαιο 4.

5.9 Ευθύνη του υπεύθυνου (Άρθρο 24)

Ο υπεύθυνος επεξεργασίας πρέπει να δημιουργεί και να εφαρμόζει πολιτικές, διαδικασίες, κώδικες δεοντολογίας και γενικά όλα τα απαραίτητα τεχνικά και οργανωτικά μέτρα ώστε να διασφαλίζει την επεξεργασία και να διαφυλάσσει τα δικαιώματα και τις ελευθερίες των υποκειμένων.

5.10 Από τον σχεδιασμό και εξ ορισμού (Άρθρο 25)

Αναλύοντας όλες τις πτυχές της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, όπως το πεδίο εφαρμογής και οι σκοποί, εξ ορισμού, κατά τον σχεδιασμό / καθορισμό των μέσων που θα χρησιμοποιηθούν και κατά την διάρκεια της επεξεργασίας εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την ελαχιστοποίηση του κινδύνου καταπάτησης των ελευθεριών και των δικαιωμάτων των υποκειμένων.

5.11 Υπεύθυνος ή εκτελών εκτός Ένωσης (Άρθρο 27)

Σε περιπτώσεις όπου η επεξεργασία των δεδομένων προσωπικού χαρακτήρα γίνεται σε υποκείμενα της Ένωσης από υπεύθυνο ή εκτελών εκτός Ένωσης θα πρέπει να οριστεί, εκτός ελαχίστων εξαιρέσεων, επίσημος εκπρόσωπος που δρα στην Ένωση.

5.12 Εκτελών την επεξεργασία (Άρθρα 28, 29)

Ο εκτελών την επεξεργασία δρα εκ μέρους του υπεύθυνου, σύμφωνα με τους σκοπούς που του ορίζει. Θα πρέπει να τηρεί τις οδηγίες και τους όρους της συμβατικής σχέσης όπως καθορίστηκαν από τον υπεύθυνο σχετικά με τα τεχνικά και οργανωτικά μέτρα που διασφαλίζουν την επεξεργασία απέναντι σε ενδεχόμενους κινδύνους.

5.13 Αρχείο των δραστηριοτήτων (Άρθρο 30)

Βασική απαίτηση του ΓΚΠΔ και υποχρέωση του υπεύθυνου αποτελεί η δημιουργία, τήρηση και κατά περίπτωση ενημέρωση ενός αρχείου όλων δραστηριοτήτων επεξεργασίας που πραγματοποιεί.

Ενδεικτικές πληροφορίες που θα πρέπει να συμπεριληφθούν στο αρχείο δραστηριοτήτων είναι το όνομα και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας, και αν υπάρχουν και απαιτούνται του εκπροσώπου του, του από κοινού υπεύθυνου επεξεργασίας και του υπεύθυνου προστασίας δεδομένων, οι σκοποί επεξεργασίας, οι κατηγορίες αποδεκτών εάν υπάρχει κοινολόγηση με διαβίβαση των εν λόγω δεδομένων και περιγραφές των υποκειμένων και των κατηγοριών των δεδομένων.

Παρόμοιο αρχείο δραστηριοτήτων επεξεργασίας θα πρέπει να τηρεί και ο εκτελών για τις επεξεργασίες εκείνες που πραγματοποιεί για λογαριασμό του υπεύθυνου επεξεργασίας.

5.14 Ασφάλεια κατά την επεξεργασία δεδομένων (Άρθρο 32)

Ο υπεύθυνος επεξεργασίας ενισχύει την ασφάλεια της επεξεργασία εφαρμόζοντας κατάλληλα τεχνικά και οργανωτικά μέτρα όπως η κρυπτογράφηση, η ψευδωνυμοποίηση και ο έλεγχος όλων των εμπλεκόμενων πληροφοριακών συστημάτων με στόχο την διασφάλιση της ακεραιότητας, εμπιστευτικότητας, διαθεσιμότητας και νομιμότητας σε όλη τη διάρκεια της επεξεργασίας είτε συμμετέχει εκτελών και τρίτοι, είτε όχι.

5.15 Παραβιάσεις και γνωστοποιήσεις προς αρχές (Άρθρο 33)

Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη ενημέρωσης της αρμόδιας εποπτικής αρχής εντός 72 ωρών για τυχόν παραβιάσεις δεδομένων προσωπικού χαρακτήρα. Όμοια ευθύνη φέρει κι ο εκτελών την επεξεργασία, καθώς οφείλει να ενημερώνει των υπεύθυνο.

Στο πλαίσιο της ενημέρωσης αυτής θα πρέπει να γνωστοποιείται στην αρχή η φύση τη παραβίασης, τα υποκείμενα και τα δεδομένα, τα στοιχεία του υπεύθυνου προστασίας, συνέπειες καθώς κι οι ενέργειες αντιμετώπισης.

