# ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ ΔΙΟΙΚΗΣΗ & ΟΡΓΑΝΩΣΗ ΕΚΠΑΙΔΕΥΤΙΚΩΝ ΜΟΝΑΔΩΝ

Διπλωματική Εργασία

## ΔΙΑΔΙΚΑΣΙΕΣ ΥΙΟΘΕΤΗΣΗΣ ΚΑΙ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ GENERAL DATA PROTECTION REGULATION (GDPR) ΩΣ ΔΕΙΚΤΗΣ ΠΟΙΟΤΗΤΑΣ ΣΤΑ ΑΕΙ.

## ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΤΟΥ Π.Μ.Σ. ΔΙΟΙΚΗΣΗ ΚΑΙ ΟΡΓΑΝΩΣΗ ΕΚΠΑΙΔΕΥΤΙΚΩΝ ΜΟΝΑΔΩΝ ΤΟΥ ΑΤΕΙΘ.

του

ΠΑΝΑΓΙΩΤΗ ΠΑΠΑΓΕΩΡΓΙΟΥ

Επιβλέπουσα Καθηγήτρια

Βάϊα Παπανικολάου

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του μεταπτυχιακού διπλώματος ειδίκευσης στη διοίκηση & οργάνωση εκπαιδευτικών μονάδων.

Θεσσαλονίκη, Σεπτέμβριος 2018

**Υπεύθυνη Δήλωση**

Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις που προβλέπονται από τον Κανονισμό Σπουδών του Μεταπτυχιακού Προγράμματος στη Διοίκηση & Οργάνωση Εκπαιδευτικών Μονάδων του Αλεξάνδρειου ΤΕΙ Θεσσαλονίκης, δηλώνω υπεύθυνα ότι:

- Η παρούσα Διπλωματική Εργασία αποτελεί έργο αποκλειστικά δικής μου δημιουργίας, έρευνας, μελέτης και συγγραφής.
- Για τη συγγραφή της Διπλωματικής μου Εργασίας δεν χρησιμοποίησα ολόκληρο ή μέρος έργου άλλου δημιουργού ή τις ιδέες και αντιλήψεις άλλου δημιουργού χωρίς να γίνεται σαφής αναφορά στην πηγή προέλευσης(βιβλίο, άρθρο από επιστημονικό περιοδικό, ιστοσελίδα κλπ.).

Θεσσαλονίκη, 21, Σεπτεμβρίου 2018

Ο Δηλών: Παναγιώτης Παπαγεωργίου

# ΠΕΡΙΛΗΨΗ

Η προστασία των φυσικών προσώπων έναντι της επεξεργασίας των προσωπικών του δεδομένων αποτελεί θεμελιώδες δικαίωμα. Καίριες δομές της Πολιτείας, όπως είναι τα Εκπαιδευτικά Ιδρύματα, χειρίζονται προσωπικά δεδομένα των φοιτητών και του προσωπικού. Τα δεδομένα αυτά φυλάσσονται ψηφιακά και κάποιες φορές η αποθήκευση τους δεν συμβαίνει σε φυσικούς χώρους του Ιδρύματος αλλά σε απομακρυσμένες περιοχές. Δεδομένου ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) είναι μια Οδηγία της Ευρωπαϊκής Ένωσης άμεσα υποχρεωτική και υλοποιήσιμη από τον Μάιο του 2018, όπου η μη συμμόρφωση επιφέρει υπέρογκα πρόστιμα, προκύπτει επιτακτική ανάγκη τα Εκπαιδευτικά Ιδρύματα να προβούν στην υιοθέτηση κουλτούρας και εφαρμογή συστημάτων που θα αποσκοπούν στη συμμόρφωση τους με τις επιταγές της Οδηγίας και θα εξασφαλίζουν γενικότερα την ασφάλεια των πληροφοριακών συστημάτων.

Η εφαρμογή του ΓΚΠΔ στον ευαίσθητο τομέα της Εκπαίδευσης αποτελεί αντικείμενο διερεύνησης, μιας και δεν υπάρχουν διαθέσιμα βιβλιογραφικά δεδομένα, εξαιτίας της πρόσφατης υιοθέτησης του και συνεπώς μόνο από περιορισμένα εμπειρικά δεδομένα μπορούμε να αντλήσουμε πληροφορίες.

Η παρούσα διπλωματική εργασία σκοπό έχει να προτείνει ένα γενικό πλαίσιο οργάνωσης μίας Εκπαιδευτικής Μονάδας, προκειμένου να είναι συμμορφωμένη με τις απαιτήσεις του ΓΚΠΔ.

Για τους παραπάνω σκοπούς θα γίνει αναφορά στο Πρόγραμμα Μεταπτυχιακών Σπουδών ΄ Διοίκησης και Οργάνωση Εκπαιδευτικών Μονάδων ΄ της Σχολής Διοίκησης και Οικονομίας του Αλεξάνδρειου Τεχνολογικού Εκπαιδευτικού Ιδρύματος Θεσσαλονίκης. Θα προταθεί ένα σύστημα οργάνωσης το οποίο αν εφαρμοστεί στην καθημερινή εκπαιδευτική πραγματικότητα θα οδηγήσει σε συμμόρφωση με τις απαιτήσεις του ΓΚΠΔ. Ταυτόχρονα θα γίνει προσπάθεια να εντοπιστούν οι δυσκολίες που προκύπτουν στο στάδιο της υλοποίησης και θα προταθούν λύσεις, με απώτερο σκοπό την πρόταση ενός ολοκληρωμένου συστήματος ποιότητας συμβατό με τις ιδιαιτερότητες της Οργάνωσης μιας Εκπαιδευτικής Μονάδας.

# ABSTRACT

General Data Protection Regulation (GDPR) is an European Union (EU) regulation intended to strengthen and unify data protection for all individuals within the EU. The enforcement date is 25th May 2018, at which time organizations in non-compliance will face heavy fines. In accordance with the GDPR, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data. Crucial social structure, as the Educational Institutes must interpret and apply the new EU legislation, with regards to requesting student consent for the use of their data for learning analytics. Due to the fact, that these kind of data are stored in servers, the Educational policy must provide the Security of Informatics Systems in order to eliminate the possibility for data leakage.

Due to the fact that the GDPR legislation is extremely newly, limited bibliography data are available and few empirical studies are the only source of knowledge.

The aim of MSc thesis is to propose the general context of GDPR compliance that an Educational Institute must apply in order to avoid heavy fines. Acceptance of specific procedures guarantee the success of this undertaking.

Master of Alexander Technological Educational Institute will be referred as the case study of this purpose. Taking under consideration the difficulties and the limitations of GDPR EU legislation when is applied in an Educational Institute, here is the first systematic approach to create a complete quality system for this purpose.

In the meantime, we will try to spot the difficulties and suggest solutions in order this completed procedure could be easily applicable in the daily practical routine.

# Περιεχόμενα

***Το κλίμα εμπιστοσύνης***

*χρειάζεται χρόνια για να χτιστεί*

*δευτερόλεπτα για να γκρεμιστεί*

*και αιώνες για να επανέρθει…*

# *ΓΕΝΙΚΟ ΜΕΡΟΣ*

# Εισαγωγή

Η ανάπτυξη της πληροφορικής και η εμπλοκή της σε τομείς της καθημερινότητας ελοχεύουν κινδύνους για τον πολίτη όσον αφορά την "ασφάλεια" των προσωπικών του δεδομένων από κακόβουλες επιθέσεις υπαρκτός αυτός κίνδυνος επέβαλε τα τελευταία χρόνια τη ρυθμιστική επέμβαση του νομοθέτη προς την κατεύθυνση της προστασίας των προσωπικών δεδομένων από την αθέμιτη επεξεργασία τους. Στόχος των σχετικών νομοθεσιών είναι η διασφάλιση της προστασίας των θεμελιωδών δικαιωμάτων και ιδίως της ιδιωτικής ζωής (Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου 2002).

Ωστόσο, τα πράγματα δεν είναι μονοδιάστατα. Δεν είναι μόνο η ιδιωτική ζωή του ατόμου που πρέπει να προστατευθεί. Μέσα σε μια δημοκρατική κοινωνία υπάρχουν και άλλα έννομα αγαθά των οποίων την προστασία εγγυάται το κράτος δικαίου. Ένα από τα πλέον σημαντικά είναι η προστασία των προσωπικών δεδομένων.

Σε ένα ρευστό και μεταβαλλόμενο περιβάλλον, όπου όλα τείνουν να είναι πολύπλοκα και αντιφατικά εξαιτίας των ραγδαίων τεχνολογικών αλλαγών που συντελούνται αλλά και της εξέλιξης της γνώσης απαιτείται άμεση και αποτελεσματική προσαρμογή στα νέα δεδομένα ειδικότερα όταν αυτά επηρεάζουν οργανωτικές δομές που σχετίζονται με την ελληνική εκπαιδευτική πραγματικότητα, όπως είναι η αναφορά, αποθήκευση και προστασία των προσωπικών δεδομένων φοιτητών που ανήκουν στην πανεπιστημιακή κοινότητα. .

Η λειτουργία τμημάτων τριτοβάθμιας εκπαίδευσης ως αυτοτελών οργανισμών αλλά ταυτόχρονα και ως τμήματα του τρέχοντος εκπαιδευτικού συστήματος στη χώρα μας θα πρέπει να παρακολουθούν τις εξελίξεις αυτές, να προσαρμόζονται στα νέα δεδομένα, να επικαιροποιούν τις εκπαιδευτικές διαδικασίες και τον τρόπο οργάνωσής τους ανάλογα με τις προκύπτουσες απατήσεις, να υπολογίζουν τα ρίσκα από τη μη τήρηση των αλλαγών αυτών, να οργανώνονται εν γένει εντός ενός συστήματος που θα διέπεται από μια σειρά καλά χαρακτηρισμένων διεργασιών ως τμήματα της γενικότερης διαδικασίας.(Moskal, Dziuban, and Hartman 2013)

Συχνά γίνεται αναφορά τον τελευταίο καιρό στον Γενικό Κανονισμό Προστασίας Δεδομένων ( ΓΚΠΔ) της Ευρωπαϊκής Ένωσης (Κανονισμος, Ευρωπαϊκου, Συμβουλιου 2016) που έχει ανακοινωθεί από το 2016 και όπου έχει τεθεί σε ισχύ από τις 25 Μαΐου 2018 ο οποίος και αντικαθιστά τον νόμο περί προστασίας δεδομένων 2472/1997(Κανονισμός, Ευρωπαϊκου,

Συμβουλιου 2016) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ο οποίος και καταργείται.

Η πρόσφατη δραστηριότητα σχετικά με τις παραβιάσεις δεδομένων που υφίστανται οργανισμοί και ιδιώτες συνεχίζει να καθιστά τον τομέα προστασίας προσωπικών δεδομένων ένα θέμα άμεσης προτεραιότητας για τα εκπαιδευτικά ιδρύματα. Είναι σημαντικό ένα εκπαιδευτικό ίδρυμα να έχει σαφή και κατανοητή πολιτική χειρισμού προσωπικών δεδομένων προκειμένου να αποφεύγει παραβιάσεις που μπορεί να προκύψουν από(UNIVERSITY OF CAMBRIDGE UPDATE ON PREPARATIONS FOR THE GDPR 2018):

- κλοπή,
- σκόπιμη επίθεση στα συστήματα διαχείρισης δεδομένων ,
- μη εξουσιοδοτημένη ή κακόβουλη χρήση προσωπικών δεδομένων από μέλος του προσωπικού
- τυχαία απώλεια ή αποτυχία εξοπλισμού.

Ένα εκπαιδευτικό ίδρυμα ανέκαθεν είχε και θα έχει προσωπικά δεδομένα των φοιτητών που και όλο και περισσότερο αυτά τα δεδομένα κρατούνται ψηφιακά και προσβάσιμα όχι μόνο στους χώρους του ιδρύματος αλλά και σε απομακρυσμένες τοποθεσίες. Είναι σημαντικό να τονιστεί ότι οι νόμοι για την προστασία των δεδομένων ισχύουν για όλες τις μορφές δεδομένων προσωπικού χαρακτήρα, ανεξάρτητα αν τηρούνται σε χαρτί ή ηλεκτρονική μορφή. Ωστόσο δεδομένου ότι αποτελεί μέρος ενός γενικού προτύπου πολιτικής ασφάλειας online, το έγγραφο αυτό δίνει ιδιαίτερη έμφαση στα δεδομένα που διατηρούνται ή μεταβιβάζονται ψηφιακά. Η επανεξέταση της πολιτικής προστασίας των προσωπικών δεδομένων κρίνεται πλέον υποχρεωτική σύμφωνα με τον Κανονισμό της Ευρωπαϊκής Ένωσης 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών(Κανονισμός, Ευρωπαϊκου, Συμβουλιου 2016)

Η υιοθέτηση των απαιτήσεων που επιβάλλονται από τον ΓΚΠΔ, ιδιαίτερα στα εκπαιδευτικά ιδρύματα, αποτελεί θέμα έντονης συζήτησης. Είναι σημαντικό το εκπαιδευτικό ίδρυμα να έχει μια σαφή και κατανοητή πολιτική χειρισμού προσωπικών δεδομένων, προκειμένου να ελαχιστοποιηθεί ο κίνδυνος παραβίασης προσωπικών δεδομένων.

Μια παραβίαση μπορεί να προκύψει εξαιτίας πολλών λόγων, π.χ από κλοπή, σκόπιμη επίθεση στα συστήματά σας, μη εξουσιοδοτημένη ή κακόβουλη χρήση προσωπικών δεδομένων από μέλος του προσωπικού, τυχαία απώλεια ή αποτυχία εξοπλισμού. Είναι απόλυτα κατανοητό ότι κανένα σχολείο ή άτομο δεν θα ήθελε να είναι η αιτία παραβίασης των δεδομένων. Η δημιουργία μίας τέτοιας κατάστασης θα ήταν ιδιαίτερα επιζήμια για το ίδρυμα λόγω του γεγονότος ότι ο αντίκτυπος της απώλειας δεδομένων στα άτομα θα μπορούσε δυνητικά ακόμα και να θέσει σε κίνδυνο τα άτομα και να επηρεάσει την προσωπική ή επαγγελματική φήμη

Μέσα σε αυτό το πλαίσιο, τα εκπαιδευτικά ιδερύματα είναι «πλούσια σε δεδομένα» και η εισαγωγή της ηλεκτρονικής αποθήκευσης και διαβίβασης δεδομένων έχει δημιουργήσει πρόσθετες δυνατότητες για την απώλεια δεδομένων

Τα πανεπιστήμια οφείλουν να αποφύγουν την κριτική και την αρνητική δημοσιότητα που μπορεί να δημιουργηθεί από οποιαδήποτε παραβίαση προσωπικών δεδομένων και γι αυτό το λόγο οφείλουν να υπόκεινται σε ένα ευρύ φάσμα νομοθεσίας σχετικά με την προστασία δεδομένων και τη χρήση δεδομένων, με σημαντικές κυρώσεις για μη τήρηση της σχετικής νομοθεσίας

Είναι καίριας σημασίας για όλα τα εκπαιδευτικά ιδερύματα να έχουν πολιτική προστασίας δεδομένων.

Τα πανεπιστήμια ανέκαθεν είχαν προσωπικά δεδομένα για τους μαθητές που βρίσκονταν στη φροντίδα τους και όλο και περισσότερο αυτά τα δεδομένα κρατούνται ψηφιακά και προσβάσιμα όχι μόνο στο σχολείο αλλά και σε απομακρυσμένες τοποθεσίες. Είναι σημαντικό να τονιστεί ότι οι νόμοι για την προστασία των δεδομένων ισχύουν για όλες τις μορφές δεδομένων προσωπικού χαρακτήρα, ανεξάρτητα από το αν τηρούνται σε χαρτί ή σε ηλεκτρονική μορφή. Ωστόσο, δεδομένου ότι αποτελεί μέρος ενός γενικού προτύπου πολιτικής ασφάλειας online, το έγγραφο αυτό δίνει ιδιαίτερη έμφαση στα δεδομένα που διατηρούνται ή μεταβιβάζονται ψηφιακά.

Τα εκπαιδευτικά ιδρύματα θα πρέπει να επανεξετάσουν προσεκτικά την πολιτική τους, υπό το πρίσμα των σχετικών κανονισμών και καθοδήγησης της περιφερειακής δομής / αρμόδιου φορέα και των νομοθετικών αλλαγών. Τα σχολεία και το προσωπικό τους πρέπει να κάνουν ό, τι είναι δυνατόν για να διασφαλίσουν την ασφάλεια και την ασφάλεια οποιουδήποτε

υλικού προσωπικής ή ευαίσθητης φύσης, συμπεριλαμβανομένων των προσωπικών δεδομένων.

Είναι ευθύνη όλων των μελών της σχολικής κοινότητας να φροντίζουν όταν χειρίζονται, χρησιμοποιούν ή μεταφέρουν προσωπικά δεδομένα, ότι αυτά δεν μπορούν να είναι προσβάσιμα σε κανέναν που δεν:

1. έχει άδεια πρόσβασης στα δεδομένα αυτά

2. πρέπει να έχει πρόσβαση σε αυτά τα δεδομένα.

Οι παραβιάσεις δεδομένων ενδέχεται να έχουν σοβαρές επιπτώσεις στα ενδιαφερόμενα άτομα ή / και ιδρύματα, να οδηγήσουν το σχολείο σε δυσφήμιση και μπορεί να οδηγήσουν σε πειθαρχική ή ποινική δίωξη. Ιδιαίτερα, κάθε μεταφορά δεδομένων υπόκειται σε κίνδυνο απώλειας ή μόλυνσης.

Από τα παραπάνω εύκολα γίνεται αντιληπτή ,σύμφωνα με τα παραπάνω, η αναγκαιότητα οργάνωσης των εκπαιδευτικών ιδρυμάτων μέσα σε συγκεκριμένα πλαίσια ασφάλειας των πληροφοριακών τους συστημάτων.(Data and Bill 2018) Παρόλα αυτά δεν θα πρέπει να λησμονεί κάποιος το γεγονός ότι η διοίκηση των εκπαιδευτικών ιδρυμάτων είναι ένα ΄΄ γρανάζι ΄΄ μόνο του ελληνικού διοικητικού συστήματος το οποίο χαρακτηρίζεται από όλες τις ΄΄ αδυναμίες της δημόσιας διοίκησης, (Κυριακή Σπανού 1996) από πολυνομία συχνά αντικρουόμενη , δυσκίνητη γραφειοκρατία και φυσικά μη επικαιροποιημένες διοικητικές διαδικασίες που την καθιστούν ανελαστική, χρονοβόρα και τελικά μη αποτελεσματική και παραγωγική.

Συμπερασματικά η άποψη που ευρέως είναι αποδεκτή αναγνωρίζει τις δυσκολίες εφαρμογής του κανονισμού αυτού βασισμένο στην ασφάλεια των προσωπικών δεδομένων στο χώρο της εκπαίδευσης ως μέρος του δημόσιου βίου του ανθρώπου. Παρόλες τις εγγενείς δυσκολίες εφαρμογής του, αναγνωρίζεται ταυτόχρονα η επιτακτική ανάγκη υλοποίησης ενός τέτοιου συστήματος προκειμένου να αποφύγουμε τις κυρώσεις μη υλοποίησης του Κανονισμού αυτού.

Το ερώτημα λοιπόν που παραμένει είναι κατά πόσο οι κοινωνοί της εκπαίδευσης αλλά και οι ανώτεροί τους θα υιοθετήσουν και θα εφαρμόσουν αυτόν τον Κανονισμό.

Παρακάτω θα γίνει μια προσπάθεια να καταγραφούν οι απαιτήσεις του Κανονισμού και να προσαρμοστούν αυτές στο περιβάλλον ενός εκπαιδευτικού ιδρύματος και συγκεκριμένα στο

Πρόγραμμα Μεταπτυχιακών Σπουδών ΄΄Διοίκηση και Οργάνωση Εκπαιδευτικών Μονάδων της Σχολής Διοίκησης και Οικονομίας του Αλεξάνδρειου Τεχνολογικού Εκπαιδευτικού Ιδρύματος Θεσσαλονίκης. Θα διερευνηθεί ο τρόπος υιοθέτησης της διαδικασίας στην καθημερινή εκπαιδευτική πραγματικότητα και θα καταγραφούν οι δυσκολίες από την εφαρμογή.

Στόχος της παραπάνω εργασίας είναι να διερευνηθεί η δυνατότητα δόμησης ενός συστήματος το οποίο θα πληροί όλες τις απαιτήσεις του ΓΚΠΔ και το οποίο δυνητικά θα μπορεί να εφαρμοστεί από τη συγκεκριμένη εκπαιδευτική μονάδα. Μέσα στα πλαίσια της διπλωματικής εργασίας θα γίνει προσπάθεια να εντοπιστούν οι δυσκολίες υλοποίησης του συστήματος εξαιτίας των ιδιαιτεροτήτων που χαρακτηρίζουν μία οργανωμένη εκπαιδευτική μονάδα. Το γεγονός ότι το Π.Μ.Σ. χρησιμοποιείται ως μελέτη περίπτωσης δεν θα πρέπει να μειώνει τη δυσκολία και την αξία του εγχειρήματος, μιας και το Π.Μ.Σ αποτελεί ένα μικρό μόνο μέρος του συνολικού εκπαιδευτικού ιδρύματος του ΑΤΕΙΘ και θα πρέπει η οργάνωση του συστήματος του Π.Μ.Σ να λειτουργεί αρμονικά με το σύνολο των επιμέρους δομών του ΑΤΕΙΘ, ικανοποιώντας ταυτόχρονα τις απαιτήσεις για συμμόρφωση με το ΓΚΠΔ.

Το γεγονός ότι ο Κανονισμός τέθηκε σε ισχύ μόλις τον Μάιο του 2018, δυσκολεύει ακόμα περισσότερο την ολοκλήρωση του εγχειρήματος αφού τα βιβλιογραφικά δεδομένα είναι ελάχιστα και ταυτόχρονα η εμπειρία πάνω στο συγκεκριμένο πεδίο είναι περιορισμένη.

## Κεφάλαιο 1 . Προσωπικά δεδομένα vs ευαίσθητα προσωπικά δεδομένα

Ως προσωπικό δεδομένο ορίζεται οποιοδήποτε στοιχείο πληροφορίας συνδέεται με ένα άτομο ( υποκείμενο δεδομένων ) και μπορεί να χρησιμοποιηθεί άμεσα ή έμμεσα για την ταυτοποίηση του.(Ευρωπαϊκή Ένωση 2016) Μπορεί να είναι ένα όνομα, αριθμός ταυτότητας, δεδομένα θέσης ακόμη και online ID. Επίσης ένα ή περισσότερα στοιχεία που προσδιορίζουν τη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα ενός φυσικού προσώπου.

Ως ευαίσθητα προσωπικά δεδομένα χαρακτηρίζονται τα προσωπικά δεδομένα που αναφέρονται στον πυρήνα της ιδιωτικής ζωής ενός ατόμου και σχετίζονται με τα ιατρικά δεδομένα ενός ατόμου, με τις σεξουαλικές του προτιμήσεις, με τα θρησκευτικά του πιστεύω κ.ο.κ.. (Ευρωπαϊκή Ένωση 2016)

Σύμφωνα με τους παραπάνω ορισμούς εύκολα μπορούμε να καταλάβουμε ότι με τον όρο "προσωπικά δεδομένα" δεν αναφερόμαστε στις ίδιες πληροφορίες και δεν μπορούμε όλες να τις αντιμετωπίζουμε με τον ίδιο τρόπο. Κάποια παρουσιάζουν κάποιο ιδιαίτερο βαθμό σημαντικότητας που τα διαφοροποιεί από τα απλά δεδομένα και για αυτό ακριβώς το λόγω χρειάζονται ιδιαίτερη προστασία και ιδιαίτερο τρόπο χειρισμού.

Για την ιδιαίτερη προστασία αυτών λοιπόν των δεδομένων έχει δημιουργηθεί η Οδηγία 95/46ΕΚ (Επίσημη Εφημερίδα τον Ευρωπαϊκών Κοινοτήτων 1995) η οποία προβλέπει την απαγόρευση επεξεργασίας ορισμένων κατηγοριών προσωπικών δεδομένων λόγω του ιδιαίτερου "πληροφοριακού βάρους" που φαίνεται να διαθέτουν. Συγκεκριμένα στο άρθρο 8 της Οδηγίας αναφέρει ότι τέτοιου είδους δεδομένα αποτελούν :

- η Φυλετική ή εθνική καταγωγή
- τα πολιτικά φρονήματα
- οι θρησκευτικές και φιλοσοφικές πεποιθήσεις
- η συμμετοχή σε συνδικαλιστικές οργανώσεις
- η σεξουαλική ζωή

Η ελληνική νομοθεσία ακολουθώντας την συγκεκριμένη κατεύθυνση πρόσθεσε σε αυτήν την κατηγορία δεδομένων και άλλα στοιχεία δημιουργώντας πλέον μια κλειστή κατηγορία ευαίσθητων προσωπικών δεδομένων. Οπότε στα είδη αρχικά δεδομένα που υπήρχαν προστέθηκαν και

- Η κοινωνική πρόνοια
- η συμμετοχή σε ενώσεις και σωματεία
- οι ποινικές διώξεις και καταδίκες

Με την διαδικασία αυτή και δημιουργώντας αυτήν την κλειστή ομάδα ο νομοθέτης προστατεύει θα λέγαμε εις διπλούν τον κάθε πολίτη από οποιαδήποτε μορφή μη νόμιμης επεξεργασίας χωρίς όμως να απαγορεύει το γεγονός δημιουργίας υποομάδων ευαίσθητων προσωπικών δεδομένο που απορρέουν από τα είδη υπάρχοντα δεδομένα της ομάδας αυτής και τα οποία προσθέτονται μετά από αξιολόγηση του κάθε νομοθέτη. Σε αυτές τις υποομάδες για παράδειγμα μπορούμε να αναφέρουμε(Επίσημη Εφημερίδα τον Ευρωπαϊκών Κοινοτήτων 1995) :

1. Τα στοιχεία αναγνώρισης ατόμων ( στοιχεία ταυτότητας, στοιχεία ληξιαρχείων, καταγωγή ).
2. Προσωπικά χαρακτηριστικά ( ενδιαφέροντα, συνήθειες, ταξίδια)
3. Συνθήκες οικογένειας ( έγγαμος βίος, οικογενειακή κατάσταση, κοινωνικές επαφές ).
4. Εκπαίδευση ( ακαδημαϊκά δεδομένα, πιστοποιητικά, φοιτητικά/ μαθητικά αρχεία)
5. Οικονομική κατάσταση ( έσοδα, δάνεια , περιουσιακά στοιχεία, δεδομένα ασφάλισης)

Σύμφωνα με τα παραπάνω μπορούμε να γίνει εύκολα αντιληπτό γιατί τα προσωπικά δεδομένα πρέπει να προστατεύονται. Η ανάπτυξη της τεχνολογίας έχει αυξήσει τους κινδύνους της προσβολής της ιδιωτικότητας της ζωής μας. Μέσα σε λίγα δευτερόλεπτα είναι δυνατόν να αντληθούν διάφορα στοιχεία για την προσωπική μας ζωή, την οικονομική και κοινωνική κατάσταση κάποιου ατόμου που σε συνδυασμό με άλλες πληροφορίες να οδηγήσουν σε μια συνολική καταγραφή της προσωπικότητας του ατόμου στη σύνθεση δηλαδή το ατομικού του προφίλ εκθέτοντάς το.

# Κεφάλαιο 2 . Ο Γενικός Κανονισμός για την Προστασία των δεδομένων (ΓΚΠΔ)

## 2.1 Γενικά

Ο Γενικός Κανονισμός για την Προστασία των δεδομένων αφορά κάθε επιχείρηση και οργανισμό που διατηρεί ή επεξεργάζεται προσωπικά δεδομένα φυσικών προσώπων που βρίσκονται στην Ευρώπη ανεξαρτήτως ιθαγένειας ή τόπου διαμονής τους.(Ευρωπαϊκή Ένωση 2016)

Έχει σκοπό να προστατεύει τα φυσικά πρόσωπα έναντι της επεξεργασίας των προσωπικών τους δεδομένων και την ελεύθερη κυκλοφορία των δεδομένων αυτών και επίσης να καταργήσει την οδηγία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 95/46ΕΚ.(Directive 95/46/EC of the European Parliament and of the Council n.d.) Επίσης, ρυθμίζει θέματα διαβίβασης δεδομένων εκτός Ευρωπαϊκών συνόρων.

Ο Κανονισμός είναι είδη σε ισχύ από τις 25 Μαΐου 2018 και δεν απαιτείται επιπλέον έγκριση από τις κυβερνήσεις των μελών κρατών, η υλοποίηση και η εφαρμογή του. Έχει είδη ψηφιστεί από το Ευρωκοινοβούλιο, τον Απρίλιος 2016, όπου και δημοσιεύτηκε στην Εφημερίδα της Ευρωπαϊκής Ένωσης. Δεν είναι μια καινούργια νομοθεσία, αποτελεί μια ισχυρότερη και εκσυγχρονισμένη εκδοχή της Οδηγίας 95/46ΕΚ (Directive 95/46/EC of the European Parliament and of the Council n.d.) με τη διαφορά τώρα ότι ο Κανονισμός έχει καθολική ισχύ στα κράτη μέλη ορίζει αυστηρότερες απαιτήσεις και προβλέπει υψηλά πρόστιμα για τους παραβάτες.

Τα πρόστιμα που προβλέπει ο Κανονισμός είναι δυσβάσταχτα και ανέρχονται στα 20 εκατομμύρια ευρώ ή στο 4% του παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, εφόσον πρόκειται για επιχείρηση. Το πρόστιμο αυτό δύναται να επιβληθεί σε σοβαρές παραβιάσεις του Κανονισμού, όπως παραβιάσεις που αφορούν την συγκατάθεση του ατόμου, τις βασικές αρχές προστασίας δεδομένων Ευρωπαίων Πολιτών, τη μη συμμόρφωση με τις υποδείξεις των εποπτικών αρχών. Υπάρχουν όμως και περιπτώσεις που προβλέπεται πρόστιμο 10 εκατομμυρίων ευρώ ή το 2% του παγκόσμιου ετήσιου κύκλου εργασιών για παράδειγμα τη μη τήρηση οργανωμένων αρχείων, τη μη γνωστοποίηση για παραβίαση ασφαλείας, την παράλειψη ορισμού Υπεύθυνου προστασίας Δεδομένων ( DPO) στις περιπτώσεις που επιβάλλεται, την ατελή εφαρμογή ή απουσία τεχνικών και οργανωτικών μέτρων για την εξασφάλιση της προστασίας δεδομένων από το σχεδιασμό εξ΄ορισμού (

Άρθρο 83), στοιχεία δηλαδή που άπτονται στην εφαρμογή του ISO 27001, που αφορά την ασφάλεια των πληροφοριακών συστημάτων.

## 2.2 Βασικές Αρχές και απαιτήσεις του Κανονισμού

Οι αρχές και οι απαιτήσεις που διέπουν τον Κανονισμό (Miroslav Hrubý 2016) είναι :

1. Αρχές επεξεργασίας
   1.1. Νομιμότητα, αντικειμενικότητα και διαφάνεια
   1.2. Περιορισμός του σκοπού ( τεκμηρίωση του σκοπού που συλλέγει και επεξεργάζεται τα δεδομένα).
   1.3. Ελαχιστοποίηση των δεδομένων (τα απολύτως απαραίτητα δεδομένα για τους σκοπούς που έχουν οριστεί).
   1.4. Ακρίβεια ( ορθά και επίκαιρα δεδομένα).
   1.5. Περιορισμός περιόδου αποθήκευσης (να τηρούνται για λίγο χρονικό διάστημα, να απαιτείται σύμφωνα με το νόμιμο σκοπό)
   1.6. Ακεραιότητα και εμπιστευτικότητα (διασφάλιση προστασίας και παράνομης επεξεργασίας των δεδομένων).
   1.7. Λογοδοσία ή αρχή-ομπρέλα (του υπεύθυνου επεξεργασίας ο οποίος φέρει την ευθύνη και επιπλέον να είναι σε θέση να αποδείξει την συμμόρφωση όλων των παραπάνω). (Άρθρο 5)(Ευρωπαϊκή Ένωση 2016)
2. Ρητή συγκατάθεση του ατόμου που είναι και το υποκείμενο των δεδομένων να συμφωνεί με δήλωση ή με σαφή θετική ενέργεια τα δεδομένα του προσωπικού του χαρακτήρα να αποτελέσουν αντικείμενο επεξεργασίας. Η μη αντίδραση του ατόμου όπως π.χ η παθητική παραμονή σε λίστες newsletter, δεν ισοδυναμεί με συγκατάθεση, σύμφωνα με τον νέο Κανονισμό. Για προσωπικά δεδομένα ανηλίκων κάτω των 16 ετών, απαιτείται η συγκατάθεση γονέα ή κηδεμόνα. Ο εκάστοτε οργανισμός οφείλει να τηρεί αρχείο και διαδικασία η οποία να επιτρέπει στο άτομο να διαφοροποιήσει τη συγκατάθεση που έδωσε για μια συγκεκριμένη χρήση, όσες φορές αλλάξει γνώμη. (Άρθρο 6-8)(Ευρωπαϊκή Ένωση 2016)
3. Σαφής πολιτική απορρήτου. Οι οργανισμοί απαιτούνται να δηλώνουν με διαφάνεια, σαφή γλώσσα και κατανοητό τρόπο την πολιτική απορρήτου που εφαρμόζουν ( συλλογή δεδομένων, ποιος ο νόμιμος σκοπός , ποια η διαχείριση αυτών και ποιο το χρονικό διάστημα διατήρησης των δεδομένων). (Άρθρο 12)(Ευρωπαϊκή Ένωση 2016)

4. Ατομικά δικαιώματα
    4.1. Όλα τα άτομα να έχουν δικαίωμα να επέμβουν στα δεδομένα τους προκειμένου να τα διορθώσουν – Δικαίωμα Διόρθωσης.
    4.2. Όλα τα άτομα να έχουν δικαίωμα παραλαβής των δεδομένων σε δομημένο, συμβατό μορφότυπο προκειμένου να διαβιβαστούν σε άλλον υπεύθυνο επεξεργασίας – Δικαίωμα στη Φορητότητα
    4.3. Όλα τα άτομα να έχουν δικαίωμα στη διαγραφή των δεδομένων τους – Δικαίωμα στη Λήθη. (Άρθρο 13-23)(Ευρωπαϊκή Ένωση 2016)
5. Ευθύνη και λογοδοσία. Οι οργανισμοί είναι διαρκώς υπόλογοι στα άτομα και στις Αρχές. Οφείλουν, όχι απλώς να εφαρμόζουν το νέο Κανονισμό, αλλά και να είναι κάθε στιγμή σε θέση να αποδείξουν ότι συμμορφώνονται με όλες τις απαιτήσεις του ( Άρθρο 24) (Ευρωπαϊκή Ένωση 2016)
6. Προστασία από τον αρχικό σχεδιασμό εξ ορισμού. Ο οργανισμός οφείλει να εφαρμόζει αποτελεσματικά τα κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδοανωνυμοποίηση, η ελαχιστοποίηση των δεδομένων και η ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία τους κατά τρόπο ώστε να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων. (Άρθρο 25)(Ευρωπαϊκή Ένωση 2016)
7. Ασφάλεια Επεξεργασίας. Ο οργανισμός που τηρεί και διαχειρίζεται προσωπικά δεδομένα οφείλει να εφαρμόζει τα απαραίτητα συστήματα, πολιτικές και διαδικασίες που εξασφαλίζουν τα απαιτούμενα επίπεδα προστασίας των δεδομένων αυτών, συμπεριλαμβανομένης της προστασίας από την παράνομη πρόσβαση και επεξεργασία, τόσο από το προσωπικό του οργανισμού, όσο και από τρίτους, την κατά λάθος απώλεια, καταστροφή ή αλλοίωση τους (Άρθρο 32)(Ευρωπαϊκή Ένωση 2016)
8. Γνωστοποίηση παραβίασης εντός 72 ωρών. Σε περίπτωση παραβίασης ασφαλείας που αφορά προσωπικά δεδομένα οι οργανισμοί οφείλουν να ενημερώνουν εντός 72 ωρών από τη στιγμή που αποκτούν γνώση του γεγονότος, τις αρμόδιες αρχές ( Άρθρο 33-34)(Ευρωπαϊκή Ένωση 2016)
9. Εκτίμηση αντίκτυπου. Θα πρέπει να διεξάγονται μελέτες εκτίμησης αντίκτυπου με σκοπό την εκτίμηση των επιπτώσεων της επεξεργασίας προσωπικών δεδομένων, τον εντοπισμό των κινδύνων ασφαλείας και τον σχεδιασμό της αντιμετώπισης αυτών. (Άρθρα 35-36)(risk analysis).(Ευρωπαϊκή Ένωση 2016)
10. Υπεύθυνος προστασίας δεδομένων (Data Protection Officer - DPO). Οι οργανισμοί οφείλουν υπό προϋποθέσεις να ορίσουν έναν υπεύθυνο Προστασίας Δεδομένων. Ο ρόλος του είναι να παρακολουθεί τη διαρκή και επαρκή συμμόρφωση του οργανισμού με το

νόμο, ενώ παράλληλα αποτελεί τον σύνδεσμο του οργανισμού με την αρμόδια εποπτική αρχή. Υποχρέωση για διορισμό DPO έχουν : α) όσοι διενεργούν μεγάλης κλίμακας συστηματική επεξεργασία και παρακολούθηση. β) όσοι διενεργούν μεγάλης κλίμακας επεξεργασία ευαίσθητων προσωπικών δεδομένων του Άρθρου 9(Ευρωπαϊκή Ένωση 2016) και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα του Άρθρου 10.(Ευρωπαϊκή Ένωση 2016) γ) το δημόσιο.

11. Εκπαίδευση προσωπικού. Οι οργανισμοί οφείλουν να εκπαιδεύσουν το προσωπικό τους στο πώς να εφαρμόζει καθημερινά την πολιτική προστασίας προσωπικών δεδομένων.

# Κεφάλαιο 3. Ασφάλεια Πληροφοριακών Συστημάτων

## 3.1 Ορισμός και γενικά χαρακτηριστικά

Ασφάλεια Πληροφοριακού Συστήματος είναι το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία ενός πληροφοριακού συστήματος, αλλά και το σύστημα ολόκληρο από κάθε σκόπιμη ή τυχαία απειλή.

Η διαφύλαξη των πόρων και η προστασία των δεδομένων δεν ορίζεται αόριστα, αλλά στη βάση των τριών θεμελιωδών ιδιοτήτων της ασφάλειας των πληροφοριακών συστημάτων (Laudon 2014)

1. Εμπιστευτικότητα: αφορά την προστασία της πληροφορίας από μη εξουσιοδοτημένη αποκάλυψη (ανάγνωση) της
2. Ακεραιότητα: αφορά την προστασία της πληροφορίας από μια εξουσιοδοτημένη μεταβολή ( τροποποίηση ή διαγραφή )
3. Διαθεσιμότητα: αφορά τη διαφύλαξη της εξουσιοδοτημένης πρόσβασης (είτε για αποκάλυψη είτε για μεταβολή) στην πληροφορία, χωρίς εμπόδια ή καθυστέρηση

Εκτός από τις παραπάνω βασικές ιδιότητες η ασφάλεια συσχετίζεται με την επιτυχημένη εφαρμογή των ακόλουθων μηχανισμών(UNIVERSITY OF STIRLING 2018) :

- Αναγνώριση: αφορά τη διαδικασία παρουσίασης της ταυτότητας μιας οντότητας στο σύστημα
- Αυθεντικοποίηση: αφορά την διαδικασία επιβεβαίωσης της ταυτότητας που έχει παρουσιάσει μια οντότητα στο σύστημα
- Εξουσιοδότηση: αφορά τη διαδικασία λήψης απόφασης σχετικά με την αποδοχή ή την απόρριψη ενός αιτήματος πρόσβασης μιας αυθεντικοποιημένης οντότητας στο σύστημα, στη βάση των δικαιωμάτων πρόσβασης που της έχουν είδη εκχωρηθεί και της πολιτικής ελέγχου πρόσβασης του συστήματος.
- Αδυναμία αποποίησης: αφορά τη διαδικασία αδιαμφισβήτητου καταλογισμού ευθύνης για την επιτέλεσή μιας ενέργειας στο σύστημα.

Η ασφάλεια αποτελεί ή θα έπρεπε να αποτελεί ένα σημαντικό μέλημα κατά τη διάρκεια υλοποίησης οποιουδήποτε πληροφοριακού συστήματος. Για να μπορέσουμε να κατανοήσουμε καλύτερα τα θέματα ασφαλείας που προκύπτουν στο σχεδιασμό, την

υλοποίηση και τη συντήρηση πληροφοριακών συστημάτων, είναι βασικό να χρησιμοποιούνται σωστά οι σχετικοί πρωτοαναφερόμενοι ορισμοί.

## 3.2 Ασφάλεια πληροφοριακών συστημάτων και ΓΚΠΔ. Αλληλεπίδραση του ISO 27001 με το ΓΚΠΔ.

Το πρότυπο ISO 27001 (Iso-Iec Standards 2011) αποτελώντας ένα σύστημα διαχείρισης ασφάλειας πληροφοριών και δεδομένου ότι στον Κανονισμό Προστασίας Προσωπικών Δεδομένων γίνεται εκτενής αναφορά στα συστήματα πιστοποίησης θα μπορούσαμε να καταλήξουμε ότι ο ΓΚΠΔ ενθαρρύνει τη χρήση συστημάτων πιστοποίησης όπως το ISO 27001 με απώτερο σκοπό ο οργανισμός να διαχειρίζεται ενεργά την ασφάλεια των δεδομένων του σύμφωνα με τις βέλτιστες πρακτικές. Το συγκεκριμένο πρότυπο έχει ευρεία βάση και περιλαμβάνει τρεις βασικές πτυχές ενός ολοκληρωμένου καθεστώτος ασφαλείας των πληροφοριών.

- Ανθρώπους
- Διαδικασίες
- Τεχνολογία

Εφαρμόζοντας τα μέτρα αυτά για την προστασία της πληροφορίας ο οργανισμός μπορεί να υπερασπιστεί όχι μόνο τους κινδύνους που οφείλονται στην τεχνολογία αλλά και άλλους όπως το ανεπαρκές ενημερωμένο προσωπικό ή οι αναποτελεσματικές διαδικασίες.

Μπορεί όμως να υπάρξει συσχέτιση μεταξύ του ISO 27001 και του ΓΚΠΔ ;

Στο παράρτημα Α, του προτύπου ISO 27001 περιγράφονται οι στόχοι και τα σημεία ελέγχου, που απαιτεί το πρότυπο(British and Bureau 2016). Ακολουθούν παραδείγματα τέτοιων σημείων ελέγχου του προτύπου 27001 που μπορούν να χρησιμοποιηθούν για την υποστήριξη συμμόρφωσης με τον κανονισμό ΓΚΠΔ και σχετικά του άρθρα.

- Οι κρυπτογραφικοί μηχανισμοί που αναφέρει το πρότυπο *(A.10.1)*(Iso-Iec Standards 2011) και οι σχετικές τεχνολογίες μπορούν να χρησιμοποιηθούν για την προστασία προσωπικών πληροφοριών που βρίσκονται αποθηκευμένες ή μεταφέρονται σε δίκτυα. Η χρήση της κρυπτογράφησης σε συνδυασμό με τεχνικές ψευδωανονυμοποίησης σε μεγάλες βάσεις δεδομένων μπορεί να εξασφαλίσει την εμπιστευτικότητα των

προσωπικών δεδομένων (ΠΔ) και των πληροφοριών προσωπικής ταυτότητας (ΠΠΤ) ικανοποιώντας τις απαιτήσεις του ΓΚΠΔ (άρθρο 32). (Ευρωπαϊκή Ένωση 2016) Τεχνικές κρυπτογράφησης ήδη ενσωματώνονται σε τεχνολογίες μεταφοράς δεδομένων όπως η Virtual Private Network (VPN), και η Secure Sockets Layer (SSL), η ακόμη και σε διακομιστές ηλεκτρονικού ταχυδρομείου.

- Ο ΓΚΠΔ ορίζει ρόλους υπεύθυνων επεξεργασίας δεδομένων και εκτελούντες την επεξεργασία δεδομένων για τις επεξεργασίες, υποχρεώνοντας τους πρώτους να συνεργάζονται μόνο με τους εκτελούντες που παρέχουν εγγυήσεις για την επάρκεια των ελεγκτικών μηχανισμών στην επεξεργασία των πληροφοριών προσωπικών δεδομένων (ΠΔ) (*άρθρα 24, 26 – 29*)(Ευρωπαϊκή Ένωση 2016), ενώ το πρότυπο ISO 27001 εστιάζει στην διαχείριση προμηθευτών και τρίτων (*A.15*)(Iso-Iec Standards 2011). Με την αξιολόγηση των εκτελούντων της επεξεργασίας δεδομένων ή μια εγκεκριμένη πιστοποίησή τους, οι υπεύθυνοι επεξεργασίας δεδομένων μπορούν να υποστηρίξουν την κανονιστική συμμόρφωση, μέσα από συμφωνίες/συμβάσεις μεταξύ των δύο μερών.