5.16 Παραβιάσεις και ενημέρωση των υποκειμένων (Άρθρο 34)

Αν τα δικαιώματα και οι ελευθερίες των υποκειμένων τίθενται σε κίνδυνο μέσω μιας παραβίασης δεδομένων προσωπικού χαρακτήρα, το υποκείμενο των δεδομένων θα πρέπει να ενημερώνεται από τον υπεύθυνο επεξεργασίας. Οι πληροφορίες που πρέπει να παρέχονται στο υποκείμενο είναι οι ίδιες που οφείλει ο υπεύθυνος επεξεργασίας να δώσει στην αρμόδια αρχή σε περίπτωση παραβίασης.

Τα υποκείμενα των δεδομένων δεν απαιτείται να ενημερώνονται αν ο υπεύθυνος επεξεργασίας έχει εφαρμόσει κατάλληλα τεχνικά και οργανωτικά μέτρα τα οποία καθιστούν την ταυτοποίηση των υποκειμένων, μέσω των δεδομένων που έχουν διαρρεύσει, αδύνατη.

5.17 Εκτίμηση αντικτύπου επεξεργασίας υψηλού κινδύνου (Άρθρα 35, 36)

Στις περιπτώσεις που ο υπεύθυνος προστασίας δεδομένων και η αρμόδια εποπτική αρχή κρίνουν ότι μία επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων, ο υπεύθυνος επεξεργασίας οφείλει να προβεί σε μία εκτίμηση του αντικτύπου που μπορεί να έχει αυτή η επεξεργασία.

Η εκτίμηση, που θα πραγματοποιηθεί από τον υπεύθυνο επεξεργασίας με την συνδρομή του υπεύθυνου προστασίας δεδομένων, πρέπει να περιλαμβάνει την νομική βάση, την περιγραφή και τον σκοπό της επεξεργασίας, μία εκτίμηση της αναγκαιότητας και της αναλογικότητας, τα δικαιώματα και τις ελευθερίες που ενδέχεται να παραβιαστούν καθώς και τα μέτρα που εφαρμόζει ή θα εφαρμόσει ο υπεύθυνος επεξεργασίας για να μετριάσει τον κίνδυνο.

5.18 Υπεύθυνος προστασίας δεδομένων (Άρθρα 37 έως 39)

Σε περιπτώσεις δραστηριοτήτων επεξεργασίας υψηλού κινδύνου ή επεξεργασιών που τελούνται από δημόσια αρχή ή φορέα, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία οφείλουν να ορίσουν και να στηρίζουν στις δράσεις του υπεύθυνο, προστασίας δεδομένων ο οποίος λογοδοτεί απευθείας στην ανώτατη διοίκηση του οργανισμού, φορέα ή επιχείρησης.

Ο υπεύθυνος προστασίας δεδομένων διαθέτει όλα τα απαραίτητα προσόντα για ανταποκριθεί επαρκώς στις αρμοδιότητες και τα καθήκοντα που θα του ανατεθούν, όπως μεταξύ άλλων η παροχή συμβουλών στον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία αναφορικά με όλες τις πτυχές της επεξεργασίας καθώς και της ενδεχόμενης εκτίμησης αντικτύπου. Παράλληλα συνεργάζεται με την αρμόδια εποπτική αρχή, βρίσκεται σε συχνή επικοινωνία με υποκείμενα των δεδομένων, βοηθάει στην άσκηση των δικαιωμάτων τους και είναι υπεύθυνος για την πλήρη συμμόρφωση με τον Κανονισμό.

5.19 Διαβίβαση δεδομένων κατόπιν απόφασης ή κατάλληλων εγγυήσεων (Άρθρα 45, 46, 48)

Η Επιτροπή κατόπιν εκτίμησης του επιπέδου προστασίας δεδομένων προσωπικού χαρακτήρα που διασφαλίζει μία τρίτη χώρα ή διεθνής οργανισμός αποφασίζει αν επιτρέπεται η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς αυτήν από τον.

Σε περιπτώσεις που η επιτροπή δεν έχει αποφανθεί, η διαβίβαση δεδομένων προσωπικού χαρακτήρα από τον εκτελών την επεξεργασία ή τον υπεύθυνο επεξεργασίας προς μία τρίτη χώρα ή διεθνή οργανισμό θεωρείται αποδεκτή κατόπιν κατάλληλων εγγυήσεων όπως οι δεσμευτικοί εταιρικοί κανόνες, κώδικας δεοντολογίας και ρήτρες προστασίας δεδομένων που εκδίδει η εποπτική αρχή.