- Ένα αξιοσημείωτο σημείο ελέγχου για το πρότυπο ISO 27001 αφορά την διαχείριση της επιχειρηματικής συνέχειας (*A.17*)(Iso-Iec Standards 2011), όπου κατάλληλοι μηχανισμοί και συστήματα μπορούν να χρησιμοποιηθούν για την εξασφάλιση της διαρκούς διαθεσιμότητας της πληροφορίας, ικανοποιώντας και τις αντίστοιχες απαιτήσεις του ΓΚΠΔ (άρθρο 32.1(γ)(Ευρωπαϊκή Ένωση 2016).

- Συνοπτικά η δημιουργία ενός ολοκληρωμένου συστήματος διαχείρισης της ασφάλειας των πληροφοριών, όπως προτείνεται από το πρότυπο ISO 27001, επιτρέπει στους οργανισμούς που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, να αποδεικνύουν ότι οι κίνδυνοι για τα προσωπικά δεδομένα επανεξετάζονται (άρθρα 32.1(δ), 32.2)(Ευρωπαϊκή Ένωση 2016), και οι σχετικές διαδικασίες ενημερώνονται και βελτιώνονται συνεχώς. Ένα εδραιωμένο σύστημα είναι το ιδανικό πλαίσιο για τη διαχείριση των κινδύνων για όλα τα περιουσιακά στοιχεία της επιχείρησης, και μπορεί να παρέχει τη συνεχή διαβεβαίωση ότι ο οργανισμός λαμβάνει σοβαρά υπόψη τις προδιαγραφές ασφάλειας ISO 27001 αλλά και του ΓΚΠΔ (άρθρο 32)(Κανονισμός, Ευρωπαϊκου, and Συμβουλιου 2016).

- Συμπερασματικά η συμμόρφωση με το πρότυπο ISO 27001 μπορεί να λειτουργήσει συμπληρωματικά για την συνολική συμμόρφωση με τον ΓΚΠΔ, διότι ότι οι

απαιτήσεις συμμόρφωσης του ΓΚΠΔ επεκτείνονται και στην συμμόρφωση του οργανισμού με της αρχές επεξεργασίας, την εξασφάλιση της άσκησης των δικαιωμάτων των φυσικών προσώπων και την γενικότερη ισορροπία μεταξύ της ελεύθερης κυκλοφορίας και της προστασίας της ελευθερίας και των δικαιωμάτων των φυσικών προσώπων.

# ΕΙΔΙΚΟ ΜΕΡΟΣ

# ΚΕΦΑΛΑΙΟ 4: ΠΡΟΕΤΟΙΜΑΣΙΑ ΦΟΡΕΑ ΓΙΑ ΤΟ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (ΓΚΠΔ)

## 4.1 Προκαταρκτικές ενέργειες υλοποίησης έργου.

Κομβικής σημασίας διαδικασία για την επιτυχή ολοκλήρωση του έργου που θα σηματοδοτεί τη πλήρης συμμόρφωση όλων των διαδικασιών με τις απαιτήσεις του ΓΚΠΔ, αποτελεί η συζήτηση όλων των εμπλεκομένων μερών ανά διαδικασία, αλλά και στο σύνολο των διαδικασιών και η λεπτομερής καταγραφή των απαιτήσεων, των αναγκών αλλά και των προσδοκιών που αποβλέπει ο φορέας από την υλοποίηση και εφαρμογή του συστήματος(MANCHESTER METROPOLTAN UNIVERSITY 2018).

Για τον λόγο αυτό, άτομα που έχουν άριστη γνώση των απαιτήσεων του ΓΚΠΔ (σύμβουλοι συστημάτων ποιότητας, νομικοί κ.α) και που θα διαδραματίσουν σημαντικό ρόλο στην υλοποίηση του έργου, κατευθύνοντας τις ενέργειες και τις διαδικασίες με τελικό σκοπό την επιτυχή ολοκλήρωση του έργου, θα πρέπει να οργανώσουν μία σειρά συναντήσεων αρχικά του συνόλου των εμπλεκομένων, παραθέτοντας μία γενική ενημέρωση περί του Κανονισμού και των απαιτήσεων αυτού. Έπειτα, μία σειρά μεμονωμένων συναντήσεων θα βοηθήσει στο να ολοκληρωθεί η σύνθεση του «παζλ» που συνθέτει ο οργανισμός – φορέας, αναδεικνύοντας σημεία στα οποία θα πρέπει να δοθεί μεγαλύτερη βαρύτητα σχεδιασμού αλλά και διαδικασίες που ενδεχομένων είναι πιο επισφαλής στη διαρροή των προσωπικών δεδομένων. (UNIVERSITY OF CAMBRIDGE GDPR DATA PROTECTION WORKING 2018)

Ακριβής καταγραφή των θεμάτων που συζητήθηκαν ανά άτομο και των συμπερασμάτων από πού προέκυψαν θα πρέπει να υλοποιηθεί και στη συνέχεια να κοινοποιηθούν άμεσα στα άτομα προκειμένου να τα διαβάσουν και να επιβεβαιώσουν την ορθότητα τους.

Η αρχική σωστή καταγραφή των διαδικασιών, των απαιτήσεων αλλά και των προσδοκιών αποτελεί καίριας σημασίας διαδικασία για την επιτυχή ολοκλήρωση του εγχειρήματος.

Τα δεδομένα από τις συζητήσεις θα πρέπει τελικά να καταγράφονται σε συγκεκριμένες φόρμες, οι οποίες θα αποτελούν έντυπα του συστήματος και θα ανανεώνονται όταν προκύπτουν νέες απαιτήσεις.

Τα έντυπα αυτά θα πρέπει να έχουν συγκεκριμένη αλλά ταυτόχρονα απλή μορφή και δομή προκειμένου η συμπλήρωση τους να είναι εύκολη από όλους.

## 4.2 Παράδειγμα Εντύπου αρχικής καταγραφής των απαιτήσεων του Φορέα.

Το έντυπο θα πρέπει να είναι απλό στη σύνταξη και δομή του, κατανοητό και εύχρηστο. (Έντυπο 1)

Στην κεφαλίδα του εντύπου θα πρέπει να φαίνεται:

- ο φορέας με την τοποθέτηση του λογότυπου και
- η ένδειξη "**confidential**" (Εμπιστευτικό έγγραφο).

Στο υποσέλιδο θα πρέπει να αναγράφεται:

- ο κωδικός του εγγράφου και η έκδοση του,
- οι σελίδες να είναι αριθμημένες και
- η ημερομηνία αρχικής σύνταξης του εγγράφου όπως επίσης και οι μεταγενέστερες ημερομηνίες τροποποίησης του.

Στο κυρίως κείμενο θα πρέπει να αναφέρονται:

- τα θέματα που συζητήθηκαν,
- οι απαραίτητες ενέργειες που απαιτούνται
- χρονοδιάγραμμα υλοποίησης αυτών των ενεργειών
- τελικές αποφάσεις.

Λογότυπος του φορέα

*Εμιστευτικό*

## Meeting Minutes

| | | | |
|---|---|---|---|
| **Ημερομηνία:** | | **Ώρα:** | |
| **Τοποθεσία:** | | **Σκοπός:** | **Συνέντευξη** |
| **Συμμετέχοντες:** | | | |
| | | | |
| **Διάρκεια:** | | **Σχόλια** | |

| **Θέματα που συζητήθηκαν** | |
|---|---|
| **Α/Α** | **ΘΕΜΑ** |
| **1.** | |
| **2.** | |

| **Ενέργειες** | | | |
|---|---|---|---|
| **Α/Α.** | **Ενέργεια** | **Ποιός** | **Έως** |
| **1.** | | | |
| **2.** | | | |

| **Αποφάσεις που λήφθηκαν** | |
|---|---|
| **Α/Α.** | **Απόφαση** |

| | |
|---|---|
| **1.** | |
| **2.** | |

| Κωδικός εντύπου | Αρ.σελίδων | Ημ.αρχικής σύνταξης |
|---|---|---|
| | | Ημ. αναθεώρησης |

Αφού ολοκληρωθεί η αρχική καταγραφή των δράσεων και διαδικασιών και οριστούν οι άμεσα εμπλεκόμενοι αλλά και οι υπεύθυνοι υλοποίησης του έργου, συντάσσεται το « έγγραφο έναρξης έργου συμμόρφωσης με το ΓΚΠΔ».

Στο μακροσκελές αυτό κείμενο γίνεται αναφορά στα παρακάτω θέματα:

**1. Ιστορικό**: Αναφορά στον ΓΚΠΔ, τις απαιτήσεις του και πώς αυτές θα υλοποιηθούν στο συγκεκριμένο φορέα. Δομή ενδεικτικού κειμένου φαίνεται παρακάτω:

*«Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ), που δημιουργήθηκε από την Ευρωπαϊκή Ένωση (ΕΕ), είναι η πιο σημαντική αλλαγή στη νομοθεσία για την προστασία προσωπικών δεδομένων τα τελευταία είκοσι χρόνια. Θέτει απαιτήσεις σε οργανισμούς που ελέγχουν και επεξεργάζονται προσωπικά δεδομένα φυσικών προσώπων εντός της Ευρωπαϊκής Ένωσης, ώστε να εφαρμόσουν κατάλληλη προστασία γι' αυτά.*

*Ο Κανονισμός τέθηκε σε πλήρη εφαρμογή στις 25 Μαΐου 2018 και εφαρμόζεται όχι μόνο σε οργανισμούς με έδρα την ΕΕ, αλλά και εκτός της ΕΕ που διατηρούν και επεξεργάζονται δεδομένα πολιτών της ΕΕ.*

*Η θέσπιση αυτού του Κανονισμού απαιτεί να εξετάσουμε προσεκτικά τα δεδομένα προσωπικού χαρακτήρα που συλλέγουμε και επεξεργαζόμαστε και να διασφαλίσουμε ότι αυτό γίνεται με τρόπο καταλλήλως διαφανή και δίκαιο, λαμβάνοντας σοβαρά υπόψη τα δικαιώματα των προσώπων στα οποία αναφέρονται τα δεδομένα στα πλαίσια του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ).*

*Το έγγραφο αυτό θέτει την έναρξη του έργου για την διεκπεραίωση των εργασιών που πρέπει να γίνουν στο Π.Μ.Σ «Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ ώστε να ευθυγραμμιστούν οι διεργασίες και οι διαδικασίες του με το Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) και για την επίτευξη της συμμόρφωσης του Π.Μ.Σ «Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ με αυτόν.»*

# 2. Στόχοι και Οφέλη

## 2.1 Στόχοι Έργου

Οι στόχοι του έργου είναι οι εξής:

1. Διασφάλιση ότι το Π.Μ.Σ. είναι σε θέση να επιδείξει συμμόρφωση με το Γενικό Κανονισμό Προστασίας Δεδομένων
2. Δημιουργία κουλτούρας Προστασίας Προσωπικών Δεδομένων στον φορέα
3. Κατανόηση, καταγραφή και επικαιροποίηση των προσωπικών δεδομένων που συλλέγουμε, επεξεργαζόμαστε και διαγράφουμε
4. Διεξαγωγή αξιολόγησης των επιπτώσεων για την προστασία προσωπικών δεδομένων για οποιαδήποτε επεξεργασία υψηλού κινδύνου εντός του Π.Μ.Σ *«Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ*
5. Κατανόηση και αξιολόγηση του κινδύνου μη συμμόρφωσης σε συνεχή βάση

## 2.2 Αναμενόμενα Οφέλη

Τα σημαντικότερα οφέλη που θα προκύψουν από την επιτυχή υλοποίηση του έργου είναι τα εξής:

1. Μείωση του κινδύνου όσον αφορά τη διαχείριση προσωπικών δεδομένων
2. Αποφυγή διώξεων σε πιθανές παραβάσεις του Γενικού Κανονισμού Προστασίας Δεδομένων
3. Αυξημένη ποιότητα διασφάλισης για τους φοιτητές, τους ερευνητές, τους υπαλλήλους, τους εξωτερικούς συνεργάτες και τους προμηθευτές ότι τα Προσωπικά τους Δεδομένα προστατεύονται κατάλληλα
4. Καλύτερη κατανόηση των Προσωπικών Δεδομένων που συλλέγουμε και επεξεργαζόμαστε

Θα ληφθούν μέτρα, όπου είναι δυνατόν, για την ποσοτικοποίηση της επίτευξης του έργου σε σχέση με τα ανωτέρω αναμενόμενα οφέλη.

# 3. Πεδίο Εφαρμογής, Εξαρτήσεις, Περιορισμοί και Υποθέσεις

## 3.1 Πεδίο εφαρμογής

Το έργο περιλαμβάνει όλες τις δραστηριότητες του Π.Μ.Σ. *«Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ*, οι οποίες πραγματοποιούνται στις εγκαταστάσεις του στο Αλεξάνδρειο Τεχνολογικό Εκπαιδευτικό Ίδρυμα Θεσσαλονίκης .

## 3.2 Αλληλεπιδράσεις Έργου

Το έργο αυτό έχει τις ακόλουθες αλληλεπιδράσεις με άλλα έργα που σχεδιάζονται ή βρίσκονται σε εξέλιξη στον οργανισμό:

| **Έργο** | **Φύση Αλληλεπίδρασης** | **Χρονοδιάγραμμα** |
|---|---|---|
| Εφαρμογή Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) το οποίο καλύπτει όλες τις δραστηριότητες του Π.Μ.Σ *«Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ* | Το ΣΔΑΠ και τα οργανωτικά και τεχνικά μέτρα που θα εφαρμοστούν, π.χ. Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών, Αξιολόγηση & Διαχείριση Κινδύνων, Σχέδιο Ασφάλειας, Σχέδιο Ανάκαμψης από Καταστροφές και Σχέδιο Επιχειρησιακής Συνέχειας, πρέπει να ολοκληρωθούν τουλάχιστον δύο μήνες πριν από την ολοκλήρωση του έργου συμμόρφωσης με το ΓΚΠΔ. | |

*Πίνακας 1 – Αλληλεπιδράσεις έργου*

## 3.3. Περιορισμοί

Οι παρακάτω περιορισμοί εφαρμόζονται στο έργο:

- Το έργο θα πρέπει να επιτευχθεί μέσα στο δηλωθέν χρονοδιάγραμμα
- Ο Υπεύθυνος Προστασίας Δεδομένων του φορέα αφιερώνει 1 ημέρα κάθε 2 εβδομάδες για το έργο
- Η ομάδα υλοποίησης του Γενικού Κανονισμού Προστασίας Δεδομένων του *«Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ* αφιερώνει 1 ημέρα κάθε 2 εβδομάδες για το έργο
- Το έργο θα διεξαχθεί ταυτόχρονα με αρκετά άλλα έργα και συνεπώς θα πρέπει να ανταγωνιστεί για πόρους κατά προτεραιότητα, όπως αποφασίστηκε από την ανώτατη διοίκηση του Π.Μ.Σ *«Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ*

## 3.4 Παραδοχές

Κατά την προετοιμασία του εγγράφου έναρξης του έργου θεωρείται ότι:

- Οι Υπεύθυνοι των Μονάδων και των Τομέων είναι πρόθυμοι και διαθέσιμοι να συμμετάσχουν σε τακτικές συνεδριάσεις αναθεώρησης όπου χρειάζεται
- Επαρκείς οικονομικοί πόροι θα πρέπει να είναι διαθέσιμοι όπου απαιτείται για τις απαραίτητες δαπάνες που συνιστώνται από το έργο
- Διαθέσιμο επαρκές ανθρώπινο δυναμικό για την έγκαιρη πρόοδο του έργου

# 4. Οργάνωση Έργου και Αρμόδιες Αρχές

Είναι σημαντικό να οριστεί ο τρόπος με τον οποίο θα οργανωθεί το έργο, ώστε να είναι δυνατή μια σαφής κατεύθυνση διαχείρισης.

## 4.1 Οργάνωση Έργου

Το έργο θα επιβλέπεται από μια Επιτροπή έργου το οποίο θα έχει πρωταρχική ευθύνη για τη διαχείριση του έργου και την επίτευξη των στόχων του.

## Επιτροπή Έργου

Η Επιτροπή του έργου θα αποτελείται από:

| **Ρόλος** | **Όνομα** | **Τίτλος** |
|---|---|---|
| Χορηγός Έργου | | Επιστημονικός Υπεύθυνος του έργου |
| Υπεύθυνος Υλοποίησης και Διαχειριστής Έργου | | Σύμβουλος, Νομικός |
| Ανώτερος προμηθευτής/πάροχος | | Ομάδα Υλοποίησης Συμμόρφωσης με το ΓΚΠΔ (SH GDPR team) |
| Ανώτερος Χρήστης | | |

*Πίνακας 2 – Επιτροπή έργου*

Το καθηκοντολόγιο των μελών της επιτροπής συγκεκριμένο και καλά οριοθετημένο ανάλογα με τον ρόλο. Πιο συγκεκριμένα:

**Χορηγός Έργου**

- Αναθεώρηση και έγκριση της τεκμηρίωσης του έργου
- Αναθεώρηση και έγκριση των διαδικασιών που ορίζονται από το έργο
- Έγκριση του ελέγχου των αλλαγών του έργου
- Κατεύθυνση προς αυτό το σκοπό
- Έγκριση ολοκλήρωσης του έργου

**Αρχηγός Υλοποίησης και Διαχειριστής Έργου**

- Εξασφάλιση ότι καθορίζεται το επιθυμητό αποτέλεσμα του έργου και μετριούνται τα κριτήρια επιτυχίας
- Διαχείριση της δημιουργίας των απαιτούμενων παραδοτέων
- Σχεδιασμός και παρακολούθηση του έργου
- Ανάληψη ευθύνης για τη συνολική πρόοδο του σχεδίου
- Διαχείριση κινδύνων και ζητημάτων
- Προσδιορισμός και διαχείριση των αλλαγών του έργου
- Αναφορά και επικοινωνία σχετικά με το έργο

**Ανώτερος Προμηθευτής/Πάροχος**

- Παρακολούθηση συναντήσεων του συμβουλίου του έργου
- Εκπροσώπηση των συμφερόντων του προμηθευτή
- Ορισμός προτεραιοτήτων και διάθεση πόρων που βρίσκονται υπό τον έλεγχό του

**Ανώτεροι Χρήστες**

- Παρακολούθηση συναντήσεων της επιτροπής του έργου
- Εκπροσώπηση των συμφερόντων των εμπλεκομένων τομέων
- Λειτουργία ως σύνδεσμος μεταξύ του έργου και των εμπλεκόμενων τομέων

## 4.2 Ομάδα έργου

Η υλοποίηση των παραδοτέων του έργου θα πραγματοποιηθεί από την ομάδα του έργου. Η ομάδα του έργου θα αποτελείται από τους εξής ανθρώπους:

| **Ρόλος** | **Όνομα** | **Τίτλος** |
|---|---|---|
| Υπεύθυνος Υλοποίησης | Ομάδα Υλοποίησης Συμμόρφωσης με τον ΓΚΠΔ | Πιστοποιημένη Υπεύθυνη Επεξεργασίας Δεδομένων - Ομάδα |

| | | |
|---|---|---|
| | | Υλοποίησης Συμμόρφωσης με τον ΓΚΠΔ |
| Εκπαιδευτής | Ομάδα Υλοποίησης Συμμόρφωσης με τον ΓΚΠΔ | Ομάδα Υλοποίησης Συμμόρφωσης με τον ΓΚΠΔ |
| Εσωτερικός Έλεγχος | Ομάδα Υλοποίησης Συμμόρφωσης με τον ΓΚΠΔ | Ομάδα Υλοποίησης Συμμόρφωσης με τον ΓΚΠΔ |
| Διαχείριση Έργου | Ομάδα Υλοποίησης Συμμόρφωσης με τον ΓΚΠΔ | Project Manager - Ομάδα Υλοποίησης Συμμόρφωσης με τον ΓΚΠΔ |
| Υπεύθυνος Πληροφορικής | | Υπεύθυνος Πληροφορικής Π.Μ.Σ - ΑΤΕΙΘ |
| Συντάκτης Εγγράφου | Ομάδα Υλοποίησης Συμμόρφωσης με τον ΓΚΠΔ | Ομάδα Υλοποίησης Συμμόρφωσης με τον ΓΚΠΔ |
| Υπεύθυνος Προστασίας Προσωπικών Δεδομένων | | DPO |
| Συντονιστής διαχείρισης σημαντικών προμηθευτών | Σύμβουλος | Γενική Υπεύθυνη έργου ( Ομάδα Υλοποίησης Συμμόρφωσης με τον ΓΚΠΔ) |

*Πίνακας 3 – Ομάδα έργου*

Οι ευθύνες της Ομάδας Έργου είναι οι εξής:

- Συμμετοχή σε ένα ή περισσότερα από τα απαιτούμενα παραδοτέα
- Ανασκόπηση της τεκμηρίωσης και των παραδοτέων του έργου
- Παρακολούθηση των συναντήσεων του έργου
- Εισαγωγή στη διαχείριση κινδύνων και ζητημάτων
- Επικοινωνία με τρίτους σε ότι αφορά τον τομέα ευθύνης τους

## 5. Πόροι του έργου

Οι κάτωθι πόροι θα διατεθούν στο έργο από την ανώτατη διοίκηση.(Εκτενής αναφορά των διαθέσιμων πόρων για την υλοποίηση του έργου και δέσμευση της Διοίκησης ότι θα ανατεθούν αποκλειστικά για τον σκοπό αυτό.

## 5.1 Ανθρώπινοι Πόροι

Οι ακόλουθοι άνθρωποι θα είναι διαθέσιμοι στο έργο για τις προσδιοριζόμενες περιόδους (αναφορά στα παρακάτω πεδία όλων των εμπλεκομένων ατόμων του έργου υλοποίησης):

| **Όνομα** | **Ρόλος** | **Διαθέσιμη Περίοδος** | **Δέσμευση** |
|---|---|---|---|
| Υπεύθυνος του Έργου. | Σύνδεσμος επικοινωνίας μεταξύ της ομάδας Υλοποίησης Συμμόρφωσης με το ΓΚΠΔ και των εργαζομένων του Π.Μ.Σ | ΧΧ μήνες | ΧΧ ημέρα (ες) ανά χχ εβδομάδα (ες). |

Αντίστοιχες λεπτομερειακές αναφορές γίνονται και στους:

- Τεχνικούς ( Πόρος- Σκοπός- Παρέχεται από)

- Πληροφοριακούς ( Πηγή- Σκοπός- Παρέχεται από) και
- Οικονομικούς πόρους ( Πηγή – Ποσό- Διαθεσιμότητα).

## 6. Χρονοδιάγραμμα Υλοποίησης

Οφείλουμε να κάνουμε λεπτομερή αναφορά στο Χρονοδιάγραμμα Υλοποίησης του έργου ( κεφ. 6) όπου θα αναφέρεται η δράση και συγκεκριμένο χρονικό διάστημα υλοποίησης.

Τέλος στο κεφάλαιο 7. Θα πρέπει να περιγράφεται ο τρόπος «Επικοινωνίας του Έργου». Πιο συγκεκριμένα:

## 7. Επικοινωνία του Έργου

### 7.1 Ενδιαφερόμενα μέρη

Στο πλαίσιο του δεδομένου πεδίου εφαρμογής του έργου, τα ενδιαφερόμενα μέρη είναι:

| Μέρος | Φύση Ενδιαφέροντος | Μέθοδος Επικοινωνίας |
|---|---|---|
| Επιτροπή Έργου | Διασφάλιση επιτυχίας του έργου | Επισύναψη αναφορών κάθε 2 εβδομάδες |
| Υπεύθυνοι Διευθύνσεων του Π.Μ.Σ | Όταν εφαρμοστούν νέοι έλεγχοι και διαδικασίες | Συμμετοχή στις ανασκοπήσεις της διοίκησης |
| Συνεργαζόμενα μέρη (φοιτητές, εξ. Συνεργάτες του Π.Μ.Σ, άλλοι φορείς του Π.Μ.Σ) | Συμμόρφωση με τις απαιτήσεις ελέγχου | Αποστολή ηλεκτρονικής αλληλογραφίας σε όλους τους εμπλεκόμενους, συναντήσεις με βασικούς εμπλεκόμενους και πιθανοί εσωτερικοί έλεγχοι συμμόρφωσης σε κρίσιμους εμπλεκόμενους |
| Φοιτητές | Προστασία προσωπικών | Αποστολή ηλεκτρονικής |

| | | |
|---|---|---|
| | δεδομένων των ασθενών | αλληλογραφίας σε όλους τους φοιτητές |

*Πίνακας 9 – Ενδιαφερόμενα μέρη*

## 7.2 Αναφορά προόδου έργου

Ο υπεύθυνος έργου θα εκπονεί αναφορά κάθε 2 εβδομάδες για την Επιτροπή έργου, όπου θα αναλυθεί η πρόοδος των τελευταίων 2 εβδομάδων, οι προγραμματισμένες εργασίες για τις επόμενες 2 εβδομάδες, τα εκκρεμή θέματα, οι ενέργειες διαχείρισης κινδύνου και η εκτίμηση του τρέχοντος επιπέδου συμμόρφωσης με το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων.

## 7.3 Risk Actions (or Assumptions) - Issues- Decisions (or Dependencies) (RAID) log

Ο υπεύθυνος έργου θα διατηρεί ένα αρχείο καταγραφής το οποίο θα περιλαμβάνει:

- Τους κινδύνους προς την επιτυχία του έργου
- Ενέργειες που συμφωνήθηκαν κατά τη διάρκεια των συνεδριάσεων του έργου
- Ζητήματα που επηρεάζουν το έργο
- Αποφάσεις που λαμβάνονται κατά τη διάρκεια του έργου

Αυτό το αρχείο καταγραφής θα αναθεωρείται σε κάθε προγραμματισμένη συνάντηση έργου και μετά από σημαντικές αλλαγές που επηρεάζουν το έργο.

## 8. Παραδοτέα.

Εκτενής αναφορά των παραδοτέων (περιγραφή αυτών) , με χρόνους υλοποίησης και αναφορά των εμπλεκόμενων ατόμων.

Το σύνολο του παραπάνω εγγράφου θα πρέπει να μελετηθεί από το σύνολο των ατόμων υλοποίησης του έργου, να είναι όλοι τελικά σύμφωνοι για το πλαίσιο υλοποίησης και να παρακολουθείται η εξέλιξη του έργου εντατικά στα πρώτα στάδια υλοποίησης του.

## 8.1 Έγγραφο Δέσμευσης της Διοίκησης.

Προκειμένου να γνωστοποιηθεί στο ευρύ κοινό η προσπάθεια του φορέα να συμμορφωθεί με το ΓΚΠΔ αφενός και αφετέρου να αποκομίσει ο φορέας τα οφέλη από αυτήν την διαδικασία (αύξηση κύρους, αποφυγή καταγγελιών και απόδοση προστίμων), μπορεί να συνταχθεί το έγγραφο που αφορά τη Δέσμευση της Διοίκησης για την υλοποίηση του συγκεκριμένου εγχειρήματος και προσυπογράφεται από τον Επιστημονικό Υπεύθυνο του Π.Μ.Σ.

Το παραπάνω κείμενο μπορεί να αναφέρει τα παρακάτω:

*«Το Π.Μ.Σ «Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ. αναγνωρίζει την ανάγκη για τη συμμόρφωση με το ΓΚΠΔ καθώς και για τη λήψη αποτελεσματικών μέτρων, που αφορούν την προστασία των προσωπικών δεδομένων των φοιτητών, των εξωτερικών συνεργατών, καθηγητών και άλλων ενδιαφερόμενων μερών.*

*Στο πλαίσιο της εκπλήρωσης των νομικών μας υποχρεώσεων, έχει αναπτυχθεί και εφαρμόζεται κατάλληλη Πολιτική για την Ιδιωτικότητα και την Προστασία των Προσωπικών Δεδομένων, η οποία είναι διαθέσιμη σε έντυπη και σε ηλεκτρονική μορφή. Η Πολιτική αυτή θα κοινοποιηθεί τόσο εντός του φορέα όσο και προς όλα τα εμπλεκόμενα τρίτα ή ενδιαφερόμενα μέρη.*

*Η δέσμευση του Π.Μ.Σ «Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ. στην Προστασία των Προσωπικών Δεδομένων αποδεικνύεται με την υλοποίηση ολοκληρωμένου Προγράμματος Προστασίας Προσωπικών Δεδομένων και την παροχή των απαραίτητων πόρων για την εφαρμογή και την ανάπτυξη αποτελεσματικών τεχνικών και οργανωτικών μέτρων ώστε να διασφαλιστεί το κατάλληλο επίπεδο ασφάλειας για τα προσωπικά δεδομένα.*

*Το Π.Μ.Σ «Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ. θα εξασφαλίσει επίσης τη διεξαγωγή, σε τακτική βάση, συστηματικής αναθεώρησης της απόδοσης του προγράμματος, προκειμένου να διασφαλιστεί η επίτευξη των στόχων και ο εντοπισμός σχετικών ζητημάτων μέσω διαδικασιών ελέγχου και διαχείρισης.*

*Οι κίνδυνοι για την προστασία των προσωπικών δεδομένων θα καταγραφούν και θα αντιμετωπιστούν σε διάφορα επίπεδα εντός του οργανισμού μέσω μιας διαδικασίας διαχείρισης των κινδύνων, η οποία θα είναι σύμφωνη με τις απαιτήσεις και τις συστάσεις του GDPR και των σχετικών διεθνών προτύπων όπως το ISO / IEC 27001.*

*Σε αυτό το πλαίσιο θα υλοποιείται:*

*• Αξιολόγηση των κινδύνων για την επίτευξη της προστασίας προσωπικών δεδομένων*

*• Τακτικές αξιολογήσεις κινδύνων για την προστασία των προσωπικών δεδομένων σε συγκεκριμένους τομείς του Π.Μ.Σ «Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ.(π.χ γραμματεία, Ε.Λ.Κ.Ε)*

*• Αξιολόγηση του κινδύνου ως μέρος της διαδικασίας διαχείρισης αλλαγών*

*Παροτρύνουμε όλους τους εργαζόμενους και τα υπόλοιπα ενδιαφερόμενα μέρη του Π.Μ.Σ «Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ. να συμμετέχουν στη διαδικασία συνεχούς συμμόρφωσης με το ΓΚΠΔ και στην επίτευξη των στόχων μας για την προστασία των προσωπικών δεδομένων.*

*Με εκτίμηση,*

*Όνομα Επώνυμο*

*Επιστημονικός Υπεύθυνος*

*Π.Μ.Σ «Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ.»*

# ΚΕΦΑΛΑΙΟ 5: ΡΟΛΟΙ, ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ, ΕΚΠΑΙΔΕΥΣΗ

## 5.1 Ρόλοι, αρμοδιότητες και δικαιοδοσίες για τον ΓΚΠΔ.

Όπως σε κάθε σύστημα ποιότητας, έτσι και σε αυτό, θα πρέπει να γίνεται ξεκάθαρη αναφορά στους ρόλους, τις αρμοδιότητες, τα καθήκοντα και τις δικαιοδοσίες ανά εμπλεκόμενο άτομο. Θα πρέπει αυτές να συζητηθούν με κάθε άτομο χωριστά και πάντα παρουσία της Διοίκησης και να υπάρχει ετερόπλευρη διάθεση συνεργασίας αλλά και δέσμευση ως προς την υλοποίηση και μετέπειτα συντήρηση του συστήματος.

Στο πλαίσιο αυτό θα πρέπει να συνταχθεί ένα εκτενές συνολικό έγγραφο όλων των ρόλων που θα εμπλέκονται στο σύστημα και να γίνεται αναφορά των καθηκόντων, απαιτήσεων της θέσης και της δικαιοδοσίας του καθενός. Με αυτόν τον τρόπο θα εξασφαλίζεται η απρόσκοπτη λειτουργία τους συστήματος, αποφεύγοντας καταστάσεις που δυνητικά θα μπορούσαν να επηρεάσουν αρνητικά το κύρος του φορέα.

*Το Κεφάλαιο IV (Υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία) και η Ενότητα 4. (Υπεύθυνος Προστασίας Δεδομένων)* καλύπτονται από το παρακάτω κείμενο. Σε αυτό το στάδιο θα πρέπει να αναφέρεται ότι το Π.Μ.Σ. «Διοίκηση και Οργάνωση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ αντιμετωπίζει την ασφάλεια των προσωπικών δεδομένων, που έχει στην κατοχή του, πολύ σοβαρά. Ένα από τα πιο σημαντικά στοιχεία μίας αποτελεσματικής προσέγγισης στην ασφάλεια των προσωπικών δεδομένων και των πληροφοριών είναι ο ξεκάθαρος καταμερισμός των ρόλων, ώστε να υπάρχουν συγκεκριμένες και καθορισμένες αρμοδιότητες και δικαιοδοσίες. Ο καθένας από αυτούς τους ρόλους θα πρέπει να ανατίθεται σε συγκεκριμένα άτομα ή ομάδες ατόμων του οργανισμού.

Είναι λοιπόν, ζωτικής σημασίας ο κάθε εργαζόμενος ή συνεργάτης του οργανισμού να αντιλαμβάνεται το ρόλο του στη διατήρηση της ασφάλειας των πληροφοριών, που αφορούν φυσικά πρόσωπα και τις οποίες αποθηκεύουμε και επεξεργαζόμαστε. Η ανάγνωση αυτού του εγγράφου θα πρέπει να γίνεται σε συνδυασμό με ορισμένα έγγραφα, που καθορίζουν τον τρόπο διαχείρισης της ασφάλειας πληροφοριών εντός του Π.Μ.Σ συμπεριλαμβανομένων των εξής:

- *Πολιτική για την Ιδιωτικότητα και την Προστασία των Προσωπικών Δεδομένων*
- *Διαδικασία Ανάπτυξης Δεξιοτήτων για το ΓΚΠΔ*

- *Διαδικασία Εκτίμησης Αντικτύπου για την Προστασία των Δεδομένων*
- *Διαδικασία Απόκρισης σε Περιστατικά Ασφάλειας Πληροφοριών*
- *Διαδικασία Ενημέρωσης για Παραβίαση Προσωπικών Δεδομένων*
- *Διαδικασία Αιτημάτων των Φυσικών Προσώπων*

Διασφαλίζοντας ότι οι ρόλοι, οι αρμοδιότητες και οι δικαιοδοσίες έχουν οριστεί σαφώς, θα είμαστε ικανοί να αποτρέψουμε, σε ικανοποιητικό βαθμό, πολλά περιστατικά ασφάλειας πληροφοριών, οι οποίες αφορούν προσωπικά δεδομένα, και να αντιδράσουμε αποτελεσματικά και κατάλληλα αν και όταν υπάρξουν τέτοιου είδους περιστατικά.

Στο πλαίσιο της προστασίας των προσωπικών δεδομένων και της ασφάλειας των πληροφοριών, που αφορούν στη συμμόρφωσή μας στο ΓΚΠΔ, οι ακόλουθοι ρόλοι, ύψιστης σημασίας, θα πρέπει να οριστούν και να διανεμηθούν:

- Επιτροπή για την Προστασία των Προσωπικών Δεδομένων και την Ασφάλεια των Πληροφοριών.
- Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών (CISO)
- Υπεύθυνος Προστασίας Δεδομένων (DPO)

Οι συγκεκριμένες αρμοδιότητες και δικαιοδοσίες για τον καθένα από αυτούς τους ρόλους θα αναλυθούν εκτενώς παρακάτω.

Υπάρχουν επίσης ειδικά καθήκοντα σχετικά με την προστασία των προσωπικών δεδομένων που θα πρέπει να εκτελούνται από υπάρχοντες ρόλους εντός του οργανισμού και επίσης περιγράφονται συνοπτικά σε αυτό το έγγραφο.

Οι ρόλοι αυτοί είναι:

- Οι Διευθυντές των Τμημάτων
- Οι Τεχνικοί του IT
- Οι Χρήστες του IT

## 5.2 Ειδικές Αρμοδιότητες Ρόλων

Αυτή η ενότητα περιγράφει αναλυτικά τις ειδικές αρμοδιότητες και τις δικαιοδοσίες του κάθε ρόλου εντός του Π.Μ.Σ., σχετικά με την προστασία των προσωπικών δεδομένων. Οι απαραίτητες ικανότητες για την εκπόνηση του κάθε ρόλου ορίζονται στο έγγραφο *Διαδικασία Ανάπτυξης Δεξιοτήτων για το ΓΚΠΔ* που παρατίθεται στη συνέχεια.

### 5.2.1 Επιτροπή για την Προστασία των Προσωπικών Δεδομένων και την Ασφάλεια των Πληροφοριών.

Η Επιτροπή για την Προστασία των Προσωπικών Δεδομένων και την Ασφάλεια των Πληροφοριών εποπτεύει τη συμμόρφωση με το ΓΚΠΔ και τη λειτουργία των μέτρων ασφάλειας πληροφοριών και έχει τη γενική ευθύνη για την αποτελεσματικότητά της.

Η Επιτροπή αποτελείται από μέλη της ομάδας της ανώτατης διοίκησης και θα περιλαμβάνει, κατ' ελάχιστο τους παρακάτω ρόλους:

- Τεχνικός Υπεύθυνος
- Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών (CISO)
- Υπεύθυνος Προστασίας Δεδομένων (DPO)

**Αρμοδιότητες**

Η Επιτροπή για την Προστασία των Προσωπικών Δεδομένων και την Ασφάλεια των Πληροφοριών έχει τα παρακάτω καθήκοντα:

- Διατήρηση μίας ξεκάθαρης και βάσιμης κατανόησης της νομοθεσίας σχετικά με το ΓΚΠΔ και των επιπτώσεων που έχει στις δραστηριότητες του Π.Μ.Σ.
- Θέσπιση και διατήρηση των στόχων και των σχεδίων της Πολιτικής για την Ιδιωτικότητα και την Προστασία των Προσωπικών Δεδομένων και των Πολιτικών Ασφάλειας των Πληροφοριών.
- Μετάδοση της σημασίας της συμμόρφωσης με το ΓΚΠΔ και, εκπλήρωση των στόχων και της ανάγκης για συνεχή βελτίωση σε όλο το εύρος του οργανισμού.
- Διαρκής επίγνωση των αναγκών του Π.Μ.Σ. και των μεγάλων αλλαγών.

- Διασφάλιση ότι οι απαιτήσεις της προστασίας των προσωπικών δεδομένων και της ασφάλειας των πληροφοριών είναι καθορισμένες και πληρούνται στο πλαίσιο της ελαχιστοποίησης του κινδύνου και της διατήρησης αποτελεσματικών ελέγχων για το Π.Μ.Σ, τους φοιτητές και τους εξωτερικούς και εσωτερικούς συνεργάτες.

- Καθορισμός και παροχή των πόρων για το σχεδιασμό, την εφαρμογή, την παρακολούθηση, την αναθεώρηση και τη βελτίωση της διαχείρισης της προστασίας των προσωπικών δεδομένων και της ασφάλειας των πληροφοριών π.χ. πρόσληψη του κατάλληλου προσωπικού, διαχείριση του κύκλου εργασιών

- Εποπτεία της διαχείρισης των κινδύνων, για τον οργανισμό και τις υπηρεσίες του

- Διεξαγωγή αναθεωρήσεων της διοίκησης, για την προστασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών, σε καθορισμένα διαστήματα, για να εξασφαλίζεται διαρκώς η καταλληλόλητα, η επάρκεια και η αποτελεσματικότητα

- Εγκαθίδρυση μιας πολιτικής συνεχούς βελτίωσης, σε ευθυγράμμιση με την προστασία των προσωπικών δεδομένων και τη ασφάλεια των πληροφοριών για το φορέα.

- Ανασκόπηση των σημαντικών περιστατικών, που αφορούν τα προσωπικά δεδομένα και την ασφάλεια των πληροφοριών

- Διασφάλιση ότι οι διακανονισμοί, που περιέχουν την παροχή πρόσβασης στα πληροφοριακά συστήματα και τις υπηρεσίες σε εξωτερικούς οργανισμούς, βασίζονται σε ένα επίσημο συμφωνητικό, που ορίζει όλες τις απαραίτητες απαιτήσεις ασφάλειας.

**Δικαιοδοσίες**

Η Επιτροπή για την Προστασία των Προσωπικών Δεδομένων και την Ασφάλεια των Πληροφοριών έχει τη δικαιοδοσία να:

- Εγκρίνει σημαντικά ποσά για δαπάνη σε θέματα, που σχετίζονται με την προστασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών

- Επιστρατεύει καινούργιους πόρους για τη διαχείριση της προστασίας των προσωπικών δεδομένων και της ασφάλειας των πληροφοριών

- Εγκρίνει πολιτικές υψηλού επιπέδου για την προστασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών
- Εκκινήσει υψηλού επιπέδου ενέργειες διαχείρισης περιστατικών.

**Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών**

Ο Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών είναι ο πρωταρχικός ρόλος που επικεντρώνεται εξ ολοκλήρου στην ασφάλεια των πληροφοριών και τα σχετικά ζητήματα.

**Αρμοδιότητες**

Ο Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών έχει τις παρακάτω αρμοδιότητες:

- Ενημέρωση της Διευθύνουσας Επιτροπής για την Προστασία των Προσωπικών Δεδομένων και την Ασφάλεια των Πληροφοριών, σχετικά με όλα τα θέματα ασφάλειας, σε τακτική βάση και όποτε προκύπτει ανάγκη
- Μετάδοση της πολιτικής ασφάλειας πληροφοριών σε όλα τα σχετικά ενδιαφερόμενα μέρη, που απαιτείται, συμπεριλαμβανομένων και των ασθενών
- Εφαρμογή των απαιτήσεων της πολιτικής ασφάλειας πληροφοριών
- Διαχείριση των κινδύνων, οι οποίοι σχετίζονται με την πρόσβαση στις υπηρεσίες ή στα συστήματα
- Εξασφάλιση ότι τα μέτρα ασφάλειας εφαρμόζονται και τεκμηριώνονται
- Ποσοτικοποίηση και παρακολούθηση των τύπων, των όγκων και των επιπτώσεων των περιστατικών ασφάλειας και των δυσλειτουργιών
- Παρακολούθηση των επιτευγμάτων έναντι των στόχων
- Θέσπιση και διατήρηση μίας λίστας δράσεων συνεχούς βελτίωσης
- Ενημέρωση για τις δραστηριότητες που σχετίζονται με τη βελτίωση
- Αναγνώριση και διαχείριση των περιστατικών ασφάλειας πληροφοριών σύμφωνα με μία διαδικασία
- Συμμετοχή σε συνεδριάσεις αναθεώρησης της διοίκησης σε τακτική βάση

**Δικαιοδοσίες**

Ο Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών έχει την δικαιοδοσία να:

- Δηλώσει τα περιστατικά ασφάλειας πληροφοριών
- Εγκρίνει τις περιορισμένες δαπάνες σε θέματα που αφορούν την ασφάλεια των πληροφοριών
- Αναθεωρήσει τη λειτουργία των μέτρων εντός όλων των τομέων του Π.Μ.Σ.

**Υπεύθυνος Προστασίας Δεδομένων**

Ο Υπεύθυνος Προστασίας Δεδομένων είναι μία απαιτούμενη θέση για την ευθυγράμμιση με τον Γενικό Κανονισμό Προστασίας Δεδομένων της ΕΕ και έχει συγκεκριμένες αρμοδιότητες, που αφορούν την προστασία των προσωπικών δεδομένων των φυσικών προσώπων.

**Αρμοδιότητες**

Ο Υπεύθυνος Προστασίας Δεδομένων έχει τις ακόλουθες αρμοδιότητες:

- Να ενημερώνει και να συμβουλεύει τον υπεύθυνο της επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους εργαζόμενους, που εκτελούν επεξεργασία στα πλαίσια των υποχρεώσεων τους σχετικά με τη νομοθεσία για την προστασία των δεδομένων
- Να παρακολουθεί τη συμμόρφωση με τη νομοθεσία για την προστασία των δεδομένων και με τις πολιτικές του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία σχετικά με την προστασία των προσωπικών δεδομένων
- Να αναθέτει τις αρμοδιότητες, την ευαισθητοποίηση και την εκπαίδευση του προσωπικού που εμπλέκεται στην επεξεργασία των προσωπικών δεδομένων και τις σχετικές επιθεωρήσεις
- Να παρέχει συμβουλές όπου απαιτείται σχετικά με τις αξιολογήσεις των επιπτώσεων για την προστασία των δεδομένων και να παρακολουθεί την απόδοσή τους
- Να συνεργάζεται με όλες τις σχετικές εποπτικές αρχές για την προστασία των δεδομένων

- Να λειτουργεί ως το σημείο επικοινωνίας με τις εποπτικές αρχές για θέματα που αφορούν την επεξεργασία των προσωπικών δεδομένων και να τις συμβουλεύεται, όπου απαιτείται, σχετικά με οποιοδήποτε άλλο ζήτημα.