5.20 Δεσμευτικοί εταιρικοί κανόνες (Άρθρο 47)

Οι δεσμευτικοί εταιρικοί κανόνες, οι οποίο εγκρίνονται από την αρμόδια εποπτική αρχή περιλαμβάνουν πληροφορίες όπως το σύνολο των διαβιβάσιμων δεδομένων, τον σκοπό της επεξεργασίας, τον τύπο των υποκειμένων, την εφαρμογή των αρχών προστασίας δεδομένων, τα δικαιώματα των υποκειμένων, τα καθήκοντα του υπεύθυνου προστασίας, τις διαδικασίες καταγγελίας και τους μηχανισμούς αναφοράς στην αρμόδια εποπτική αρχή.

5.21 Διαβίβαση κατόπιν άλλων προϋποθέσεων (Άρθρο 49)

Σε περιπτώσεις που δεν υπάρχει σχετική απόφαση της επιτροπής και κατάλληλες εγγυήσεις υπάρχουν προϋποθέσεις που καθιστούν αποδεκτή την διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, όπως η διαβίβαση να είναι απαραίτητη λόγω δημόσιου συμφέροντος, νομικών αξιώσεων, για την προστασία ζωτικών συμφερόντων ή να έχει δοθεί ρητή συγκατάθεση από το υποκείμενο των δεδομένων.

6. Εργαλείο εκτίμησης συμμόρφωσης

Παρουσιάζοντας τα δικαιώματα των υποκειμένων, τις υποχρεώσεις του υπεύθυνου επεξεργασίας σύμφωνα με τον ΓΚΠΔ, και προσδιορίζοντας τις δυνητικές κυρώσεις σε περίπτωση μη συμμόρφωσης, καθίσταται πλέον εμφανές η σοβαρότητα και το επίπεδο πολυπλοκότητας που εισάγει ο νέος Κανονισμός. Οι δυσκολίες αυτές αποτέλεσαν το έναυσμα για τη δημιουργία ενός εργαλείου εκτίμησης συμμόρφωσης.

6.1 Επισκόπηση

Το εργαλείο εκτίμησης συμμόρφωσης με τον ΓΚΠΔ δημιουργήθηκε χρησιμοποιώντας το εργαλείο MS Excel 2013, προς διευκόλυνση και υποστήριξη επιχειρήσεων και οργανισμών στην προσπάθεια διαχείρισης θεμάτων ιδιωτικότητας και τέλεσης όλων των αναγκαίων ενεργειών προς απόδειξη συμμόρφωσης με τον Κανονισμό.

Αποτελείται από ένα λίστα δραστηριοτήτων, ομαδοποιημένες σε δεκατρείς διακριτές ενότητες ανάλογα με τον σκοπό που ικανοποιούν. Ορισμένες από τις δραστηριότητες είναι υποχρεωτικό να εκτελεστούν καθώς ορίζονται άμεσα ή έμμεσα από τον Κανονισμό και συγκεκριμένα από τα άρθρα που αναλύθηκαν στο Κεφάλαιο 5. Ωστόσο έχουν συμπεριληφθεί και δραστηριότητες οι οποίες, αν και δεν δηλώνονται ρητά από τον Κανονισμό, κατόπιν εκτέλεσης τους βοηθούν εξίσου στην απόδειξη συμμόρφωσης.

Κάθε δραστηριότητα συνοδεύεται από μια αναλυτικότερη περιγραφή / αιτιολογία των ενεργειών στις οποίες οφείλει να προβεί ο οργανισμός ή επιχείρηση στο πλαίσιο ενίσχυσης της ασφάλειας των δεδομένων προσωπικού χαρακτήρα και της διασφάλισης της ιδιωτικότητας, των ελευθεριών και των δικαιωμάτων των υποκειμένων. Παράλληλα παρέχεται η δυνατότητα η δυνατότητα επιλογής της κατάστασης στην οποία βρίσκεται η εκάστοτε δραστηριότητα, όπως για παράδειγμα αν χρήζει βελτίωσης, μέσω της οποίας υπολογίζεται ο κίνδυνος που φέρει για τον οργανισμό ή την επιχείρηση σε σχέση με την διασφάλισης της ιδιωτικότητας και κατ’ επέκταση την συμμόρφωση με το Κανονισμό.

Παράλληλα παρέχεται απεικόνιση, μέσω γραφημάτων, του επιπέδου συμμόρφωσης του οργανισμού ή της επιχείρησης μετά το πέρας της εκτίμησης.

6.2 Κατηγορίες δραστηριοτήτων

Η εικόνα που ακολουθεί παρουσιάζει τις 13 κατηγορίες και τον αριθμό των δραστηριοτήτων που συγκεντρώνει η κάθε μία.

Κατηγορίες Δραστηριοτήτων Διαχείρισης Ιδιωτικότητας	Αριθμός Δραστηριοτήτων
Τήρηση Δομής Διακυβέρνησης	14
Τήρηση αρχείου καταγραφής δεδομένων προσωπικού χαρακτήρα και μηχανισμών μεταφοράς δεδομένων	12
Τήρηση εσωτερικής πολιτικής απορρήτου	5
Ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα στις λειτουργίες του οργανισμού	26
Τήρηση προγράμματος εκπαίδευσης και ευαισθητοποίησης	12
Διαχείριση κινδύνου ασφάλειας πληροφοριών	12
Διαχείριση κινδύνου ως προς τρίτους	9
Τήρηση δηλώσεων	7
Απαντήσεις αιτημάτων και παραπόνων	9
Παρακολούθηση νέων επιχειρησιακών πρακτικών	7
Τήρηση προγράμματος διαχείρισης παραβίασης δεδομένων προσωπικού χαρακτήρα	8
Παρακολούθηση πρακτικών διαχείρισης δεδομένων	7
Παρακολούθηση εξωτερικών κριτηρίων	7

Εικόνα 2 - Κατηγορίες Δραστηριοτήτων

6.2.1 Τήρηση δομής διακυβέρνησης

Η διασφάλιση της ιδιωτικότητας αποτελεί ένα δύσκολο εγχείρημα για οποιοδήποτε οργανισμό ιδίως όταν το εύρος των δραστηριοτήτων επεξεργασίας είναι υψηλού κινδύνου. Η κατηγορία αυτή περιλαμβάνει όλες τις βασικές ενέργειες τις οποίες οφείλει να κάνει ο υπεύθυνος επεξεργασίας, όντας στις περισσότερες περιπτώσεις ο ίδιος ο οργανισμός ή η επιχείρηση, ώστε να αναθέσει την ευθύνη της προστασίας των δεδομένων προσωπικού χαρακτήρα στις αρμόδιες οντότητες εντός οργανισμού, όπως σε ένα άτομο που θα διορισθεί υπεύθυνος προστασίας δεδομένων ή σε ολόκληρες ομάδες ατόμων και γενικά στους υπαλλήλους.

6.2.2 Τήρηση αρχείου καταγραφής δεδομένων προσωπικού χαρακτήρα και μηχανισμών μεταφοράς δεδομένων

Το εύρος των δεδομένων προσωπικού χαρακτήρα που δύναται να επεξεργάζεται ένας οργανισμός ή μια επιχείρηση καθιστά συχνά το έργο διασφάλισης τους ιδιαίτερα δύσκολο. Παράλληλα για την ικανοποίηση ενός σκοπού επεξεργασίας ή επειδή απαιτείται από κάποιο κανονιστικό πλαίσιο, συνηθίζεται η αποστολή των δεδομένων σε τρίτες χώρες ή διεθνής οργανισμούς. Με στόχο την διευκόλυνση του υπεύθυνου επεξεργασίας στην διασφάλιση των δεδομένων, η κατηγορία αυτή περιλαμβάνει όλες τις δραστηριότητες που οφείλει ή θα μπορούσε να εκτελέσει για καταγράψει όλες τις μεταφορές δεδομένων που πραγματοποιούνται, τα δεδομένα που επεξεργάζεται και τηρεί, καθώς και τα συστήματα που τα φιλοξενούν.

Τέτοια αρχεία καταγραφής βοηθούν στην απόδειξη της νομιμότητας των μεταφορών δεδομένων, στην συμμόρφωση με την αρχή της ελαχιστοποίησης των δεδομένων και τον εντοπισμό όλων των πληροφοριακών συστημάτων που εμπλέκονται στην επεξεργασία ώστε να εφαρμοστούν τα κατάλληλα τεχνικά και οργανωτικά μέτρα.

6.2.3 Τήρηση εσωτερικής πολιτικής απορρήτου

Οι στόχοι του οργανισμού ή της επιχείρησης όσον αφορά την προστασία δεδομένων πρέπει να είναι γνωστοί σε όλους το εργαζόμενους καθώς απαιτείται από κοινού προσπάθεια όλων. Η κατηγορία αυτή περιλαμβάνει την δημιουργία πολιτικής απορρήτου και κώδικα δεοντολογίας που παρέχουν στους εργαζόμενους την απαραίτητη καθοδήγηση και διέπουν την συμπεριφορά τους στο πλαίσιο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

6.2.4 Ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα στις λειτουργίες του οργανισμού

Επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιείται στις περισσότερες λειτουργίες ενός οργανισμού ή μιας επιχείρησης, όπως η προώθηση υπηρεσιών και αγαθών και αυτοματοποιημένες διαδικασίες λήψης απόφασης. Αυτό έχει ως αποτέλεσμα την ανάγκη ενσωμάτωσης της προστασίας των δεδομένων σε όλες αυτές τις λειτουργίες.