**Δικαιοδοσίες**

Ο Υπεύθυνος Προστασίας Δεδομένων έχει την δικαιοδοσία να:

- Λάβει αποφάσεις σχετικά με τα αιτήματα των φυσικών προσώπων, που είναι επιτρεπτά από τη σχετική νομοθεσία για την προστασία των δεδομένων
- Εκπροσωπεί τον οργανισμό στις εποπτικές αρχές σχετικά με ζητήματα που αφορούν την προστασία των δεδομένων

## 5.3.Άλλοι Ρόλοι με Αρμοδιότητες σχετικές με την Προστασία Προσωπικών Δεδομένων

Υπάρχει ένα σύνολο από εσωτερικούς ρόλους εντός του Π.Μ.Σ, που ενώ δεν είναι αποκλειστικά αφιερωμένοι στην προστασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών, έχουν αρμοδιότητες και δικαιοδοσίες, που σχετίζονται άμεσα με αυτήν.

**Τεχνικοί Πληροφορικής**

Επειδή, τα ζητήματα που αφορούν την προστασία των προσωπικών δεδομένων είναι συνήθως τεχνικής φύσεως, οι Τεχνικοί Πληροφορικής παίζουν σημαντικό ρόλο στην παροχή και τη διατήρηση των μέτρων ασφάλειας.

**Αρμοδιότητες**

Οι Τεχνικοί Πληροφορικής έχουν σε γενικές γραμμές τα παρακάτω καθήκοντα:

- Λειτουργία των διαδικασιών, όπως η διαχείριση περιστατικών και η διαχείριση αλλαγών
- Παροχή τεχνικών εξειδικεύσεων σε θέματα προστασίας προσωπικών δεδομένων και ασφάλειας πληροφοριών
- Εφαρμογή τεχνικών μέτρων

- Διαχείριση συστήματος π.χ. δημιουργία χρήστη, αντίγραφα ασφαλείας
- Παρακολούθηση ασφάλειας π.χ. εισβολές στο δίκτυο

**Δικαιοδοσίες**

Ένας Τεχνικός Πληροφορικής έχει τη δικαιοδοσία να:

- Ενεργήσει για να αποτρέψει ένα περιστατικό, που αφορά την προστασία προσωπικών δεδομένων, από το να συμβεί ή να εξελιχθεί, όταν είναι δυνατό.

**Χρήστες Πληροφορικής**

Οι αρμοδιότητες των χρηστών πληροφορικής ορίζονται σε ένα αρκετά μεγάλο μέρος των πολιτικών του οργανισμού, και περιγράφονται παρακάτω μόνο περιληπτικά.

**Αρμοδιότητες**

Ένας χρήστης πληροφορικής έχει τις παρακάτω κύριες ευθύνες:

- Να εξασφαλίσει ότι είναι ενημερωμένος και συμμορφωμένος με όλες τις πολιτικές προστασίας προσωπικών δεδομένων και ασφάλειας πληροφοριών του οργανισμού, που σχετίζονται με το ρόλο του στο φορέα
- Να αναφέρει οποιαδήποτε πραγματική ή πιθανή παραβίαση ασφάλειας
- Να συνεισφέρει στην αξιολόγηση των κινδύνων όταν απαιτείται

**Δικαιοδοσίες**

Ένας χρήστης πληροφορικής έχει τις εξής δικαιοδοσίες:

- Να ενεργήσει για να αποτρέψει ένα περιστατικό, που αφορά την προστασία προσωπικών δεδομένων, από το να συμβεί ή να εξελιχθεί, όταν είναι δυνατό.

## 5.4 Διαδικασία ανάπτυξης δεξιοτήτων για το ΓΚΠΔ

Το παρακάτω κείμενο δομήθηκε έτσι ώστε το σύστημα να πληροί τις απαιτήσεις του άρθρου 32 του ΓΚΠΔ για την ασφάλεια της επεξεργασίας.

Προκειμένου να προστατευτούν τα προσωπικά δεδομένα που συλλέγονται, αποθηκεύονται και τίθενται σε επεξεργασία από τον οργανισμό, είναι ύψιστης σημασίας το προσωπικό και τα υπόλοιπα ενδιαφερόμενα μέρη, που εμπλέκονται στην αποτελεσματική προστασία των προσωπικών δεδομένων και την ασφάλεια πληροφοριών, να έχουν τις απαιτούμενες ικανότητες. Οι συνέπειες της έλλειψης επαρκών δεξιοτήτων μπορεί να οδηγήσει σε αποτυχία συμμόρφωσης με τις νομικές απαιτήσεις.

Το Π.Μ.Σ δίνει έμφαση στην παροχή εκπαίδευσης για την κάλυψη των αναγκών του και την ανέλιξη των εργαζομένων, ώστε να μπορούν να διεκπεραιώσουν καλύτερα τις αρμοδιότητές τους που περιλαμβάνει την εκπαίδευση του προσωπικού σε σχέση με τις νέες εκδόσεις λογισμικών ή με την εισαγωγή νέων συστημάτων και τεχνολογικών μέτρων.

Για το σκοπό αυτό, θα πρέπει να εντοπιστούν και να συγκριθούν τα απαιτούμενα επίπεδα των δεξιοτήτων για τον κάθε ρόλο, που αφορά ο ΓΚΠΔ και η ασφάλεια των πληροφοριών. Για να επιτευχθεί αυτό θα πρέπει να υπάρχει η απαραίτητη κατανόηση των υπαρχόντων επιπέδων δεξιοτήτων από τους ανθρώπους, που είναι υπεύθυνοι για τη διατύπωση συστάσεων για περαιτέρω ανάπτυξη ικανοτήτων.

Αυτή η διαδικασία θα πρέπει να διαβάζεται σε συνδυασμό με τα παρακάτω έγγραφα, τα οποία δίνουν περισσότερες λεπτομέρειες σχετικά με το περιεχόμενο, το σκοπό, τους στόχους, τους πόρους και τους ρόλους, τις αρμοδιότητες και τις δικαιοδοσίες, που σχετίζονται με τη συμμόρφωση με το ΓΚΠΔ:

- *Πολιτική για την Ιδιωτικότητα και την Προστασία των Προσωπικών Δεδομένων*
- *Διαδικασία Εκτίμησης Αντικτύπου για την Προστασία των Δεδομένων*
- *Ρόλοι, Αρμοδιότητες και Δικαιοδοσίες*
- *Διαδικασία Απόκρισης στα Περιστατικά Ασφάλειας Πληροφοριών*

### 5.4.1. Αξιολόγηση Απαιτήσεων Δεξιοτήτων ανά Ρόλο

Προκειμένου να εκπληρωθούν τα καθήκοντα ενός ρόλου, ο αρμόδιος θα πρέπει να διαθέτει έναν αριθμό καθορισμένων δεξιοτήτων σε ικανοποιητικό επίπεδο. Στην συνέχεια παρατίθεται

λίστα των καθορισμένων δεξιοτήτων, οι οποίες είναι απαραίτητες για τον κάθε ρόλο , προβλέπεται αξιολόγηση των υπαρχόντων επιπέδων δεξιοτήτων, προκειμένου να κατατάξει τα άτομα στις παρακάτω ομάδες ανάλογα με την επάρκεια τους ή μη στις αντίστοιχες δεξιότητες. Η λίστα αυτή θα πρέπει να ενημερώνεται κάθε φορά, που αυτή η διαδικασία χρησιμοποιείται για να αντικατοπτρίσει αλλαγές στις δεξιότητες που χρειάζονται λόγω τεχνολογικών, οργανωτικών ή άλλων λόγων. Παραδείγματα των παραπάνω αναφερόμενων πινάκων (αξιολόγησης των δεξιοτήτων αλλά και αναφορά των ρόλων και αρμοδιοτήτων φαίνονται παρακάτω:

| **Επίπεδο Δεξιότητας** | **Περίληψη** | **Καθοδήγηση** |
|---|---|---|
| 0 | Κανένα | Δεν έχετε καμία γνώση ή εμπειρία σε αυτόν τον τομέα και δεν είναι μέρος των καθηκόντων σας. |
| 1 | Χαμηλό | Το πεδίο αρμοδιοτήτων εξασκείται σπάνια και είναι αρκετά βασισμένο στην παρατήρηση του τρόπου με τον οποίο γίνεται από τους άλλους, έχοντας λίγη κατανόηση του γιατί εκτελούνται συγκεκριμένα καθήκοντα.<br><br>Ενδεχομένως, ο τομέας δεξιοτήτων να έχει εξασκηθεί για σχετικά μικρό χρονικό διάστημα και δε θεωρείται μέρος της εργασίας του ατόμου. Δεν έχει γίνει καμία επίσημη εκπαίδευση. Μία γενική ευαισθητοποίηση. |
| 2 | Μεσαίο | Το πεδίο αρμοδιοτήτων εξασκείται τακτικά ως μέρος του εργασιακού ρόλου και αυτό πιθανόν συμβαίνει για αρκετό χρονικό διάστημα, ώστε το άτομο να αισθάνεται άνετα εξασκώντας το (πάνω από ένα χρόνο). Μπορεί να έχει γίνει άτυπη και σε μερικές περιπτώσεις επίσημη εκπαίδευση και υπάρχει κατανόηση των αρχών που διέπουν την ικανότητα. Το άτομο αισθάνεται ικανό σε αυτόν τον τομέα |

| | | |
|---|---|---|
| 3 | Υψηλό | Το πεδίο αρμοδιοτήτων θεωρείται ως ιδιαίτερη ικανότητα και υποστηρίζεται από σημαντική εκπαίδευση, προσόντα και εμπειρία για ένα μεγάλο χρονικό διάστημα (πιθανόν πάνω από τρία χρόνια). Οι αρχές είναι πλήρως κατανοητές και το άτομο ενημερώνεται διαρκώς για τις εξελίξεις σε αυτόν τον τομέα. Μπορεί να έχουν εκπαιδεύσει άλλους και είναι υπεύθυνοι για την ανάπτυξη των διεργασιών και των διαδικασιών και να έχουν εμπλακεί σε διάφορα σχετικά έργα. |
| 4 | Εξαιρετικό | Το άτομο είναι εξωτερικά αναγνωρισμένο ως εξειδικευμένο άτομο στο θέμα. Λαμβάνει μέρος σε επιχειρησιακά γεγονότα, όπως η παρουσίαση σε συνέδρια και σεμινάρια. Βρίσκεται ψηλά στην υπόληψη των ενδιαφερόμενων και μπορεί να βοηθήσει στην ανάπτυξη και τον έλεγχο νέων προϊόντων και υπηρεσιών. |

Πίνακας κατάταξης των εργαζομένων μετά την αξιολόγηση τους με τη διαδικασία συμπλήρωσης ερωτηματολογίων.

Οι απαντήσεις των ατόμων θα πρέπει, έπειτα, να επικυρώνονται από κάποιο άλλο πρόσωπο ή ομάδα, αναλόγως με τη φύση του ρόλου του ατόμου. Αυτός μπορεί να είναι ο διευθυντής ή ο προϊστάμενος ή σε κατάλληλες περιπτώσεις μπορεί να χρησιμοποιηθεί μια μέθοδος αξιολόγησης από έναν συνάδελφο. Αυτό θα εξασφαλίσει ένα αυξημένο επίπεδο συνέπειας στις απαντήσεις, καθώς μερικοί άνθρωποι είναι πολύ πιθανό να υπερεκτιμήσουν ή να υποτιμήσουν τα επίπεδα των δεξιοτήτων τους. Όπου υπάρχει διαφωνία για κάποιο επίπεδο δεξιοτήτων, η κατάσταση θα πρέπει να συζητηθεί με το σχετικό πρόσωπο, ώστε να γίνει κατανοητός ο λόγος της ύπαρξης απόκλισης. Αν εξακολουθεί να υπάρχει διαφωνία, μία απόφαση θα πρέπει να παρθεί από τη διοίκηση σχετικά με το πιο επίπεδο δεξιότητας θα πρέπει να χρησιμοποιηθεί.

Οι δεξιότητες των ατόμων που θα συμμετέχουν στην Επιτροπή για την Προστασία Προσωπικών Δεδομένων και την Ασφάλεια Πληροφοριών αναφέρονται στον πίνακα που ακολουθεί καθώς επίσης και το απαιτούμενο επίπεδο γνώσης ανά δεξιότητα.

| **Δεξιότητα** | **Απαιτούμενο Επίπεδο** |
|---|---|
| Νομοθεσία, ερμηνεία και νομολογία για το ΓΚΠΔ | 3 |
| Έννοιες, σχέδια και μέτρα, που αφορούν την προστασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών | 3 |
| Διαχείριση κινδύνων για την προστασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών | 3 |
| Πολιτικές την προστασία των προσωπικών δεδομένων και ασφάλειας πληροφοριών | 3 |
| Διεξαγωγή ανασκοπήσεων της διοίκησης | 3 |
| Αρχές Επιθεώρησης | 2 |
| Συνεχής βελτίωση | 2 |
| Διαχείριση περιστατικών για την Προστασία Προσωπικών Δεδομένων | 2 |

Αντίστοιχα για τον Υπεύθυνο Ασφάλειας Πληροφοριών θα πρέπει να ακολουθείτε ο παρακάτω πίνακας:

| **Δεξιότητα** | **Απαιτούμενο Επίπεδο** |
|---|---|
| Νομοθεσία, ερμηνεία και νομολογία για το ΓΚΠΔ | 3 |
| Έννοιες, σχέδια και μέτρα που αφορούν την προστασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών | 3 |
| Διαχείριση κινδύνων για την προστασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών | 3 |
| Διεξαγωγή ανασκοπήσεων της διοίκησης | 2 |

| **Δεξιότητα** | **Απαιτούμενο Επίπεδο** |
|---|---|
| Αρχές Επιθεώρησης | 3 |
| Συνεχής βελτίωση | 3 |
| Αρχές ελέγχων προστασίας προσωπικών δεδομένων και ασφάλειας πληροφοριών | 3 |
| Παρακολούθηση και δημιουργία αναφορών για την προστασία των προσωπικών δεδομένων και την ασφάλεια πληροφοριών | 3 |
| Διαχείριση πόρων | 2 |
| Πολιτικές Προστασίας Προσωπικών Δεδομένων και Ασφάλειας Πληροφοριών | 3 |
| Οργάνωση προστασίας των προσωπικών δεδομένων και ασφάλειας πληροφοριών | 3 |
| Ασφάλεια ανθρωπίνων πόρων | 3 |
| Διαχείριση περιουσιακών στοιχείων | 3 |
| Έλεγχος πρόσβασης | 3 |
| Κρυπτογραφία | 3 |
| Φυσική και περιβαλλοντική ασφάλεια | 3 |
| Ασφάλεια λειτουργιών | 3 |
| Ασφάλεια επικοινωνιών | 3 |
| Απόκτηση, ανάπτυξη και συντήρηση συστήματος | 3 |
| Σχέσεις προμηθευτών | 3 |
| Διαχείριση περιστατικών ασφάλειας πληροφοριών | 3 |
| Πτυχές της προστασίας των προσωπικών δεδομένων και της | 3 |

| **Δεξιότητα** | **Απαιτούμενο Επίπεδο** |
|---|---|
| ασφάλειας πληροφοριών στη διαχείριση της επιχειρησιακής συνέχειας | |
| Συμμόρφωση | 3 |

Τέλος, για το άτομο που θα αναλάβει την θέση Υπεύθυνος Προστασίας Δεδομένων τα παρακάτω προσόντα απαιτούνται.

| Δεξιότητα | Απαιτούμενο Επίπεδο |
|---|---|
| Νομοθεσία, ερμηνεία και νομολογία για το ΓΚΠΔ | 4 |
| Έννοιες, σχέδια και έλεγχοι που αφορούν την προστασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών | 4 |
| Σχετική νομοθεσία για την προστασία των δεδομένων | 4 |
| Εκτίμηση επιπτώσεων για την προστασία των δεδομένων | 4 |
| Διαχείριση κινδύνων για την προστασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών | 4 |
| Αρχές ελέγχων για την προστασία των προσωπικών δεδομένων και την ασφάλεια πληροφοριών | 4 |

### 5.4.2 Δημιουργία δράσεων ανάπτυξης δεξιοτήτων

Η παραπάνω διαδικασία μπορεί να επιτευχθεί με την υλοποίηση των παρακάτω ενεργειών και διαδικασιών:

- Ανεπίσημη εκπαίδευση από το υπάρχον προσωπικό, το οποίο έχει μεγαλύτερο επίπεδο δεξιοτήτων π.χ. καθοδήγηση
- Επίσημη εκπαίδευση μέσω μαθημάτων στο διαδίκτυο ή σε αίθουσα

- Πρόσληψη επιπλέον προσωπικού με τις σχετικές δεξιότητες
- Χρήση πόρων τρίτων για το συγκεκριμένο σκοπό π.χ. εργολάβους ή συμβουλευτικές υπηρεσίες.
- Χρήση πόρων τρίτων μέσω ενός συμβολαίου υποστήριξης που δίνει εγγυημένη πρόσβαση στο απαιτούμενο επίπεδο δεξιοτήτων

Η επιλογή της προσέγγισης εξαρτάται από τον αριθμό των παραγόντων, συμπεριλαμβανομένων των εσωτερικών πόρων, του οικονομικού προϋπολογισμού και του χρονοδιαγράμματος.

Σε μερικές περιπτώσεις μπορεί να αποφασιστεί να μη γίνει καμία ενέργεια για την αντιμετώπιση μίας αντιληπτής έλλειψης δεξιοτήτων π.χ. αν η απαίτηση είναι πιθανόν να μειωθεί η να εξαφανιστεί στο κοντινό μέλλον λόγω γνωστών αλλαγών. Οι κίνδυνοι, που εμπλέκονται, πρέπει να δηλωθούν σαφώς.

Έπειτα, οι ενέργειες ανάπτυξης και οι κίνδυνοι, που προτείνονται για αποδοχή, υποβάλλονται στη διοίκηση για έγκριση.

### 5.4.3. Αξιολόγηση Αποτελεσματικότητας

Οι εγκεκριμένες ενέργειες, που εντοπίστηκαν για την ανάπτυξη των δεξιοτήτων σε συγκεκριμένα άτομα, θα πρέπει να αναθεωρηθούν ως προς την αποτελεσματικότητά τους και ως μέρος των αξιολογήσεων της απόδοσης των εργαζομένων και των τακτικών αξιολογήσεων της διοίκησης για τη συμμόρφωση με το ΓΚΠΔ.

Μόλις ολοκληρωθεί μία δράση ανάπτυξης, θα πρέπει να γίνει μία επανεκτίμηση για να ελεγχθεί ότι το άτομο κατέχει το απαιτούμενο επίπεδο δεξιοτήτων. Σε περίπτωση που αυτό δε συμβαίνει, θα πρέπει να εντοπιστούν οι λόγοι και, εφόσον είναι απαραίτητο, θα πρέπει να γίνουν περαιτέρω δράσεις για την επίτευξη του απαιτούμενου αποτελέσματος.

Θα πρέπει να διατηρηθούν τα κατάλληλα έγγραφα, που αποδεικνύουν όλες τις ενέργειες που έγιναν. Αυτό περιλαμβάνει τα έγγραφα των εκπαιδεύσεων (πρόγραμμα εκπαίδευσης), την καταγραφή της καθοδήγησης ή τα συμβόλαια με τρίτα μέρη.

### 5.4.4 Πρόγραμμα Επικοινωνίας για τον Φορέα και συμμόρφωσης με το ΓΚΠΔ

Το άρθρο 24 σχετικά με την ευθύνη του Υπεύθυνου Επεξεργασίας, αποτελεί κομβικής σημασίας διαδικασία, ο σωστός σχεδιασμός της οποίας και η υλοποίηση της προαπαιτούνται για την πλήρη συμμόρφωση του Π.Μ.Σ με το ΓΚΠΔ.

Πιο συγκεκριμένα, ο Γενικός Κανονισμός Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (ΓΚΠΔ) έχει νομική ισχύ από το Μάιο του 2018 και επεκτείνει και διασαφηνίζει τα δικαιώματα του υποκειμένου των δεδομένων και τους τρόπους με τους οποίους οι οργανισμοί, οι οποίοι διατηρούν και επεξεργάζονται τα προσωπικά δεδομένα των κατοίκων της ΕΕ, πρέπει να λειτουργούν. Καθώς αποτελεί μέρος της Ευρωπαϊκής νομοθεσίας, η συμμόρφωση με το ΓΚΠΔ δεν είναι προαιρετική και το Π.Μ.Σ. είναι πλήρως δεσμευμένο στο να διασφαλίσει ότι πληροί όλες τις απαιτήσεις.

Μέσω των εκατό εβδομήντα τριών αιτιολογικών σκέψεων και των ενενήντα εννέα άρθρων, ο ΓΚΠΔ περιέχει μερικές σημαντικές αλλαγές σε σχέση με τον προηγούμενο νόμο περί προστασίας δεδομένων, ο οποίος ποικίλει στα διάφορα κράτη-μέλη της ΕΕ. Σε αυτές τις αλλαγές συμπεριλαμβάνονται η υποχρεωτική ειδοποίηση σε περίπτωση παραβίασης των δεδομένων, πρόστιμα, που φτάνουν το 4 τις εκατό του παγκόσμιου ετήσιου κύκλου εργασιών των οργανισμών, τον ορισμό ενός Υπευθύνου Προστασίας Δεδομένων και τη διεξαγωγή εκτίμησης των επιπτώσεων για την προστασία των δεδομένων.

Είναι πολύ σημαντικό για το Π.Μ.Σ. να φροντίσει ώστε αυτές οι αλλαγές, οι επιπτώσεις τους, και η προσέγγισή του οργανισμού να κοινοποιηθούν σε όλα τα ενδιαφερόμενα μέρη, όπως είναι οι εργαζόμενοι, οι φοιτητές και οι εξωτερικοί και εσωτερικοί συνεργάτες (καθηγητές και λοιπό εκπαιδευτικό προσωπικό) έτσι ώστε όλοι να είναι ενήμεροι για το τι συμβαίνει όσον αφορά το ΓΚΠΔ.

Το παρόν έγγραφο ορίζει τον τρόπο με τον οποίο θα έρθουμε σε επικοινωνία με τα ενδιαφερόμενα μέρη εντός και εκτός του Π,Μ,Σ. για το θέμα του ΓΚΠΔ και τα μέτρα προστασίας προσωπικών δεδομένων και ασφάλειας των πληροφοριών, που θα λάβουμε για να υποστηρίξουμε τη συμμόρφωσή μας. Στο έγγραφο αυτό προσδιορίζονται τα ενδιαφερόμενα μέρη και ο τρόπος με τον οποίο θα οριστεί μία αποτελεσματική δίοδος επικοινωνίας.

Η γενική προσέγγιση για τη διασφάλιση της αποτελεσματικής δέσμευσης και επικοινωνίας, όσον αφορά το ΓΚΠΔ μέσα στο Π.Μ.Σ., περιγράφεται παρακάτω:

1. Προσδιορισμός του κοινού/των ενδιαφερόμενων μερών
2. Ορισμός των κατάλληλων θεμάτων επικοινωνίας για κάθε ενδιαφερόμενο μέρος
3. Συμφωνία όσον αφορά τις καταλληλότερες μεθόδους δέσμευσης και επικοινωνίας
4. Υλοποίηση του προγράμματος
5. Ανατροφοδότηση και απαιτούμενες ενέργειες για την επιτυχία της επικοινωνίας, μέσω ενός πλάνου συνεχούς βελτίωσης.

### 5.4.4.1 Κοινό

Το πρόγραμμα επικοινωνίας στοχεύει στα ενδιαφερόμενα μέρη, τόσο εσωτερικά όσο και εξωτερικά, είτε με σύμβαση εργασίας είτε μόνιμα, που διαδραματίζουν ένα ρόλο στην προστασία των προσωπικών δεδομένων εντός του Π.Μ.Σ..

Στα ενδιαφερόμενα μέρη περιλαμβάνονται:

- Οι εργαζόμενοι
- Οι φοιτητές.
- Οι κανονιστικές αρχές και άλλες κυβερνητικές υπηρεσίες
- Τα υπουργεία και οι υπηρεσίες έκτακτης ανάγκης (π.χ. πυροσβεστική, αστυνομία, Εθνικό Κέντρο Άμεσης Βοήθειας, κ.λπ.)
- Οι προμηθευτές και οι συνεργάτες

### 5.4.4.2 Θέματα επικοινωνίας

Το πρόγραμμα επικοινωνίας έχει ως στόχο να μεταδώσει τις βασικές πληροφορίες στους ακόλουθους κύριους τομείς:

- Οι κύριες απαιτήσεις του ΓΚΠΔ και πως αυτές σχετίζονται με την επεξεργασία των προσωπικών δεδομένων στη λειτουργία του Π.Μ.Σ..

- Το γενικό πλαίσιο, που ακολουθείται για την εκπλήρωση των απαιτήσεων του ΓΚΠΔ, συμπεριλαμβανομένου του οράματος, των πολιτικών, των σχεδίων και των στόχων, οι οποίοι πρέπει να επιτευχθούν

- Το ρόλο, που αναμένεται να παίξει κάθε ένα από τα ενδιαφερόμενα μέρη, στη διασφάλιση της συμμόρφωσης.

- Νέες και τροποποιημένες επεξεργασίες και διαδικασίες, που εφαρμόζονται ήδη ή πρόκειται να εφαρμοστούν

- Τον τρόπο με τον οποίο τα μέτρα προστασίας προσωπικών δεδομένων και ασφάλειας πληροφοριών, που εφαρμόζονται σχετίζονται με τη συμμόρφωση στο ΓΚΠΔ, τόσο στην παρούσα φάση όσο και στη συνέχεια

- Οποιεσδήποτε άλλες κανονιστικές και συμβατικές απαιτήσεις και περιορισμούς στο πλαίσιο των οποίων ο οργανισμός πρέπει να λειτουργεί, όσον αφορά τα προσωπικά δεδομένα.

- Αναβαθμίσεις όσον αφορά τον τρόπο με τον οποίο θα εξελιχθούν τα σχέδια με σκοπό την εκπλήρωση των απαιτούμενων στόχων του πλαισίου συμμόρφωσης με το ΓΚΠΔ

- Ευαισθητοποίηση σε θέματα προστασίας προσωπικών δεδομένων και ασφάλειας πληροφοριών και πιθανών κινδύνων, καθώς και η προσέγγισή μας στην αντιμετώπισή τους

Το επίπεδο της λεπτομέρειας, που απαιτείται στους παραπάνω τομείς θα ποικίλει ανάλογα με τα ενδιαφερόμενα μέρη, που εμπλέκονται και την φύση των προσωπικών δεδομένων που επεξεργάζονται.

### 5.4.4.3 Μέθοδοι επικοινωνίας

Υπάρχει ένας αριθμός καθορισμένων μεθόδων επικοινωνίας εσωτερικά στο Π.Μ.Σ οι οποίες θα χρησιμοποιηθούν όπου είναι δυνατό. Αυτές θα πρέπει να περιλαμβάνουν:

- Την ανακοίνωση του προγράμματος συμμόρφωσης του Π.Μ.Σ. στο ΓΚΠΔ σε όλα τα ενδιαφερόμενα μέρη, μέσω της ιστοσελίδας μας

- Τακτικές συνεδριάσεις και ενημερώσεις της ομάδας έργου για τη συμμόρφωση με το ΓΚΠΔ

- Επίσημες εκπαιδεύσεις όσον αφορά την Προστασία Προσωπικών Δεδομένων, σε όλους τους εργαζόμενους του Π.Μ.Σ.
- Νέα πολιτική για την ιδιωτικότητα και την προστασία προσωπικών δεδομένων στην ιστοσελίδα μας
- Ηλεκτρονικά μηνύματα ευαισθητοποίησης σε όλους τους εργαζομένους
- Ηλεκτρονικά μηνύματα ευαισθητοποίησης στους καθηγητές / φοιτητές / λοιπούς εργαζόμενους, καθώς επίσης και αποστολή της πολιτικής για την ιδιωτικότητα και την προστασία προσωπικών δεδομένων σε αυτούς

Η επικοινωνία διακρίνεται σε εσωτερική και εξωτερική ανάλογα με τη σύνθεση των ενδιαφερομένων μερών που συμμετέχουν στη διαδικασία της επικοινωνίας και διαφορετικές διαδικασίες θα πρέπει να ενεργοποιήσει ο Φορέας ανά περίπτωση.

Τέλος, σημαντικός είναι και ο σχεδιασμός διαδικασίας που σκοπό θα έχει την ανατροφοδότηση σχετικά με την επικοινωνία και αξιολόγηση της διαδικασίας που ακολουθήθηκε ως επιτυχημένη ή να οδηγεί σε αναθεωρήσεις σχετικές προκειμένου να γίνει πιο αποτελεσματική.

Συνοψίζοντας, η αποτελεσματική επικοινωνία με τα ενδιαφερόμενα μέρη είναι ύψιστης σημασίας για τη διασφάλιση της συμμόρφωσης με το ΓΚΠΔ εντός του Π.Μ.Σ. Οι μέθοδοι επικοινωνίας που θα υλοποιηθούν θα βοηθήσουν στο να διασφαλιστεί ότι όλοι οι εμπλεκόμενοι θα παραμένουν καλά πληροφορημένοι σχετικά με την προστασία των δεδομένων και την ασφάλεια των πληροφοριών.

# ΚΕΦΑΛΑΙΟ 6: ΑΝΑΛΥΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

## 6.1 ΑΡΧΕΙΑ ΤΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Ο ΓΚΠΔ με το Άρθρο 30 (Αρχεία των δραστηριοτήτων επεξεργασίας) μας υποχρεώνει να ορίσουμε τις διαδικασίες που υλοποιούνται εντός του φορέα Π.Μ.Σ και κατ' επέκταση να γίνει αναφορά και στα αρχεία των προσωπικών δεδομένων που διατηρούνται και αποσκοπούν στην εύρυθμη λειτουργία του Π.Μ.Σ.

Προκειμένου λοιπόν να συμμορφωθούμε με τη συγκεκριμένη απαίτηση του συστήματος θα πρέπει να δομηθεί ένα έγγραφο όπου θα καταγράφονται τα παρακάτω στοιχεία ανά επιμέρους δραστηριότητα του φορέα με τελικό σκοπό να συνοψίσει την επεξεργασία των προσωπικών δεδομένων από τον φορέα.

Για τον παραπάνω σκοπό, η δομή του εντύπου θα μπορούσε να παραπέμπει σε ένα λογιστικό φύλλο excel με στήλες που θα ανέγραφαν τα παρακάτω. Οι Έννοιες των αναγραφομένων στηλών επίσης διευκρινίζονται.

| **Στήλη** | **Έννοια** |
|---|---|
| Α/Α | Ένας διαδοχικός αριθμός αναφοράς που αρχίζει με 1 |
| Όνομα και στοιχεία επικοινωνίας του υπεύθυνου της επεξεργασίας | Ποιος είναι ο υπεύθυνος των δεδομένων, δηλ. Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, ο οργανισμός ή άλλος φορέας ο οποίος, από μόνος του ή από κοινού με άλλους, καθορίζει τους σκοπούς και τα μέσα επεξεργασίας δεδομένων προσωπικού χαρακτήρα |
| Όνομα και στοιχεία επικοινωνίας του από κοινού υπεύθυνου της επεξεργασίας (κατά περίπτωση) | Ποιος είναι ο από κοινού υπεύθυνος της επεξεργασίας (εάν υπάρχει) των δεδομένων. Αυτό ισχύει όταν δύο ή περισσότεροι υπεύθυνοι της επεξεργασίας καθορίζουν από κοινού τους |

| | |
|---|---|
| | σκοπούς και τα μέσα επεξεργασίας |
| Όνομα και στοιχεία επικοινωνίας του εκπροσώπου του υπεύθυνου της επεξεργασίας | Όταν ο υπεύθυνος της επεξεργασίας δεν βρίσκεται στην Ευρωπαϊκή Ένωση |
| Όνομα και στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων (κατά περίπτωση) | Όταν υπάρχει απαίτηση ορισμού υπεύθυνου προστασίας δεδομένων |
| Σκοποί της επεξεργασίας | Οι λόγοι για τους οποίους πραγματοποιείται η επεξεργασία |
| Κατηγορίες υποκειμένων δεδομένων | Ορίστε ποιοι είναι τα υποκείμενα των δεδομένων π.χ. ανά χώρα, φύλο, αποδέκτες υπηρεσιών |
| Κατηγορίες προσωπικών δεδομένων | Καθορίστε τους τύπους στοιχείων δεδομένων που εμπλέκονται |
| Κατηγορίες των αποδεκτών δεδομένων που κοινοποιήθηκαν | Ποια είναι τα δεδομένα τα οποία έχουν τακτικά πρόσβαση ή ότι έχουν πρόσβαση σε αυτά |
| Διεθνής προορισμός μεταφοράς | Χώρες ή διεθνείς οργανισμοί στους οποίους μεταφέρονται τακτικά τα δεδομένα |
| Χρονικά όρια για τη διαγραφή | Πόσο καιρό θα διατηρηθούν τα προσωπικά δεδομένα πριν να διαγραφούν |
| Εφαρμόζονται τεχνικά και οργανωτικά μέτρα ασφαλείας | Σύντομη περιγραφή των στοιχείων ελέγχου, που χρησιμοποιούνται για την προστασία των προσωπικών δεδομένων (ανατρέξτε στις πρόσθετες πληροφορίες, εάν απαιτείται) |
| Σχόλια | Οποιεσδήποτε άλλες παρατηρήσεις θέλετε να κάνετε σχετικά με τις πληροφορίες |

## 6.2 Προσωπικά Δεδομένα – Αρχικό Ερωτηματολόγιο.

Η λεπτομερής καταγραφής των προσωπικών δεδομένων είναι καίριας σημασίας για την σωστή δόμηση του συστήματος, προκειμένου να υπακούει τον ΓΚΠΔ.

Το έντυπο που ακολουθεί πρέπει να χρησιμοποιείται για την καταγραφή των βασικών πληροφοριών σχετικά με τα προσωπικά δεδομένα, που συλλέγονται και υποβάλλονται σε επεξεργασία στο πλαίσιο μιας δραστηριότητας του Π.Μ.Σ. Οι πληροφορίες θα χρησιμοποιηθούν ως σημείο εκκίνησης για μια λεπτομερέστερη χαρτογράφηση δεδομένων αργότερα.

**Λεπτομέρειες Δραστηριότητας του φορέα (Π.Μ.Σ)**

| | |
|---|---|
| **Δραστηριότητα του Π.Μ.Σ:** | |
| **Περιγραφή δραστηριότητας:** | |

**Προσωπικά δεδομένα που συλλέγονται**

*[Περιγράψτε τα προσωπικά δεδομένα που συλλέγονται στο πλαίσιο της διαδικασίας του Φορέα π.χ. όνομα και διεύθυνση, αριθμός τηλεφώνου]*

**Πως συλλέγονται τα προσωπικά δεδομένα;**

*[Δηλώστε τη μέθοδο που χρησιμοποιήθηκε για τη συλλογή των προσωπικών δεδομένων π.χ. μέσω ιστοσελίδας ή πρόσωπο με πρόσωπο. Συμπεριλάβετε εάν τα δεδομένα λαμβάνονται απευθείας από το πρόσωπο στο οποίο αναφέρονται τα δεδομένα ή έμμεσα από τρίτο μέρος και, ανάλογα με την περίπτωση, ποιος συλλέγει τα δεδομένα]*

**Τι συμβαίνει με τα προσωπικά δεδομένα μετά τη συλλογή;**

*[Για ποιο λόγο θα χρησιμοποιηθούν τα δεδομένα; Θα υποστούν επεξεργασία εσωτερικά ή από ένα ή περισσότερα τρίτα μέρη;]*

**Που θα αποθηκευτούν τα δεδομένα;**

*[Πού θα αποθηκευτούν τα δεδομένα π.χ. σε ένα ντουλάπι αρχειοθέτησης, σε ένα διακομιστή, στο cloud?]*

**Ποιος έχει πρόσβαση στα δεδομένα και πως;**

*[Ποιος εντός και εκτός του οργανισμού θα έχει πρόσβαση στα δεδομένα;]*

**Πόσο καιρό θα διατηρηθούν τα δεδομένα;**

*[Για πόσο καιρό θα διατηρηθούν τα δεδομένα και γιατί;]*

**Χρησιμοποιούνται τα δεδομένα για άλλους σκοπούς;**

*[Είναι πιθανό τα δεδομένα να χρησιμοποιηθούν για σκοπούς άλλους από εκείνους για τους οποίους συλλέγονται και αν ναι, για τι;]*

**Τα δεδομένα μεταφέρονται οπουδήποτε και αν ναι, πού και υπό ποιες συνθήκες;**

*[Θα αποστέλλονται τα δεδομένα σε άλλες τοποθεσίες ή σε τρίτους σε άλλες χώρες; Εάν ναι, τι θα μπορούσε να προκαλέσει τη μεταφορά και γιατί;]*

**Παρακαλείστε να αναφέρετε κάθε άλλη σχετική πληροφορία**

| | |
|---|---|
| **Όνομα:** | |
| **Τομέας:** | |
| **Ημερομηνία:** | |

Μόλις ολοκληρωθεί, αυτό το έντυπο θα πρέπει να υποβληθεί μέσω e-mail στο dpo@master-ateith.gr .

## 6.3 Διαδικασία Εκτίμησης Έννομου Συμφέροντος

Το άρθρο 6 του ΓΚΠΔ αναφέρεται στη νομιμότητα της επεξεργασίας. Υπάρχουν έξι διαφορετικοί τρόποι με τους οποίους μπορεί να διαπιστωθεί η νομιμότητα μίας συγκεκριμένης περίπτωσης επεξεργασίας προσωπικών δεδομένων σύμφωνα με το ΓΚΠΔ.

Οι επιλογές είναι οι εξής:

- Συγκατάθεση
- Εκτέλεση μίας σύμβασης
- Έννομη υποχρέωση
- Διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων
- Εκπλήρωση καθήκοντος, που εκτελείται προς το δημόσιο συμφέρον
- Έννομο συμφέρον

Η διαδικασία αυτή προορίζεται για χρήση, στην περίπτωση που διαπιστωθεί, ότι η νόμιμη βάση της επεξεργασίας σε μια συγκεκριμένη περίπτωση μπορεί να βασίζεται σε έννομο συμφέρον.

Αυτή η διαδικασία θα πρέπει να εξετάζεται σε συνδυασμό με τα παρακάτω σχετικά έγγραφα:

- *Πολιτική για την Ιδιωτικότητα και την Προστασία Προσωπικών Δεδομένων*
- *Πολιτική Διατήρησης και Προστασίας Αρχείων*
- *Διαδικασία Χαρτογράφησης Προσωπικών Δεδομένων*
- *Διαδικασία Υποβολής Αιτήματος από το Υποκείμενο των Δεδομένων*
- *Διαδικασία Εκτίμησης Αντικτύπου για την Προστασία των Δεδομένων*

Ο ΓΚΠΔ επιτρέπει την επεξεργασία των προσωπικών δεδομένων όταν:

*«η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που*

*επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.» (ΓΚΠΔ Άρθρο 6 , σημείο στ')*

Σε γενικές γραμμές, το έννομο συμφέρον θα ισχύει σε περιπτώσεις όπου η επεξεργασία μπορεί εύλογα να αναμένεται από το υποκείμενο των δεδομένων και όπου η επίπτωση στην ιδιωτικότητα του υποκειμένου των δεδομένων δεν είναι σημαντική. Μπορεί επίσης να εφαρμόζεται, όπου υπάρχει ισχυρή αιτιολόγηση για να διεξαχθεί η επεξεργασία από τον οργανισμό.

Προκειμένου να καθιερωθεί πλήρως και να αποδειχτεί, ότι το έννομο συμφέρον αποτελεί εύλογη βάση για την επεξεργασία σε μία συγκεκριμένη περίπτωση, πρέπει να εφαρμοστεί ένα τεστ τριών μερών.

Αυτό το τεστ απαιτεί από τον οργανισμό να επιδείξει:

1. την ακριβή φύση του έννομου συμφέροντος ( το τεστ του *Σκοπού*)
2. ότι η επεξεργασία είναι απαραίτητη για το έννομο συμφέρον (το τεστ της *Αναγκαιότητας*)
3. ότι τα συμφέροντα, τα δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων δεν υπερισχύουν των έννομων συμφερόντων του οργανισμού (το τεστ της *Εξισορρόπησης*)

Γι' αυτή τη διαδικασία χρησιμοποιείται η *Φόρμα Εκτίμησης Έννομου Συμφέροντος (ακολουθεί σχετικό έντυπο)* για την τεκμηρίωση καθενός από τα παραπάνω τεστ και την παροχή αποδεικτικών στοιχείων, όταν απαιτείται, που υποστηρίζουν το γεγονός ότι εκτελέστηκε μία ορθή εκτίμηση.

### 6.3.1 Το τεστ του Σκοπού

Το τεστ του σκοπού έχει ως στόχο να εξακριβώσει, αν το συμφέρον, που δηλώθηκε, είναι όντως έννομο για τον οργανισμό, ή για κάποιον τρίτο. Αυτό το τεστ περιλαμβάνει τον ακριβή καθορισμό των λόγων, για τους οποίους γίνεται η επεξεργασία και τα οφέλη που προσφέρει.

Θα πρέπει να γίνεται λεπτομερής περιγραφή του τι σκοπεύει να πετύχει η επεξεργασία, και πιο συγκεκριμένα:

- Ποιοι είναι οι στόχοι της επεξεργασίας;
- Πως θα γίνει αντιληπτό αν επετεύχθη ο σκοπός;
- Πόσο πιθανό είναι να επιτευχθούν οι στόχοι μέσω της επεξεργασίας;

Θα πρέπει να αξιολογούνται τα αποτελέσματα της επεξεργασίας και να αναφέρονται τα οφέλη που προκύπτουν από αυτή την επεξεργασία. Στο πλαίσιο αυτής της διαδικασίας θα πρέπει να γίνεται εκτενής αναφορά στα:

- Ποια είναι τα οφέλη, που θα μπορούσαν να προκύψουν από την επεξεργασία;
- Πόσο σημαντικά είναι αυτά τα οφέλη (ποσοτικοποίηση όπου είναι δυνατόν);
- Ποιος θα λάβει τα πλεονεκτήματα της επεξεργασίας, π.χ. ο οργανισμός, το κοινό, το υποκείμενο των δεδομένων;

Σημαντικό κομμάτι της παραπάνω διαδικασίας είναι η περιγραφή των επιπτώσεων που πηγάζουν από την μη επεξεργασία των δεδομένων αυτών. Λεπτομερής περιγραφή του πιθανού αντίκτυπου της μη επεξεργασίας των προσωπικών δεδομένων με τον τρόπο που προτείνεται.

- Πόσο σημαντική θα ήταν η επίπτωση;
- Πόσο πιθανό είναι να γίνει αισθητός ο αντίκτυπος;
- Ποιος θα επηρεαστεί από το να μη γίνει η επεξεργασία;

Σε αυτό το στάδιο θα μπορούσε να γίνει αναφορά και σε οποιοδήποτε άλλο ζήτημα θεωρούμε ότι θα ενίσχυε την άποψη του Φορέα για την αναγκαιότητα της επεξεργασίας των συγκεκριμένων δεδομένων. Οποιοδήποτε άλλο ζήτημα, που μπορεί να είναι σχετικό.

Τέλος, αναγκαία είναι η αναφορά σε άλλους παράγοντες υπέρ και κατά της επεξεργασίας και είναι σημαντικό να παρουσιαστεί μια ισορροπημένη άποψη. Θα πρέπει να αποφεύγεται η αναφορά σε υποκειμενικές απόψεις.

### 6.3.2 Το τεστ της Αναγκαιότητας

Προκειμένου το έννομο συμφέρον να αποτελεί έγκυρη νόμιμη βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, πρέπει να αποδειχθεί ότι η επεξεργασία είναι πράγματι αναγκαία για να αποκτηθεί το όφελος. Εξετάστε κατά πόσο υπάρχουν άλλοι τρόποι για την επίτευξη των στόχων που αναφέρονται στο τεστ του σκοπού, οι οποίοι δεν απαιτούν την επεξεργασία των προσωπικών δεδομένων ή απαιτούν την επεξεργασία λιγότερων από αυτά.

Στη *Φόρμα Εκτίμησης Έννομου Συμφέροντος* εξηγείστε γιατί η επεξεργασία πρέπει να γίνεται με τον τρόπο που περιγράφεται για τα προβλεπόμενα οφέλη, που πρέπει να επέλθουν. Συγκεκριμένα:

- Πώς σχετίζεται η επεξεργασία με τα αναμενόμενα οφέλη;
- Είναι η επεξεργασία, όπως προτείνεται, ο καλύτερος τρόπος για να επιτευχθεί το τελικό αποτέλεσμα;
- Ποιες εναλλακτικές λύσεις εξετάστηκαν και γιατί απορρίφθηκαν;

### 6.3.3 Το τεστ της Εξισορρόπησης

Έχοντας διαπιστώσει τη φύση του συμφέροντος, τα οφέλη του και το γεγονός, ότι η επεξεργασία είναι απαραίτητη για τα οφέλη αυτά, το τελευταίο βήμα είναι να εκτιμηθεί κατά πόσον το συγκεκριμένο συμφέρον υπερισχύει των συμφερόντων ιδιωτικότητας των εμπλεκόμενων υποκειμένων των δεδομένων.