Ιδιαίτερη προσοχή πρέπει να δίνεται όταν η επεξεργασία περιλαμβάνει δεδομένα ειδικών κατηγοριών ή αλλιώς «ευαίσθητα» ή όταν τα υποκείμενα των δεδομένων είναι παιδιά και ανήλικοι. Παράλληλα όταν

για μία επεξεργασία απαιτείται συγκατάθεση του υποκειμένου των δεδομένων, αυτή θα πρέπει να λαμβάνεται με τρόπο έγκυρο.

Αυτή η κατηγορία περιλαμβάνει τις δραστηριότητες ανάπτυξης και χρήσης διαδικασιών και πολιτικών που ορίζουν τις αποδεκτές μεθόδους εκτέλεσης όλων των λειτουργιών του οργανισμού ή της επιχείρησης.

6.2.5 Τήρηση προγράμματος εκπαίδευσης και ευαισθητοποίησης

Με το στόχο την εναρμόνιση του οργανισμού ή της επιχείρησης με τις απαιτήσεις του ΓΚΠΔ όλοι οι υπάλληλοι που συμμετέχουν άμεσα ή έμμεσα σε δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα πρέπει να είναι πλήρως ενήμεροι σχετικά με όλα τα θέματα που αφορούν την διασφάλιση της ιδιωτικότητας.

Για την υλοποίηση του στόχου αυτού θεωρείται απαραίτητη η εκτέλεση όλων των δραστηριοτήτων που θα παρέχουν στους υπαλλήλους την αναγκαία εκπαίδευση και ενημέρωση ώστε να συμμετέχουν ενεργά στην προσπάθεια προστασίας των δεδομένων προσωπικού χαρακτήρα.

6.2.6 Διαχείριση κινδύνου ασφάλειας πληροφοριών

Η διασφάλιση της ιδιωτικότητας είναι άρρηκτα συνδεδεμένη με την ασφάλεια των πληροφοριακών συστημάτων που συμμετέχουν στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

Στην συγκεκριμένη κατηγορία έχουν συγκεντρωθεί όλες οι απαιτούμενες και μη, δραστηριότητες που πρέπει να εκτελέσει ο οργανισμός ή η επιχείρηση ώστε να αξιολογεί συχνά την ασφάλεια των πληροφοριακών συστημάτων, να εντοπίζει τα κενά ασφαλείας που μπορεί να οδηγήσουν σε παραβιάσεις και να ενισχύει όπου και όποτε απαιτείται τα τεχνικά μέτρα προστασίας των δεδομένων.

6.2.7 Διαχείριση κινδύνου που σχετίζεται με τρίτους

Παρά τα τεχνικά και οργανωτικά μέτρα που έχει εφαρμόσει ο υπεύθυνος επεξεργασίας με στόχο την διασφάλιση της ιδιωτικότητας υπάρχει περίπτωση για μια ενδεχόμενη παραβίαση να οφείλεται ένας τρίτος που συμμετέχει στην επεξεργασία, όπως ο εκτελών την επεξεργασία.

Ο κίνδυνος μιας παραβίασης τέτοιου είδους μετριάζεται αν ο οργανισμός ή η επιχείρηση προβεί σε εκτενή αξιολόγηση των τρίτων

με τους οποίους συνεργάζεται, προσθέτει στις συμβάσεις τους απαραίτητους όρους και προϋποθέσεις που πρέπει να πληρούν και διαθέτει διαδικασίες σε περίπτωση μη συμμόρφωσης με μια υπάρχουσα σύμβαση.

6.2.8 Τήρηση δηλώσεων

Η κατηγορία αυτή περιλαμβάνει τις απαραίτητες ενέργειες που πρέπει να κάνει ο υπεύθυνος επεξεργασίας δεδομένων προς ενημέρωση των υποκειμένων αναφορικά με την επικείμενη επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Βασική δραστηριότητα προς υλοποίηση είναι η δημιουργία δήλωσης απορρήτου και η διάθεση της σε όλα τα ενδιαφερόμενα τρίτα μέρη και τα υποκείμενα των δεδομένων μέσω διαφόρων μηχανισμών προώθησης όπως η ηλεκτρονική αλληλογραφία και τα συμβόλαια που πρόκειται να υπογραφούν.