Εδώ επιβάλλεται η χρήση της « *Φόρμας Εκτίμησης Έννομου Συμφέροντος*» για να αξιολογήσετε αυτή την ισορροπία συμφερόντων απευθυνόμενοι στις ακόλουθες ερωτήσεις:

- Ποια είναι τα υποκείμενα των δεδομένων;

Πώς μπορούν να κατηγοριοποιηθούν τα υποκείμενα των δεδομένων; Δώστε ιδιαίτερη προσοχή στο εάν κάποιο από αυτά ανήκει σε ευαίσθητες ομάδες όπως παιδιά ή εάν υπάρχουν πολιτιστικές παράμετροι.

- Ποια είναι η σχέση του οργανισμού με το υποκείμενο των δεδομένων;

Εξετάστε αν ο οργανισμός είναι γνωστός στο υποκείμενο των δεδομένων και εάν ναι, ποια είναι η φύση της σχέσης π.χ. *ασθενής* ή αιτών;

- Ποια προσωπικά δεδομένα εμπλέκονται στην επεξεργασία;

Αν τα προσωπικά δεδομένα που υποβάλλονται σε επεξεργασία ανήκουν σε ειδικές ή ευαίσθητες κατηγορίες, όπως ιατρικά στοιχεία π.χ. ιατρικό ιστορικό.

- Ποια είναι η πιθανή αντίδραση του υποκειμένου των δεδομένων στην επεξεργασία;

Θα μπορούσε το υποκείμενο των δεδομένων εύλογα να αναμένει την επεξεργασία ή είναι πιθανό να τη θεωρήσει παρεμβατική ή ακατάλληλη; Οποιαδήποτε διαβούλευση με τους εκπροσώπους των υποκειμένων των δεδομένων θα προσέδιδε βάρος στην περίπτωση σε αυτόν τον τομέα.

- Ποιες είναι οι πιθανές επιπτώσεις στο υποκείμενο των δεδομένων;

Ποιες συνέπειες θα μπορούσε να έχει η επεξεργασία για το υποκείμενο των δεδομένων π.χ. θα μπορούσε καταναλώσει το χρόνο τους, να επηρεάσει τη φήμη τους ή να τους κοστίσει χρήματα;

- Πώς θα μπορούσε να μειωθεί ο αντίκτυπος στο υποκείμενο των δεδομένων;

Υπάρχουν τεχνικές ή προσεγγίσεις, που θα μπορούσαν να χρησιμοποιηθούν για τη μείωση των επιπτώσεων στο θέμα των δεδομένων π.χ. να σταλούν μηνύματα ηλεκτρονικού ταχυδρομείου αντί της διεξαγωγής τηλεφωνικών κλήσεων ή να τους δώσετε ένα στοιχείο επιλογής, π.χ. μια διαγραφή ή μια εξαίρεση;

### 6.3.4 Αξιολόγηση Απόφασης

Μετά την ολοκλήρωση των τριών τεστ, πρέπει να γίνει μια εκτίμηση σχετικά με το κατά πόσο η επεξεργασία μπορεί να θεωρηθεί νόμιμη με βάση το έννομο συμφέρον.

Η απόφαση, που πάρθηκε, θα πρέπει να καταγραφεί στη «*Φόρμα Εκτίμησης Έννομου Συμφέροντος»,* μαζί με τα στοιχεία του ποιος πραγματοποίησε την αξιολόγηση και πότε και ποιος ενέκρινε την απόφαση.

Τα αρχεία αξιολόγησης των έννομων συμφερόντων πρέπει να διατηρούνται ως απόδειξη ότι πραγματοποιήθηκε μια τέτοια αξιολόγηση και ως ένδειξη για τη σχετική Ενημέρωση του Υποκειμένου των Δεδομένων.

## 6.4 Φόρμα Εκτίμησης Έννομου Συμφέροντος

Το εν λόγω έντυπο προορίζεται για να εξακριβωθεί αν απαιτείται η χρήση του έννομου συμφέροντος ως νόμιμης βάσης της επεξεργασίας σε μία συγκεκριμένη περίπτωση, σύμφωνα με το ΓΚΠΔ. Είναι αυτονόητο ότι τα στοιχεία που αναφέρονται παρακάτω θα πρέπει να είναι με την μορφή επίσημου εντύπου του συστήματος με συγκεκριμένα κείμενα που απαρτίζουν την κεφαλίδα και τα υποσέλιδα κάθε σελίδας και να φυλάσσεται στα έντυπα του συστήματος προκειμένου να επιδεικνύεται σε οποιαδήποτε ζήτηση.

**Λεπτομέρειες Αξιολόγησης**

| | |
|---|---|
| **Τίτλος επεξεργασίας που αξιολογείται:** | |
| **Περιγραφή της επεξεργασίας:** | |
| **Όνομα αξιολογητή(ών):** | |
| **Ημερομηνία αξιολόγησης:** | |

**Το τεστ του Σκοπού**

Στόχοι:

1. Ποιοι είναι οι στόχοι της επεξεργασίας;

2. Πώς θα ξέρετε αν έχει επιτευχθεί ο σκοπός της;

3. Πόσο πιθανό είναι να καλυφθούν οι στόχοι από την επεξεργασία;

Οφέλη:

1. Ποια είναι τα οφέλη (που θα μπορούσαν) να προκύψουν από την επεξεργασία;
2. Πόσο σημαντικά είναι αυτά τα οφέλη (ποσοτικοποιήστε αν είναι δυνατόν);
3. Ποιος θα λάβει τα οφέλη της επεξεργασίας π.χ. ο οργανισμός, το κοινό, το υποκείμενο των δεδομένων;

Επιπτώσεις της μη επεξεργασίας

1. Πόσο σημαντικός θα ήταν ο αντίκτυπος;
2. Πόσο πιθανό είναι να γίνει αισθητός ο αντίκτυπος;
3. Ποιος θα επηρεαστεί από τη μη επεξεργασία;

Άλλα θέματα

1. Έχει γίνει αυτή η επεξεργασία πριν, και αν ναι, ποια ήταν τα αποτελέσματα;
2. Είναι ηθική η επεξεργασία;
3. Θα μπορούσε η επεξεργασία να έχει αρνητική επίπτωση, και αν ναι, τι και για ποιον;
4. Άλλα θέματα

Το τεστ της Αναγκαιότητας

1. Πώς σχετίζεται η επεξεργασία με τα αναμενόμενα οφέλη;
2. Είναι η επεξεργασία, όπως προτείνεται, ο καλύτερος τρόπος για να επιτευχθεί το τελικό αποτέλεσμα;
3. Ποιες εναλλακτικές λύσεις εξετάστηκαν και γιατί απορρίφθηκαν;

Το τεστ της Εξισορρόπησης

1. Ποιοι είναι τα υποκείμενα των δεδομένων;
2. Ποια είναι η σχέση του οργανισμού με το υποκείμενο των δεδομένων;
3. Ποια προσωπικά δεδομένα εμπλέκονται στην επεξεργασία;
4. Ποια είναι η πιθανή αντίδραση του υποκειμένου των δεδομένων στην επεξεργασία;
5. Ποιες είναι οι πιθανές επιπτώσεις στο υποκείμενο των δεδομένων;
6. Πώς θα μπορούσε να μειωθεί ο αντίκτυπος στο υποκείμενο των δεδομένων;

**Απόφαση Αξιολόγησης**

| | |
|---|---|
| **Απόφαση:** | |
| **Κύριοι λόγοι για την απόφαση:** | |
| **Ημερομηνία απόφασης:** | |
| **Εγκρίθηκε από:** | |
| **Ημερομηνία έγκρισης:** | |

Εάν εγκριθεί, τα περιεχόμενα αυτού του εντύπου θα χρησιμοποιηθούν για τη δημιουργία κατάλληλου εγγράφου ενημέρωσης του υποκειμένου των δεδομένων, το οποίο θα εφίσταται την προσοχή των σχετικών προσώπων στα οποία αναφέρονται τα δεδομένα.

# ΚΕΦΑΛΑΙΟ 7 :ΠΟΛΙΤΙΚΗ ΓΙΑ ΤΗΝ ΙΔΙΩΤΙΚΟΤΗΤΑ ΚΑΙ ΤΗΝ ΕΝΗΜΕΡΩΣΗ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ

## 7.1 Κεφάλαιο ΙΙ- Αρχές

Στις καθημερινές λειτουργίες του, το Π.Μ.Σ συλλέγει και αποθηκεύει αρχεία διαφορετικών τύπων και μορφών. Η σημαντικότητα και η ευαισθησία αυτών των αρχείων ποικίλει και υπόκειται στο σχήμα διαβάθμισης, που εφαρμόζει ο φορέας.

Είναι σημαντικό τα αρχεία να προστατεύονται από απώλεια, καταστροφή, παραποίηση, μη εξουσιοδοτημένη πρόσβαση και μη εξουσιοδοτημένη ανακοίνωση και να χρησιμοποιείται ένα εύρος μέτρων ασφάλειας για να διασφαλίσουν αυτήν την προστασία, συμπεριλαμβανομένων των αντιγράφων ασφαλείας, τον έλεγχο πρόσβασης και την κρυπτογράφηση.

Επίσης, το Π.Μ.Σ έχει ευθύνη να διασφαλίσει ότι είναι συμμορφωμένο με όλες τις σχετικές νομικές, κανονιστικές και συμβατικές απαιτήσεις σχετικά με τη συλλογή, την αποθήκευση, την ανάκτηση και την καταστροφή των αρχείων. Ιδιαίτερη σχέση με αυτό έχει ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) της Ευρωπαϊκής Ένωσης και οι απαιτήσεις του σχετικά με την αποθήκευση και την επεξεργασία των προσωπικών δεδομένων.

Αυτός ο έλεγχος εφαρμόζεται σε όλα τα συστήματα, τους ανθρώπους και τις διεργασίες, που συγκροτούν τα πληροφοριακά συστήματα του φορέα.

### 7.1.1 Πολιτική Διατήρησης και Προστασίας Αρχείων

Αυτή η πολιτική ξεκινά με τον καθορισμό των βασικών αρχών, που πρέπει να υιοθετηθούν όταν εξετάζεται η διατήρηση και η προστασία των αρχείων. Έπειτα, ορίζει τους τύπους των αρχείων, που διατηρούνται από το Π.Μ.Σ. και τις γενικές απαιτήσεις τους πριν συζητηθεί η προστασία, η καταστροφή και η διαχείριση των αρχείων.

### 7.1.2 Γενικές Αρχές

Υπάρχει ένας αριθμός βασικών γενικών αρχών, που πρέπει να υιοθετηθούν όταν εξετάζεται η πολιτική διατήρησης και προστασίας αρχείων. Αυτές είναι:

- Τα αρχεία πρέπει να διατηρούνται σε συμμόρφωση με όλες τις εφαρμοσμένες νομικές, κανονιστικές και συμβατικές απαιτήσεις

- Τα αρχεία δεν πρέπει να διατηρούνται για περισσότερο χρόνο απ' όσο απαιτείται
- Η προστασία των αρχείων με όρους εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας πρέπει να είναι σύμφωνη με τη διαβάθμιση της ασφάλειας τους
- Τα αρχεία θα πρέπει να παραμένουν διαθέσιμα συνεχώς για ανάκτηση σύμφωνα με τις απαιτήσεις του φορέα
- Όπου ενδείκνυται, τα αρχεία, που περιέχουν προσωπικά δεδομένα θα πρέπει να υποβληθούν σε τεχνικές, που αποτρέπουν την ταυτοποίηση του φυσικού προσώπου το συντομότερο δυνατό

### 7.1.3 Τύποι Αρχείων και Κατευθυντήριες Γραμμές

Προκειμένου να διευκολυνθεί ο ορισμός των κατευθυντήριων γραμμών για τη διατήρηση και την προστασία των αρχείων, τα αρχεία, που κρατούνται από το Π.Μ.Σ. είναι χωρισμένα σε κατηγορίες, που παρατίθενται στον πίνακα της επόμενης σελίδας. Για κάθε μία από αυτές τις κατηγορίες, δίνεται επίσης η απαιτούμενη ή η προτεινόμενη περίοδος διατήρησης και τα επιτρεπόμενα μέσα αποθήκευσης, μαζί με το λόγο για τη σύσταση ή την απαίτηση.

Μπορεί να υπάρχουν ειδικές περιστάσεις, στις οποίες τα αρχεία χρειάζεται να διατηρηθούν για ένα μεγαλύτερο ή μικρότερο χρονικό διάστημα. Αυτό θα πρέπει να αποφασίζεται κατά περίπτωση, ως μέρος του σχεδιασμού των στοιχείων ασφάλειας των πληροφοριών από νέες ή σημαντικά μεταβαλλόμενες διαδικασίες και υπηρεσίες.

| **Κατηγορία Αρχείου** | **Περιγραφή** | **Περίοδος Διατήρησης** | **Λόγος για την Περίοδο Διατήρησης** | **Επιτρεπόμενα Μέσα Αποθήκευσης** |
|---|---|---|---|---|
| Λογιστικά | Τιμολόγια, παραγγελίες αγορών, λογαριασμοί και άλλα ιστορικά οικονομικά αρχεία | 10 χρόνια | Οικονομικοί και Εφοριακοί έλεγχοι | Ηλεκτρονικά/ Έντυπα |
| Προϋπολογισμοί και Προβλέψεις | Οικονομικές προβλέψεις και σχέδια | 10 χρόνια | Οικονομικοί και Εφοριακοί έλεγχοι | Ηλεκτρονικά/ Έντυπα |
| Αρχεία καταγραφής συναλλαγών συστήματος | Αρχεία καταγραφής που χρησιμοποιούνται για την ανάκτηση βάσεων δεδομένων | 2 χρόνια | Βασίζεται στη στρατηγική δημιουργίας αντιγράφων ασφαλείας και ανάκτησης | Ηλεκτρονικά /tape media |
| Λειτουργικές διαδικασίες | Εγγραφές που σχετίζονται με την ολοκλήρωση των λειτουργικών διαδικασιών | 2 χρόνια | Μέγιστο χρονικό διάστημα εντός του οποίου μπορεί να προκύψει διαφωνία | Ηλεκτρονικά/ Έντυπα |

| | | | | |
|---|---|---|---|---|
| Προμηθευτής | Ονόματα προμηθευτών, διευθύνσεις, στοιχεία του Φορέα | 10 χρόνια μετά το πέρας της προμήθειας | Μέγιστη περίοδος εντός της οποίας μπορεί να προκύψει διαφωνία | Ηλεκτρονικά /Έντυπα |
| Ανθρώπινοι Πόροι | Όνομα εργαζομένων, φοιτητές, διευθύνσεις, τραπεζικά στοιχεία, φορολογικοί κωδικοί, ιστορικό απασχόλησης ή και εκπαίδευσης | 20 χρόνια μετά το τέλος της απασχόλησης, εκπαίδευσης | Απαίτηση για την προστασία των δεδομένων, Εργατικό Δίκαιο | Ηλεκτρονικά /Έντυπα |
| Συμβόλαια | Νομικές συμβάσεις, όροι και προϋποθέσεις, μισθώσεις | 10 χρόνια μετά το πέρας του συμβολαίου | Μέγιστη περίοδος εντός της οποίας μπορεί να προκύψει διαφωνία | Ηλεκτρονικά/ Έντυπα |
| Άλλες κατηγορίες | | | | |

### 7.1.4 Χρήση της κρυπτογράφησης

Όπου ενδείκνυται για τη διαβάθμιση των πληροφοριών και του μέσου αποθήκευσης, πρέπει να χρησιμοποιούνται τεχνικές κρυπτογράφησης, προκειμένου να εξασφαλιστεί η εμπιστευτικότητα και η ακεραιότητα των αρχείων.

Πρέπει να ληφθεί μέριμνα, ώστε τα κλειδιά, που χρησιμοποιούνται για την κρυπτογράφηση των αρχείων να αποθηκεύονται με ασφάλεια κατά την περίοδο διατήρησης των σχετικών αρχείων και να είναι συμμορφωμένα με την πολιτική του φορέα για την κρυπτογράφηση.

### 7.1.5 Επιλογή των μέσων αποθήκευσης

Η επιλογή μακροπρόθεσμων μέσων αποθήκευσης πρέπει να λαμβάνει υπόψη τα φυσικά χαρακτηριστικά του μέσου και το χρονικό διάστημα που θα χρησιμοποιηθεί.

Όταν τα αρχεία πρέπει να αποθηκεύονται για νομικούς (ή πρακτικούς) λόγους σε έγγραφη μορφή, θα πρέπει να λαμβάνονται επαρκείς προφυλάξεις ώστε να εξασφαλίζεται ότι οι περιβαλλοντικές συνθήκες παραμένουν κατάλληλες για τον τύπο των χρησιμοποιούμενων εγγράφων. Όπου είναι δυνατόν, αντίγραφα ασφαλείας τέτοιων αρχείων πρέπει να λαμβάνονται με μεθόδους, όπως η σάρωση ή η δημιουργία μικροδιαφανειών. Πρέπει να γίνονται τακτικοί έλεγχοι για να εκτιμηθεί ο βαθμός αλλοίωσης των εγγράφων και η ανάληψη δράσης για τη διατήρηση των αρχείων, εφόσον απαιτείται.

Για τα αρχεία που είναι αποθηκευμένα σε ηλεκτρονικά μέσα, όπως κασέτες, πρέπει να λαμβάνονται παρόμοιες προφυλάξεις για να εξασφαλιστεί η μακροζωία των υλικών, συμπεριλαμβανομένης της σωστής αποθήκευσης και αντιγραφής σε πιο εύρωστα μέσα, εάν είναι απαραίτητο. Η δυνατότητα ανάγνωσης του περιεχομένου της συγκεκριμένης μορφής κασέτας (ή άλλης παρόμοιας μορφής) πρέπει να διατηρείται με τη χρήση μιας συσκευής ικανής να την επεξεργαστεί. Εάν αυτό δεν είναι πρακτικό, μπορεί να χρησιμοποιηθεί εξωτερικό τρίτο μέρος για τη μετατροπή των μέσων σε μια εναλλακτική μορφή.

### 7.1.6 Ανάκτηση εγγράφων

Δεν έχει νόημα η διατήρηση αρχείων εάν δεν είναι δυνατή η πρόσβασή σε αυτά, σύμφωνα με τις λειτουργίες του φορέα ή νομικές απαιτήσεις. Η επιλογή και η συντήρηση των εγκαταστάσεων αποθήκευσης αρχείων πρέπει να εξασφαλίζουν, ότι τα αρχεία μπορούν να ανακτηθούν σε χρήσιμη μορφή εντός αποδεκτής χρονικής περιόδου. Πρέπει να επιτευχθεί η κατάλληλη ισορροπία μεταξύ του κόστους αποθήκευσης και της ταχύτητας ανάκτησης, έτσι ώστε να καλύπτονται επαρκώς οι πιο πιθανές περιστάσεις.

### 7.1.7 Καταστροφή Αρχείων

Μόλις τα αρχεία φθάσουν στο τέλος της ζωής τους σύμφωνα με την καθορισμένη πολιτική, πρέπει να καταστραφούν με ασφάλεια, ώστε να μην μπορούν πλέον να χρησιμοποιηθούν. Η διαδικασία καταστροφής περιλαμβάνει την ορθή καταγραφή των λεπτομερειών της καταστροφής, οι οποίες πρέπει να διατηρούνται ως αποδεικτικά στοιχεία.

### 7.1.8 Ανασκόπηση εγγράφων

Η διατήρηση και η αποθήκευση των αρχείων πρέπει να υπόκεινται σε τακτική διαδικασία επανεξέτασης, η οποία θα εκτελείται υπό την καθοδήγηση της διοίκησης, ώστε να εξασφαλίζεται ότι:

- Η πολιτική διατήρησης και προστασίας αρχείων παραμένει έγκυρη
- Τα αρχεία διατηρούνται σύμφωνα με την πολιτική
- Τα αρχεία καταστρέφονται με ασφάλεια όταν δε χρειάζονται πλέον
- Πληρούνται οι νομικές, κανονιστικές και συμβατικές απαιτήσεις
- Οι διαδικασίες για την ανάκτηση εγγράφων ανταποκρίνονται στις απαιτήσεις του φορέα

Τα αποτελέσματα αυτών των ανασκοπήσεων πρέπει να καταγράφονται.

## 7.2 Πολιτική για την Ιδιωτικότητα και την προστασία των προσωπικών δεδομένων

### 7.2.1 Εισαγωγή

Στις καθημερινές του δραστηριότητες, το Π.Μ.Σ. χρησιμοποιεί μία πληθώρα δεδομένων, τα οποία αφορούν σε ταυτοποιημένα άτομα, συμπεριλαμβανομένων και δεδομένων, που σχετίζονται με:

- Παλιούς εργαζόμενους ή εξωτερικούς συνεργάτες με σύμβαση συνεργασίας
- Προμηθευτές
- Φοιτητές
- Χρήστες των ιστοσελίδων του Π.Μ.Σ.
- Άλλα ενδιαφερόμενα μέρη

Ο σκοπός της συγκεκριμένης πολιτικής είναι να περιγράψει τη σχετική νομοθεσία και να παρουσιάσει τα βήματα, που θα πρέπει να ακολουθεί το Π.Μ.Σ. για να εξασφαλίσει τη συμμόρφωσή του σε αυτή.

### 7.2.2 Ο Γενικός Κανονισμός Προστασίας Δεδομένων

Ο Γενικός Κανονισμός Προστασίας Δεδομένων 679/2016 (ΓΚΠΔ) είναι ένα από τα πιο σημαντικά κομμάτια της νομοθεσίας, που προσδιορίζει τον τρόπο με τον οποίο το Π.Μ.Σ. θα πρέπει να εκτελεί δραστηριότητες σχετικές με την επεξεργασία δεδομένων. Σε περίπτωση που υπάρξει παραβίαση του ΓΚΠΔ, ο οποίος είναι σχεδιασμένος για να προστατεύει τα δεδομένα προσωπικού χαρακτήρα όλων όσων βρίσκονται στην Ευρωπαϊκή Ένωση, είναι πιθανό να επιβληθούν σημαντικά πρόστιμα. Θα πρέπει να είναι πολιτική του Π.Μ.Σ . να εξασφαλίσει ότι η συμμόρφωσή με το ΓΚΠΔ και άλλες σχετικές νομοθεσίες είναι ξεκάθαρη και μπορεί να αποδειχτεί ανά πάσα στιγμή.

### 7.2.3 Ορισμοί

Στο ΓΚΠΔ εμπεριέχονται συνολικά 26 ορισμοί εκ των οποίων οι πιο βασικοί σχετικά με τη συγκεκριμένη πολιτική παρατίθενται παρακάτω:

*Τα δεδομένα Προσωπικού Χαρακτήρα ορίζονται ως:*

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

***Ως «επεξεργασία» ορίζεται:***

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

***«υπεύθυνος επεξεργασίας»* σημαίνει:**

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

### 7.2.4 Αρχές, που Διέπουν την Επεξεργασία των Δεδομένων Προσωπικού Χαρακτήρα

Υπάρχουν κάποιες βασικές αρχές στις οποίες στηρίζεται ο ΓΚΠΔ.

Αυτές παρατίθενται παρακάτω:

1. *Τα Δεδομένα Προσωπικού Χαρακτήρα πρέπει να :*

*(α) υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»),*

*(β) συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 («περιορισμός του σκοπού»),*

*(γ) είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»),*

*(δ) είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας («ακρίβεια»),*

*(ε) διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»),*

*(στ) υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).*

2. *Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 («λογοδοσία»).*

Το Π.Μ.Σ. πρέπει να διασφαλίσει, ότι συμμορφώνεται με όλες αυτές τις αρχές, τόσο στις τρέχουσες επεξεργασίες, όσο και κατά την εισαγωγή νέων μεθόδων επεξεργασίας, όπως νέων πληροφοριακών συστημάτων.

### 7.2.5 Ατομικά Δικαιώματα

Το υποκείμενο των δεδομένων έχει επίσης δικαιώματα, αναφορικά με το ΓΚΠΔ. Σε αυτά περιλαμβάνονται:

1. Το δικαίωμα της πληροφόρησης
2. Το δικαίωμα της πρόσβασης
3. Το δικαίωμα της διόρθωσης
4. Το δικαίωμα της διαγραφής
5. Το δικαίωμα του περιορισμού της επεξεργασίας
6. Το δικαίωμα της φορητότητας των δεδομένων
7. Το δικαίωμα της εναντίωσης
8. Δικαιώματα που σχετίζονται με την αυτοματοποιημένη λήψη αποφάσεων για το άτομο και την κατάρτιση προφίλ.

Κάθε ένα από τα δικαιώματα των φυσικών προσώπων θα πρέπει να υποστηρίζεται από κατάλληλες διαδικασίες του Π.Μ.Σ  Οι διαδικασίες αυτές εξασφαλίζουν ότι λαμβάνουν χώρα οι απαραίτητες ενέργειες στο πλαίσιο των χρονοδιαγραμμάτων, τα οποία υποδηλώνονται στο ΓΚΠΔ.

Αυτά τα χρονοδιαγράμματα παρουσιάζονται στον παρακάτω πίνακα.

| Αίτημα του Υποκειμένου των Δεδομένων | Χρονοδιάγραμμα |
|---|---|
| Το δικαίωμα της πληροφόρησης | Τη στιγμή που συλλέγονται τα δεδομένα (εφόσον συλλέγονται από το υποκείμενο των δεδομένων) ή μέσα σε ένα μήνα (εφόσον δε συλλέγονται από το υποκείμενο των δεδομένων) |
| Το δικαίωμα της πρόσβασης | Ένας μήνας |
| Το δικαίωμα της διόρθωσης | Ένας μήνας |
| Το δικαίωμα της διαγραφής | Χωρίς αναίτια καθυστέρηση |
| Το δικαίωμα του περιορισμού της επεξεργασίας | Χωρίς αναίτια καθυστέρηση |
| Το δικαίωμα της φορητότητας των δεδομένων | Ένας μήνας |
| Το δικαίωμα της εναντίωσης | Τη στιγμή λήψης μίας ένστασης |
| Δικαιώματα που σχετίζονται με την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ. | Δε διευκρινίζεται |

*Χρονοδιαγράμματα αιτημάτων των υποκειμένων δεδομένων*

### 7.2.6 Συγκατάθεση

Εκτός και αν είναι απαραίτητο για λόγους, που επιτρέπονται από το ΓΚΠΔ, πρέπει να ληφθεί σαφής συγκατάθεση από το υποκείμενο των δεδομένων για τη συλλογή και την επεξεργασία των δεδομένων του. Τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται για τα δικαιώματά τους –σε σχέση με τα προσωπικά δεδομένα τους- όπως για παράδειγμα το δικαίωμα της συγκατάθεσης, τη χρονική στιγμή, που λαμβάνεται η συγκατάθεσή τους. Οι

πληροφορίες, που αφορούν τα δικαιώματα των υποκειμένων των δεδομένων, πρέπει να είναι εύκολα προσβάσιμες, χωρίς χρέωση, και γραμμένες με σαφή τρόπο.

Εάν η συλλογή των προσωπικών δεδομένων δε γίνεται απευθείας από το υποκείμενο των δεδομένων, τότε αυτές οι πληροφορίες πρέπει να δίνονται σε ένα λογικό χρονικό διάστημα μετά την απόκτηση των δεδομένων και σίγουρα όχι αργότερα από το διάστημα ενός μήνα.

### 7.2.7 Προστασία των δεδομένων ήδη από το σχεδιασμό

Το Π.Μ.Σ θα πρέπει να υιοθετήσει την αρχή της προστασίας των δεδομένων ήδη από το σχεδιασμό και θα εξασφαλίσει ότι ο ορισμός και ο σχεδιασμός όλων των καινούριων ή των σημαντικά τροποποιημένων συστημάτων, που συλλέγουν ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα θα λάβουν τη δέουσα προσοχή σε ζητήματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων.

Η αξιολόγηση των επιπτώσεων στην προστασία των δεδομένων περιλαμβάνει:

- Τον τρόπο με τον οποίο τα δεδομένα προσωπικού χαρακτήρα τίθενται σε επεξεργασία και για ποιους σκοπούς
- Αξιολόγηση του κατά πόσο η προτεινόμενη επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι ταυτόχρονα απαραίτητη και ανάλογη του σκοπού (ή των σκοπών)
- Αξιολόγηση των κινδύνων στους οποίους εκτίθενται τα άτομα, λόγω της επεξεργασίας των προσωπικών τους δεδομένων
- Την επιλογή των απαραίτητων μέτρων, για την αντιμετώπιση των κινδύνων, που εντοπίστηκαν και αποδεικνύουν συμμόρφωση με τη νομοθεσία.

Η χρήση τεχνικών όπως η ελαχιστοποίηση των δεδομένων και η ψευδονυμοποίηση πρέπει να ληφθεί υπόψη, σε περιπτώσεις, που είναι κατάλληλη και δυνατή η εφαρμογή τους.

### 7.2.8 Διαβίβαση Δεδομένων Προσωπικού Χαρακτήρα

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα εκτός της Ευρωπαϊκής Ένωσης πρέπει να εξετάζεται προσεκτικά και πριν η διαβίβαση λάβει χώρα, προκειμένου να εξασφαλιστεί ότι γίνεται σύμφωνα με το πλαίσιο, που έχει οριστεί από το ΓΚΠΔ. Αυτό εξαρτάται εν μέρει από την κρίση της Ευρωπαϊκής Επιτροπής, καθώς και από την επάρκεια της ασφάλειας, που

εφαρμόζεται σχετικά με τα δεδομένα προσωπικού χαρακτήρα στη χώρα, που θα δεχτεί τα δεδομένα, και μπορεί να μεταβληθεί σε βάθος χρόνου.

Οι διεθνείς μεταφορές δεδομένων εντός οργανισμών πρέπει να υποβάλλονται σε νομικά δεσμευτικές συμφωνίες, που παρέχουν δικαιώματα στα υποκείμενα των δεδομένων.

### 7.2.9 Υπεύθυνος Προστασίας Δεδομένων

Στα πλαίσια του ΓΚΠΔ απαιτείται η ανάδειξη Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ), σε περίπτωση που ο οργανισμός είναι δημόσια αρχή, εκτελεί επεξεργασίες μεγάλης κλίμακας ή επεξεργάζεται ιδιαίτερα ευαίσθητες κατηγορίες δεδομένων σε μεγάλη κλίμακα. Ο ΥΠΔ πρέπει να κατέχει το κατάλληλο επίπεδο γνώσεων και μπορεί να προέρχεται είτε από τον ίδιο τον οργανισμό είτε να είναι εξωτερικός συνεργάτης.

Με βάση αυτά τα κριτήρια, θεωρούμε ότι είναι απαραίτητος ο ορισμός Υπευθύνου Προστασίας Δεδομένων στο Π.Μ.Σ.

### 7.2.10 Ειδοποίηση Παραβίασης

Θα πρέπει να αποτελεί πολιτική του Π.Μ.Σ. να ενημερώνει όλους όσους απαιτείται, σε περίπτωση παραβίασης, που αφορά προσωπικά δεδομένα, με δίκαιο και ανάλογο τρόπο. Σε ευθυγράμμιση με το ΓΚΠΔ, όταν γίνεται γνωστό ότι έλαβε χώρα μία παραβίαση, η οποία είναι πιθανό να έχει ως αποτέλεσμα τη διακύβευση των δικαιωμάτων και των ελευθεριών των ατόμων, θα ενημερωθεί η Αρχή Προστασία Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) εντός 72 ωρών. Αυτό θα γίνει σύμφωνα με τη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας Πληροφοριών του Π.Μ.Σ**.**

Υπό το ΓΚΠΔ, η αντίστοιχη ΑΠΔΠΧ έχει την εξουσιοδότηση να επιβάλει ένα εύρος προστίμων έως το 4 τοις εκατό του ετήσιου παγκόσμιου κύκλου εργασιών ή τα είκοσι εκατομμύρια ευρώ, όποιο από τα δύο είναι μεγαλύτερο, για παραβίαση του Κανονισμού.

### 7.2.11 Εφαρμογή της Συμμόρφωσης προς το ΓΚΠΔ

Οι παρακάτω ενέργειες θα πρέπει να γίνουν προκειμένου να εξασφαλιστεί ότι, το Π.Μ.Σ. συμμορφώνεται σε κάθε περίπτωση με την αρχή της λογοδοσίας του ΓΚΠΔ:

- Η νόμιμη βάση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα είναι ξεκάθαρη και αδιαμφισβήτητη.

- Ορίζεται Υπεύθυνος Προστασίας Δεδομένων με αρμοδιότητα την προστασία των δεδομένων εντός του οργανισμού.
- Όλο το προσωπικό, που εμπλέκεται στη διαχείριση των προσωπικών δεδομένων, αντιλαμβάνεται τις ευθύνες του, και ακολουθεί τις βέλτιστες πρακτικές προστασίας δεδομένων.
- Όλο το προσωπικό έχει εκπαιδευτεί στην προστασία των δεδομένων.
- Τηρούνται οι υποχρεώσεις σχετικά με τη συγκατάθεση.
- Υπάρχουν διαθέσιμες οδοί, μέσω των οποίων τα υποκείμενα δεδομένων, που επιθυμούν να ασκήσουν τα δικαιώματα τους σχετικά με τα προσωπικά τους δεδομένα έχουν αυτή τη δυνατότητα.
- Διεξάγονται τακτικά ανασκοπήσεις των διαδικασιών, που αφορούν προσωπικά δεδομένα.
- Η προστασία των δεδομένων ήδη από το σχεδιασμό υιοθετείται για όλα τα νέα συστήματα και διαδικασίες ή σε σημαντικές αλλαγές των υπαρχόντων.
- Στο έγγραφο, όπου περιγράφονται οι ενέργειες, που λαμβάνουν χώρα σε μία επεξεργασία καταγράφεται:
    - Το όνομα του οργανισμού και οι σχετικές λεπτομέρειες
    - Οι σκοποί της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα
    - Οι κατηγορίες των ατόμων και των δεδομένων προσωπικού χαρακτήρα, που είναι υπό επεξεργασία
    - Οι κατηγορίες των παραληπτών των προσωπικών δεδομένων
    - Οι συμφωνίες και οι μηχανισμοί, βάσει των οποίων γίνονται οι μεταφορές των προσωπικών δεδομένων σε χώρες εκτός της Ευρωπαϊκής Ένωσης, συμπεριλαμβανομένων και λεπτομερειών για τα μέτρα που ελήφθησαν
    - Χρόνος διατήρησης των προσωπικών δεδομένων
    - Τα κατάλληλα τεχνικά και οργανωτικά μέτρα, που έχουν υλοποιηθεί.

Αυτές οι ενέργειες θα επιθεωρούνται σε τακτική βάση, ως κομμάτι της διαδικασίας επιθεώρησης διαχείρισης του Προγράμματος Προστασίας Προσωπικών Δεδομένων.

## 7.3 Διαδικασία της ενημέρωσης των υποκειμένων των δεδομένων.

### 7.3.1 Εισαγωγή

Στο παρακάτω κείμενο γίνεται αναφορά στις διαδικασίες που θα πρέπει να ακολουθηθούν προκειμένου να υπάρχει συμμόρφωση με το *Άρθρο 13 ( Πληροφορίες που πρέπει να παρέχονται όταν συλλέγονται προσωπικά δεδομένα από το υποκείμενο των δεδομένων) και το Άρθρο 14 ( Πληροφορίες που πρέπει να παρέχονται όταν τα προσωπικά δεδομένα δεν έχουν ληφθεί από το υποκείμενο των δεδομένων)*

Αυτή η διαδικασία θα χρησιμοποιηθεί, όταν πρόκειται να εφαρμοστεί μια νέα ή τροποποιημένη διαδικασία στο Π.Μ.Σ., η οποία απαιτεί τη συλλογή προσωπικών δεδομένων από τα υποκείμενα των δεδομένων, τα οποία εντάσσονται στο πλαίσιο του Γενικού Κανονισμού Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης.

Ο ΓΚΠΔ, κυρίως στα άρθρα 13 και 14, προϋποθέτει ότι θα δίνονται σαφείς πληροφορίες κατά τη συλλογή ή την παραλαβή των δεδομένων, με σκοπό την ενημέρωση του υποκειμένου των δεδομένων για το πώς θα χρησιμοποιηθούν τα δεδομένα, καθώς και για τα δικαιώματά του σε σχέση με αυτά. Αυτές οι πληροφορίες θα διαφέρουν ανάλογα με την περίσταση και αυτή η διαδικασία θα πρέπει να χρησιμοποιείται για να εξασφαλίζει, ότι δίνονται οι σωστές πληροφορίες, στη σωστή μορφή, έτσι ώστε ο φορέας να παραμένει συνεχώς συμμορφωμένο με το ΓΚΠΔ.

### 7.3.2 Διαδικασία Ενημέρωσης των Υποκειμένων των Δεδομένων

Υπάρχουν δύο κύριοι τρόποι απόκτησης προσωπικών δεδομένων, που καλύπτονται από το ΓΚΠΔ. Αυτοί είναι:

1. Όταν τα προσωπικά δεδομένα συλλέγονται από το υποκείμενο των δεδομένων *(ΓΚΠΔ Άρθρο 13)*
2. Όταν τα προσωπικά δεδομένα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων *(ΓΚΠΔ Άρθρο 14)*

Και στις δύο περιπτώσεις, ο ΓΚΠΔ καταγράφει τις πληροφορίες, που πρέπει να παρέχονται στο υποκείμενο των δεδομένων.

### 7.3.2.1 Το υποκείμενο των δεδομένων διαθέτει ήδη τις πληροφορίες;

Ο ΓΚΠΔ απαιτεί να δοθούν στο φυσικό πρόσωπο οι καταγεγραμμένες πληροφορίες ***εκτός αν το πρόσωπο αυτό τις έχει ήδη***. Είναι σημαντικό επομένως, να καθοριστεί αν είναι λογικό ή όχι να θεωρηθεί ότι το φυσικό πρόσωπο γνωρίζει ήδη όλες τις πληροφορίες, που σε άλλη περίπτωση θα έπρεπε να του δοθούν.

Αν θεωρηθεί ότι το φυσικό πρόσωπο γνωρίζει ήδη τις πληροφορίες, που έχουν συλλεχθεί γι' αυτό, τότε θα πρέπει να καταγραφούν τα λογικά βήματα, που οδήγησαν σε αυτό το συμπέρασμα ως απόδειξη της συμμόρφωσης με το ΓΚΠΔ. Πρέπει να δίνεται προσοχή ώστε να διασφαλίζεται, ότι αυτό ισχύει για **όλες** τις απαιτούμενες πληροφορίες και **όλα** τα εμπλεκόμενα υποκείμενα των δεδομένων. Σε άλλη περίπτωση θα πρέπει να γίνουν ενέργειες για να αντιμετωπιστούν τυχόν κενά.

### 7.3.2.2 Όταν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων

Σε περίπτωση, που το υποκείμενο των δεδομένων δεν έχει τις απαιτούμενες πληροφορίες, τη στιγμή που αποκτούνται τα προσωπικά του δεδομένα, θα πρέπει να του παρέχονται τα παρακάτω:

1. Η ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και κατά περίπτωση του εκπροσώπου του υπευθύνου επεξεργασίας.
2. Τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων
3. Οι σκοποί και η νόμιμη βάση της επεξεργασίας
4. Τα έννομα συμφέροντα, που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή κάποιο τρίτο μέρος
5. Τους αποδέκτες ή τις κατηγορίες αποδεκτών των προσωπικών δεδομένων, εάν υπάρχουν
6. Λεπτομέρειες για οποιαδήποτε σχέδια διαβίβασης των προσωπικών δεδομένων σε τρίτη χώρα ή διεθνή οργανισμό
7. Το χρονικό όριο διατήρησης των προσωπικών δεδομένων (ή τα κριτήρια που καθορίζουν το εν λόγω χρονικό διάστημα)

8. Το δικαίωμα του υποκειμένου των δεδομένων για πρόσβαση, διόρθωση, διαγραφή και φορητότητα των προσωπικών του δεδομένων.

9. Το δικαίωμα του υποκειμένου των δεδομένων για περιορισμό ή εναντίωση στην επεξεργασία των προσωπικών του δεδομένων

10. Το δικαίωμα του υποκειμένου των δεδομένων να ανακαλέσει τη συγκατάθεσή του οποιαδήποτε στιγμή

11. Το δικαίωμα του υποκειμένου των δεδομένων να υποβάλλει καταγγελία σε εποπτική αρχή

12. Κατά πόσο η συλλογή των προσωπικών δεδομένων αποτελεί νομική υποχρέωση ή απαίτηση από τη σύναψη κάποιας σύμβασης, καθώς και κατά πόσο το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα

13. Κατά πόσο υπάρχει αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης και της κατάρτισης προφίλ (profiling) και στις περιπτώσεις αυτές, τη λογική που ακολουθείται και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας.

### 7.3.2.3. Όταν τα προσωπικά δεδομένα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων

Αν τα προσωπικά δεδομένα δεν έχουν συλλεγεί απευθείας από το υποκείμενο των δεδομένων, υπάρχει ένα πλήθος επιπλέον περιπτώσεων (επιπρόσθετα της περίπτωσης που το φυσικό πρόσωπο διαθέτει ήδη τις πληροφορίες) τις οποίες επιτρέπει ο ΓΚΠΔ, οπότε δεν χρειάζεται να παρέχονται επιπλέον πληροφορίες. Αυτές είναι:

- Εάν η παροχή τέτοιων πληροφοριών αποδεικνύεται αδύνατη ή συνεπάγεται δυσανάλογη προσπάθεια

- Εάν υπάρχει κάλυψη από άλλη ισχύουσα νομοθεσία που παρέχει τα κατάλληλα μέτρα για την προστασία των έννομων συμφερόντων του υποκειμένου των δεδομένων *(ΓΚΠΔ Άρθρο 14)*

- Εάν τα δεδομένα είναι εμπιστευτικά λόγω νομικής υποχρέωσης

Σε τέτοιες περιπτώσεις, η λογική που οδήγησε σε αυτή τη θεώρηση πρέπει να καταγραφεί και να τεκμηριωθεί ως απόδειξη της συμμόρφωσης με το ΓΚΠΔ. Πρέπει να δίνεται προσοχή ώστε να διασφαλίζεται ότι αυτό ισχύει για **όλες** τις απαιτούμενες πληροφορίες και **όλα** τα εμπλεκόμενα φυσικά πρόσωπα. Σε άλλη περίπτωση θα πρέπει να γίνουν ενέργειες για να αντιμετωπιστούν τυχόν κενά.

Εάν δεν ισχύει καμία από τις παραπάνω περιπτώσεις, οι πληροφορίες πρέπει να παρέχονται στο φυσικό πρόσωπο:

- εντός εύλογου χρονικού διαστήματος και το αργότερο εντός ενός μήνα από τη συλλογή των προσωπικών δεδομένων.
- εάν τα δεδομένα χρησιμοποιηθούν για επικοινωνία (π.χ. διευθύνσεις email), το αργότερο κατά την πρώτη επικοινωνία
- όταν τα προσωπικά δεδομένα γνωστοποιούνται σε άλλον αποδέκτη (εφόσον προβλέπεται)

Οι πληροφορίες που πρέπει να παρέχονται είναι οι ακόλουθες:

1. Η ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και κατά περίπτωση του εκπροσώπου του υπευθύνου επεξεργασίας.
2. Τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων
3. Οι σκοποί και η νόμιμη βάση της επεξεργασίας
4. Οι σχετικές κατηγορίες προσωπικών δεδομένων
5. Τους αποδέκτες ή τις κατηγορίες αποδεκτών των προσωπικών δεδομένων, εάν υπάρχουν
6. Λεπτομέρειες για οποιαδήποτε σχέδια διαβίβασης των προσωπικών δεδομένων σε τρίτη χώρα ή διεθνή οργανισμό
7. Το χρονικό όριο διατήρησης των προσωπικών δεδομένων (ή τα κριτήρια που καθορίζουν το εν λόγω χρονικό διάστημα)
8. Το δικαίωμα του υποκειμένου των δεδομένων για πρόσβαση, διόρθωση, διαγραφή και φορητότητα των προσωπικών του δεδομένων.

9. Το δικαίωμα του υποκειμένου των δεδομένων για περιορισμό ή εναντίωση στην επεξεργασία των προσωπικών του δεδομένων

10. Το δικαίωμα του υποκειμένου των δεδομένων να ανακαλέσει τη συγκατάθεσή του οποιαδήποτε στιγμή

11. Το δικαίωμα του υποκειμένου των δεδομένων να υποβάλλει καταγγελία σε εποπτική αρχή

12. Την πηγή από την οποία προέρχονται τα προσωπικά δεδομένα

13. Κατά πόσο υπάρχει αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης και της κατάρτισης προφίλ (profiling) και στις περιπτώσεις αυτές, τη λογική που ακολουθείται και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας

### 7.3.2.4 Ενημέρωση του Υποκειμένου των Δεδομένων

Όπως όλες οι πληροφορίες που παρέχονται στα υποκείμενα των δεδομένων σύμφωνα με το ΓΚΠΔ, αυτές οι πληροφορίες θα πρέπει να είναι σε κατανοητή και προσβάσιμη μορφή και να είναι γραμμένες σε καθαρή και απλή γλώσσα. Η καλύτερη μέθοδος παροχής των πληροφοριών στο υποκείμενο των δεδομένων εξαρτάται από τις ιδιαιτερότητες των διαδικασιών του Π.Μ.Σ. και μπορεί να είναι μία ή περισσότερες από τις εξής:

- Ως γνωστοποίηση στην ιστοσελίδα
- Μέσω ηλεκτρονικού ταχυδρομείου
- Μέσω φυσικού ταχυδρομείου
- Μέσω τηλεφωνικής επικοινωνίας

Με όποιον τρόπο και αν αποκτηθούν οι πληροφορίες, σε περίπτωση που αποφασιστεί η χρήση των προσωπικών δεδομένων για σκοπό διαφορετικό από εκείνον για τον οποίο τα δεδομένα αποκτήθηκαν ή συλλέχθηκαν, θα πρέπει να δοθεί στο υποκείμενο των δεδομένων περαιτέρω πληροφόρηση για τον εν λόγω σκοπό, πριν λάβει χώρα η επεξεργασία.

## 7.4 Φόρμα σχεδιασμού για την ενημέρωση των υποκειμένων των δεδομένων

Αυτή η φόρμα θα χρησιμοποιηθεί, σύμφωνα με το ΓΚΠΔ, ως μέρος του σχεδιασμού για την Ενημέρωση των Υποκειμένων των Δεδομένων στην περίπτωση νέων ή τροποποιημένων συστημάτων.

**Λεπτομέρειες Απαιτήσεων**

| | |
|---|---|
| **Τίτλος του εγγράφου Ενημέρωσης των Υποκειμένων των Δεδομένων:** | |
| **Ημερομηνία συμπλήρωσης της φόρμας:** | |
| **Όνομα του ατόμου που συμπλήρωσε τη φόρμα:** | |
| **Σύντομη περιγραφή της απαίτησης:** | |
| **Περίπτωση Α – Τα προσωπικά δεδομένα** | |

| | |
|---|---|
| **θα συλλεχθούν από το υποκείμενο των δεδομένων:** | Ναι / Όχι |
| **Περίπτωση Β – Τα προσωπικά δεδομένα θα αποκτηθούν από πηγή διαφορετική από το υποκείμενο των δεδομένων:** | Ναι / Όχι |

**Πληροφορίες που πρέπει να παρασχεθούν**

1. Λεπτομέρειες επικοινωνίας του υπεύθυνου της επεξεργασίας και όπου μπορεί να εφαρμοστεί, του νόμιμου εκπρόσωπου του υπεύθυνου επεξεργασίας
2. Λεπτομέρειες επικοινωνίας του Υπεύθυνου Προστασίας Δεδομένων
3. Οι σκοποί και η νόμιμη βάση της επεξεργασίας
4. Τα έννομα συμφέροντα που έχει ο υπεύθυνος επεξεργασίας, ή ένα τρίτο μέρος (Μόνο στην περίπτωση Α)
5. Οι κατηγορίες των προσωπικών δεδομένων (Μόνο στην περίπτωση Β)
6. Οι παραλήπτες ή οι κατηγορίες των παραληπτών των δεδομένων, εφόσον υπάρχουν
7. Λεπτομέρειες για προγραμματισμένες μεταφορές προσωπικών δεδομένων σε τρίτη χώρα ή διεθνή οργανισμό
8. Χρονικό διάστημα διατήρησης των προσωπικών δεδομένων (ή τα κριτήρια που χρησιμοποιούνται για να προσδιορίσουν αυτή την περίοδο)
9. Περιγραφή των δικαιωμάτων του υποκειμένου των δεδομένων στην πρόσβαση, τη διόρθωση, τη διαγραφή και τη φορητότητα των προσωπικών του δεδομένων

10. Περιγραφή των δικαιωμάτων του υποκειμένου των δεδομένων στον περιορισμό ή στην αντίρρηση στην επεξεργασία των προσωπικών δεδομένων του

11. Περιγραφή των δικαιωμάτων του υποκειμένου των δεδομένων για την ανάκληση της συγκατάθεσης οποιαδήποτε στιγμή

12. Λεπτομέρειες για το δικαίωμα του υποκειμένου των δεδομένων να υποβάλλει καταγγελία σε μία εποπτική αρχή

13. Εάν τα προσωπικά δεδομένα απαιτούνται από κάποια νομοθεσία ή συμβόλαιο και υπάρχει υποχρέωση για την παροχή τους (Μόνο στην περίπτωση Α)

14. Την πηγή των προσωπικών δεδομένων (Μόνο στην περίπτωση Β)

15. Δηλώστε εάν τα προσωπικά δεδομένα θα χρησιμοποιηθούν για αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης και της κατάρτισης προφίλ. Αν ναι περιγράψτε τη λογική και τις πιθανές συνέπειες που αυτό συνεπάγεται

Μόλις συμπληρωθεί αυτή η φόρμα, τα περιεχόμενά της θα πρέπει να χρησιμοποιηθούν για να τη δημιουργία ενός κατάλληλο εγγράφου Ενημέρωσης του Υποκειμένου των Δεδομένων, η οποία θα κοινοποιηθεί στα σχετικά υποκείμενα των δεδομένων.

## 7.5 Επιπλέον ενέργειες διασφάλισης της Ιδιωτικότητας.

Προκείμενου να διασφαλίσουμε την Ιδιωτικότητα και στις περιπτώσεις αποστολής εγγράφων με το ηλεκτρονικό ταχυδρομείο (emails), θα μπορούσε να αναγράφεται αυστηρά σε κάθε επικοινωνία μας το παρακάτω μήνυμα:

«Η επικοινωνία αυτή είναι εμπιστευτική και ενδεχομένως να προστατεύεται από νομικά πλαίσια. Εάν λάβατε αυτό το e-mail, ενώ δεν προορίζεται για εσάς, σας ενημερώνουμε ότι απαγορεύεται οποιαδήποτε διανομή, αντιγραφή ή χρήση της επικοινωνίας ή/ και των πληροφοριών που περιέχονται σε αυτό. Σας παρακαλούμε να ενημερώσετε κατάλληλα τον αποστολέα και να σβήσετε ή να καταστρέψετε τυχόν αντίγραφά της.

Οι επικοινωνίες μέσω του Διαδικτύου δεν είναι ασφαλείς και για τον λόγο αυτό το Π.Μ.Σ δεν αποδέχεται νομική ευθύνη για τα περιεχόμενα του παρόντος μηνύματος και για οποιαδήποτε ζημιά προκληθεί από ιούς που είναι δυνατόν να εισαγάγει.»

“This communication is confidential and It may also be protected by legal rules. If you are not an intended recipient please note that any form of distribution, copying or use of this communication or the information in it, is prohibited. Please inform the sender appropriately and delete or destroy any copies of it from your system.

Internet communications are not secure and therefore the MSc does not accept legal responsibility for the contents of this message and for any damage whatsoever that is caused by viruses being passed”

# ΚΕΦΑΛΑΙΟ 8: ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ

## 8.1 Διαδικασία υποβολής αιτημάτων από το Υποκείμενο των Δεδομένων

Αυτή η διαδικασία έχει θεσπιστεί προκειμένου να υπάρχει συμμόρφωση με το Άρθρο 7 (Προϋποθέσεις για συγκατάθεση) και το Κεφάλαιο ΙΙΙ ( Δικαιώματά του υποκειμένου των δεδομένων). Έχει ως στόχο να χρησιμοποιηθεί όταν ένα υποκείμενο των δεδομένων ασκήσει ένα ή περισσότερα από τα δικαιώματα, που του παραχωρούνται μέσω του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) της ΕΕ.

Κάθε ένα από τα δικαιώματα, που εμπλέκονται έχει τις δικές του ειδικές πτυχές και προκλήσεις για το Π.Μ.Σ, ως προς τη συμμόρφωση με αυτά, τηρώντας ταυτόχρονα τα απαιτούμενα χρονοδιαγράμματα. Σε γενικές γραμμές, θα υιοθετηθεί μια προορατική προσέγγιση, που θα δίνει όσο το δυνατόν μεγαλύτερη δυνατότητα ελέγχου στα προσωπικά δεδομένα από το υποκείμενο των δεδομένων, με ελάχιστο ποσοστό παρέμβασης ή συμμετοχής από την πλευρά του Π.Μ.Σ. Αυτό μπορεί να επιτευχθεί με την παροχή ηλεκτρονικής πρόσβασης στα προσωπικά δεδομένα, έτσι ώστε το υποκείμενο των δεδομένων να μπορεί να τα ελέγξει και να τα τροποποιήσει όπως απαιτείται.

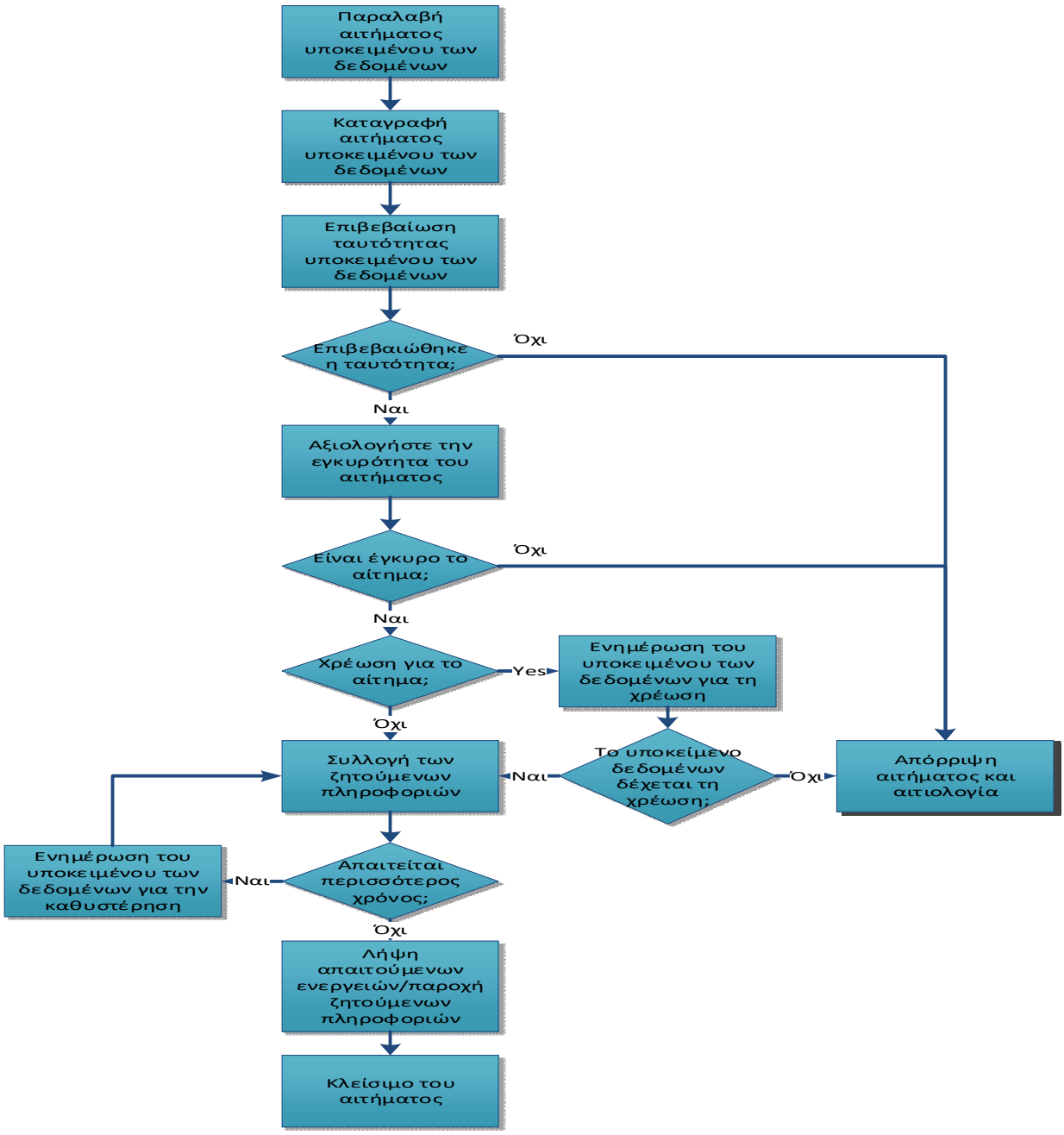
Τα παρακάτω γενικά σημεία εφαρμόζονται σε όλα τα αιτήματα που περιγράφονται σε αυτό το έγγραφο και βασίζονται στο *Άρθρο 12* του ΓΚΠΔ:

1. Οι πληροφορίες θα πρέπει να παρέχονται στο υποκείμενο των δεδομένων σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη ειδικά σε παιδιά
2. Οι πληροφορίες παρέχονται γραπτώς, ηλεκτρονικώς ή με άλλα μέσα
3. Το υποκείμενο των δεδομένων μπορεί να ζητήσει τις πληροφορίες προφορικά (π.χ. μέσω τηλεφώνου ή πρόσωπο με πρόσωπο), υπό την προϋπόθεση ότι η ταυτότητα του υποκειμένου των δεδομένων είναι αποδεδειγμένη
4. Θα πρέπει να ενεργήσουμε κατόπιν αιτήματος του υποκειμένου των δεδομένων εκτός αν δεν είμαστε σε θέση να εξακριβώσουμε την ταυτότητα του υποκειμένου των δεδομένων
5. Θα πρέπει να παρέχουμε τις πληροφορίες χωρίς αναίτια καθυστέρηση και σε κάθε περίπτωση εντός ενός μήνα από την παραλαβή του αιτήματος

6. Η εν λόγω προθεσμία μπορεί να παραταθεί κατά δύο ακόμη μήνες για πολύπλοκα αιτήματα ή σε περίπτωση υψηλού αριθμού αιτημάτων – το υποκείμενο των δεδομένων θα πρέπει να ενημερώνεται για την εν λόγω παράταση εντός ενός μήνα από την παραλαβή του αιτήματος, καθώς και για τους λόγους της καθυστέρησης
7. Εάν το υποκείμενο των δεδομένων υποβάλλει το αίτημα με ηλεκτρονικά μέσα, η ενημέρωση παρέχεται, εάν είναι δυνατόν, με ηλεκτρονικά μέσα, εκτός εάν το υποκείμενο των δεδομένων ζητήσει κάτι διαφορετικό
8. Αν αποφασιστεί να μην ενεργήσουμε επί κάποιου αιτήματος, θα πρέπει να ενημερωθεί το υποκείμενο των δεδομένων, χωρίς καθυστέρηση και το αργότερο εντός ενός μήνα από την παραλαβή του αιτήματος, δηλώνοντας τους λόγους για τους οποίους δεν ενηργήσαμε και ενημερώνοντας το υποκείμενο των δεδομένων για τη δυνατότητα υποβολής καταγγελίας σε εποπτική αρχή
9. Γενικά, όλες οι απαντήσεις στα αιτήματα θα παρέχονται δωρεάν, εκτός αν τα αιτήματα είναι «*προδήλως αβάσιμα ή υπερβολικά*» *(ΓΚΠΔ Άρθρο 12)*, όπου είτε θα επιβάλουμε την καταβολή εύλογου τέλους είτε θα αρνηθούμε να δώσουμε συνέχεια στο αίτημα.
10. Εάν υπάρχουν εύλογες αμφιβολίες σχετικά με την ταυτότητα του υποκειμένου των δεδομένων που υποβάλλει το αίτημα μπορεί να ζητηθεί η παροχή πρόσθετων πληροφοριών αναγκαίων για την επιβεβαίωση της ταυτότητας του υποκειμένου των δεδομένων

Η διαδικασία για την ανταπόκριση στα αιτήματα των υποκειμένων των δεδομένων παρατίθεται στο Σχήμα 1 και επεκτείνεται στον πίνακα που ακολουθεί. Οι ιδιαιτερότητες κάθε σταδίου της διαδικασίας ποικίλλουν ανάλογα με τον τύπο του αιτήματος

*8.1.1 Διάγραμμα Διαδικασίας*




*Διάγραμμα διαδικασίας αιτήματος του υποκειμένου των δεδομένων*

### 8.1.2 Βήματα Διαδικασίας

Τα βήματα που απεικονίζονται στο διάγραμμα ροής επεκτείνονται στον παρακάτω πίνακα και περαιτέρω στην ενότητα που αναφέρεται σε κάθε τύπο αιτήματος.

| **Βήμα** | **Περιγραφή** | **Άτομο** |
|---|---|---|
| Λήψη αιτήματος του υποκειμένου των δεδομένων | Το υποκείμενο των δεδομένων υποβάλλει αίτημα μέσω μιας από τις πολλές μεθόδους, συμπεριλαμβανομένης της ηλεκτρονικής (μέσω ηλεκτρονικού ταχυδρομείου ή μέσω της ιστοσελίδας μας), με επιστολή ή μέσω τηλεφώνου. Αυτό μπορεί να ληφθεί από οποιοδήποτε μέρος του οργανισμού, αλλά θα πρέπει ιδανικά να διευθετείται μέσω της εξυπηρέτησης πολιτών ή μέσω του Υπεύθυνου Προστασίας Δεδομένων. Μία *Φόρμα Υποβολής Αιτήματος από το Υποκείμενο των Δεδομένων* είναι διαθέσιμη για αυτό το σκοπό. | Κέντρο Εξυπηρέτησης Πολιτών, Υπεύθυνος Προστασίας Δεδομένων |
| Καταγραφή αιτήματος του υποκειμένου των δεδομένων | Το γεγονός ότι το αίτημα έχει ληφθεί καταχωρείται στο *Αρχείο Αιτημάτων των Υποκειμένων των Δεδομένων* και καταγράφεται η ημερομηνία του αιτήματος. | Υπεύθυνος Προστασίας Δεδομένων |
| Επιβεβαίωση ταυτότητας του υποκειμένου των δεδομένων | Η ταυτότητα του υποκειμένου των δεδομένων επιβεβαιώνεται με μία εγκεκριμένη μέθοδο. Περισσότερες πληροφορίες μπορεί να ζητηθούν για την επιβεβαίωση της ταυτότητας, εάν απαιτείται. Εάν δεν είναι δυνατόν να επιβεβαιωθεί η ταυτότητα του υποκειμένου των δεδομένων, το αίτημα απορρίπτεται και ο λόγος για τον οποίο απορρίφθηκε κοινοποιείται στο υποκείμενο των | Υπεύθυνος Προστασίας Δεδομένων |

| Βήμα | Περιγραφή | Άτομο |
|---|---|---|
| | δεδομένων. | |
| Αξιολόγηση της εγκυρότητας του αιτήματος | Ελέγχεται αν το αίτημα είναι «*προδήλως αβάσιμο ή υπερβολικό*». Αν ναι, αποφασίζεται εάν θα απορριφθεί το αίτημα ή θα επιβληθεί σχετική επιβάρυνση.<br><br>Σε περίπτωση αιτημάτων για διόρθωση, διαγραφή, περιορισμό ή εναντίωση για την επεξεργασία, λαμβάνεται επίσης απόφαση σχετικά με το αν το αίτημα είναι εύλογο και νόμιμο. Εάν όχι, απορρίπτεται το αίτημα και ενημερώνεται το υποκείμενο των δεδομένων για την απόφαση και το δικαίωμά του να υποβάλει καταγγελία στην εποπτική αρχή. | Υπεύθυνος Προστασίας Δεδομένων |
| Χρέωση για το αίτημα | Εάν εφαρμόζεται χρέωση, το υποκείμενο των δεδομένων ενημερώνεται για την επιβάρυνση και έχει την ευκαιρία να αποφασίσει εάν θα συνεχίσει ή όχι. Εάν το υποκείμενο των δεδομένων αποφασίσει να μην προχωρήσει, το αίτημα απορρίπτεται και ο λόγος για τον οποίο απορρίφθηκε κοινοποιείται στο υποκείμενο των δεδομένων. | Υπεύθυνος Προστασίας Δεδομένων |
| Συλλογή απαιτούμενων πληροφοριών | Οι σχετικές πληροφορίες συλλέγονται ανάλογα με τον τύπο του αιτήματος. Αυτό μπορεί να περιλαμβάνει τον προγραμματισμό του τρόπου με τον οποίο θα εκπληρωθεί το αίτημα, π.χ. διαγραφή ή περιορισμός της επεξεργασίας. Παρέχεται κατ 'ανώτατο όριο ένας μήνας. Αν το αίτημα διαρκέσει περισσότερο από αυτό τότε επιτρέπονται κατ 'ανώτατο όριο δύο επιπλέον μήνες και το υποκείμενο των δεδομένων πρέπει να ενημερωθεί για την καθυστέρηση και τους λόγους αυτής εντός | Υπεύθυνος Προστασίας Δεδομένων |

| Βήμα | Περιγραφή | Άτομο |
|---|---|---|
| | ενός μήνα από την υποβολή του αιτήματος. | |
| Λήψη απαιτούμενων ενεργειών / παροχή απαιτούμενων πληροφοριών | Η ζητούμενη ενέργεια εκτελείται (κατά περίπτωση) και οι πληροφορίες που ζητούνται παρέχονται στο υποκείμενο των δεδομένων ηλεκτρονικά, εάν αυτή είναι η προτιμώμενη μέθοδος ή με άλλα μέσα. | Υπεύθυνος Προστασίας Δεδομένων |
| Κλείσιμο του αιτήματος του υποκειμένου των δεδομένων | Το γεγονός ότι το αίτημα έχει εκπληρωθεί καταχωρείται στο *Αρχείο Αιτημάτων των Υποκειμένων των Δεδομένων* μαζί με την ημερομηνία της εκπλήρωσης. | Υπεύθυνος Προστασίας Δεδομένων |

## 8.2 Το δικαίωμα άρσης συναίνεσης

Το υποκείμενο των δεδομένων έχει το δικαίωμα να αποσύρει τη συγκατάθεσή του όταν η βάση για την επεξεργασία των προσωπικών του δεδομένων είναι η συναίνεση (δηλαδή η επεξεργασία δε βασίζεται σε διαφορετική αιτιολόγηση που επιτρέπεται από το ΓΚΠΔ, όπως συμβατική ή νομική υποχρέωση).

Πριν από την εξαίρεση των προσωπικών δεδομένων του υποκειμένου των δεδομένων από την επεξεργασία, πρέπει να επιβεβαιωθεί ότι η συναίνεση είναι πράγματι η βάση της επεξεργασίας. Εάν όχι, τότε το αίτημα μπορεί να απορριφθεί με την αιτιολογία ότι η επεξεργασία δεν απαιτεί τη συγκατάθεση του υποκειμένου των δεδομένων. Διαφορετικά, θα πρέπει το αίτημα να γίνει δεκτό.

Σε πολλές περιπτώσεις, η παροχή και η απόσυρση της συγκατάθεσης θα είναι διαθέσιμη ηλεκτρονικά, δηλ. στο διαδίκτυο, και αυτή η διαδικασία δε θα απαιτείται.

## 8.3 Το δικαίωμα της ενημέρωσης

Στο σημείο όπου συλλέγονται δεδομένα προσωπικού χαρακτήρα από το υποκείμενο των δεδομένων ή προέρχονται από άλλη πηγή, απαιτείται η ενημέρωση του υποκειμένου των δεδομένων σχετικά με τη χρήση αυτών των δεδομένων και τα δικαιώματά τους έναντι αυτής.

## *8.4* Το δικαίωμα της πρόσβασης

Ένα υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από το Π.Μ.Σ εάν γίνεται επεξεργασία δεδομένων που το αφορούν, να έχει πρόσβαση σε αυτά τα δεδομένα και επιπλέον στις ακόλουθες πληροφορίες:

1. Τους σκοπούς της επεξεργασίας
2. Τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα
3. Τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινοποιήθηκαν ή πρόκειται να κοινοποιηθούν τα δεδομένα προσωπικού χαρακτήρα, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς
4. Το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα (ή τα κριτήρια που καθορίζουν το εν λόγω διάστημα)
5. Την ύπαρξη δικαιώματος υποβολής αιτήματος για διόρθωση ή διαγραφή ή περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που αφορά το υποκείμενο των δεδομένων ή δικαιώματος αντίρρησης στην εν λόγω επεξεργασία
6. Το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή
7. Όταν τα δεδομένα προσωπικού χαρακτήρα δε συλλέγονται από το υποκείμενο των δεδομένων, τις πληροφορίες σχετικά με την προέλευσή τους
8. Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.
9. Αν τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονται σε τρίτη χώρα ή σε διεθνή οργανισμό, το υποκείμενο των δεδομένων έχει το δικαίωμα να ενημερώνεται για τις κατάλληλες εγγυήσεις

Στις περισσότερες περιπτώσεις, η διαδικασία λήψης αποφάσεων για τέτοιου είδους αιτήματα θα είναι απλή, εκτός εάν κριθεί ότι το αίτημα είναι προδήλως αβάσιμο ή υπερβολικό.

## 8.5 Δικαίωμα διόρθωσης

Όταν τα δεδομένα προσωπικού χαρακτήρα είναι ανακριβή, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει τη διόρθωσή τους και να συμπληρώσει τα ατελή προσωπικά δεδομένα με βάση τις πληροφορίες που θα παράσχει.

Όπου είναι απαραίτητο, το Π.Μ.Σ θα λάβει μέτρα για την επιβεβαίωση των πληροφοριών που παρέχονται από το υποκείμενο των δεδομένων για να εξασφαλίσει ότι είναι ακριβή πριν την τροποποίησή τους.

## 8.6 Το δικαίωμα στη διαγραφή

Επίσης, γνωστό ως «το δικαίωμα στη λήθη», το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από το Π.Μ.Σ., να διαγράψει προσωπικά δεδομένα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση, όταν ισχύει ένα από τα ακόλουθα:

- Τα προσωπικά δεδομένα δεν είναι πλέον απαραίτητα για το σκοπό για τον οποίο συλλέχθηκαν
- Το υποκείμενο των δεδομένων αποσύρει τη συναίνεση και δεν υπάρχει άλλη νομική βάση για την επεξεργασία
- Το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία των προσωπικών δεδομένων
- Τα προσωπικά δεδομένα έχουν υποστεί επεξεργασία παράνομα

Πρέπει να καταβληθούν εύλογες προσπάθειες για τη διασφάλιση της διαγραφής, όταν τα προσωπικά δεδομένα έχουν δημοσιοποιηθεί.

Το Π.Μ.Σ. θα πρέπει να αποφασίσει για κάθε περίπτωση τέτοιων αιτημάτων σχετικά με το αν το αίτημα μπορεί ή πρέπει να απορριφθεί για έναν από τους ακόλουθους λόγους:

- Δικαίωμα ελευθερίας έκφρασης και ενημέρωσης
- Συμμόρφωση με νομική υποχρέωση
- Δημόσιο συμφέρον στον τομέα της δημόσιας υγείας
- Προστασία του αρχείου για λόγους δημοσίου συμφέροντος

- Τα προσωπικά δεδομένα σχετίζονται με μια νομική απαίτηση

Είναι πιθανό ότι τέτοιες αποφάσεις θα απαιτήσουν τη συμμετοχή του Υπεύθυνου Προστασίας Δεδομένων του Π.Μ.Σ. και σε μερικές περιπτώσεις της Ανώτατης Διοίκησης.

## *8.7* Το δικαίωμα στον περιορισμό της επεξεργασίας

Το υποκείμενο των δεδομένων μπορεί να ασκήσει το δικαίωμα για περιορισμό της επεξεργασίας των προσωπικών δεδομένων του σε μία από τις ακόλουθες περιπτώσεις:

- Όταν το υποκείμενο των δεδομένων αμφισβητεί την ακρίβεια των δεδομένων, μέχρι να μπορέσουμε να επαληθεύσουμε την ακρίβειά τους
- Ως εναλλακτική λύση στη διαγραφή σε περίπτωση που η επεξεργασία είναι παράνομη
- Όταν το υποκείμενο των δεδομένων χρειάζεται τα δεδομένα για νομικές αξιώσεις, αλλά αυτά πλέον δεν είναι απαραίτητα για εμάς
- Ενώ εκκρεμεί απόφαση σχετικά με ένσταση για επεξεργασία

Το Π.Μ.Σ. θα πρέπει να αποφασίσει για κάθε περίπτωση τέτοιων αιτημάτων σχετικά με το αν θα πρέπει να επιτραπεί το αίτημα. Είναι πιθανό ότι τέτοιες αποφάσεις θα απαιτήσουν τη συμμετοχή του Υπεύθυνου Προστασίας Δεδομένων του φορέα και σε μερικές περιπτώσεις της Ανώτατης Διοίκησης.

Όταν υπάρχει περιορισμός της επεξεργασίας, τα δεδομένα μπορούν να αποθηκεύονται αλλά να μην υποβάλλονται σε επεξεργασία χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων, εκτός εάν υπάρχουν νομικοί λόγοι (στην περίπτωση αυτή το πρόσωπο στο οποίο αναφέρονται τα δεδομένα πρέπει να ενημερωθεί). Άλλοι οργανισμοί που μπορούν να επεξεργάζονται τα δεδομένα για λογαριασμό μας πρέπει επίσης να ενημερώνονται για τον περιορισμό.

## 8.8 Το δικαίωμα στη φορητότητα των δεδομένων

Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει να του παρασχεθούν τα προσωπικά του δεδομένα *σε «δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο" (ΓΚΠΔ Άρθρο 20)* και για τη μεταφορά αυτών των δεδομένων σε άλλο μέρος, π.χ. πάροχος υπηρεσιών. Αυτό ισχύει για τα προσωπικά δεδομένα για τα οποία η επεξεργασία βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων και στην επεξεργασία που γίνεται με αυτοματοποιημένα μέσα.

Όπου αυτό είναι εφικτό, το υποκείμενο των δεδομένων μπορεί επίσης να ζητήσει να μεταφερθούν τα προσωπικά δεδομένα απευθείας από τα συστήματα του φορέα που ανήκουν σε εκείνα άλλου παρόχου.

## 8.9 Το Δικαίωμα εναντίωσης

Το υποκείμενο των δεδομένων έχει το δικαίωμα να αντιταχθεί σε επεξεργασία που βασίζεται στις ακόλουθες νομικές αιτιολογήσεις:

- Για την εκτέλεση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή για την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας
- Για τους σκοπούς των νόμιμων συμφερόντων του υπεύθυνου επεξεργασίας

Μόλις γίνει μία εναντίωση, το Π.Μ.Σ. πρέπει να αιτιολογήσει τους λόγους στους οποίους βασίζεται η επεξεργασία και να αναστείλει την επεξεργασία μέχρις ότου γίνει αυτό. Όπου τα προσωπικά δεδομένα χρησιμοποιούνται για άμεση εμπορική προώθηση, δεν έχουμε άλλη επιλογή παρά να μην επεξεργαζόμαστε πλέον τα δεδομένα.

# ΚΕΦΑΛΑΙΟ 9: ΥΠΕΥΘΥΝΟΙ ΚΑΙ ΕΚΤΕΛΟΥΝΤΕΣ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ

## 9.1 Διαδικασία αξιολόγησης των Προμηθευτών

Η παρακάτω διαδικασία καλύπτει τις απαιτήσεις του Άρθρου 6 (Νομιμότητα της επεξεργασίας) και του Άρθρου 35 (Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων) .

Η χρήση κατάλληλων, ασφαλών και αποτελεσματικών προμηθευτών είναι καθοριστικής σημασίας για τη συμμόρφωση του φορέα με το Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ). Οι προμηθευτές (εσωτερικοί και εξωτερικοί συνεργάτες του Π.Μ.Σ) χρησιμοποιούνται όχι μόνο για να βοηθήσουν στη λειτουργία ενός αποτελεσματικού οργανισμού αλλά σε πολλές περιπτώσεις έχουν άμεση επικοινωνία με τους φοιτητές.

Όμως, οι προμηθευτές πρέπει όχι μόνο να προσφέρουν άριστες υπηρεσίες, αλλά και να το κάνουν με έναν ασφαλή τρόπο, που δε θέτει σε κίνδυνο τα προσωπικά δεδομένα του φορέα και των φοιτητών του. Η διαδικασία αυτή αποσκοπεί στην εξασφάλιση επαρκών ενεργειών και στην ολοκλήρωση της έρευνας ώστε να καταλήξει σε εύλογη κρίση σχετικά με το κατά πόσον ένας προμηθευτής ανταποκρίνεται στις υποχρεώσεις του βάσει το ΓΚΠΔ.

## 9.2 Διαδικασία Αξιολόγησης των Προμηθευτών για το ΓΚΠΔ

### 9.2.1 Προ απαιτούμενα

Πριν ξεκινήσει η διαδικασία, πρέπει να υπάρχουν οι ακόλουθες προϋποθέσεις:

- Έχουν καθοριστεί απαιτήσεις για μια υπηρεσία
- Ο προμηθευτής θα αποθηκεύει ή ήδη αποθηκεύει και επεξεργάζεται τα προσωπικά δεδομένα των φοιτητών, των εργαζομένων ή άλλων ενδιαφερομένων μερών

### 9.2.2 Χρονοδιάγραμμα και προγραμματισμός

Αυτή η διαδικασία μπορεί να ξεκινήσει ανά πάσα στιγμή, αλλά είναι ιδιαίτερα σχετική με τις διαδικασίες χαρτογράφησης προσωπικών δεδομένων.

### 9.2.3 Διαδικασία

Η αξιολόγηση του προμηθευτή σε σχέση με το ΓΚΠΔ θα πρέπει να καταγράφεται χρησιμοποιώντας τη φόρμα Αξιολόγησης Προμηθευτή σύμφωνα με το ΓΚΠΔ και να διατηρείται ως απόδειξη της αξιολόγησης.

Η πρόοδος των αξιολογήσεων θα πρέπει να παρακολουθείται τουλάχιστον εβδομαδιαίως, ενώ βρίσκεται σε εξέλιξη η συνεργασία, παρ' όλα αυτά πολλές θα ολοκληρωθούν εντός ενός βραχύτερου χρονικού πλαισίου.

## 9.3 Δήλωση ετοιμότητας του φορέα με το ΓΚΠΔ

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) είναι ένας Κανονισμός της Ευρωπαϊκής Ένωσης και από τις 25 Μαΐου 2018 εφαρμόζεται σε όλους τους οργανισμούς που συλλέγουν και επεξεργάζονται προσωπικά δεδομένα πολιτών της ΕΕ.

Το Π.Μ.Σ «Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του Α.Τ.Ε.Ι.Θ , αναγνωρίζει την ανάγκη που υπάρχει για συμμόρφωση με το ΓΚΠΔ και για τη λήψη αποτελεσματικών μέτρων, που αφορούν την προστασία των προσωπικών δεδομένων των φοιτητών αλλά και των υπολοίπων συνεργαζόμενων μερών (των εργαζομένων, των συνεργατών) και άλλων ενδιαφερόμενων μερών, ώστε να διασφαλιστεί ότι η επεξεργασία τους γίνεται με νόμιμο, δίκαιο και διαφανή τρόπο.

Η δέσμευση για την ασφάλεια των προσωπικών δεδομένων επεκτείνεται στα ανώτερα επίπεδα του οργανισμού και αποδεικνύεται μέσα από τις σχετικές πολιτικές και την παροχή των απαραίτητων πόρων για την εφαρμογή και την ανάπτυξη αποτελεσματικών τεχνικών και οργανωτικών μέτρων, ώστε να διασφαλιστεί το κατάλληλο επίπεδο ασφάλειας για τα προσωπικά δεδομένα.

Στο πλαίσιο της τήρησης των νομικών υποχρεώσεων, το Π.Μ.Σ θα πρέπει να έχει καθιερώσει ένα ολοκληρωμένο πρόγραμμα για την κατανόηση και επικαιροποίηση της χρήσης των προσωπικών δεδομένων, που βρίσκονται στην κατοχή του φορέα και την επιβεβαίωση της νόμιμης βάσης της επεξεργασίας τους.

Επιπλέον, έχουν υλοποιηθεί τα παρακάτω:

- Υπάρχει πολιτική για την προστασία των προσωπικών δεδομένων στο Π.Μ.Σ. η οποία έχει εγκριθεί από τη διοίκηση και έχει κοινοποιηθεί σε όλους τους εργαζόμενους του Π.Μ.Σ. και σε άλλα ενδιαφερόμενα μέρη
- Όλοι οι εργαζόμενοι έχουν λάβει εκπαίδευση σχετικά με την προστασία δεδομένων και το ΓΚΠΔ
- Ο καθένας καταλαβαίνει το ρόλο που διαδραματίζει σχετικά με την προστασία των προσωπικών δεδομένων και έχει λάβει εκπαίδευση, όπου χρειάζεται
- Έχουν εντοπίστεί τα προσωπικά δεδομένα που είναι προς επεξεργασία, συμπεριλαμβανομένων και των ειδικών κατηγοριών
- Για κάθε περίπτωση στην οποία επεξεργάζονται προσωπικά δεδομένα, έχει ορίσθει η νόμιμη βάση της επεξεργασίας σύμφωνα με το ΓΚΠΔ
- Στις περιπτώσεις που θα χρησιμοποιηθεί το έννομο συμφέρον ως νόμιμη βάση επεξεργασίας, θα πρέπει να διεξαχθεί τεκμηριωμένος έλεγχος ώστε να αξιολογηθούν τα οφέλη σε σχέση με τον αντίκτυπο της επεξεργασίας στο υποκείμενο των δεδομένων
- Στις περιπτώσεις όπου η επεξεργασία βασίζεται στη συγκατάθεση, έχουν ληφθεί τα μέτρα για να διασφαλιστεί ότι έχει δοθεί σαφής και ελεύθερη συγκατάθεση η οποία διατηρείται σαν αρχείο καταγραφής
- Ακολουθείτε μια συνολική προσέγγιση, μέσα από ενημερώσεις για την προστασία των προσωπικών δεδομένων και κοινοποίησης της πολιτικής προστασίας προσωπικών δεδομένων, προκειμένου να διασφαλιστεί ότι οι απαιτούμενες πληροφορίες παρέχονται σε σαφή γλώσσα κάθε φορά που συλλέγονται προσωπικά δεδομένα
- Υπάρχουν καταγεγραμμένες διαδικασίες για την άμεση ανταπόκριση στα αιτήματα των φυσικών προσώπων, όπως η απόσυρση της συγκατάθεσης, η πρόσβαση και η διόρθωση
- Η χρονική διάρκεια που διατηρούνται τα προσωπικά δεδομένα ή ο τρόπος με τον οποίο αποφασίζεται ο χρόνος διατήρησης έχει καθοριστεί σε κάθε τομέα επεξεργασίας και έχει ελαχιστοποιηθεί
- Τα αρχεία επεξεργασίας διατηρούνται όπως απαιτείται από το ΓΚΠΔ
- Στις περιπτώσεις που υπάρχει υπεύθυνος επεξεργασίας, όλες οι συμβάσεις , με τους εκτελούντες την επεξεργασία έχουν αναθεωρηθεί ώστε να συμμορφώνονται με τις απαιτήσεις του ΓΚΠΔ

- Όλοι, όσοι εκτελούν σύμβαση εργασίας ορισμένου χρόνου στο Π.Μ.Σ., υπόκεινται σε υποχρεώσεις εμπιστευτικότητας, όσον αφορά τα προσωπικά δεδομένα
- Κατά περίπτωση, θα χρησιμοποιηθεί μια προσέγγιση εκτίμησης επιπτώσεων για την προστασία των δεδομένων, η οποία θα είναι σύμφωνη με τις απαιτήσεις και τις συστάσεις του ΓΚΠΔ, καθώς επίσης και με τις σχετικές βέλτιστες πρακτικές
- Σχεδιάζεται εξ ορισμού η προστασία των δεδομένων σε νέες ή τροποποιημένες υπηρεσίες και συστήματα, συμπεριλαμβανομένης της ελαχιστοποίησης της χρήσης των προσωπικών δεδομένων
- Έχουν ελεγχθεί οι διαδικασίες για την εκπλήρωση των υποχρεώσεών σε περίπτωση παραβίασης προσωπικών δεδομένων
- Διατίθενται πολιτικές και άλλα μέτρα για την παροχή κατάλληλης προστασίας των προσωπικών δεδομένων, βάσει αξιολόγησης του κινδύνου
- Έχει ορίσθεί έναν Υπεύθυνο Προστασίας Προσωπικών Δεδομένων, του οποίου τα στοιχεία επικοινωνίας έχουν ως εξής: dpo@master-ateith.gr

Θα πρέπει να υπάρχει συνεχής βελτίωση και ανάπτυξη των πολιτικών και των μέτρων προστασίας δεδομένων με την πάροδο του χρόνου, βάσει των νομικών απαιτήσεων και των αναγκών και των ασθενών, των εργαζομένων, των φοιτητών, των συνεργατών και άλλων ενδιαφερόμενων μερών.

Με εκτίμηση,

Όνομα Επώνυμο

Επιστημονικός Υπεύθυνος Π.Μ.Σ

# ΚΕΦΑΛΑΙΟ 10: ΔΙΑΔΙΚΑΣΙΑ ΓΙΑ ΔΙΕΘΝΕΙΣ ΜΕΤΑΦΟΡΕΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (ΜΕΤΑΚΙΝΗΣΗ ΦΟΙΤΗΤΩΝ ΣΤΑ ΠΛΑΙΣΙΑ ERASMUS)

## 10.1 Εισαγωγή

Προκειμένου να ληφθεί μέριμνα για τις απαιτήσεις του Κεφάλαιο V ( Μεταφορά δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς), θα μπορούσε να θεσπιστεί η παρακάτω διαδικασία. Αυτή η διαδικασία έχει ως στόχο να χρησιμοποιηθεί όταν θα δημιουργείται μια νέα συμφωνία για την μεταφορά των προσωπικών δεδομένων σε μια χώρα εκτός της Ευρωπαϊκής Ένωσης ή σε ένα διεθνή οργανισμό. Μπορεί επίσης να χρησιμοποιηθεί για να βεβαιωθεί ότι οι υπάρχουσες συμφωνίες πληρούν τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ).

Ένας διεθνής οργανισμός ορίζεται από το ΓΚΠΔ ως «*ο οργανισμός και οι υπαγόμενοι σε αυτόν φορείς που διέπονται από το δημόσιο διεθνές δίκαιο ή οποιοσδήποτε άλλος φορέας που έχει ιδρυθεί δυνάμει ή επί τη βάσει συμφωνίας μεταξύ δύο ή περισσότερων χωρών*» *(ΓΚΠΔ Άρθρο 4).*

Ο σκοπός του ΓΚΠΔ είναι να προστατεύσει τα προσωπικά δεδομένα των πολιτών της ΕΕ όπου αυτά αποθηκεύονται. Υπάρχουν αυστηρές απαιτήσεις που διέπουν το που μπορούν να μεταφερθούν τα προσωπικά δεδομένα και τα μέτρα που πρέπει να ληφθούν, ώστε να είναι νόμιμη μία τέτοια μεταφορά. Οι ποινές για την παράβαση του ΓΚΠΔ είναι σημαντικές και ο φορέας πρέπει να δίνει προσοχή συνεχώς, για να εξασφαλίζει ότι παραμένει συμμορφωμένο με τον Κανονισμό.

## 10.2 Καθορισμός της χώρας ή των χωρών προορισμού

Προκειμένου να καθοριστεί αν η μεταφορά προσωπικών δεδομένων είναι νόμιμη σε σχέση με το ΓΚΠΔ, θα πρέπει η χώρα ή οι χώρες προορισμού να είναι εδραιωμένες, μαζί με όποιες άλλες χώρες που θα λάβουν περαιτέρω διαβίβαση των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της συμφωνίας.

Αυτό μπορεί να περιλαμβάνει επίσης τη σαφή κατανόηση της νομικής βάσης των διεθνών οργανισμών που θα λαμβάνουν τα δεδομένα προσωπικού χαρακτήρα, ιδίως των χωρών που αποτελούν μέρος της συμφωνίας που διέπει τους εν λόγω οργανισμούς.

## 10.3 Καθορισμός του αν μία απόφαση επάρκειας έχει εφαρμογή

Μόλις έχει καθοριστεί σαφώς η χώρα ή οι χώρες προορισμού των προσωπικών δεδομένων, θα πρέπει να ληφθεί υπ' όψιν η λίστα με τις χώρες και τους διεθνείς οργανισμούς για τους οποίους έχει εφαρμογή μία απόφαση επάρκειας. Αυτή η λίστα είναι δημοσιευμένη στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης και στον ιστότοπο της Ευρωπαϊκής Επιτροπής (ec.europa.eu).