6.2.9 Απαντήσεις αιτημάτων και παραπόνων

Προς συμμόρφωση με τα δικαιώματα των υποκειμένων ο υπεύθυνος επεξεργασίας οφείλει να αξιολογεί και να πράττει αναλόγως στα παράπονα και στα αιτήματα των υποκειμένων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Με σκοπό την επίτευξη του στόχου αυτού η κατηγορία αυτή περιλαμβάνει τις δραστηριότητες που πρέπει να εκτελεί ο υπεύθυνος επεξεργασίας όπως ο σχεδιασμός κι η εφαρμογή όλων των διαδικασιών για την εξυπηρέτηση των αιτημάτων των υποκειμένων και την διευκόλυνση άσκησης των δικαιωμάτων τους όπως αυτά ορίζονται από τον Κανονισμό.

6.2.10 Παρακολούθηση νέων επιχειρησιακών πρακτικών

Οι επιχειρήσεις και οι οργανισμοί οφείλουν να εκτελούν τακτικές εκτιμήσεις αντικτύπου σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα κατά την δημιουργία νέων συστημάτων και διαδικασιών, καθώς επίσης οφείλουν σε κάθε υλοποίηση να εφαρμόζουν την προστασία των δεδομένων προσωπικού χαρακτήρα ήδη από τον σχεδιασμό.

Τα αποτελέσματα της εκτίμησης θα πρέπει να γνωστοποιούνται στην ανώτατη διοίκηση και στις αρμόδιες αρχές για την υλοποίηση αλλαγών που θα δυνητικά θα μετριάσουν τον κίνδυνο ή εναλλακτικά για την αποδοχή του.

6.2.11 Τήρηση προγράμματος διαχείρισης παραβίασης της ιδιωτικότητας

Παρά την αποτελεσματικότητα των τεχνικών και των οργανωτικών μέτρων που έχει εφαρμόσει ο υπεύθυνος επεξεργασίας, πάντα υπάρχει ο υπολειπόμενος κίνδυνος μιας πιθανής παραβίασης δεδομένων προσωπικού χαρακτήρα.

Η κατηγορία αυτή περιλαμβάνει όλες τις απαραίτητες δραστηριότητες που θα πρέπει να εκτελέσει ο υπεύθυνος επεξεργασίας σε μία ενδεχόμενη παραβίαση ώστε να είναι σύννομος, όπως η παροχή κατάλληλων ενημερώσεων στα υποκείμενα των οποίων τα δεδομένα έχουν διαρρεύσει.

6.2.12 Παρακολούθηση πρακτικών διαχείρισης δεδομένων

Με στόχο την συνεχή βελτίωση του προγράμματος προστασίας δεομένων προσωπικού χαρακτήρα ο υπεύθυνος επεξεργασίας οφείλει να εκτελεί ανά τακτά χρονικά διαστήματα αξιολογήσεις και εσωτερικούς ελέγχους ώστε να προσδιορίζει την αποτελεσματικότητα των εφαρμοσμένων τεχνικών και οργανωτικών μέτρων.

Παράλληλα, προς απόδειξη συμμόρφωσης με τον Κανονισμό όλα τα αποτελέσματα των αξιολογήσεων και των ελέγχων θεωρούνται αποδεικτικά τα οποία φανερώνουν το επίπεδο συμμόρφωσης του οργανισμού ή της επιχείρησης.

6.2.13 Παρακολούθηση εξωτερικών κριτηρίων

Η τελευταία κατηγορία δραστηριοτήτων αφορά την ανάγκη συνεχούς ενημέρωσης σχετικά με νέους κανονισμούς και νόμους ή τροποποιήσεις των υπαρχόντων αναφορικά με την προστασία δεδομένων προσωπικού χαρακτήρα. Βασικός στόχος των δραστηριοτήτων αυτών είναι ο προσδιορισμός των εξελισσόμενων απαιτήσεων, η συμμόρφωση σε αυτές και η διασφάλιση της ιδιωτικότητας.

6.3 Αξιολόγηση κινδύνου

Ο υπεύθυνος επεξεργασίας που θα χρησιμοποιήσει το εργαλείο εκτίμησης της συμμόρφωσης με το Γενικό Κανονισμό για την Προστασία Δεδομένων καλείται, μελετώντας όλες τις δραστηριότητες ανά κατηγορία, να αξιολογήσει το επίπεδο εκτέλεσης τους.