Μια απόφαση επάρκειας σημαίνει ότι η Ευρωπαϊκή Επιτροπή θεωρεί το επίπεδο προστασίας των προσωπικών δεδομένων αυτής της χώρας επαρκές και επομένως για τέτοιες διαβιβάσεις δεν απαιτείται η εφαρμογή περαιτέρω νομικών διασφαλίσεων. Οι αποφάσεις επάρκειας επανεξετάζονται τακτικά, τουλάχιστον κάθε τέσσερα χρόνια και μπορούν να καταργηθούν σε περίπτωση που η Ευρωπαϊκή Επιτροπή δε θεωρεί πλέον ότι η εν λόγω χώρα πληροί τις απαιτήσεις προστασίας των δεδομένων προσωπικού χαρακτήρα.

Μια ειδική περίπτωση σε αυτόν τον τομέα είναι το EU-US Privacy Shield, το οποίο καλύπτει τη διαβίβαση των προσωπικών δεδομένων των πολιτών της ΕΕ στις ΗΠΑ. Οι οργανισμοί των ΗΠΑ που έχουν εγγραφεί στο EU-US Privacy Shield μπορούν να αποθηκεύουν και να επεξεργάζονται τέτοια προσωπικά δεδομένα, εφόσον πληρούν αυστηρές διασφαλίσεις που είναι ισοδύναμες με τις απαιτήσεις του GDPR. Τα προσωπικά δεδομένα μπορούν να μεταφερθούν αποτελεσματικά σε οργανισμούς των ΗΠΑ εφόσον εφαρμόζεται μια απόφαση επάρκειας.

## 10.4 Εφαρμογή κατάλληλων διασφαλίσεων

Σε περίπτωση που μία ή περισσότερες από τις χώρες στις οποίες πρόκειται να μεταφερθούν τα προσωπικά δεδομένα δεν υπόκειται σε απόφαση επάρκειας από την Ευρωπαϊκή Επιτροπή, πρέπει να θεσπιστούν κατάλληλες διασφαλίσεις για την εξασφάλιση των δικαιωμάτων των υποκειμένων των δεδομένων και εκτελεστικά ένδικα μέσα.

Υπάρχουν διάφοροι τρόποι με τους οποίους ο ΓΚΠΔ επιτρέπει την παροχή αυτών των διασφαλίσεων. Αυτοί είναι:

α) μόνο μεταξύ δημόσιων αρχών ή φορέων, μέσω νομικά δεσμευτικής συμφωνίας που μπορεί να εφαρμοστεί

β) χρησιμοποιώντας δεσμευτικούς εταιρικούς κανόνες

γ) χρησιμοποιώντας τις τυποποιημένες ρήτρες προστασίας δεδομένων που έχουν εγκριθεί είτε από την Ευρωπαϊκή Επιτροπή είτε από την αρμόδια εποπτική αρχή

δ) μέσω εγκεκριμένου κώδικα δεοντολογίας

ε) μέσω ενός συστήματος πιστοποίησης

Η κατάσταση ορισμένων από τις προαναφερόμενες διασφαλίσεις μπορεί να μεταβληθεί με την πάροδο του χρόνου, καθώς ο ΓΚΠΔ καθίσταται πιο ώριμος και εκδίδεται περαιτέρω καθοδήγηση τόσο από την Ευρωπαϊκή Επιτροπή όσο και από τις επιμέρους εποπτικές αρχές.

Η πλέον κατάλληλη μέθοδος προστασίας των δικαιωμάτων των προσώπων των οποίων τα δεδομένα θα μεταφερθούν πρέπει να επιλεγεί και να ενσωματωθεί στις συμβατικές ρήτρες της σχετικής συμφωνίας.

## 10.5 Δεσμευτικοί Εταιρικοί Κανόνες

Η εποπτική αρχή που σχετίζεται με τη μεταφορά (συνήθως στη χώρα του υπεύθυνου επεξεργασίας των δεδομένων) έχει την εξουσία να εγκρίνει ένα σύνολο δεσμευτικών εταιρικών κανόνων που μπορούν να χρησιμοποιηθούν για την κάλυψη της μεταφοράς δεδομένων προσωπικού χαρακτήρα από τη σκοπιά της προστασίας των δεδομένων.

Αυτοί οι δεσμευτικοί εταιρικοί κανόνες απαιτούνται από το ΓΚΠΔ για τον προσδιορισμό όλων των πτυχών της μεταφοράς, συμπεριλαμβανομένου του τρόπου παροχής της προστασίας δεδομένων, του τρόπου με τον οποίο τα υποκείμενα δεδομένων θα ασκήσουν τα δικαιώματά τους και τον τρόπο επαλήθευσης της συμμόρφωσης. Οι πλήρεις απαιτήσεις παρατίθενται στο άρθρο 47 ("δεσμευτικοί εταιρικοί κανόνες"), παράγραφος 2, στοιχεία α) έως η) του ΓΚΠΔ.

Η αρχική δημιουργία και έγκριση (από την εποπτική αρχή) των Δεσμευτικών Εταιρικών Κανόνων αποτελεί σημαντικό έργο που πρέπει να προσεγγιστεί με την πλήρη δέσμευση της ανώτατης διοίκησης του Π.Μ.Σ και μπορεί να χρειαστεί πολύς χρόνος για να επιτευχθεί (δεν είναι ασύνηθες να πάρει πάνω από δώδεκα μήνες). Μπορεί να δημιουργηθεί ένα υπάρχον σύνολο Δεσμευτικών Εταιρικών Κανόνων που θα ισχύσει για τη μεταφορά που εξετάζεται και να ζητηθούν συμβουλές από τον νομικό σύμβουλο εφόσον πρόκειται να χρησιμοποιηθεί αυτή η οδός για τη συμμόρφωση με το ΓΚΠΔ, όσον αφορά τη μεταφορά δεδομένων.

## 10.6 Τυπικές Ρήτρες Προστασίας Δεδομένων

Η Ευρωπαϊκή Επιτροπή και κάθε μία από τις επιμέρους εποπτικές αρχές μπορούν να δημιουργούν και να διατηρούν σύνολα υποδειγμάτων ρητρών προστασίας δεδομένων που προορίζονται να χρησιμοποιηθούν σε συμβάσεις που εφαρμόζονται για τη διεθνή διαβίβαση δεδομένων προσωπικού χαρακτήρα. Όταν χρησιμοποιούνται στο σύνολό τους, οι εν λόγω ρήτρες είναι γενικά αποδεκτές για την πλήρωση των απαιτήσεων του ΓΚΠΔ, σχετικά με την παροχή επαρκών διασφαλίσεων.

Η τελευταίας έκδοση αυτών των ρητρών είναι διαθέσιμη στον ιστότοπο της αρμόδιας εποπτικής αρχής.

## 10.7 Κώδικες Δεοντολογίας

Το Άρθρο 40 του ΓΚΠΔ προβλέπει την κατάρτιση κατάλληλων κωδίκων δεοντολογίας από οργανισμούς, όπως ενώσεις και βιομηχανικούς φορείς, για τη συμμόρφωση με το ΓΚΠΔ. Έπειτα οι οργανισμοί συμφωνούν να συμμορφώνονται με τον κώδικα δεοντολογίας και η συμμόρφωσή τους παρακολουθείται από τη σχετική ένωση.

Ένας τέτοιος κώδικας συμπεριφοράς μπορεί να χρησιμοποιηθεί για να καλύψει μια διεθνή μεταφορά προσωπικών δεδομένων και εάν το Π.Μ.Σ. έχει ήδη ή θα μπορούσε να υπογράψει έναν τέτοιο κώδικα, μπορεί να διερευνηθεί ως μια πιθανή οδός για την παροχή των κατάλληλων διασφαλίσεων.

## 10.8 Σχέδια Πιστοποίησης

Για να αποδειχθεί ότι υπάρχουν κατάλληλες διασφαλίσεις για την προστασία της μεταφοράς δεδομένων προσωπικού χαρακτήρα διεθνώς μπορεί επίσης να χρησιμοποιηθεί η πιστοποίηση σε ένα εγκεκριμένο σύστημα. Αυτό ισχύει τόσο για τον αποστολέα όσο και για τον παραλήπτη των δεδομένων και θα απαιτείται να υπάρχει ένα διαθέσιμο εγκεκριμένο σχέδιο πιστοποίησης στη χώρα του παραλήπτη.

## 10.9 Άλλες αποδεκτές προϋποθέσεις για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα

Σε περίπτωση που μια απόφαση επάρκειας δεν ισχύει για τη χώρα προορισμού και δεν μπορούν να εφαρμοστούν κατάλληλες διασφαλίσεις μέσω των παραπάνω μεθόδων, η διαβίβαση δεδομένων προσωπικού χαρακτήρα μπορεί να γίνει μόνο σε διεθνές επίπεδο, εάν ισχύει μία από τις ακόλουθες περιπτώσεις:

*α) το υποκείμενο των δεδομένων συγκατατέθηκε ρητώς στην προτεινόμενη διαβίβαση, αφού ενημερώθηκε για τους πιθανούς κινδύνους που εγκυμονούν τέτοιες διαβιβάσεις για το υποκείμενο των δεδομένων λόγω απουσίας απόφασης επάρκειας και κατάλληλων εγγυήσεων,*

*β) η διαβίβαση είναι απαραίτητη για την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας ή για την εφαρμογή προσυμβατικών μέτρων τα οποία λαμβάνονται κατόπιν αιτήματος του υποκειμένου των δεδομένων,*

*γ) η διαβίβαση είναι απαραίτητη για τη σύναψη ή την εκτέλεση σύμβασης η οποία έχει συναφθεί προς όφελος του υποκειμένου των δεδομένων μεταξύ του υπευθύνου επεξεργασίας και άλλου φυσικού ή νομικού προσώπου,*

*δ) η διαβίβαση είναι απαραίτητη για σημαντικούς λόγους δημόσιου συμφέροντος,*

*ε) η διαβίβαση είναι απαραίτητη για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων,*

*στ) η διαβίβαση είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλων προσώπων, εφόσον το υποκείμενο των δεδομένων δεν έχει τη φυσική ή νομική ικανότητα να παράσχει τη συγκατάθεσή του,*

*ζ) η διαβίβαση πραγματοποιείται από μητρώο το οποίο σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους προορίζεται για την παροχή πληροφοριών στο κοινό και είναι ανοικτό για αναζήτηση πληροφοριών είτε στο ευρύ κοινό είτε σε οποιοδήποτε πρόσωπο μπορεί να επικαλεστεί έννομο συμφέρον, αλλά μόνο εφόσον πληρούνται στην εκάστοτε περίπτωση οι προϋποθέσεις που προβλέπονται στο δίκαιο της Ένωσης ή στο δίκαιο του κράτους μέλους για την αναζήτηση πληροφοριών.*

## 10.10 Ειδικές Καταστάσεις Μεταβιβάσεων

Εάν δεν εφαρμόζεται κανένας από τους όρους που καθορίζονται στην παρούσα διαδικασία, τότε μια διεθνής μεταφορά δεδομένων προσωπικού χαρακτήρα μπορεί να πραγματοποιηθεί μόνο εφόσον ισχύουν **όλοι** οι ακόλουθοι όροι:

α) Η μεταφορά δεν είναι επαναλαμβανόμενη

β) Συμπεριλαμβάνεται περιορισμένος αριθμός υποκειμένων των δεδομένων

γ) Είναι για επιτακτικούς νόμιμους σκοπούς που δεν υπερισχύονται από εκείνα του υποκειμένου των δεδομένων

δ) Έχουν αξιολογηθεί όλες οι περιστάσεις της μεταφοράς δεδομένων

ε) Παρέχονται κατάλληλες διασφαλίσεις, βάσει της αξιολόγησης

στ) Η αξιολόγηση και οι διασφαλίσεις τεκμηριώνονται

ζ) Η εποπτική αρχή ενημερώνεται για τη μεταβίβαση

η) Το υποκείμενο των δεδομένων ενημερώνεται για τη διαβίβαση των δεδομένων και τους λόγους για τους οποίους γίνεται η διαβίβαση

i) Το υποκείμενο των δεδομένων ενημερώνεται για τα δικαιώματά του βάσει του ΓΚΠΔ

## 10.11 Εφαρμόζοντας τη Μεταβίβαση

Μόλις η νομική βάση της μεταβίβασης των προσωπικών δεδομένων έχει εγκαθιδρυθεί και εγκριθεί, πρέπει να καθοριστούν οι μηχανισμοί για την επίτευξη της μεταφοράς. Αυτοί θα ποικίλλουν ανάλογα με παράγοντες όπως ο τύπος και ο όγκος των δεδομένων, ο προορισμός και η χρησιμοποιούμενη τεχνολογία.

Πρέπει να ληφθεί μέριμνα ώστε να διασφαλιστεί ότι τηρούνται οι εγγυήσεις που έχουν συμφωνηθεί ως μέρος της σύστασης της μεταφοράς και ότι τα αποδεικτικά στοιχεία σχετικά με τη χρήση τους διατηρούνται για μελλοντικούς σκοπούς ελέγχου.

Ο ιστότοπος της Ευρωπαϊκής Επιτροπής και η σχετική εποπτική αρχή πρέπει να παρακολουθούνται ώστε να εντοπίζονται οι αλλαγές που επηρεάζουν τη νομιμότητα ή την απόδοση της μεταφοράς και να γίνονται οι σχετικές ενέργειες.

# ΚΕΦΑΛΑΙΟ 11: ΔΙΑΧΕΙΡΗΣΗ ΠΑΡΑΒΙΑΣΕΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

## 11.1 Εισαγωγή

Στην θέσπιση της παρακάτω διαδικασίας καλύπτονται οι απαιτήσεις του Άρθρου 33 (Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή) και του

Άρθρου 34 ( Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων).

Αυτό το έγγραφο προορίζεται να χρησιμοποιηθεί όταν συμβεί κάποιο είδος περιστατικού που επηρεάζει την ασφάλεια των πληροφοριών του Π.Μ.Σ , συμπεριλαμβανομένων εκείνων που ενδέχεται να επηρεάζουν τα προσωπικά δεδομένα για τα οποία ο οργανισμός είναι υπεύθυνος επεξεργασίας. Σκοπός του είναι να εξασφαλίσει μια γρήγορη, αποτελεσματική και τακτική απόκριση στην παραβίαση της ασφάλειας των πληροφοριών.

Οι διαδικασίες που ορίζονται στο παρόν έγγραφο πρέπει να χρησιμοποιούνται μόνο ως καθοδήγηση κατά την απόκριση σε ένα περιστατικό. Η ακριβής φύση ενός συμβάντος και ο αντίκτυπός του δεν μπορούν να προβλεφθούν σε κανένα βαθμό βεβαιότητας και, ως εκ τούτου, είναι σημαντικό να χρησιμοποιείται ένας καλός βαθμός κοινής λογικής όταν αποφασίζονται οι ενέργειες που πρέπει να γίνουν.

Ωστόσο, προβλέπεται ότι οι δομές που παρουσιάζονται εδώ θα αποδειχθούν χρήσιμες για να καταστεί δυνατή η ταχύτερη λήψη των ορθών ενεργειών και η παροχή ακριβέστερων πληροφοριών.

Οι στόχοι αυτής της διαδικασίας αντιμετώπισης περιστατικών είναι:

- Η παροχή μια συνοπτικής επισκόπησης του τρόπου με τον οποίο ο φορέας θα απαντήσει σε ένα περιστατικό
- Ο ορισμός του ποιος θα ανταποκριθεί σε ένα περιστατικό και οι ρόλοι και οι ευθύνες του
- Η περιγραφή των υποδομών που υπάρχουν για βοήθεια στη διαχείριση του συμβάντος
- Ο καθορισμός του τρόπου με τον οποίο θα ληφθούν αποφάσεις σχετικά με την απόκρισή σε ένα περιστατικό

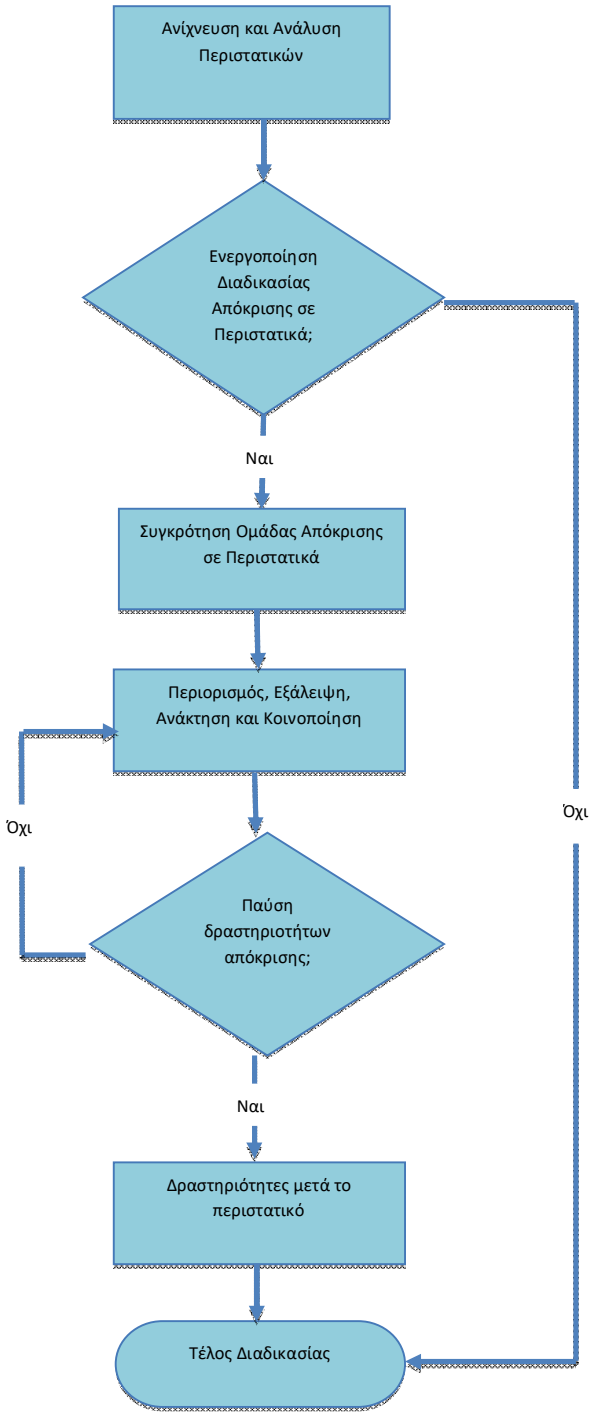
- Να εξηγεί πώς θα γίνεται η επικοινωνία εντός του οργανισμού και με τα εξωτερικά μέρη
- Η παροχή στοιχείων επικοινωνίας των βασικών ανθρώπων και των εξωτερικών φορέων
- Καθορισμός του τι θα συμβεί όταν επιλυθεί το περιστατικό και αποσυρθούν οι ανταποκριτές

Όλα τα μέλη του προσωπικού που αναφέρονται σε αυτό το έγγραφο θα λάβουν ένα αντίγραφο το οποίο πρέπει να έχουν στη διάθεσή τους όταν απαιτείται.

Τα στοιχεία επικοινωνίας θα ελέγχονται και θα ενημερώνονται τουλάχιστον τρεις φορές το χρόνο. Οι αλλαγές στις επαφές ή άλλες σχετικές λεπτομέρειες που προκύπτουν εκτός αυτών των προγραμματισμένων ελέγχων θα πρέπει να σταλούν στο **dpo @master-ateith.gr** το συντομότερο δυνατό μετά την πραγματοποίηση της αλλαγής.

Όλες οι προσωπικές πληροφορίες που συλλέγονται στο πλαίσιο της διαδικασίας αντιμετώπισης περιστατικών και περιλαμβάνονται στο παρόν έγγραφο θα χρησιμοποιηθούν αποκλειστικά για τους σκοπούς της διαχείρισης περιστατικών ασφάλειας πληροφοριών και υπόκεινται σε σχετική νομοθεσία για την προστασία των δεδομένων.

## 11.2 Διάγραμμα ροής απόκρισης σε περιστατικά.




Η ροή της διαδικασίας απόκρισης σε περιστατικά φαίνεται στο παρακάτω διάγραμμα.

## 11.3 Ανίχνευση και Ανάλυση Περιστατικών

Ένα περιστατικό μπορεί να εντοπιστεί αρχικά με πολλούς τρόπους και μέσω διαφόρων πηγών, ανάλογα με τη φύση και τη θέση του περιστατικού. Ορισμένα περιστατικά ενδέχεται να ανιχνευθούν αυτομάτως μέσω εργαλείων λογισμικού που χρησιμοποιούνται από το Π.Μ.Σ ή από εργαζόμενους που παρατηρούν κάποια ασυνήθιστη δραστηριότητα. Άλλοι μπορεί να ειδοποιηθούν από τρίτους, όπως ο φοιτητής, ο προμηθευτής ή η υπηρεσία επιβολής του νόμου, που έχει λάβει γνώση παραβίασης, ίσως επειδή οι κλεμμένες πληροφορίες χρησιμοποιήθηκαν για κακόβουλους σκοπούς.

Δεν είναι ασυνήθιστο να υπάρξει καθυστέρηση μεταξύ της προέλευσης του συμβάντος και της πραγματικής ανίχνευσής του· ένας από τους στόχους μιας προληπτικής προσέγγισης για την ασφάλεια των πληροφοριών είναι η μείωση αυτής της χρονικής περιόδου. Ο σημαντικότερος παράγοντας είναι ότι η διαδικασία απόκρισης σε περιστατικό πρέπει να ξεκινήσει το συντομότερο δυνατό μετά την ανίχνευση, ώστε να μπορεί να δοθεί αποτελεσματική απάντηση.

Μόλις εντοπιστεί το περιστατικό, πρέπει να γίνει μία αρχική εκτίμηση του αντικτύπου προκειμένου να αποφασιστεί η κατάλληλη απάντηση.

Αυτή η εκτίμηση του αντικτύπου θα πρέπει να αξιολογεί:

- Την έκταση των επιπτώσεων στην πληροφοριακή υποδομή, συμπεριλαμβανομένων υπολογιστών, δικτύων, εξοπλισμού και εγκαταστάσεων
- Τα πληροφοριακά αγαθά (συμπεριλαμβανομένων των προσωπικών δεδομένων) που ενδέχεται να κινδυνεύουν ή να διακυβεύονται
- Τη πιθανή διάρκεια του συμβάντος, δηλαδή πότε μπορεί να είχε αρχίσει
- Τις μονάδες του Π.Μ.Σ., που επηρεάζονται και την έκταση των επιπτώσεων σε αυτές
- Για τις παραβιάσεις που αφορούν τα προσωπικά δεδομένα, το βαθμό κινδύνου για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων
- Την αρχική ένδειξη της πιθανής αιτίας του συμβάντος

Αυτές οι πληροφορίες θα πρέπει να τεκμηριώνονται έτσι ώστε μια σαφής κατανόηση της κατάστασης, ως προς το χρόνο, όπως αυτή προκύπτει, να είναι διαθέσιμη για τρέχουσα χρήση και αργότερα για αναθεώρηση.

Θα πρέπει να δημιουργηθεί ένας κατάλογος των πληροφοριακών αγαθών (συμπεριλαμβανομένων των προσωπικών δεδομένων), των δραστηριοτήτων του Π.Μ.Σ., των προϊόντων, των υπηρεσιών, των ομάδων και των διαδικασιών υποστήριξης που ενδέχεται να έχουν επηρεαστεί από το περιστατικό, μαζί με μια εκτίμηση της έκτασης των επιπτώσεων.

Ως αποτέλεσμα αυτής της αρχικής ανάλυσης, οποιοδήποτε μέλος της ομάδας διαχείρισης έχει την εξουσία να επικοινωνήσει με τον Υπεύθυνο της Ομάδας Απόκρισης σε Περιστατικά οποιαδήποτε στιγμή για να του ζητήσει να αξιολογήσει εάν πρέπει να ενεργοποιηθεί η Διαδικασία Απόκρισης σε Περιστατικά.

## 11.4 Ενεργοποίηση της Διαδικασίας Απόκρισης σε Περιστατικά

Μόλις κοινοποιηθεί ένα συμβάν, ο Υπεύθυνος της Ομάδας πρέπει να αποφασίσει εάν η κλίμακα και οι πραγματικές ή δυνητικές επιπτώσεις του συμβάντος δικαιολογούν την ενεργοποίηση της Διαδικασίας Απόκρισης σε Περιστατικά και την σύγκληση της Ομάδας Απόκρισης σε Περιστατικά.

Οι κατευθυντήριες γραμμές για το αν πρέπει να ξεκινήσει επίσημη αντίδραση για κάποιο συγκεκριμένο συμβάν το οποίο έχει κοινοποιηθεί στον επικεφαλής της ομάδας είναι εάν ισχύει κάποιο από τα παρακάτω:

- Υπάρχει σημαντική πραγματική ή ενδεχόμενη απώλεια διαβαθμισμένων πληροφοριών, συμπεριλαμβανομένων των προσωπικών δεδομένων
- Υπάρχει σημαντική πραγματική ή ενδεχόμενη διακοπή των δραστηριοτήτων του Π.Μ.Σ.
- Υπάρχει σημαντικός κίνδυνος για τη φήμη του Π.Μ.Σ.
- Οποιαδήποτε άλλη κατάσταση που μπορεί να έχει σημαντικές επιπτώσεις στον οργανισμό

Σε περίπτωση διαφωνίας ή αβεβαιότητας σχετικά με το αν θα ενεργοποιηθεί ή όχι μια απόκριση σε περιστατικό, η απόφαση του Υπεύθυνου της Ομάδας θα είναι οριστική.

Εάν αποφασιστεί να μην ενεργοποιηθεί η διαδικασία, τότε θα πρέπει να δημιουργηθεί ένα σχέδιο που να επιτρέπει μια ανταπόκριση χαμηλότερου επιπέδου στο περιστατικό.

Εάν το περιστατικό απαιτεί εγγυημένα την ενεργοποίηση της διαδικασίας Απόκρισης σε Περιστατικά, ο Υπεύθυνος της Ομάδας θα αρχίσει να συγκεντρώνει την Ομάδα Απόκρισης σε Περιστατικά.

## 11.5 Συγκέντρωση της Ομάδας Απόκρισης σε Περιστατικά

Μόλις ληφθεί η απόφαση για την ενεργοποίηση της διαδικασίας αντιμετώπισης περιστατικών, ο Υπεύθυνος της Ομάδας (ή ο αναπληρωτής) θα εξασφαλίσει ότι όλοι οι κάτοχοι ρόλων (ή οι αναπληρωτές τους εάν οι κύριοι κάτοχοι δεν μπορούν να ειδοποιηθούν) έρχονται σε επαφή, ενημερώνονται για τη φύση του συμβάντος και τους ζητείται να συγκεντρωθούν σε μια κατάλληλη τοποθεσία.

Η εξαίρεση είναι ο Σύνδεσμος Επικοινωνίας των Περιστατικών, ο οποίος θα κληθεί να παρακολουθήσει τη θέση του συμβάντος (αν είναι διαφορετική) προκειμένου να αρχίσει να συγκεντρώνει πληροφορίες για την εκτίμηση περιστατικών που θα διεξαγάγει η Ομάδα Απόκρισης σε Περιστατικά, ώστε να μπορεί να προσδιοριστεί η κατάλληλη απάντηση.

### 11.5.1 Ρόλοι και Καθήκοντα

Οι ευθύνες των ρόλων στην ομάδα απόκρισης σε περιστατικά είναι οι εξής:

*Υπεύθυνος Ομάδας*

- Αποφασίζει αν θα ξεκινήσει ή όχι μία απόκριση
- Συγκεντρώνει την ομάδα απόκρισης σε περιστατικά
- Γενική διαχείριση της ομάδας απόκρισης σε περιστατικά
- Λειτουργεί ως διασύνδεση με το διοικητικό συμβούλιο και άλλους ενδιαφερόμενους υψηλού επιπέδου
- Λαμβάνει την τελική απόφαση σε περιπτώσεις διαφωνίας

*Συντονιστής Ομάδας*

- Υποστηρίζει την ομάδα απόκρισης σε περιστατικά
- Συντονίζει τους πόρους
- Ετοιμάζεται για τα συμβούλια και καταγράφει τις δράσεις και τις αποφάσεις

- Ενημερώνει τα μέλη της ομάδας για την τελευταία κατάσταση
- Συντονίζει την επικοινωνία μέσω email, fax, τηλεφώνου ή άλλων μεθόδων
- Παρακολουθεί εξωτερικές πηγές πληροφοριών όπως ειδήσεις

*Σύνδεσμος Επικοινωνίας των Περιστατικών*

- Παρευρίσκεται στον τόπο του συμβάντος το συντομότερο δυνατόν
- Αξιολογεί την έκταση και τον αντίκτυπο του συμβάντος
- Παρέχει τον απολογισμό της κατάστασης στην Ομάδα Απόκρισης σε Περιστατικά
- Είναι σε επαφή με την Ομάδα Απόκρισης σε Περιστατικά σε συνεχή βάση για την παροχή ενημερώσεων και την απάντηση σε οποιεσδήποτε ερωτήσεις που απαιτούνται για τη λήψη αποφάσεων από την Ομάδα

*Πληροφορική*

- Ενεργεί σε τεχνολογικά ζητήματα
- Βοηθά στην αξιολόγηση του αντικτύπου

*Διαδικασίες του Π.Μ.Σ.*

Συμβάλλει στη λήψη αποφάσεων με βάση τη γνώση των δραστηριοτήτων, των προϊόντων και των υπηρεσιών *του Π.Μ.Σ.*

- Ενημερώνει άλλα μέλη της ομάδας για ζητήματα του φορέα
- Βοηθά στην αξιολόγηση πιθανών επιπτώσεων στους φοιτητές του Π.Μ.Σ.

Διαχείριση Εγκαταστάσεων

- Ασχολείται με πτυχές φυσικής ασφάλειας και πρόσβασης
- Παρέχει παρουσία ασφάλειας, εάν απαιτείται

*Ανθρώπινοι Πόροι*

- Αντιπροσωπεύει τα συμφέροντα των εργαζομένων του οργανισμού

- Δίνει συμβουλές σχετικά με πειθαρχικά ζητήματα και ζητήματα ικανοτήτων

*Σχεδιασμός Επιχειρησιακής Συνέχειας*

- Παρέχει συμβουλές για επιλογές που αφορούν την επιχειρησιακή συνέχεια
- Ενεργοποιεί το σχέδιο επιχειρησιακής συνέχειας, εάν απαιτείται

Επικοινωνίες (Σχέσεις με τα Media)

- Υπεύθυνοι για την εξασφάλιση της αποτελεσματικότητας των εσωτερικών επικοινωνιών
- Αποφασίζει τον επίπεδο, τη συχνότητα και το περιεχόμενο των επικοινωνιών με εξωτερικά μέρη όπως τα μέσα μαζικής ενημέρωσης
- Ορίζει την προσέγγιση στην ενημέρωση των επηρεαζόμενων μελών π.χ. φοιτητών

Νομικό και Κανονιστικό Τμήμα

- Δίνει συμβουλές για το τι πρέπει να γίνει για να διασφαλιστεί η συμμόρφωση με τους σχετικούς νόμους και κανονιστικά πλαίσια
- Αξιολογεί τις πραγματικές και πιθανές νομικές επιπτώσεις του περιστατικού και των επακόλουθων ενεργειών

### 11.5.2 Διαχείριση Περιστατικών, Καταγραφή και Επικοινωνία

Μόλις καθοριστεί μία κατάλληλη απόκριση για το περιστατικό, η Ομάδα Απόκρισης σε Περιστατικά πρέπει να είναι ικανή να διαχειριστεί την συνολική απόκριση, να παρακολουθεί την κατάσταση του περιστατικού και να εξασφαλίσει ότι υπάρχει αποτελεσματική επικοινωνία σε όλα τα επίπεδα.

Θα πρέπει να λαμβάνουν χώρα τακτικά συμβούλια της Ομάδας Απόκρισης σε Περιστατικά σε μία κατάλληλη συχνότητα που αποφασίζεται από τον Υπεύθυνο της Ομάδας. Ο σκοπός αυτών των συμβουλίων είναι να εξασφαλιστεί ότι οι πόροι για τη διαχείριση των περιστατικών είναι αποτελεσματικοί και ότι οι βασικές αποφάσεις λαμβάνονται έγκαιρα, με βάση επαρκείς πληροφορίες. Ο Συντονιστής Ομάδας θα καταγράφει τα πρακτικά κάθε συμβουλίου.

Ο Σύνδεσμος Επικοινωνίας των Περιστατικών θα παρέχει ενημερώσεις στην Ομάδα Απόκρισης σε Περιστατικά σε συχνότητα που αποφασίζεται από τον Υπεύθυνο της Ομάδας. Αυτές οι ενημερώσεις θα πρέπει να συντονίζονται με τις συνεδριάσεις της Ομάδας Απόκρισης σε Περιστατικά, έτσι ώστε να είναι διαθέσιμες οι πιο πρόσφατες πληροφορίες για κάθε συνεδρίαση.

### 11.5.3 Διαδικασίες Επικοινωνίας

Είναι ζωτικής σημασίας να διατηρούνται αποτελεσματικές επικοινωνίες μεταξύ όλων των μελών που εμπλέκονται στην απόκριση σε περιστατικά.

Τα πρωταρχικά μέσα επικοινωνίας κατά τη διάρκεια ενός περιστατικού θα είναι αρχικά σε προσωπική επαφή και μέσω τηλεφώνου, μέσω σταθερής και κινητής τηλεφωνίας. Δε θα πρέπει να γίνεται χρήση του ηλεκτρονικού ταχυδρομείου εκτός εάν δοθεί η άδεια από την Ομάδα Απόκρισης σε Περιστατικά.

Οι παρακάτω κατευθυντήριες γραμμές θα πρέπει να ακολουθηθούν σε όλες τις επικοινωνίες:

- Να υπάρχει ηρεμία και να αποφεύγονται οι μακροσκελείς συζητήσεις
- Τα εσωτερικά μέλη της ομάδας να ενημερώνονται για την ανάγκη υποβολής αιτημάτων πληροφοριών στην Ομάδα Απόκρισης σε Περιστατικά
- Εάν η κλήση απαντηθεί από κάποιον άλλο, εκτός του αρμόδιου :
    - Ρωτήστε αν ο αρμόδιος είναι διαθέσιμος κάπου αλλού
    - Αν η επικοινωνία δεν είναι δυνατή, αφήστε ένα μήνυμα να επικοινωνήσει μαζί σας σε νούμερο που έχει δοθεί
    - Μη δώσετε λεπτομέρειες για το περιστατικό
- Να καταγράφονται πάντοτε λεπτομέρειες για τη χρονική διάρκεια της κλήσης, οι απαντήσεις και οι ενέργειες

Όλες οι επικοινωνίες πρέπει να καταγραφούν με ξεκάθαρο και σαφή τρόπο, καθώς τα αρχεία μπορεί να χρειαστούν στο μέλλον ως μέρος μίας νομικής ενέργειας.

### 11.5.4 Επικοινωνία με την Εποπτική Αρχή Προστασίας Δεδομένων

Είναι απαίτηση του Γενικού Κανονισμού Προστασίας Δεδομένων 2016 (ΓΚΠΔ) της ΕΕ ότι τα περιστατικά που επηρεάζουν τα προσωπικά δεδομένα και ενδέχεται να αποτελέσουν κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων θα πρέπει να αναφέρονται στην εποπτική αρχή προστασίας δεδομένων αμελλητί και, εφόσον είναι εφικτό,

εντός 72 ωρών από τη στιγμή που αποκτάται γνώση του γεγονότος. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, θα πρέπει να συνοδεύεται από αιτιολόγηση για την καθυστέρηση.

### 11.5.5 Επικοινωνία με τα Υποκείμενα των Προσωπικών Δεδομένων

Όταν ένα περιστατικό επηρεάζει τα δεδομένα προσωπικού χαρακτήρα, θα πρέπει να ληφθεί μία απόφαση από την Ομάδα Απόκρισης σε Περιστατικά σχετικά με την έκταση, το χρόνο και το περιεχόμενο της επικοινωνίας με τα υποκείμενα των δεδομένων. Ο ΓΚΠΔ της ΕΕ απαιτεί ότι η επικοινωνία θα πρέπει να λάβει χώρα «χωρίς αναίτια καθυστέρηση» αν μία παραβίαση δύναται να αποτελέσει «κίνδυνο υψηλού επιπέδου στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων».

### 11.5.6 Άλλα Είδη Εξωτερικής Επικοινωνίας

Ανάλογα με το περιστατικό μπορεί να υπάρχει μία ποικιλία εξωτερικών μερών που θα ειδοποιηθούν κατά την πορεία της απόκρισης. Είναι σημαντικό οι πληροφορίες που θα δοθούν σε τρίτα μέρη να είναι υπό διαχείριση, έτσι ώστε να είναι έγκαιρες και έγκυρες.

Οι κλήσεις που δεν προέρχονται από οργανισμούς, που είναι άμεσα εμπλεκόμενοι στην απόκριση σε περιστατικά (όπως τα ΜΜΕ) θα πρέπει να προωθούνται στο μέλος της Ομάδας Απόκρισης σε Περιστατικά που είναι υπεύθυνο για τις επικοινωνίες.

Μπορεί να υπάρχει ένας αριθμός εξωτερικών μερών που, ενώ δεν είναι άμεσα εμπλεκόμενος με το περιστατικό, μπορεί να επηρεαστεί από αυτό και θα πρέπει να ειδοποιηθεί για αυτό το γεγονός. Αυτά τα μέρη μπορεί να περιλαμβάνουν:

- Φοιτητές
- Προμηθευτές – Συνεργάτες
- Κανονιστικές Αρχές

Το μέλος της Ομάδας Απόκρισης σε Περιστατικά, που είναι υπεύθυνο για τις επικοινωνίες θα πρέπει να κάνει μία λίστα με τέτοια ενδιαφερόμενα μέρη και να καθορίσει το μήνυμα που θα πρέπει να δοθεί σε αυτά.

Τα ενδιαφερόμενα μέρη που δεν έχουν ειδοποιηθεί από την Ομάδα Απόκρισης σε Περιστατικά, έχουν την δυνατότητα να καλέσουν για να αποκτήσουν πληροφορίες σχετικά με

το περιστατικό και τα αποτελέσματά του. Αυτές οι κλήσεις θα πρέπει να καταγράφονται σε ένα αρχείο μηνυμάτων και να προωθούνται στο μέλος της Ομάδας Απόκρισης σε Περιστατικά, που είναι υπεύθυνο για τις επικοινωνίες.

### 11.5.7 Επικοινωνία με τα ΜΜΕ

Σε γενικές γραμμές η στρατηγική επικοινωνίας, που αφορά στα ΜΜΕ θα είναι η έκδοση ενημερώσεων μέσω της ανώτατης διοίκησης. Κανένας υπάλληλος δεν πρέπει να δώσει συνέντευξη με τα μέσα μαζικής ενημέρωσης, εκτός εάν αυτό έχει προηγουμένως εγκριθεί από την Ομάδα Απόκρισης σε Περιστατικά.

Η προτιμώμενη επαφή με τα μέσα μαζικής ενημέρωσης είναι η έκδοση δελτίων τύπου, η συνέντευξη Τύπου για να απαντηθούν ερωτήσεις σχετικά με το περιστατικό και τα αποτελέσματά του. Είναι ευθύνη του μέλους της Ομάδας Απόκρισης σε Περιστατικά, που είναι υπεύθυνο για την επικοινωνία να οργανώσει τον τόπο διεξαγωγής τους και να επικοινωνήσει με τον τύπο που μπορεί να επιθυμεί να παρευρεθεί.

Κατά τη σύνταξη μιας δήλωσης για τα μέσα ενημέρωσης θα πρέπει να τηρηθούν οι ακόλουθες οδηγίες:

- Οι προσωπικές πληροφορίες θα πρέπει να προστατεύονται σε όλες τις περιπτώσεις
- Θα πρέπει να τηρείται η παραμονή στα γεγονότα και να μη γίνονται εικασίες για το περιστατικό ή την αιτία του
- Να εξασφαλιστεί ότι λαμβάνεται νομική υποστήριξη πριν την έκδοση οποιασδήποτε δήλωσης
- Να γίνεται προσπάθεια για να δοθούν απαντήσεις σε εύλογα ερωτήματα
- Να δοθεί έμφαση στο γεγονός ότι έχει ενεργοποιηθεί μία προετοιμασμένη απόκριση και γίνεται ότι είναι δυνατό

## 11.6 Περιορισμός, Εξάλειψη, Ανάκτηση Και Γνωστοποίηση Περιστατικών

### 11.6.1 Περιορισμός

Το πρώτο βήμα είναι να γίνει προσπάθεια διακοπής της επιδείνωσης του περιστατικού π.χ. να γίνει περιορισμός του. Στην περίπτωση ενός ξεσπάσματος ιού αυτό μπορεί να περιλαμβάνει την αποσύνδεση των προσβεβλημένων μερών από το δίκτυο· καθώς μια επίθεση hacking μπορεί να περιλαμβάνει την απενεργοποίηση ορισμένων προφίλ ή θυρών στο τείχος

προστασίας ή ίσως ακόμη και την αποσύνδεση του εσωτερικού δικτύου από το Internet εντελώς. Οι συγκεκριμένες ενέργειες που θα εκτελεστούν θα εξαρτηθούν από τις περιστάσεις του συμβάντος.

Ιδιαίτερα (αλλά όχι αποκλειστικά) εάν υπάρχει υποψία για ύποπτες ενέργειες στο περιστατικό, πρέπει να τηρούνται ακριβή αρχεία των ενεργειών που έχουν αναληφθεί και των αποδεικτικών στοιχείων που συλλέγονται σύμφωνα με τις οδηγίες της ψηφιακής εγκληματολογίας (digital forensics). Οι βασικές αρχές αυτών των κατευθυντήριων γραμμών είναι οι εξής:

**Αρχή 1 -** Μην αλλάζετε κανένα στοιχείο. Εάν γίνει κάτι που έχει ως αποτέλεσμα την αλλοίωση των δεδομένων στο σχετικό σύστημα με οποιονδήποτε τρόπο, τότε αυτό θα επηρεάσει κάθε μεταγενέστερη δικαστική υπόθεση.

**Αρχή 2 -** Προσπελάστε τα αρχικά δεδομένα μόνο σε εξαιρετικές περιπτώσεις. Ένας εξειδικευμένος ειδικός θα χρησιμοποιήσει εργαλεία για να πάρει ένα κομμάτι των δεδομένων που διατηρούνται στη μνήμη, είτε πρόκειται για σκληρό δίσκο, μνήμη flash είτε για κάρτα SIM σε τηλέφωνο. Όλες οι αναλύσεις θα πραγματοποιηθούν στο αντίγραφο και το πρωτότυπο δεν θα πρέπει ποτέ να αγγιχτεί παρά μόνο σε εξαιρετικές περιπτώσεις π.χ. όταν ο χρόνος είναι ουσιαστικής σημασίας και η απόκτηση πληροφοριών για την πρόληψη περαιτέρω εγκληματικών ενεργειών είναι πιο σημαντική από τη διατήρηση των αποδεικτικών στοιχείων έγκυρα.

**Αρχή 3 -** Διατηρήστε πάντα μια καταγραφή ελέγχου για όσα έχουν γίνει.

**Αρχή 4 -** Ο υπεύθυνος πρέπει να διασφαλίσει ότι ακολουθούνται οι κατευθυντήριες γραμμές.

Πριν την άφιξη ενός ειδικού θα πρέπει να συλλέγονται βασικές πληροφορίες.

Αυτές μπορεί να περιλαμβάνουν

- Φωτογραφίες ή βίντεο των σχετικών μηνυμάτων ή των πληροφοριών
- Χειρόγραφα αρχεία της χρονολογίας του περιστατικού
- Πρωτότυπα έγγραφα, συμπεριλαμβανομένων και των αρχείων που γράφουν ποιος τα βρήκε, που και πότε
- Λεπτομέρειες μαρτύρων

Μόλις συλλεχθούν, τα αποδεικτικά στοιχεία θα κρατηθούν σε ένα ασφαλές μέρος όπου δεν θα μπορούν να αλλοιωθούν και θα εγκαθιδρυθεί μία επίσημη αλυσίδα επίβλεψης.

Τα αποδεικτικά στοιχεία μπορεί να απαιτούνται:

- Για μελλοντική ανάλυση ως προς την αιτία του συμβάντος
- Ως εγκληματολογικά αποδεικτικά στοιχεία για ποινικές ή αστικές διαδικασίες
- Για την υποστήριξη τυχόν διαπραγματεύσεων αποζημίωσης με προμηθευτές λογισμικού ή υπηρεσιών

Έπειτα θα πρέπει να εδραιωθεί μία ξεκάθαρη εικόνα του τι έχει συμβεί. πρέπει να εξακριβωθεί το εύρος του περιστατικού και η επίπτωση των συνεπειών πριν να ληφθούν οποιαδήποτε μέτρα περιορισμού.

Τα αρχεία καταγραφής ελέγχου μπορούν να εξεταστούν για να ενοποιήσουν την ακολουθία των γεγονότων. Θα πρέπει να ληφθεί μέριμνα ώστε να χρησιμοποιούνται μόνο ασφαλή αντίγραφα των αρχείων καταγραφής ελέγχου που δεν έχουν παραποιηθεί.

### *11*.6.2 Εξάλειψη

Οι ενέργειες για την αποκατάσταση των ζημιών που προκλήθηκαν από το περιστατικό, όπως η διαγραφή κακόβουλου λογισμικού, πρέπει να τεθούν μέσω της διαδικασίας διαχείρισης αλλαγών (ως επείγουσα αλλαγή εάν είναι απαραίτητο). Αυτές οι ενέργειες θα πρέπει να στοχεύουν στον προσδιορισμό της τρέχουσας αιτίας και στην αποτροπή επανάληψης του περιστατικού. Πρέπει να εντοπιστούν τυχόν ευπάθειες που έχουν αξιοποιηθεί ως μέρος του συμβάντος.

Ανάλογα με τον τύπο του συμβάντος, η εξάλειψη μπορεί μερικές φορές να είναι περιττή.

### 11.6.3 Ανάκτηση

Κατά τη διάρκεια της φάσης ανάκτησης, τα συστήματα θα πρέπει να επιστρέψουν στην κατάσταση πριν το περιστατικό, αν και θα πρέπει να πραγματοποιηθούν οι απαραίτητες ενέργειες για την αντιμετώπιση τυχόν τρωτών σημείων που χρησιμοποιήθηκαν ως μέρος του συμβάντος. Αυτό μπορεί να περιλαμβάνει δραστηριότητες όπως η εγκατάσταση ενημερώσεων, η αλλαγή των κωδικών πρόσβασης, η θωράκιση των servers (hardening) και η διόρθωση των διαδικασιών.

### 11.6.4 Γνωστοποίηση

Η γνωστοποίηση ενός περιστατικού ασφάλειας πληροφοριών και η απώλεια δεδομένων που προκύπτει είναι ένα ευαίσθητο θέμα το οποίο πρέπει να αντιμετωπιστεί προσεκτικά και με πλήρη έγκριση της διοίκησης. Η Ομάδα Απόκρισης σε Περιστατικά θα αποφασίσει, βάσει νομικών συμβουλών και άλλων συμβουλών από εμπειρογνώμονες και με όσο το δυνατόν πληρέστερη κατανόηση των επιπτώσεων του συμβάντος, ποιος τρόπος κοινοποίησης απαιτείται και τη μορφή που θα πάρει.

Το Π.Μ.Σ. θα είναι πάντοτε πλήρως συμμορφωμένο με τις εφαρμοστέες νομικές και κανονιστικές απαιτήσεις σχετικά με τη γνωστοποίηση των περιστατικών και θα αξιολογεί προσεκτικά τις προσφορές που θα γίνονται στα μέρη που πιθανόν να επηρεαστούν από το περιστατικό.

Τα αρχεία που συλλέγονται ως μέρος της απόκρισης στο περιστατικό μπορεί να απαιτούνται ως μέρος οποιωνδήποτε επακόλουθων ερευνών από τις αρμόδιες κανονιστικές αρχές και το Π.Μ.Σ. θα συνεργαστεί πλήρως με τέτοιες διαδικασίες.

## 11.7 Δραστηριότητες μετά το Περιστατικό

Ο Υπεύθυνος της Ομάδας θα αποφασίσει, με βάση τις τελευταίες πληροφορίες από τον Σύνδεσμο Επικοινωνίας του Περιστατικού και τα άλλα μέλη της ομάδας, το σημείο στο οποίο θα πρέπει να λήξουν οι ενέργειες της απόκρισης και η Ομάδα Απόκρισης να αποσυρθεί. Να σημειωθεί, ότι η ανάκτηση και η εκτέλεση των σχεδίων μπορεί να συνεχιστεί και μετά από αυτό το σημείο αλλά κάτω από λιγότερο επίσημο έλεγχο διαχείρισης.

Αυτή η απόφαση θα εξαρτηθεί από την κρίση του Υπεύθυνου της Ομάδας και θα πρέπει να βασιστεί στα παρακάτω κριτήρια:

- Η κατάσταση έχει επιλυθεί πλήρως ή είναι αρκετά σταθερή
- Ο ρυθμός της αλλαγής της κατάστασης έχει επιβραδυνθεί σε σημείο όπου απαιτούνται λίγες αποφάσεις
- Η κατάλληλη απόκριση είναι αρκετά καλά δρομολογημένη και τα σχέδια της ανάκαμψης προχωρούν σύμφωνα με το πρόγραμμα
- Ο βαθμός του κίνδυνου στον οργανισμό έχει μειωθεί σε αποδεκτό βαθμό
- Τα άμεσα νομικά και κανονιστικά καθήκοντα έχουν εκπληρωθεί

Εφόσον η ανάκαμψη από το περιστατικό είναι σε εξέλιξη ο Υπεύθυνος της Ομάδας θα πρέπει να καθορίσει τις επόμενες ενέργειες που πρέπει να λάβουν χώρα. Αυτές μπορεί να περιλαμβάνουν:

- Λιγότερο συχνές συναντήσεις της Ομάδας Απόκρισης σε Περιστατικά π.χ. εβδομαδιαία αναλόγως την περίσταση
- Ενημέρωση όλων των εμπλεκόμενων μελών για την απόσυρση της Ομάδας Απόκρισης σε Περιστατικά
- Εξασφάλιση ότι όλα τα αποδεικτικά έγγραφα του περιστατικού είναι ασφαλή
- Αίτημα προς όλο το προσωπικό που δεν εμπλέκεται σε περαιτέρω ενέργειες να επιστρέψει στα κανονικά του καθήκοντα

Όλες οι ενέργειες που έγιναν ως μέρος της απόσυρσης θα πρέπει να καταγραφούν.

Αφού αποσυρθεί η Ομάδα Απόκρισης σε Περιστατικά, ο Υπεύθυνος της Ομάδας θα διεξάγει μια ενημέρωση όλων των μελών, ιδανικά εντός 24 ωρών. Τα σχετικά αρχεία του περιστατικού θα εξεταστούν από την Ομάδα Απόκρισης σε Περιστατικά για να διασφαλιστεί ότι αντικατοπτρίζουν πραγματικά γεγονότα και αντιπροσωπεύουν πλήρη και ακριβή καταγραφή του συμβάντος.

Θα καταγραφούν οποιαδήποτε άμεσα σχόλια ή ανατροφοδότηση από την ομάδα.

Μία περισσότερο επίσημη ανασκόπηση μετά το περιστατικό θα διεξαχθεί σε χρόνο που θα αποφασιστεί από την ανώτατη διοίκηση ανάλογα με το μέγεθος και τη φύση του συμβάντος.

## 11.8 Διαδικασία γνωστοποίησης της παραβίασης των προσωπικών δεδομένων

Η παρακάτω διαδικασία καλύπτει τις απαιτήσεις του Άρθρου 33 (Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή) και του Άρθρου 34 (Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων)

Αυτή η διαδικασία θα χρησιμοποιηθεί σε περίπτωση που ένα περιστατικό κάποιου είδους έχει συμβεί που είχε ως αποτέλεσμα, ή θεωρείται ότι είχε ως αποτέλεσμα, την απώλεια προσωπικών δεδομένων για τα οποία ο οργανισμός είναι υπεύθυνος επεξεργασίας..

Είναι απαίτηση του Γενικού Κανονισμού Προστασίας Δεδομένων 2016 (ΓΚΠΔ) της ΕΕ ότι τα περιστατικά που επηρεάζουν τα προσωπικά δεδομένα και ενδέχεται να αποτελέσουν κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων θα πρέπει να αναφέρονται στην εποπτική αρχή προστασίας δεδομένων αμελλητί και, εφόσον είναι εφικτό, εντός 72 ωρών από τη στιγμή που αποκτάται γνώση του γεγονότος. Σε περίπτωση που η γνωστοποίηση δεν πραγματοποιείται εντός 72 ωρών, θα πρέπει να συνοδεύεται από αιτιολόγηση για την καθυστέρηση.

Σε περίπτωση που ένα περιστατικό επηρεάζει προσωπικά δεδομένα, θα πρέπει να ληφθεί μία απόφαση σχετικά με την έκταση, το χρόνο και το περιεχόμενο της επικοινωνίας με τα υποκείμενα των δεδομένων. Ο ΓΚΠΔ απαιτεί ότι η επικοινωνία θα πρέπει να λάβει χώρα «χωρίς αναίτια καθυστέρηση» αν μία παραβίαση δύναται να αποτελέσει «κίνδυνο υψηλού επιπέδου στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων».

Η ακριβής φύση ενός περιστατικού και ο αντίκτυπος που έχει δεν μπορούν να προβλεφθούν με κανένα βαθμό βεβαιότητας και επομένως είναι σημαντικό να χρησιμοποιηθεί σε ικανοποιητικό επίπεδο η κοινή λογική όταν αποφασίζεται τι πρέπει να γίνει.

**Διαδικασία Γνωστοποίησης Παραβίασης Προσωπικών Δεδομένων**

Μόλις αποφασιστεί ότι συνέβη μία παραβίαση προσωπικών δεδομένων, υπάρχουν δύο μέρη που απαιτείται βάσει του ΓΚΠΔ να ενημερωθούν. Αυτά είναι:

1. Η εποπτική αρχή
2. Τα υποκείμενα των δεδομένων που επηρεάζονται

Δε συνάγεται αυτομάτως ότι η παράβαση πρέπει να κοινοποιηθεί. Αυτό εξαρτάται από την αξιολόγηση του κινδύνου που αντιπροσωπεύει η παραβίαση στα «δικαιώματα και τις ελευθερίες των φυσικών προσώπων» (ΓΚΠΔ Άρθρο 33).

**Η Εποπτική Αρχή**

Η εποπτική αρχή για το εκπαιδευτικό ίδρυμα. σχετικά με το ΓΚΠΔ είναι:

| | |
|---|---|
| **Όνομα:** | Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα |
| **Διεύθυνση:** | Κηφισιάς 1-3, Τ.Κ.115 23, Αθήνα |
| **Τηλέφωνο:** | +30 210 6475600 |
| **Φαξ:** | +30 210 6475628 |
| **Email:** | contact@dpa.gr |

Ο ΓΚΠΔ ορίζει ότι μία παραβίαση προσωπικών δεδομένων θα πρέπει να γνωστοποιηθεί στην εποπτική αρχή «εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.» (ΓΚΠΔ Άρθρο 33). Αυτό απαιτεί ότι ο οργανισμός θα αξιολογήσει το επίπεδο του κινδύνου πριν αποφασίσει αν θα ειδοποιήσει ή όχι την αρχή.

Οι παράγοντες που εξετάζονται ως μέρος αυτής της αξιολόγησης κινδύνου θα πρέπει να περιλαμβάνουν:

- Αν τα προσωπικά δεδομένα ήταν κρυπτογραφημένα
- Εφόσον ήταν κρυπτογραφημένα, το πόσο «ισχυρή» ήταν η κρυπτογράφηση που χρησιμοποιήθηκε
- Το επίπεδο στο οποίο τα δεδομένα ήταν «ψευδωνυμοποιημένα» (δηλ. Εάν τα φυσικά πρόσωπα μπορούν να ταυτοποιηθούν, μέσω λογικών συμπερασμάτων, από τα δεδομένα)

- Τα στοιχεία που περιλαμβάνουν τα δεδομένα π.χ. όνομα, διεύθυνση, τραπεζικά στοιχεία, βιομετρικά στοιχεία
- Ο όγκος των εμπλεκόμενων δεδομένων
- Ο αριθμός των φυσικών προσώπων που επηρεάζονται
- Η φύση της παραβίασης, π.χ. κλοπή, τυχαία καταστροφή
- Άλλοι παράγοντες που θεωρούνται σχετικοί

Τα μέρη που εμπλέκονται σε αυτή την αξιολόγηση επικινδυνότητας μπορούν να περιλαμβάνουν εκπροσώπους από τους ακόλουθους τομείς, ανάλογα με τη φύση και τις περιστάσεις της παραβίασης των προσωπικών δεδομένων:

- Ανώτατη διοίκηση
- Ερευνητικές Δραστηριότητες
- Πληροφορική
- Ασφάλεια Πληροφοριών
- Νομικό τμήμα
- Υπεύθυνος Προστασίας Δεδομένων

Η μέθοδος αξιολόγησης κινδύνου, η επιχειρηματολογία της και τα συμπεράσματά της θα πρέπει να τεκμηριώνονται πλήρως και να υπογράφονται από την ανώτατη διοίκηση. Το αποτέλεσμα της αξιολόγησης κινδύνου πρέπει να περιλαμβάνει ένα από τα ακόλουθα συμπεράσματα:

1. Η παραβίαση των προσωπικών δεδομένων δεν απαιτεί γνωστοποίηση
2. Η παραβίαση των προσωπικών δεδομένων απαιτεί μόνο γνωστοποίηση στην εποπτική αρχή
3. Η παραβίαση των προσωπικών δεδομένων απαιτεί γνωστοποίηση τόσο στην εποπτική αρχή όσο και στα ενδιαφερόμενα πρόσωπα στα οποία αναφέρονται τα δεδομένα

Αυτά τα συμπεράσματα ενδέχεται να υπόκεινται σε αλλαγές που βασίζονται στην ανατροφοδότηση από την εποπτική αρχή και σε άλλες πληροφορίες που ανακαλύφθηκαν στο πλαίσιο της διεξαγόμενης έρευνας της παραβίασης.

**Πως θα ειδοποιηθεί η Εποπτική Αρχή**

Στην περίπτωση που έχει αποφασιστεί να ειδοποιηθεί η εποπτική αρχή, ο ΓΚΠΔ απαιτεί αυτό να γίνει «αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος» (ΓΚΠΔ Άρθρο 33). Εάν η καθυστέρηση γνωστοποίησης είναι αιτιολογημένη, η γνωστοποίηση θα πρέπει να συνοδεύεται από τους λόγους για τους οποίους υπήρξε η καθυστέρηση.

Η γνωστοποίηση πρέπει να παρέχεται με τα κατάλληλα ασφαλή μέσα στον φορέα, χρησιμοποιώντας το έντυπο Φόρμα Γνωστοποίησης Παραβίασης Προσωπικών Δεδομένων ως πρότυπο.

Οι παρακάτω πληροφορίες θα πρέπει να δίνονται ως μέρος της γνωστοποίησης:

1) Η φύση της παραβίασης των προσωπικών δεδομένων, συμπεριλαμβανομένου και, όπου είναι απαραίτητο:

i. Οι κατηγορίες και ο κατά προσέγγιση αριθμός των υποκειμένων των δεδομένων που εμπλέκονται

ii. Οι κατηγορίες και ο κατά προσέγγιση αριθμός των αρχείων των προσωπικών δεδομένων που εμπλέκονται

2) Το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες

3) Μία περιγραφή των ενδεχόμενων συνεπειών της παραβίασης των δεδομένων προσωπικού χαρακτήρα

4) Μία περιγραφή των ληφθέντων ή τα προτεινόμενων προς λήψη μέτρων για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

5) Αν η γνωστοποίηση δεν πραγματοποιηθεί εντός 72 ωρών, η αιτιολόγηση για την καθυστέρηση.

Η εποπτική αρχή πρέπει να δώσει γραπτή επιβεβαίωση της παραλαβής της γνωστοποίησης παραβίασης των προσωπικών δεδομένων, συμπεριλαμβανομένης της ημερομηνίας και της ώρας κατά την οποία ελήφθη. Όπου είναι απαραίτητο, ο ΓΚΠΔ επιτρέπει την παροχή πληροφοριών σε φάσεις χωρίς αδικαιολόγητη περαιτέρω καθυστέρηση.

Η τεκμηρίωση της παραβίασης των προσωπικών δεδομένων, συμπεριλαμβανομένων των επιπτώσεών της και των διορθωτικών ενεργειών που θα γίνουν, θα παραχθεί ως μέρος του εγγράφου Διαδικασία Απόκρισης σε Περιστατικά Ασφάλειας Πληροφοριών.

**Υποκείμενα των Δεδομένων**

**Απόφαση για το αν θα ειδοποιηθούν ή όχι τα υποκείμενα των δεδομένων**

Ο ΓΚΠΔ ορίζει ότι μία παραβίαση προσωπικών δεδομένων θα πρέπει να γνωστοποιείται στο υποκείμενο των δεδομένων «όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» (ΓΚΠΔ Άρθρο 34).

Η αξιολόγηση του κινδύνου που διεξήχθη προηγουμένως σε αυτή τη διαδικασία (παράγραφος 2.1.1) θα έχει καθορίσει κατά πόσον ο κίνδυνος για τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα είναι επαρκώς υψηλός ώστε να δικαιολογείται η γνωστοποίηση της παραβίασης σε αυτά.

Ωστόσο, αν έχουν ληφθεί μεταγενέστερα μέτρα για το μετριασμό του υψηλού κινδύνου για τα πρόσωπα στα οποία αναφέρονται τα δεδομένα, έτσι ώστε να μην είναι πλέον πιθανό να συμβεί, τότε δεν απαιτείται επικοινωνία με τα υποκείμενα των δεδομένων από το ΓΚΠΔ.

Η γνωστοποίηση στα επηρεαζόμενα υποκείμενα των δεδομένων δεν αποτελεί επίσης υποχρέωση από το ΓΚΠΔ, στην περίπτωση που «προϋποθέτει δυσανάλογες προσπάθειες» (ΓΚΠΔ Άρθρο 34). Ωστόσο, στη συγκεκριμένη περίπτωση θα πρέπει να χρησιμοποιείται αντ' αυτής μία μορφή δημόσιας επικοινωνίας.

Και πάλι, αυτό μπορεί να αλλάξει με βάση την ανατροφοδότηση από την εποπτική αρχή και άλλες πληροφορίες που ανακαλύπτονται ως μέρος της τρέχουσας έρευνας της παραβίασης.

**Πως θα γίνει η ειδοποίηση των υποκειμένων των δεδομένων**

Στη γνωστοποίηση στα υποκείμενα των δεδομένων που επηρεάστηκαν «θα πρέπει να περιγράφεται με σαφήνεια η φύση της παραβίασης των δεδομένων προσωπικού χαρακτήρα» (ΓΚΠΔ Άρθρο 34) και θα πρέπει να περιλαμβάνονται επίσης:

1) Το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες

2) Μία περιγραφή των ενδεχόμενων συνεπειών της παραβίασης των δεδομένων προσωπικού χαρακτήρα

3) Μία περιγραφή των ληφθέντων ή των προτεινόμενων προς λήψη μέτρων από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των προσωπικών δεδομένων, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

Πέραν των σημείων που απαιτούνται από το ΓΚΠΔ, μπορεί να είναι σκόπιμο να παρέχονται συμβουλές στο υποκείμενο των δεδομένων σχετικά με τις ενέργειες που μπορεί να αναλάβουν προκειμένου να μειώσουν τους κινδύνους που συνδέονται με την παραβίαση των προσωπικών δεδομένων.

Στις περισσότερες περιπτώσεις, θα ήταν σκόπιμο να ειδοποιηθούν τα επηρεαζόμενα υποκείμενα των δεδομένων μέσω επιστολής ή ηλεκτρονικού ταχυδρομείου ή και των δύο, προκειμένου να διασφαλιστεί ότι το μήνυμα έχει ληφθεί και ότι έχουν την ευκαιρία να λάβουν τα απαιτούμενα μέτρα.

# ΚΕΦΑΛΑΙΟ 12: ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ - ΓΕΝΙΚΑ ΕΝΤΥΠΑ

## 12.1 Πολιτική ασφάλειας των Πληροφοριών

«Η σημερινή εποχή συχνά αναφέρεται ως η "εποχή της πληροφορίας». Έχουμε δει μια τεράστια αλλαγή στον τρόπο με τον οποίο οι άνθρωποι παράγουν, αποθηκεύουν και ανταλλάσσουν πληροφορίες. Επίσης, έχουν μεταβληθεί ριζικά οι τρόποι με τους οποίους αλληλεπιδρούμε με τους άλλους, όχι μόνο ως άτομα, αλλά και εντός και μεταξύ των θεσμικών οργάνων, των κοινωνιών και των εθνών. Έχουμε αποκομίσει μεγάλα οφέλη από αυτή τη νέα εποχή, η οποία παράλληλα φέρνει μαζί της βαθύτατες προκλήσεις στους τομείς της ασφάλειας και της ιδιωτικότητας, οι οποίες αντικατοπτρίζονται στην ανάπτυξη της νομοθεσίας σε όλο τον κόσμο όσον αφορά τη διατήρηση των πληροφοριών.

Το Π.Μ.Σ «Οργάνωση και Διοίκηση Εκπαιδευτικών Μονάδων» του ΑΤΕΙΘ έχει ηθικό, νομικό και επαγγελματικό καθήκον να διασφαλίζει ότι οι πληροφορίες που κατέχει συμμορφώνονται με τις αρχές της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Πρέπει να διασφαλίσουμε ότι οι πληροφορίες που διατηρούμε ή είμαστε υπεύθυνοι γι' αυτές, προστατεύονται, όπου απαιτείται, από την ακατάλληλη αποκάλυψη, είναι ακριβείς, έγκαιρες, ανάλογες και είναι διαθέσιμες σε όσους θα πρέπει να έχουν πρόσβαση σε αυτές.

Για την εξυπηρέτηση των παραπάνω, το Π.Μ.Σ. αναγνωρίζει τους Κινδύνους που απειλούν την Ασφάλεια των Πληροφοριών που παράγονται και διακινούνται στο πλαίσιο των δραστηριοτήτων της και διαθέτει όλους τους απαιτούμενους πόρους ώστε να προστατεύσει τις πληροφορίες της.

Αυτή η πολιτική ισχύει και θα κοινοποιείται σε όλο το προσωπικό και στα τρίτα μέρη που αλληλεπιδρούν με πληροφορίες που κατέχει το Π.Μ.Σ. και τα πληροφοριακά συστήματα που χρησιμοποιούνται για την αποθήκευση και την επεξεργασία τους. Αυτό περιλαμβάνει, αλλά δεν περιορίζεται σε, οποιαδήποτε συστήματα ή δεδομένα που συνδέονται με τα δεδομένα ή τα τηλεφωνικά δίκτυα του Π.Μ.Σ., συστήματα που διαχειρίζεται το Π.Μ.Σ., κινητές συσκευές που χρησιμοποιούνται για τη σύνδεση με τα δίκτυα του Π.Μ.Σ. ή τη διατήρηση δεδομένων του Π.Μ.Σ., δεδομένα για τα οποία το Π.Μ.Σ. κατέχει δικαιώματα πνευματικής ιδιοκτησίας, δεδομένα για τα οποία το Π.Μ.Σ. είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, επικοινωνίες που αποστέλλονται προς ή από το Π.Μ.Σ..

Η **δέσμευση** για την Ασφάλεια Πληροφοριών και για την αποφυγή περιστατικών που μπορούν να την πλήξουν υλοποιείται μέσω των ακόλουθων επιμέρους βημάτων:

- Προστασία των πόρων και της διακινούμενης πληροφορίας στις υπηρεσίες του Π.Μ.Σ. από κάθε απειλή, εσωτερική ή εξωτερική, σκόπιμη ή τυχαία,
- Συστηματική αποτίμηση και αξιολόγηση των κινδύνων που αφορούν στη διασφάλιση πληροφοριών, προσβλέποντας στην ορθή και έγκαιρη διαχείρισή τους,
- Ασφαλείς διαδικασίες ανάπτυξης και συντήρησης εφαρμογών, συστημάτων και υπηρεσιών,
- Αρχειοθέτηση δεδομένων, αποφυγή ιών και εξωτερικών εισβολών, έλεγχο πρόσβασης στα συστήματα, καταγραφή όλων των περιστατικών ασφαλείας και διαχείριση απρόσμενων εξελίξεων,
- Διαρκή ενημέρωση του προσωπικού σε θέματα ασφάλειας πληροφοριών,
- Έλεγχο των διακινούμενων και ανταλλασσόμενων πληροφοριών και δεδομένων,
- Προστασία των συμφερόντων του Π.Μ.Σ. και όσων συναλλάσσονται με αυτόν και τον εμπιστεύονται,
- Άμεσο και αποτελεσματικό χειρισμό περιστατικών και παραβάσεων ασφαλείας,
- Ενθάρρυνση της εσωτερικής επικοινωνίας σχετικά με τα θέματα Ασφάλειας Πληροφοριών.
- Δέσμευση στην πιστή εφαρμογή των Πολιτικών Ασφάλειας και όλης της κείμενης εθνικής και κοινοτικής νομοθεσίας.

Το Π.Μ.Σ. δεσμεύεται για τη συνεχή προσπάθεια βελτίωσης της προστασίας των πληροφοριών της έτσι ώστε να μπορεί να προσφέρει υψηλά επίπεδα ασφάλειας σε όσους συναλλάσσονται με το Π.Μ.Σ..

Επιπλέον, το Π.Μ.Σ. έχει αναπτύξει και εφαρμόζει Πολιτικές Ασφάλειας Πληροφοριών για θέματα Αποδεκτής Χρήσης, Φυσικής Ασφάλειας, Ελέγχου Πρόσβασης, Ελέγχου Απομακρυσμένης Πρόσβασης, Ασφάλειας Συνεργατών-Προμηθευτών, Διαχείρισης Αποθηκευτικών Μέσων, Αντιμετώπισης Κακόβουλου Λογισμικού, Χρήσης Κρυπτογραφίας και άλλα.

Οι πολιτικές ασφάλειας πληροφοριών αναθεωρούνται τουλάχιστον μία φορά το χρόνο και όποτε λάβουν χώρα σοβαρές αλλαγές, ώστε να εξασφαλιστεί η καταλληλότητα, η επάρκεια και η αποτελεσματικότητά τους.

## Δέσμευση

Οι ακόλουθες **αρχές ασφάλειας πληροφοριών** παρέχουν τη διακυβέρνηση για την ασφάλεια και τη διαχείριση των πληροφοριών στο Π.Μ.Σ.**:**

1. Οι πληροφορίες πρέπει να διαβαθμίζονται σύμφωνα με το κατάλληλο επίπεδο εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας και σύμφωνα με τις σχετικές νομοθετικές, ρυθμιστικές και συμβατικές απαιτήσεις και τις πολιτικές ασφάλειας πληροφοριών του Π.Μ.Σ.**.**
2. Το προσωπικό πρέπει να εξασφαλίζει τη διαβάθμιση των πληροφοριών, πρέπει να χειρίζεται τις πληροφορίες αυτές σύμφωνα με το επίπεδο διαβάθμισης και πρέπει να συμμορφώνεται με τυχόν συμβατικές απαιτήσεις, πολιτικές, διαδικασίες ή συστήματα για την εκπλήρωση αυτών των ευθυνών.
3. Όλοι οι χρήστες που καλύπτονται από το πεδίο εφαρμογής αυτής της πολιτικής πρέπει να χειρίζονται τις πληροφορίες κατάλληλα και σύμφωνα με το επίπεδο διαβάθμισης.
4. Οι πληροφορίες πρέπει να είναι ασφαλείς και διαθέσιμες σε όσους έχουν νόμιμη ανάγκη πρόσβασης σύμφωνα με το επίπεδο διαβάθμισης. Ως εκ τούτου, η πρόσβαση στην πληροφορία θα βασίζεται στις αρχές “least privilege” και “need to know”.
5. Οι πληροφορίες θα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και επεξεργασία σύμφωνα με το επίπεδο διαβάθμισης.
6. Οι παραβιάσεις αυτής της πολιτικής πρέπει να αναφέρονται στον Υπεύθυνο Διαχείρισης Ασφάλειας Πληροφοριών.
7. Η πρόβλεψη ασφάλειας πληροφοριών και οι πολιτικές που την καθοδηγούν θα επανεξετάζονται τακτικά, μεταξύ άλλων μέσω της χρήσης ετήσιων εσωτερικών ελέγχων και δοκιμών παρείσδυσης.

Η πολιτική ασφάλειας πληροφοριών του Π.Μ.Σ. παρέχει το πλαίσιο με το οποίο λαμβάνουμε υπόψη αυτές τις αρχές. Πρωταρχικός σκοπός του είναι να επιτρέψει σε όλο το προσωπικό του Π.Μ.Σ. να κατανοεί τόσο τις νομικές όσο και δεοντολογικές ευθύνες που αφορούν την πληροφορία και να το ενδυναμώνει να συλλέγει, να χρησιμοποιεί, να αποθηκεύει και να διανέμει τις πληροφορίες με τους κατάλληλους τρόπους.

Αυτή η πολιτική αποτελεί τον ακρογωνιαίο λίθο για τη συνεχιζόμενη δέσμευση του Π.Μ.Σ. για την υλοποίηση και τη διατήρηση των υψηλότερων προτύπων ασφάλειας σε ολόκληρο τον οργανισμό και για την ενίσχυση και αποσαφήνιση των διαδικασιών ασφάλειας των πληροφοριών μας. Έχει την πλήρη υποστήριξή μου και περιμένω από όλο το προσωπικό του Π.Μ.Σ. να μοιραστεί αυτή τη δέσμευση, να διαβάσει την Πολιτική Ασφάλειας Πληροφοριών και να συμμορφωθεί με αυτήν κατά τη διάρκεια της τέλεσης των καθηκόντων τους.

**Όνομα Επώνυμο**

**Επιστημονικός Υπεύθυνος Π.Μ.Σ»**

## 12.2 Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού – Κατευθυντήριες γραμμές για την ανάπτυξη λογισμικού

Η αρχή "***προστασία των δεδομένων ήδη από το σχεδιασμό***" βασίζεται στην αντίληψη, ότι η δημιουργία λειτουργιών προστασίας δεδομένων από την αρχή της διαδικασίας σχεδιασμού είναι προτιμότερη σε σχέση με την προσπάθεια να προσαρμοστεί ένα προϊόν ή μια διαδικασία σε επόμενο στάδιο. Η εμπλοκή στη διαδικασία του σχεδιασμού υποστηρίζει την εξέταση ολόκληρου του κύκλου ζωής των δεδομένων και της χρήσης τους. Οι αρχές προστασίας των δεδομένων είναι η διαφάνεια, η ελαχιστοποίηση των δεδομένων, η σύνδεση με το σκοπό και η ασφάλεια των δεδομένων. Η ασφάλεια των δεδομένων έχει να κάνει με τις τεχνολογίες/τεχνικές που χρησιμοποιούνται έτσι ώστε να προστατεύσουν τα δεδομένα, όπως η ψευδωνυμοποίηση, η κρυπτογράφηση, η εμπιστευτικότητα, η ακεραιότητα, η ανθεκτικότητα, η δυνατότητα ανάκτησης, η δυνατότητα επαλήθευσης/καταγραφής. Τα φυσικά πρόσωπα έχουν συγκεκριμένα δικαιώματα όσον αφορά τα δεδομένα τους, όπως πληροφόρηση/διαφάνεια, συγκατάθεση/εναντίωση, γνωστοποίηση, διόρθωση, διαγραφή, περιορισμός της επεξεργασίας και φορητότητα των δεδομένων.

Η αρχή "***προστασία των δεδομένων εξ ορισμού***" σημαίνει ότι το προκαθορισμένο περιβάλλον του χρήστη είναι ήδη προστατευμένο από κινδύνους που αφορούν την προστασία των δεδομένων και την ιδιωτικότητα. Αυτό αναφέρεται στον περιορισμό των δεδομένων ως προς το σκοπό της επεξεργασίας, το πεδίο εφαρμογής, το διάστημα αποθήκευσης και την προσβασιμότητα.

### 12.2.1 Στρατηγικές προστασίας των δεδομένων ήδη από το σχεδιασμό

**Στρατηγικές προσανατολισμένες στα δεδομένα**

Οι ακόλουθες τέσσερις στρατηγικές που είναι προσανατολισμένες στα δεδομένα μπορούν να υποστηρίξουν το στόχο προστασίας που επιτυγχάνεται καθιστώντας αδύνατη τη συσχέτιση των δεδομένων και μπορούν πρωτίστως να κατευθύνουν τις αρχές της αναγκαιότητας και της ελαχιστοποίησης των δεδομένων.

- **Ελαχιστοποίηση**

Η ποσότητα των προσωπικών δεδομένων που τίθεται υπό επεξεργασία πρέπει να είναι περιορισμένη στη μικρότερη δυνατή. Η εφαρμογή της στρατηγικής της «Ελαχιστοποίησης» σημαίνει ότι θα πρέπει να απαντηθεί εάν η επεξεργασία των προσωπικών δεδομένων είναι ανάλογη (σε σχέση με το σκοπό) και αν δεν υπάρχουν άλλα, λιγότερο επεμβατικά, μέσα για την επίτευξη του ίδιου σκοπού.

- **Απόκρυψη**

Όλα τα προσωπικά δεδομένα, και οι αλληλεξαρτήσεις τους, δεν πρέπει να βρίσκονται σε κοινή θέα. Η λογική αυτής της στρατηγικής είναι ότι, αποκρύπτοντας τα προσωπικά δεδομένα, δεν είναι εύκολη η εκμετάλλευσή τους.

Επί της ουσίας, η στρατηγική «Απόκρυψης» στοχεύει στην αδυναμία συσχέτισης των δεδομένων και στην αδυναμία παρακολούθησής τους. Η αδυναμία συσχέτισης σε αυτήν την περίπτωση διασφαλίζει ότι δεν μπορεί να γίνει η σύνδεση μεταξύ δύο γεγονότων.

- **Διαχωρισμός**

Τα προσωπικά δεδομένα πρέπει να τίθενται υπό επεξεργασία με κατανεμημένο τρόπο, σε ξεχωριστά τμήματα, όταν είναι δυνατόν. Διαχωρίζοντας την επεξεργασία ή την αποθήκευση διάφορων πηγών προσωπικών δεδομένων που ανήκουν στο ίδιο πρόσωπο, δεν είναι δυνατή η δημιουργία ολοκληρωμένων προφίλ του προσώπου. Επιπλέον, ο διαχωρισμός είναι μια καλή μέθοδος για την επίτευξη του περιορισμού του σκοπού. Η στρατηγική του διαχωρισμού δημιουργεί την ανάγκη για ξεχωριστές διαδικασίες επεξεργασίας αντί για γενικές λύσεις. Συγκεκριμένα, τα δεδομένα από διαφορετικές πηγές θα πρέπει να αποθηκεύονται σε διαφορετικές βάσεις δεδομένων, οι οποίες δεν πρέπει να συνδέονται μεταξύ τους. Οι πίνακες των βάσεων δεδομένων θα πρέπει να διαχωρίζονται, όπου είναι δυνατό. Οι σειρές αυτών των πινάκων δε θα πρέπει να συνδέονται μεταξύ τους με ευκολία, για παράδειγμα με την

αφαίρεση οποιονδήποτε αναγνωριστικών, ή με τη χρήση ειδικών ψευδώνυμων για κάθε πίνακα.

- **Συγκέντρωση (πληροφοριών)**

Η επεξεργασία των προσωπικών δεδομένων πρέπει να γίνεται στο υψηλότερο επίπεδο συγκέντρωσης και με τις λιγότερες δυνατές λεπτομέρειες, που το καθιστούν (ακόμη) χρήσιμο. Η συγκέντρωση των πληροφοριών για τις ομάδες χαρακτηριστικών ή τις ομάδες των ατόμων, περιορίζει την ποσότητα των λεπτομερειών που απομένουν. Επομένως, η πληροφορία γίνεται λιγότερο ευαίσθητη, εφόσον οι πληροφορίες είναι αρκετά χονδροειδείς (coarse grained), και το μέγεθος της ομάδας στην οποία συγκεντρώνονται είναι αρκετά μεγάλο. Σε αυτό το σημείο χονδροειδή δεδομένα (coarse grained data) σημαίνει ότι τα δεδομένα είναι τόσο γενικά ώστε η πληροφορία που περιέχουν μπορεί να σχετίζεται με πολλά άτομα ενώ λίγες πληροφορίες μπορούν να ταυτοποιήσουν ένα μοναδικό άτομο, προστατεύοντας έτσι τα δεδομένα του.

### 12.2.2. Στρατηγικές προσανατολισμένες στη διαδικασία

- **Ενημέρωση**

Αντιστοιχεί στην υψηλής σημασίας έννοια της διαφάνειας. Τα υποκείμενα των δεδομένων πρέπει να είναι επαρκώς ενημερωμένα όταν γίνεται επεξεργασία των δεδομένων τους. Κάθε φορά που τα υποκείμενα των δεδομένων χρησιμοποιούν ένα σύστημα, θα πρέπει να ενημερώνονται για το ποιες πληροφορίες τίθενται υπό επεξεργασία, για ποιο σκοπό και από ποια μέσα. Αυτό περιλαμβάνει πληροφορίες για τους τρόπους προστασίας των πληροφοριών και διαφάνεια της ασφάλειας του συστήματος. Τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται επίσης για τα τρίτα μέρη στα οποία κοινοποιούνται οι πληροφορίες. Θα πρέπει επίσης να ενημερώνονται για τα δικαιώματά τους σχετικά με την πρόσβαση στα δεδομένα τους και πως να τα ασκήσουν.

- **Έλεγχος**

Θα πρέπει να δίνεται στα φυσικά πρόσωπα η δυνατότητα παρέμβασης στην επεξεργασία των προσωπικών τους δεδομένων. Η στρατηγική του «Ελέγχου» αποτελεί για την ακρίβεια σημαντικό μέρος της στρατηγικής της «Ενημέρωσης». Χωρίς λογικά μέσα ελέγχου των προσωπικών δεδομένων ενός ατόμου, δεν υπάρχει μεγάλη χρησιμότητα στην ενημέρωση του φυσικού προσώπου για το γεγονός ότι συλλέγονται τα προσωπικά του δεδομένα. Η νομοθεσία για την προστασία των δεδομένων συχνά δίνει στο υποκείμενο των δεδομένων το

δικαίωμα να δει, να ενημερώσει ακόμα και να ζητήσει τη διαγραφή των προσωπικών δεδομένων που συλλέγονται γι' αυτό.

- **Εφαρμογή**

Θα πρέπει να υπάρχει και να εφαρμόζεται μία πολιτική για την ιδιωτικότητα που θα συμμορφώνεται με τις νομικές απαιτήσεις. Αυτό σχετίζεται με την αρχή της λογοδοσίας. Η στρατηγική της «Εφαρμογής» εξασφαλίζει ότι υπάρχει μία πολιτική για την ιδιωτικότητα. Αυτό είναι ένα σημαντικό βήμα για να διασφαλιστεί ότι ένα σύστημα σέβεται την ιδιωτικότητα κατά τη λειτουργία του. Φυσικά, το πραγματικό επίπεδο προστασίας της ιδιωτικότητας εξαρτάται από την πραγματική πολιτική. Η πολιτική αυτή θα πρέπει να είναι τουλάχιστον συμμορφωμένη με τις νομικές απαιτήσεις. Ως αποτέλεσμα, η στρατηγική αυτή καλύπτει και τον περιορισμό του σκοπού. Αυτό υποδηλώνει, ότι τουλάχιστον υπάρχουν οι κατάλληλοι μηχανισμοί προστασίας που αποτρέπουν τις παραβιάσεις της πολιτικής. Ακόμη, πρέπει να εφαρμοστούν οι κατάλληλες κυβερνητικές δομές ώστε να επιβάλουν αυτήν την πολιτική.

- **Απόδειξη**

Απαιτεί την ικανότητα ενός υπεύθυνου επεξεργασίας να αποδείξει τη συμμόρφωση με την πολιτική για την ιδιωτικότητα και άλλες ισχύουσες νομικές απαιτήσεις. Η στρατηγική αυτή υποστηρίζει την αρχή της λογοδοσίας. Προχωράει ένα βήμα παραπάνω από τη στρατηγική της «Εφαρμογής», δεδομένου ότι απαιτεί από τον υπεύθυνο επεξεργασίας να αποδείξει ότι έχει τον έλεγχο. Αυτό απαιτείται ρητά από το νέο έγγραφο του Ευρωπαϊκού κανονισμού για την ιδιωτικότητα. Συγκεκριμένα, απαιτεί από τον υπεύθυνο επεξεργασίας να είναι σε θέση να δείξει πως η πολιτική για την ιδιωτικότητα έχει εφαρμοστεί εντός του πληροφοριακού συστήματος. Σε περίπτωση παραπόνων ή προβλημάτων θα πρέπει να μπορεί να αποφασίσει αμέσως το εύρος πιθανών παραβιάσεων.

## 12.3 Αιτιολογικές Σκέψεις και Άρθρα του ΓΚΠΔ που επηρεάζουν το Λειτουργικό και Τεχνικό Σχεδιασμό και τις Απαιτήσεις του Κύκλου Ζωής Ασφαλούς Ανάπτυξης (SDLC).

**12.3.1. Η εφαρμογή της προστασίας των δεδομένων στο σύστημα και στον οργανισμό, ήδη από το σχεδιασμό και εξ ορισμού, είναι νομική απαίτηση:**

Αιτιολογική Σκέψη 78 και Άρθρο 25

**12.3.2. Τα δεδομένα είναι ασφαλή και η ακεραιότητα και η εμπιστευτικότητα διατηρούνται με τη χρήση τεχνικών και οργανωτικών μέτρων υπό τη διαχείριση του υπεύθυνου επεξεργασίας:**

Αιτιολογική Σκέψη 49 και Άρθρα 5-1(στ), 32-1(β-δ)

**12.3.3. Όπου είναι δυνατό, θα πρέπει να χρησιμοποιείται η κρυπτογράφηση των δεδομένων:**

Αιτιολογική Σκέψη 83 και Άρθρα 6-4(ε), 32-1(α)

**12.3.4. Όπου είναι δυνατό, θα πρέπει να χρησιμοποιείται η ψευδωνυμοποίηση των δεδομένων:**

Αιτιολογικές Σκέψεις 26, 28, 29, 78 και Άρθρα 6-4(ε), 25-1, 32-1(α)

**12.3.5. Τα δεδομένα θα πρέπει να είναι ανώνυμα, όπου είναι δυνατό:**

Αιτιολογική Σκέψη 26

**12.3.6. Τα χαρακτηριστικά της επεξεργασίας και τα βήματα (της επεξεργασίας) θα πρέπει να παρέχονται στο φυσικό πρόσωπο σε μορφή εύκολα κατανοητή τη στιγμή της συλλογής των δεδομένων, ηλεκτρονικά ή εγγράφως:**

Αιτιολογικές Σκέψεις 39, 58 και Άρθρα 12-1, 13-2(α-στ)

**12.3.7. Τα φυσικά πρόσωπα θα πρέπει να έχουν συνεχώς το δικαίωμα της πρόσβασης και της αναθεώρησης της επεξεργασίας των δεδομένων τους:**

Αιτιολογικές Σκέψεις 58, 61, 63 και Άρθρα12, 15-1(α, δ)

**12.3.8. Διαχωρισμός των στοιχείων των δεδομένων που μπορούν να θεωρηθούν προσωπικά δεδομένα ή κατάρτιση προσωπικού προφίλ, αν τεθούν υπό επεξεργασία ή αν συνδυαστούν ξεχωριστά ή μαζί οδηγώντας σε παράνομες ενέργειες:**

Αιτιολογική Σκέψη 30

**12.3.9. Θα πρέπει να είναι δυνατή η φορητότητα των δεδομένων, που αφορούν ένα φυσικό πρόσωπο, σε άλλον πάροχο (ή ενδεχομένως ακόμη και σε ανταγωνιστή):**

Αιτιολογική Σκέψη 68 και Άρθρα 13-2(β), 14-2(γ), 20

**12.3.10. Το φυσικό πρόσωπο θα πρέπει να έχει δικαίωμα στην αντιγραφή των δεδομένων του σε ευρέως χρησιμοποιούμενη μορφή:**

Άρθρο 15-3

**12.3.11. Το φυσικό πρόσωπο θα πρέπει να έχει το δικαίωμα στην επικαιροποίηση των δεδομένων του, χωρίς χρέωση, σε περίπτωση που υπάρχει λάθος:**

Αιτιολογικές Σκέψεις 59, 65 και Άρθρο 16, και, το φυσικό πρόσωπο θα πρέπει να έχει το δικαίωμα ηλεκτρονικής υποβολής των αιτημάτων επικαιροποίησης, Αιτιολογική Σκέψη 59

**12.3.12. Το υποκείμενο των δεδομένων θα πρέπει να έχει το δικαίωμα διαγραφής των δεδομένων του χωρίς αναίτια καθυστέρηση:**

Αιτιολογικές Σκέψεις 59, 65 και Άρθρα 13-2(β), 14-2(β), 17, και, το φυσικό πρόσωπο θα πρέπει να έχει το δικαίωμα ηλεκτρονικής υποβολής των αιτημάτων διαγραφής, Αιτιολογική Σκέψη 59 (*Σημείωση: Υπάρχουν ειδικές εξαιρέσεις σε αυτό το δικαίωμα που περιέχονται στο ΓΚΠΔ.)*

**12.3.13. Ο υπεύθυνος επεξεργασίας των δεδομένων θα πρέπει να ενημερώνει τους άλλους οργανισμούς Πληροφορικής που κρατούν τα δεδομένα του φυσικού προσώπου ότι το φυσικό πρόσωπο αιτήθηκε τη διαγραφή των δεδομένων:**

Αιτιολογική Σκέψη 66 και Άρθρο 19 (*Επομένως, το τμήμα Πληροφορικής θα πρέπει να γνωρίζει που αποθηκεύονται όλα τα δεδομένα του φυσικού προσώπου από τρίτα μέρη, έτσι ώστε εκείνοι να μπορούν να ειδοποιηθούν για το αίτημα διαγραφής των δεδομένων. Η συνεχής ενημέρωση των εσωτερικών και εξωτερικών αρχείων δεδομένων είναι ύψιστης σημασίας.)*

**12.3.14. Το φυσικό πρόσωπο θα πρέπει να έχει το δικαίωμα εναντίωσης στην επεξεργασία, ανάκλησης της συγκατάθεσης στην επεξεργασία και δυνατότητα εξαίρεσης από την επεξεργασία (opt-out). Και το υποκείμενο των δεδομένων μπορεί να αντιταχθεί ή να άρει τη συγκατάθεση του για τα θέματα επεξεργασίας ηλεκτρονικά:**

Αιτιολογικές Σκέψεις 59, 63 και Άρθρα 7-3, 18, 21 (Και με την τεχνική πρόταση του Ευρωπαϊκού Συμβουλίου: *Αιτιολογική Σκέψη 67)*

**12.3.15.Τα δεδομένα αποθηκεύονται μόνο για το διάστημα που απαιτείται για την εκπλήρωση των στόχων του υποκειμένου των δεδομένων. Τα μη ενημερωμένα προσωπικά δεδομένα δεν πρέπει να αποθηκεύονται. (Μέρος της στρατηγικής Διαχείρισης Ηλεκτρονικών Αρχείων). Και το φυσικό πρόσωπο θα πρέπει να ειδοποιείται**

**για αυτήν τη χρονική περίοδο ή τον τρόπο υπολογισμού της, τη στιγμή που συλλέγονται τα δεδομένα:**

Αιτιολογικές Σκέψεις 39, 45 και Άρθρα 13-2(α), 14-2(α), 25-2

**12.3.16. Μία απόφαση θα πρέπει να λαμβάνεται, σχεδόν αμέσως, σε περίπτωση που μία παραβίαση δεδομένων πιθανόν να αποτελεί «υψηλό κίνδυνο στα δικαιώματα και τις ελευθερίες του φυσικού προσώπου» για αυτό το σκοπό ένα τεχνικό περιβάλλον θα πρέπει να υπάρχει για να αναγνωρίζει, να παρακολουθεί και να αξιολογεί τέτοιες παραβιάσεις:**

Αιτιολογικές Σκέψεις 85, 86 (σχετικά με τις υποχρεώσεις της ειδοποίησης), 87 (Σημείωση: πολλά Άρθρα, π.χ. 33, 34) στο ΓΚΠΔ απευθύνονται στις υποχρεώσεις γνωστοποίησης προς το υποκείμενο των δεδομένων και τις αρχές, σχετικά με αυτό το θέμα.