Οι παρεχόμενες επιλογές για την δήλωση της κατάστασης στην οποία βρίσκεται η κάθε δραστηριότητα παρουσιάζονται στον ακόλουθο πίνακα:

Κατάσταση	Περιγραφή
Ικανοποιητική	Η δραστηριότητα εκτελείται ή έχει εκτελεσθεί σε τέτοιο επίπεδο που δεν απαιτείται κάποια διορθωτική ενέργεια για την απόδειξη συμμόρφωσης
Χρήζει Βελτίωσης	Απαιτείται ο επανασχεδιασμός και η βελτίωση της δραστηριότητας για την αδιαμφισβήτητη απόδειξη συμμόρφωσης
Μη Εκτελεσμένη	Η δραστηριότητα δεν εκτελείται ή δεν έχει εκτελεσθεί
Δ/Ε	Λόγω της φύσης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα δεν κρίνεται απαραίτητο να εκτελεσθεί η δραστηριότητα

Πίνακας 1 - Καταστάσεις μιας δραστηριότητας

Κατόπιν επιλογής μίας κατάστασης γίνεται αυτόματος υπολογισμός του κινδύνου που παρουσιάζει η κάθε δραστηριότητα. Τα κριτήρια που καθορίζουν τον κίνδυνο είναι:

1ον: η κατάσταση της δραστηριότητας (όπως αυτή θα επιλεχθεί από τον χρήστη του εργαλείου εκτίμησης συμμόρφωσης) και

2ον: η αναγκαιότητα εκτέλεσης μιας δραστηριότητας (όπως καθορίστηκε από τα επιμέρους άρθρα του Κανονισμού).

Στην συνέχεια παρουσιάζονται τα πιθανά επίπεδα κινδύνου που μπορεί να παρουσιάσει μία δραστηριότητα ανάλογα με τα δύο κριτήρια που προαναφέρθηκαν:

Κατάσταση της δραστηριότητας	Αναγκαιότητα Εκτέλεσης	Κίνδυνος
Δ/Ε	*Όχι*	0
	Ναι	
Ικανοποιητική	*Όχι*	
	Ναι	
Χρήζει Βελτίωσης	*Όχι*	1
	Ναι	3
Μη Εκτελεσμένη	*Όχι*	2
	Ναι	4

Πίνακας 2 - Υπολογισμός Κινδύνου

6.4 Παρουσίαση αποτελεσμάτων

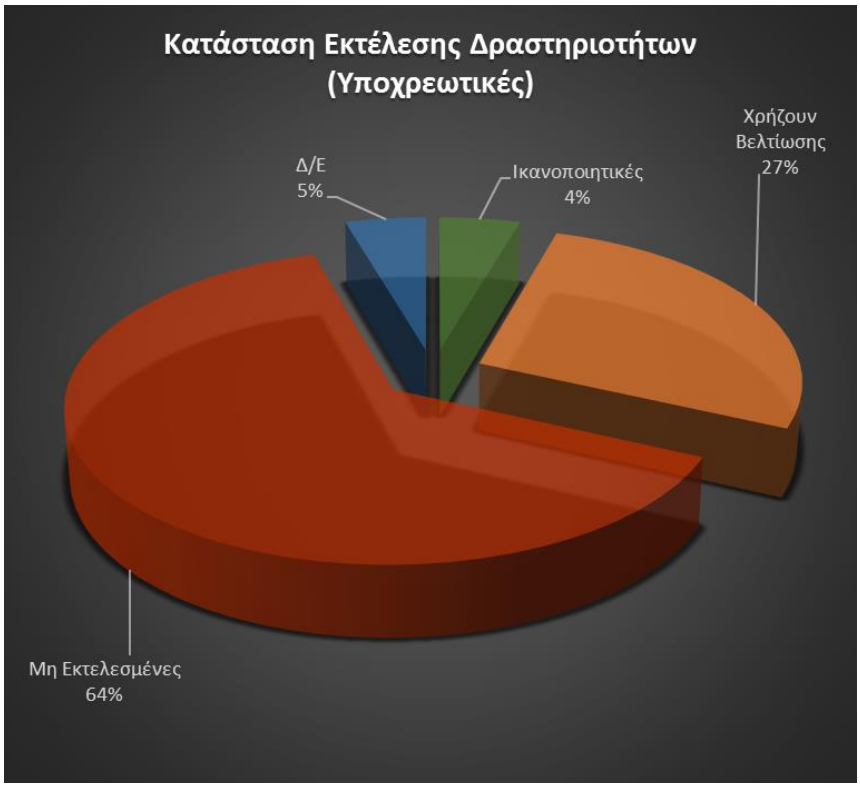
Το εργαλείο εκτίμησης συμμόρφωσης περιλαμβάνει και ένα σύνολο γραφημάτων για τη διευκόλυνση απεικόνισης συγκεντρωτικών αποτελεσμάτων της αξιολόγησης στον χρήστη, τα οποία παρουσιάζονται στη συνέχεια με τη χρήση ενδεικτικών παραδειγμάτων.

6.4.1 Ποσοστό Κινδύνου ανά Κατηγορία

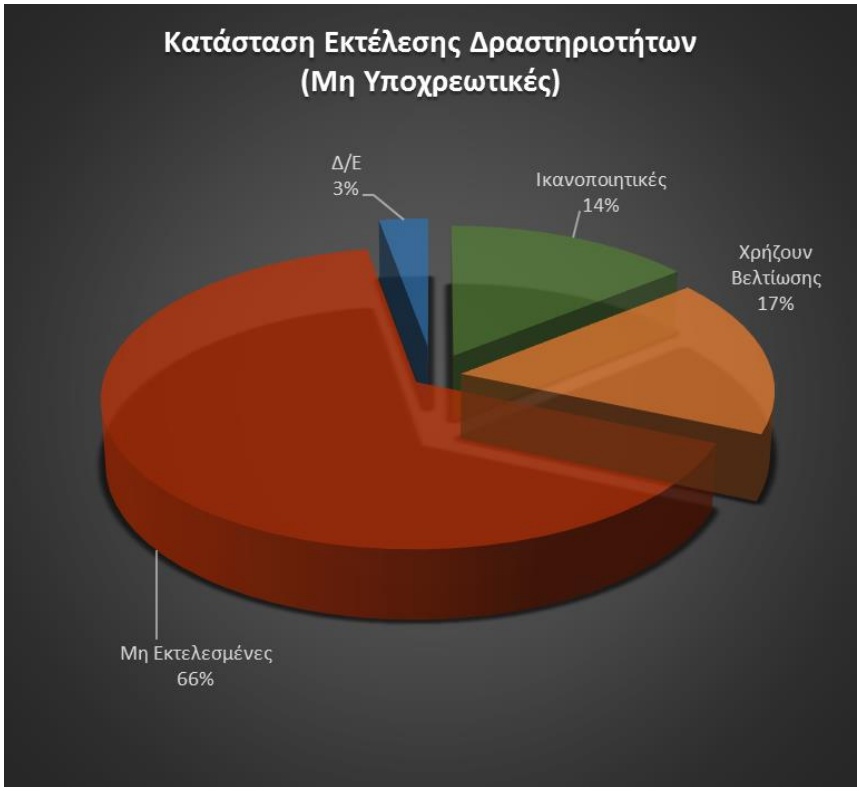
Εικόνα 3 - Κίνδυνος ανά Κατηγορία

Μέσω του γραφήματος αυτού, ανάλογα με το ποσοστό κινδύνου που συγκεντρώνει, ο χρήστης δύναται να εντοπίσει τις κατηγορίες των δραστηριοτήτων που χρήζουν άμεσης προσοχής ώστε να μπορεί να παρουσιάσει στην ανώτατη διοίκηση της επιχείρησης ή του οργανισμού τους τομείς όπου απαιτείται να διοχετευτούν επιχειρησιακοί πόροι.

6.4.2 Κατάσταση Εκτέλεσης Δραστηριοτήτων (Υποχρεωτικές / Μη Υποχρεωτικές)



Εικόνα 4 - Ποσοστό ανά κατάσταση (Υποχρεωτικές)



Εικόνα 5 - Ποσοστό ανά κατάσταση (Μη Υποχρεωτικές)

Τα γραφήματα αυτά παρουσιάζουν τα ποσοστά των δραστηριοτήτων σύμφωνα με την κατάσταση στην οποία βρίσκονται και την αναγκαιότητα - ή μη - εκτέλεσής τους. Προσφέρουν στον χρήστη μια συνολική εικόνα της συμμόρφωσης του οργανισμού ή της επιχείρησης. Τη μεγαλύτερη βαρύτητα, τη φέρει το πρώτο γράφημα καθώς απεικονίζει τις δραστηριότητες που ο Κανονισμός έχει ορίσει άμεσα ή έμμεσα ως υποχρεωτικές.

Βιβλιογραφία

[1] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679

[2] https://blog.varonis.com/gdpr-requirements-list-in-plain-english/

[3] https://www.i-scoop.eu/gdpr

[4] https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/

[5] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

[6] https://www.eugdpr.org/eugdpr.org-1.html

[7] https://ec.europa.eu/info/law/law-topic/data-protection_en

[8] https://www.lexology.com/library/detail.aspx?g=b3db89a5-ac63-4fcb-9d71-b08c00a609e3

[9] https://dma.org.uk/uploads/misc/5aabd9a90feff-gdpr-essentials-for-marketers----an-introduction-to-the-gdpr_5aabd9a90fe17.pdf

[10] https://iapp.org/media/pdf/resource_center/Nymit-Accountability-Roadmap-GDPR-Compliance.pdf

[11] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/