# ΣΥΖΗΤΗΣΗ-ΣΥΜΠΕΡΑΣΜΑΤΑ

Η πρόσφατη δραστηριότητα σχετικά με τις παραβιάσεις δεδομένων που υφίστανται οργανισμοί αλλά και ιδιώτες συνεχίζει να καθιστά τον τομέα προστασίας προσωπικών δεδομένων ένα θέμα άμεσης προτεραιότητας για τους εκπαιδευτικούς φορείς. Είναι σημαντικό ο φορέας να έχει μια σαφή και κατανοητή πολιτική χειρισμού προσωπικών δεδομένων, προκειμένου να ελαχιστοποιήσει τον κίνδυνο παραβίασης τους. Μια παραβίαση είναι δυνατό να προκύψει από κλοπή, σκόπιμη επίθεση στα πληροφοριακά συστήματά του φορέα, μη εξουσιοδοτημένη ή κακόβουλη χρήση προσωπικών δεδομένων από μέλος του προσωπικού, τυχαία απώλεια ή αποτυχία/αστοχία του εξοπλισμού.

Η υιοθέτηση διαδικασιών και «καλών πρακτικών» μέσα στα πλαίσια του ΓΚΠΔ είναι κομβικής αξίας για την ομαλή λειτουργία μιας εκπαιδευτικής μονάδας. Διασφαλίζει την διατήρηση της καλής φήμης της εκπαιδευτικής μονάδας και προασπίζει την ομαλή λειτουργία του περιορίζοντας τον κίνδυνο διαρροών. Το γεγονός ότι ο ΓΚΠΔ εφαρμόστηκε πρόσφατα και σε χώρες όπως η Ελλάδα ο εφαρμοστικός νόμος παραμένει σε διαβούλευση, δυσχεράνει ακόμα περισσότερο τη δημιουργία και εφαρμογή ενός γενικότερου συστήματος που θα λειτουργούσε ως δείκτης ποιότητας για το Π.Μ,Σ στη συγκεκριμένη περίπτωση. Ταυτόχρονα, η έλλειψη εμπειρικών δεδομένων κάθε άλλο παρά βοηθητική μπορεί να χαρακτηριστεί.

Η πρωτοτυπία της συγκεκριμένης διπλωματικής εργασίας έγκειται στο γεγονός ότι προσπαθεί να προτείνει ένα ολοκληρωμένο σύστημα ποιότητας, θεσπίζοντας διαδικασίες και σχεδιάζοντας έγγραφα, η εφαρμογή των οποίων θα εξυπηρετήσει τη συμμόρφωση του φορέα με τις απαιτήσεις του κανονισμού, ελαχιστοποιώντας τον κίνδυνο επιβολής προστίμου.

Ταυτόχρονα, η δημιουργία ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) εξασφαλίζει στον φορέα που τον υλοποιεί:

 Δημιουργία κουλτούρας Ασφάλειας Πληροφοριών

 Απτή και Εφαρμόσιμη Ασφάλεια των Πληροφοριών που ο εκπαιδευτικός φορέας έχει στην κατοχή του και αφορά όλα τα συνεργαζόμενα – συμβαλλόμενα μέρη (φοιτητές, εσωτερικοί και εξωτερικοί συνεργάτες, καθηγητές, υπάλληλοι/γραμματείες, άλλες δομές του ΑΤΙΕΘ εκτός Π.Μ.Σ που υποχρεωτικά έχουν πρόσβαση στα προσωπικά δεδομένα που ο εκπαιδευτικός φορέας διαχειρίζεται.

 Εξασφαλίζεται η προστασία των πληροφοριακών συστημάτων των υποδομών (και φυσική πρόσβαση), των δικτύων και των επικοινωνιών.

 Εντοπισμός όλων των ενδιαφερομένων μερών, καταγραφή απαιτήσεων αλλά και προσπάθεια ικανοποίησής τους.

Με τελικό σκοπό

 την τήρηση των απαιτήσεων του ISO 27001:2013 και συμμόρφωση με το κανονιστικό και ρυθμιστικό πλαίσιο καθώς και με την Ελληνική και Ευρωπαϊκή Νομοθεσία.

Κατά τη διάρκεια υλοποίησης του ΣΔΑΠ θα πρέπει ο εκπαιδευτικός φορέας να :

1. Συντάξει Πολιτικές, Οδηγίες και Διαδικασίες,

2. Να σχεδιάζει και να υλοποιεί Σχέδια Επιχειρησιακής Συνέχειας που θα αφορούν τις χρήσιμες υπηρεσίες, θα αναφέρεται ο χρόνος αντίδρασης αλλά και οι διαδικασίες ανάκτησης,

3. Να εντοπίζει και να διαχειρίζεται τους Κινδύνους,

4. Να έχει καταγεγραμμένες Πληροφορίες (Αρχεία, Διαγράμματα & Αναφορές, Έλεγχος Προσβάσεων, Διαδικασίες Ενημέρωση της Διοίκησης και Πλάνο Ασφάλειας) ,

5. Να έχει θεσπίσει και να εφαρμόζει διαδικασίες για τη Διαχείριση Συμβολαίων, να εκτελεί Εσωτερική Επιθεώρηση και Επιθεώρηση Πληροφορικών Συστημάτων και να διασφαλίζει την Φυσική Ασφάλεια των Πληροφοριών,

6. Να εξασφαλίζει τη διαρκή Εκπαίδευση, να οριοθετεί ξεκάθαρα τους Ρόλους & τις Αρμοδιότητες, να προάγει την Ευαισθητοποίηση των συνεργαζόμενων μερών.

Η υιοθέτηση του παραπάνω συστήματος θα έχει ως αποτέλεσμα τη Διαρκής Εκπαίδευση του CISO αλλά και την προετοιμασία όλων για την επιθεώρηση του φορέα Πιστοποίησης.

Καίριας σημασίας βήμα για την υλοποίηση του ΣΔΑΠ είναι η διατύπωση, υιοθέτηση και τελικά εφαρμογή των διαφόρων πολιτικών που αφορούν πλήθος διαδικασιών.

Γενικά γίνεται αναφορά στην:

1. Γενική Πολιτική Ασφάλειας Πληροφοριών

2. Πολιτική Ασφάλειας Συνεργατών-Προμηθευτών

3.Πολιτική Διαχείρισης Αποθηκευτικών Μέσων

4. Πολιτική Ανθρωπίνων πόρων

5. Πολιτική Διαχείρισης και Εγκατάστασης Πληροφοριακών και Επικοινωνιακών Συστημάτων κ.α

Η διαδικασία υλοποίησης του παραπάνω εγχειρήματος είναι τεράστια και περιλαμβάνει πολλές διαδοχικές φάσεις.

Κάποιες από αυτές αναφέρονται:

1. Συλλογή στοιχείων & Συνεντεύξεις με τα ανώτερα στελέχη και την ανώτατη διοίκηση του φορέα. Στόχος αυτής της φάσης είναι η ενημέρωσή μας για τις δραστηριότητες του φορέα, ενώ παράλληλα, εντοπίζονται οι κύριες αδυναμίες και επιτυγχάνεται σημαντική ενημέρωση των στελεχών ως προς το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών και τους στόχους του.

2. Ανάπτυξη Πολιτικών και Διαδικασιών Ασφάλειας Πληροφοριών (όπως αυτές ορίζονται από το διεθνές πρότυπο ISO 27001:2013)

3. Οδηγίες για τη δημιουργία Records, απαραίτητων για τη συντήρηση και παρακολούθηση του συστήματος και την πιστοποίηση κατά ISO 27001:2013 (π.χ. οδηγίες για την καταγραφή των information assets , των προσβάσεων στα πληροφοριακά συστήματα, για τη δημιουργία διαγραμμάτων κλπ).

4. Δημιουργία εγγράφων απαραίτητων για την πιστοποίηση

5. Ενημέρωση και Εκπαίδευση προσωπικού (Information Security Training, Cyber Security Training, Audit preparation, awareness π.χ. αποστολή emails με οδηγίες, βίντεο κλπ)

6. Διενέργεια εσωτερικών Επιθεωρήσεων- Εντοπισμός αδυναμιών του συστήματος και εφαρμογή Επιδιορθωτικών Ενεργειών.

Η υλοποίηση της παραπάνω διαδικασίας είναι επώδυνη και χρονοβόρα αλλά τα οφέλη που προκύπτουν για τον φορέα από την υλοποίηση της δρουν αντισταθμιστικά, προσφέροντας:

 Πλήρης καταγραφή πληροφοριακών συστημάτων και προσβάσεων / διαβάθμιση πληροφοριών

Αναγνώριση πιθανών κινδύνων για την ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων

Διασφάλιση των πληροφοριών από συνεργάτες που έχουν πρόσβαση σε αυτές

 Καλλιέργεια κλίματος αμοιβαίας εμπιστοσύνης με όλα τα εμπλεκόμενα μέρη σε σχέση με την ασφάλεια πληροφοριών με απώτερο σκόπο-στόχο

Την Πιστοποίηση του φορέα με το Διεθνές Πρότυπο ISO 27001:2013 .

# ΠΑΡΑΡΤΗΜΑ

## Σχέδιο Προετοιμασίας Έργου Συμμόρφωσης με το ΓΚΠΔ

| Αναφ. | Εργασία | Απαιτούμενος χρόνος ( ανθρωπο ημέρες) | Πόροι | Ημερομηνία Έναρξης | Ημερομηνία Ολοκλήρωσης | Ολοκλήρωθηκε |
|---|---|---|---|---|---|---|
| 1 | Ανασκόπηση του ΓΚΠΔ, αρχική εκπαίδευση και συμβουλές | | Ανώτατη Διοίκηση, Βασικά Στελέχη, Νομική Δ/νση, Εξωτερικός Σύμβουλος Εκπαίδευσης | 1/7/2018 | 15/7/2018 | ✓ |
| 2 | Έναρξη του έργου | | Ανώτατη Διοίκηση, Βασικά Στελέχη, Νομική Δ/νση, Ομάδα Υλοποίησης GDPR της εταιρείας συμβούλων | 1/7/2018 | 1/7/2018 | ✓ |
| 3 | Καθορισμός του τρόπου ελέγχου των εγγράφων | | Ομάδα Υλοποίησης GDPR της εταιρείας συμβούλων | 1/7/2018 | 15/7/2018 | ✓ |
| 4 | Ορισμός των ρόλων, των αρμοδιοτήτων και των αρμόδιων αρχών | | Ομάδα Υλοποίησης GDPR της εταιρείας, Ανώτατη Διοίκηση του φορέα. | 1/7/2018 | 15/7/2018 | ✓ |
| 5 | Ορισμός του Υπεύθυνου Προστασίας Δεδομένων | | Ανώτατη Διοίκηση τουφορέα., Executive DPO της εταιρείας [ως σύμβουλος] | 15/7/2018 | 31/7/2018 | |
| 6 | Ορισμός της Εποπτικής Αρχής για την Προστασία των Δεδομένων | | Ομάδα Υλοποίησης GDPR της εταιρείας | 1/7/2018 | 15/7/2018 | ✓ |
| 7 | Διαδικασίες επικοινωνιών/κοινοποίησης εγγράφων | | Ομάδα Υλοποίησης GDPR της εταιρείας, Υπεύθυνος έργου του φορέα. | 15/7/2018 | 31/7/2018 | ✓ |
| 8 | Αξιολόγηση επάρκειας και αναγκών εκπαίδευσης | | Ομάδα Υλοποίησης GDPR της εταιρείας, Υπεύθυνος έργου του φορέα, Εκπρόσωποι διευθύνσεων του φορέα | 1/7/2018 | 31/7/2018 | ✓ |
| 9 | Εκπαίδευση και εξοικείωση με το ΓΚΠΔ | | Εκπρόσωποι βασικών δραστηριοτήτων του φορέα, Ανώτατη Διοίκηση, Ομάδα Υλοποίησης GDPR της εταιρείας | 1/7/2018 | 31/10/2018 | |
| 10 | Δημιουργία Αρχείου Καταγραφής Προσωπικών Δεδομένων - Διάγραμμα Χαρτογράφησης Προσωπικών Δεδομένων - Διάγραμμα Ροής | | Ομάδα Υλοποίησης GDPR της εταιρείας, Εκπρόσωποι διευθύνσεων του φορέα | 1/8/2018 | 15/8/2018 | |
| 11 | Καθορισμός νόμιμης βάσης για την επεξεργασία προσωπικών δεδομένων | | Ομάδα Υλοποίησης GDPR της εταιρείας, Νομική Δ/νση του φορέα | 15/8/2018 | 31/8/2018 | ✓ |
| 12 | Καθορισμός πολιτικής διατήρησης και προστασίας προσωπικών δεδομένων | | Ομάδα Υλοποίησης GDPR της εταιρεία, Νομική Δ/νση του φορέα., Ανώτατη Διοίκηση του φορέα. | 1/8/2018 | 15/8/2018 | ✓ |
| 13 | Καθορισμός πολιτικών προστασίας προσωπικών δεδομένων | | Ομάδα Υλοποίησης GDPR της εταιρεία, Ανώτατη Διοίκηση του φορέα. [για την έγκριση] | 1/9/2018 | 15/9/2018 | ✓ |
| 14 | Εκπαίδευση και ευαισθητοποίηση για το ΓΚΠΔ και την ασφάλεια των πληροφοριών | | Όλοι οι εργαζόμενοι του φορέα. | 1/9/2018 | 15/9/2018 | |
| 15 | Δημιουργία ή τροποποίηση δηλώσεων διαχείρισης απορρήτου | | Ομάδα Υλοποίησης GDPR της εταιρεία, Νομική Δ/νση του φορέα. | 1/7/2018 | 31/7/2018 | ✓ |
| 16 | Αναθερωρηση και τροποποίηση μεθόδων και διαδικασιών παροχής συγκατάθεσης | | Ομάδα Υλοποίησης GDPR της εταιρεία, Νομική Δ/νση του φορέα. , Διευθυντής Τεχνολογίας | 1/7/2018 | 31/7/2018 | ✓ |
| 17 | Έλεγχοι και παροχή συγκατάθεσης ανάλογα με την ηλικία (παιδιά) | | Ομάδα Υλοποίησης GDPR της εταιρεία, Νομική Δ/νση του φορέα., Εκπρόσωποι διευθύνσεων του φορέα. | 15/7/2018 | 31/7/2018 | ✓ |
| 18 | Συμφωνίες για διεθνείς μεταφορές των προσωπικών δεδομένων | | Ομάδα Υλοποίησης GDPR της εταιρεία, Νομική Δ/νση του φορέα., Εκπρόσωποι διευθύνσεων του φορέα. | 1/8/2018 | 15/8/2018 | ✓ |
| 19 | Δημιουργία και υλοποίηση διαδικασιών υποβολής αιτημάτων από τα υποκείμενα των δεδομένων | | Ομάδα Υλοποίησης GDPR της εταιρεία | 15/8/2018 | 31/8/2018 | ✓ |
| 20 | Καθορισμός της διαδικασίας αξιολόγησης των επιπτώσεων για την προστασία των δεδομένων | | Ομάδα Υλοποίησης GDPR της εταιρεία | 1/9/2018 | 15/9/2018 | |
| 21 | Διεξαγωγή αξιολόγησης/αξιολογήσεων των επιπτώσεων για την προστασία των | | Ομάδα Υλοποίησης GDPR της εταιρεία, Νομική Δ/νση του φορέα., Εκπρόσωποι διευθύνσεων του φορέα., Διευθυντής Τεχνολογίας | 15/9/2018 | 30/9/2018 | |
| 22 | Δημιουργία διαδικασίας διαχείρισης περιστατικών που αφορούν προσωπικά δεδομένα | | Ομάδα Υλοποίησης GDPR της εταιρεία, Ανώτατη Διοίκηση [για έγκριση], Εκπρόσωποι βασικών δραστηριοτήτων του φορέα. | 1/10/2018 | 15/10/2018 | |
| 23 | Δημιουργία διαδικασίας ειδοποίησης/ενημέρωσης για παραβίαση προσωπικών δεδομένων | | Ομάδα Υλοποίησης GDPR της εταιρεία, Ανώτατη Διοίκηση [για έγκριση], Εκπρόσωποι διευθύνσεων του φορέα. | 1/10/2018 | 15/10/2018 | |
| 24 | Εκπαίδευση για τη διαχείριση περιστατικών που αφορούν προσωπικά δεδομένα | | Όλοι οι εργαζόμενοι του φορέα. | 16/10/2018 | 31/10/2018 | |
| 25 | Εσωτερικές Επιθεωρήσεις για την Προστασία Προσωπικών Δεδομένων | | Ομάδα Υλοποίησης GDPR της εταιρεία, Εκπρόσωποι διευθύνσεων του φορέα. | 16/11/2018 | 30/11/2018 | |
| 26 | Μετέπειτα Αναθερώρηση Έργου | | Ομάδα Υλοποίησης GDPR της εταιρεία, Εκπρόσωποι διευθύνσεων του φορέα. | 16/11/2018 | 30/11/2018 | |

# Συμμόρφωση με το ΓΚΠΔ

| ΚΕΦΑΛΑΙΟ | Τμήμα | Άρθρο | Τεκμηρίωση |
|---|---|---|---|
| **ΚΕΦΑΛΑΙΟ I - Γενικές διατάξεις** | | | |
| | | Άρθρο 1 Αντικείμενο και στόχοι | *Εργαλείο Αξιολόγησης Κενών για τη Συμμόρφωση με το ΓΚΠΔ* |
| | | Άρθρο 2 Ουσιαστικό πεδίο εφαρμογής | |
| | | Άρθρο 3 Εδαφικό πεδίο εφαρμογής | |
| | | Άρθρο 4 Ορισμοί | |
| | | | |
| | | | |
| **ΚΕΦΑΛΑΙΟ II - Αρχές** | | | |
| | | Άρθρο 5 - Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα | *Πολιτική για την Ιδιωτικότητα και την Προστασία των Προσωπικών Δεδομένων*<br>*Πολιτική Διατήρησης και Προστασίας Αρχείων*<br>*Executive Support Letter*<br>*Διαδικασία Εκτίμησης Έννομου Συμφέροντος* |
| | | Άρθρο 6 - Νομιμότητα της επεξεργασίας | |
| | | Άρθρο 7 - Προυποθέσεις για συγκατάθεση | |
| | | Άρθρο 8 - Προυποθέσεις που ισχύουν για την συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών | |
| | | Άρθρο 9 - Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα | |
| | | Άρθρο 10 - Επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα | |
| | | Άρθρο 11 - Επεξεργασία η οποία δεν απαιτεί εξακρίβωση ταυτότητας | |
| | | | |
| | | | |
| **ΚΕΦΑΛΑΙΟ III - Δικαιώματα του υποκειμένου των δεδομένων** | | | |
| | **Τμήμα 1 - Διαφάνεια και ρυθμίσεις** | | |
| | | Άρθρο 12 - Διαφανής ενημέρωση, ανακοίνωση και ρυθμίσεις για την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων | *Διαδικασία Αιτημάτων Υποκειμένου των Δεδομένων*<br>*Διαδικασία Δήλωσης περί Ιδιωτικού Απορρήτου*<br>*Φόρμες Σχεδιασμού Ενημέρωσης των Υποκειμένων των Δεδομένων*<br>*Ενημέρωση των Υποκειμένων των Δεδομένων* |
| | **Τμήμα 2 - Ενημέρωση και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα** | | |
| | | Άρθρο 13 - Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων | |
| | | Άρθρο 14 - Πληροφορίες που παρέχονται αν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεομδένων | |
| | | Άρθρο 15 - Δικαίωμα προσβασης του υποκειμένου των δεδομένων | |
| | **Τμήμα 3 - Διόρθωση και διαγραφή** | | |
| | | Άρθρο 16 - Δικαίωμα διόρθωσης | *Διαδικασία Αιτημάτων Υποκειμένου των Δεδομένων*<br>*Αρχείο Αιτημάτων των Υποκειμένων των Δεδομένων*<br>*Φόρμες Αιτημάτων των Υποκειμένων των Δεδομένων*<br>*Εκτίμηση Έννομου Συμφέροντος* |
| | | Άρθρο 17 - Δικαίωμα διαγραφής ("δικαίωμα στη λήθη") | |
| | | Άρθρο 18 - Δικαίωμα περιορισμού της επεξεργασίας | |
| | | Άρθρο 19 - Υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας | |
| | | Άρθρο 20 - Δικαίωμα στη φορητότητα των δεδομένων | |
| | **Τμήμα 4 - Δικαίωμα εναντίωσης και αυτοματοποιημένη λήψη αποφάσεων** | | |
| | | Άρθρο 21 - Δικαίωμα εναντίωσης | |
| | | Άρθρο 22 - Αυτοματοποιημένη λήψη αποφάσεων, περιλαμβανόμενης της κατάρτησης προφίλ | |
| | **Τμήμα 5 - Περιορισμοί** | | |
| | | Άρθρο 23 - Περιορισμοί | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| **ΚΕΦΑΛΑΙΟ IV - Υπεύθυνος της επεξεργασίας και εκτελών την επεξεργασία** | | | |
| | **Τμήμα 1 - Γενικές υποχρεώσεις** | | |
| | | Άρθρο 24 - Ευθύνη του υπεύθυνου επεξεργασίας | *Πολιτική για την Ιδιωτικότητα και την Προστασία των Προσωπικών Δεδομένων*<br>*Πρόγραμμα Επικοινωνίας για το Έργο Συμμόρφωσης με το ΓΚΠΔ*<br>*Πολιτική Συμφωνίας Μεταξύ του Υπεύθυνου Επεξεργασίας και του Εκτελούντα την Επεξεργασίας για το ΓΚΠΔ*<br>*Διαδικασία Αξιολόγησης των Προμηθευτών για το ΓΚΠΔ*<br>*Συμφωνία Εμπιστευτικότητας μεταξύ του υπεύθυνου και του εκτελούντα την επεξεργασία* |
| | | Άρθρο 25 - Προστασία δεδομένων από το σχεδιασμό και εξ' ορισμού | |
| | | Άρθρο 26 - Από κοινού υπεύθυνοι επεξεργασίας | |
| | | Άρθρο 27 - Εκπρόσωποι υπεύθυνων επεξεργασίας ή εκτελούντων την επεξεργασία η εγκατεστημένων στην Ένωση | |
| | | Άρθρο 28 - Εκτελών την επεξεργασία | |
| | | Άρθρο 29 - Επεξεργασία υπό την εποπτεία του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία | |
| | | Άρθρο 30 - Αρχεία των δραστηριοτήτων επεξεργασίας | *Αρχείο Προσωπικών Δεδομένων σε Επίπεδο Οργανισμού*<br>*Αρχεία των Δραστηριοτήτων Επεξεργασίας* |
| | | Άρθρο 31 - Συνεργασία με την εποπτική αρχή | *Πολιτική για την Ιδιωτικότητα και την Προστασία των Προσωπικών Δεδομένων* |
| | **Τμήμα 2 - Ασφάλεια δεδομένων προσωπικού χαρακτήρα** | | |
| | | Άρθρο 32 - Ασφάλεια επεξεργασίας | *Διαδικασία Ανάπτυξης Δεξιοτήτων για το ΓΚΠΔ*<br>*Εκπαίδευση για την Ασφάλεια των Πληροφοριών και την προστασία των Προσωπικών Δεδομένων* |
| | | Άρθρο 33 - Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή | *Διαδικασία Απόκρισης σε Περιστατικά Ασφάλειας Πληροφοριών*<br>*Διαδικασία Γνωστοποίησης Παραβίασης Προσωπικών Δεδομένων* |
| | | Άρθρο 34 - Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων | |
| | **Τμήμα 3 - Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και προηγούμενη διαβούλευση** | | |
| | | Άρθρο 35 - Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων | *Διαδικασία Εκτίμησης Επιπτώσεων για την Προστασία των Δεδομένων*<br>*Ερωτηματολόγια Εκτίμησης Επιπτώσεων για την Προστασία των Δεδομένων*<br>*Εκθέσεις Εκτίμησης Επιπτώσεων για την Προστασία των Δεδομένων*<br>*Διαδικασία Χαρτογράφησης Προσωπικών Δεδομένων*<br>*Εργαλείο Χαρτογράφησης Προσωπικών Δεδομένων*<br>*Αρχείο Καταγραφής Προσωπικών Δεδομένων*<br>*Αρχείο Προσωπικών Δεδομένων σε Επίπεδο Οργανισμού*<br>*Διαδικασία Αξιολόγησης των Προμηθευτών για το ΓΚΠΔ*<br>*Φόρμες Αξιολόγησης των Προμηθευτών για το ΓΚΠΔ* |
| | | Άρθρο 36 - Προηγούμενη διαβούλευση | |
| | **Τμήμα 4 - Υπεύθυνος προστασίας δεδομένων** | | |
| | | Άρθρο 37 - Ορισμός του υπευθύνου προστασίας δεδομένων | *Ρόλοι, Αρμοδιότητες και Δικαιοδοσίες για το ΓΚΠΔ* |
| | | Άρθρο 38 - Θέση του υπευθύνου προστασίας δεδομένων | |
| | | Άρθρο 39 - Καθήκοντα του υπεύθυνου προστασίας δεδομένων | |
| | **Τμήμα 5 - Κώδικες δεοντολογίας και πιστοποίηση** | | |
| | | Άρθρο 40 - Κώδικες δεοντολογίας και πιστοποίηση | Δεν απαιτείται |
| | | Άρθρο 41 - Παρακολούθηση των εγκεκριμένων κωδίκων δεοντολογίας | |
| | | Άρθρο 42 - Πιστοποίηση | |
| | | Άρθρο 43 - Φορείς πιστοποίησης | |
| | | | |
| | | | |
| **ΚΕΦΑΛΑΙΟ V - Διαβιβάσεις δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ή διεθνείς οργανισμούς** | | | |
| | | Άρθρο 44 - Γενικές αρχές για διαβιβάσεις | *Διαδικασία για Διεθνείς Μεταφορές Προσωπικών Δεδομένων*<br>*Εργαλείο Χαρτογράφησης Προσωπικών Δεδομένων*<br>*Αρχείο Καταγραφής προσωπικών Δεδομένων* |
| | | Άρθρο 45 - Διαβιβάσεις βάσει απόφαση επάρκειας | |
| | | Άρθρο 46 - Διαβιβάσεις που υπόκεινται σε κατάλληλες εγγυήσεις | |
| | | Άρθρο 47 - Δεσμευτικοί εταιρικοί κανόνες | |
| | | Άρθρο 48 - Διαβιβάσεις ή κοινοποίησεις που δεν επιτρέπονται από το δίκαιο της Ένωσης | |
| | | Άρθρο 49 - Παρεκκλίσεις για ειδικές καταστάσεις | |
| | | Άρθρο 50 - Διεθνής συνεργασία για την προστασία δεδομένων προσωπικού χαρακτήρα | Δεν απαιτείται |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| **ΚΕΦΑΛΑΙΟ VI - Ανεξάρτητες εποπτικές αρχές** | | | |
| | **Τμήμα 1 - Ανεξάρτητο καθεστώς** | | Δεν απαιτείται |
| | | Άρθρο 51 - Εποπτική αρχή | |
| | | Άρθρο 52 - Ανεξαρτησία | |
| | | Άρθρο 53 -Γενικές προϋποθέσεις για τα μέλη της εποπτικής αρχής | |
| | | Άρθρο 54 - Κανόνες για τη σύσταση της εποπτικής αρχής | |
| | **Τμήμα 2 - Αρμοδιότητα, καθήκοντα και εξουσίες** | | |
| | | Άρθρο 55 - Αρμοδιότητα | |
| | | Άρθρο 56 - Αρμοδιότητα της επικεφαλής εποπτικής αρχής | |
| | | Άρθρο 57 - Καθήκοντα | |
| | | Άρθρο 58 - Εξουσίες | |
| | | Άρθρο 59 - Εκθέσεις δραστηριοτήτων | |
| | | | |
| | | | |
| **ΚΕΦΑΛΑΙΟ VII - Συνεργασία και συνεκτικότητα** | | | |
| | **Τμήμα 1 - Συνεργασία** | | |
| | | Άρθρο 60 - Συνεργασία μεταξύ της επικεφαλής εποπτικής αρχής και των άλλων ενδιαφερόμενων εποπτικών αρχών | Δεν απαιτείται |
| | | Άρθρο 61 - Αμοιβαία συνδρομή | |
| | | Άρθρο 62 - Κοινές επιχειρήσεις αρχών ελέγχου | |
| | **Τμήμα 2 - Συνεκτικότητα** | | |
| | | Άρθρο 63 - Μηχανισμός συνεκτικότητας | |
| | | Άρθρο 64 - Γνώμη του Συμβουλίου | |
| | | Άρθρο 65 - Επίλυση διαφορών από το Συμβούλιο Προστασίας Δεδομένων | |
| | | Άρθρο 66 - Επίγουσα διαδικασία | |
| | | Άρθρο 67 - Ανταλλαγή πληροφοριών | |
| | **Τμήμα 3 - Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων** | | |
| | | Άρθρο 68 - Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων | |
| | | Άρθρο 69 - Ανεξαρτησία | |
| | | Άρθρο 70 - Καθήκοντα του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων | |
| | | Άρθρο 71 - Εκθέσεις | |
| | | Άρθρο 72 - Διαδικασία | |
| | | Άρθρο 73 - Πρόεδρος | |
| | | Άρθρο 74 - Καθήκοντα του Προέδρου | |
| | | Άρθρο 75 - Γραμματεία | |
| | | Άρθρο 76 - Εμπιστευτικότητα | |
| | | | |
| | | | |
| **ΚΕΦΑΛΑΙΟ VIII - Προσφυγές, ευθύνη και κυρώσεις** | | | |
| | | Άρθρο 77 - Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή | Δεν απαιτείται |
| | | Άρθρο 78 - Δικαίωμα πραγματικής δικαστικής προσφυγής κατά αρχής ελέγχου | |
| | | Άρθρο 79 - Δικαίωμα πραγματικής δικαστικής προσυγής κατά υπεύθυνου επεξεργασίας ή εκτελούντος την επεξεργασια | |
| | | Άρθρο 80 - Εκπροσώπηση υποκειμένων των δεδομένων | |
| | | Άρθρο 81 - Αναστολή τω διαδικάσιών | |
| | | Άρθρο 82 - Δικαίωμα αποζημίωσης και ευθύνη | |
| | | Άρθρο 83 - Γενικοί όροι υποβολής διοικητικών προστίμων | |
| | | Άρθρο 84 - Κυρώσεις | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| **ΚΕΦΑΛΑΙΟ IX - Διατάξεις που αφορούν ειδικές περιπτώσεις επεξεργασίας** | | | |
| | | Άρθρο 85 - Επεξεργασία και ελευθερία έκφρασης και πληροφόρησης | Γενικά δεν απαιτείται, αλλά εξαρτάται από τη φύση του οργανισμού |
| | | Άρθρο 86 - Επεξεργασία και πρόσβαση του κοινού σε επίσημα έγγραφα | |
| | | Άρθρο 87 - Επεξεργασία του εθνικού αριθμού ταυτότητας | |
| | | Άρθρο 88 - Επεξεργασία στο πλαίσιο της απασχόλησης | |
| | | Άρθρο 89 - Διασφαλίσεις και παρεκκλίσεις σχετικά με την επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς | |
| | | Άρθρο 90 - Υποχρεώσεις τήρησης απορρήτου | |
| | | Άρθρο 91 - Υφιστάμενοι κανόνες προστασίας των δεδομένων εκκλησιών και θρησκευτικών ενώσεων | |
| | | | |
| | | | |
| **ΚΕΦΑΛΑΙΟ X - Κατ' εξουσιοδότηση πράξεις και εκτελεστικές πράξεις** | | | |
| | | Άρθρο 92 - Άσκηση της εξουσιοδότησης | Δεν απαιτείται |
| | | Άρθρο 93 - Διαδικασία επιτροπής | |
| | | | |
| | | | |
| **ΚΕΦΑΛΑΙΟ XI - Τελικές διατάξεις** | | | |
| | | Άρθρο 94 - Κατάργηση της οδηγίας 95/46/ΕΚ | Δεν απαιτείται |
| | | Άρθρο 95 - Σχέση με την οδηγία 2002/58/ΕΚ | |
| | | Άρθρο 96 - Σχέση με συμφωνίες που έχουν συναφθεί παλαιότερα | |
| | | Άρθρο 97 - Εκθέσεις της επιτροπής | |
| | | Άρθρο 98 - Επισκόπηση άλλων νομικών πράξεων της Ένωσης για την προστασία των δεδομένων | |
| | | Άρθρο 99 - Έναρξη ισχύος και εφαρμογή | |
| | | | |
| | | | |

# Ερωτηματολόγιο για τον εντοπισμό και την ανάπτυξη δεξιοτήτων σχετικά με το ΓΚΠΔ

Ο σκοπός του παρόντος ερωτηματολογίου είναι να καταλάβουμε το βαθμό γνώσης και το επίπεδο των δεξιοτήτων σας σε διάφορα θέματα, που άπτονται της προστασίας των προσωπικών δεδομένων. Αυτό θα μας βοηθήσει να εκτιμήσουμε κατά πόσο έχουμε τις δεξιότητες, που χρειαζόμαστε ως οργανισμός, προκειμένου να συμμορφωθούμε με τον ΓΚΠΔ και -ταυτόχρονα- να εντοπίσουμε τις εκπαιδευτικές ανάγκες, που πρέπει να ικανοποιήσουμε.

| | |
|---|---|
| **Ονοματεπώνυμο** | |
| **Καθήκοντα** | |
| **Τίτλος** | |
| **Ημερομηνία συμπλήρωσης του ερωτηματολογίου** | |

Επίπεδο γνώσεων & δεξιοτήτων: 0=Καθόλου, 1=Χαμηλό, 2=Μέτριο, 3=Υψηλό, 4=Εξαιρετικό (δείτε τι σημαίνει το κάθε επίπεδο στο διπλανό φύλλο εργασίας)

| Γνώση/δεξιότητα | Επίπεδο | Σχόλια |
|---|---|---|
| Γνωρίζω τους στόχους του οργανισμού για την προστασία των προσωπικών δεδομένων καθώς και την ισχύουσα και παλαιότερη σχετική νομοθεσία | 3 | π.χ. Έχω εκπαιδευτεί στην Νομοθεσία που ίσχυε πριν τον ΓΚΠΔ |
| Έχω γενική γνώση του Κανονισμού | 2 | π.χ.Έχω διαβάσει τον Κανονισμό 2 φορές |
| Γνωρίζω τις βασικές αρχές προστασίας προσωπικών δεδομένων | 2 | |
| Γνωρίζω σχετικά με τη νόμιμη βάση της επεξεργασίας | 1 | |
| Γνωρίζω τι ισχύει για τη συναίνεση | 2 | π.χ. Έχω συνεργαστεί με τον κ. ..... και τη δικηγόρο της εταιρίας μας στη σύνταξη συναίνεσης για ..... |
| Γνωρίζω σχετικά με τις ειδικές κατηγορίες προσωπικών δεδομένων (δηλ. τα ευαίσθητα | 0 | |
| Γνωρίζω για τα δικαιώματα των φυσικών προσώπων | 2 | π.χ. Έχω εργαστεί σε τμήματα προσωπικού στο παρελθόν |
| Γνωρίζω για τις υποχρεώσεις των υπευθύνων της επεξεργασίας και των εκτελούντων την επεξεργασία | 1 | |
| Γνωρίζω για τη διαχείριση των παραβιάσεων ασφάλειας πληροφοριών ή προσωπικών δεδομένων | 3 | π.χ είχα διαχειριστεί μία διαρροή δεδομένων πέρυσι |
| Γνωρίζω σχετικά με τη Μελέτη Αντικτύπου | 1 | |
| Γνωρίζω για τα καθήκοντα του Υπευθύνου Προστασίας Δεδομένων | 2 | |
| Γνωρίζω για τους κώδικες δεοντολογίας και τις πιστοποιήσεις | 0 | |
| Γνωρίζω τα θέματα μεταφοράς δεδομένων εκτός ΕΕ | 0 | |
| Γνωρίζω πώς να χειριστώ την επικοινωνία με την ΑΠΔΠΧ (Αρχή Προστασίας Δεδομένων Προσωπικού | 2 | π.χ. στην προηγούμενη δουλειά μου είχα έρθει σε επαφή με την ΑΠΔΠΧ σε αρκετές περιπτώσεις |
| Γνωρίζω για τα διοικητικά πρόστιμα του ΓΚΠΔ | 1 | |
| Γνωρίζω τις αρχές της ασφάλειας πληροφοριών | 2 | |
| Γνωρίζω για τη Διαχείριση Κινδύνων | 3 | π.χ. έχω καλή γνώση των αρχών διαχείρισης κινδύνων |
| Γνωρίζω τα διεθνή πρότυπα για την ασφάλεια των πληροφοριών (π.χ. ISO 27001) | 2 | |
| Γνωρίζω τεχνικά μέτρα ασφαλείας π.χ. κρυπτογράφηση και διαχείριση προσβάσεων | 1 | π.χ. Έχω βασικές γνώσεις για τις μεθοδολογίες κρυπτογράφησης και προστασίας δεδομένων |
| Άλλες σχετικές γνώσεις (παρακαλώ επεξηγείστε) | | |
| Γνωρίζω σχετικά με την καταγραφή και την ανάλυση των προσωπικών δεδομένων | 3 | |

# Κατάταξη σε επίπεδο

| Επίπεδο | Περιγραφή | Επεξήγηση |
|---|---|---|
| 0 | Καθόλου | Ο εργαζόμενος δεν έχει γνώσεις ή εμπειρία στο θέμα και αυτό δεν αποτελεί μέρος των καθηκόντων του. |
| 1 | Χαμηλό | Ασχολείται σπάνια με το θέμα και οι γνώσεις του βασίζονται στην παρατήρηση του τρόπου εργασίας των άλλων, χωρίς να καταλαβαίνει λεπτομέρειες. Ίσως έχει ασχοληθεί με το θέμα για πολύ μικρό χρονικό διάστημα και δεν αποτέλεσε ποτέ μέρος των καθηκόντων του. Δεν έχει εκπαιδευτεί στο θέμα, έχει απλώς μια πολύ γενική γνώση. |
| 2 | Μέτριο | Ασχολείται συχνά με το θέμα ως μέρος των καθηκόντων του για αρκετό διάστημα ώστε να αισθάνεται ότι το κατέχει (για περισσότερο από ένα χρόνο). Σε κάποιες περιπτώσεις έλαβε εκπαίδευση για το θέμα και κατανοεί τις βασικές αρχές. Ο εργαζόμενος αισθάνεται ότι γνωρίζει το αντικείμενο. |
| 3 | Υψηλό | Θεωρείται ότι αποτελεί σημαντική δεξιότητα του εργαζόμενου, έχει εμπειρία, έχει εκπαιδευτεί και πιστοποιηθεί στο αντικείμενο για σημαντικό χρονικό διάστημα (πιθανόν περισσότερο από 3 χρόνια). Οι αρχές προστασίας προσωπικών δεδομένων του είναι απόλυτα κατανοητές και ενημερώνεται για τις εξελίξεις. Μπορεί να έχει εκπαιδεύσει και άλλους ή να είναι υπεύθυνος για την ανάπτυξη διαδικασιών σχετικών με το θέμα. |
| 4 | Εξαιρετικό | Είναι αναγνωρισμένος και εκτός εταιρίας ως ειδικός στο θέμα και μπορεί να έχει συμμετάσχει σε συνέδρια και σεμινάρια ως εισηγητής. Τόσο οι πελάτες όσο και οι συνεργάτες τον έχουν σε μεγάλη εκτίμηση.Ο εργαζόμενος μπορεί να βοηθήσει στην ανάπτυξη του Προγράμματος Προστασίας Προσωπικών Δεδομένων. |

# Εγγραφή αιτήματος δεδομένων δεδομένων - Οδηγίες συμπλήρωσης

Ο σκοπός αυτού του λογιστικού φύλλου είναι να καταγράψει τις λεπτομέρειες των αιτημάτων των υποκειμένων των δεδομένων σχετικά με τα προσωπικά δεδομένα. Για περισσότερες λεπτομέρειες σχετικά με τη διεκπεραίωση των αιτημάτων, ανατρέξτε στη Διαδικασία αίτησης για θέμα δεδομένων.

Οι σημασίες των αναγραφόμενων στηλών είναι οι ακόλουθες.

| Στήλη | Σημασία |
|---|---|
| **Ημερομηνία αιτήματος** | Η ημερομηνία παραλαβής του αιτήματος. Αυτό μπορεί να είναι σημαντικό καθώς υπάρχουν χρονικά όρια για τις απαντήσεις σε ορισμένους τύπους αιτημάτων |
| **Τίτλος** | Ο προτιμώμενος τίτλος του υποκειμένου δεδομένων π.χ. Κύριος, κυρία, Δρ. |
| **Ονοματεπώνυμο** | Το όνομα και το επώνυμο του υποκειμένου των δεδομένων |
| **Διεύθυνση** | Η διεύθυνση που δόθηκε από το υποκείμενο των δεδομένων |
| **Αριθμός πολίτη / λογαριασμού** | Εάν ισχύει, η αναφορά με την οποία το πρόσωπο στο οποίο αναφέρονται τα δεδομένα είναι γνωστό από τον οργανισμό μας |
| **Τύπος αιτήματος** | Ο τύπος της αίτησης υποβολής δεδομένων Οι κύριοι τύποι αιτημάτων είναι:<br>Αίτηση συγκατάθεσης<br>Αίτημα πρόσβασης<br>Διόρθωση των προσωπικών δεδομένων<br>Διαγραφή προσωπικών δεδομένων<br>Περιορισμός της επεξεργασίας δεδομένων προσωπικού χαρακτήρα<br>Αίτημα φορητότητας προσωπικών δεδομένων<br>Αμφισβήτηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα<br>Αίτημα σχετικά με την αυτοματοποιημένη λήψη αποφάσεων και τη δημιουργία προφίλ |
| **Δεδομένα προσωπικού χαρακτήρα που εμπλέκονται** | Περιγραφή των προσωπικών δεδομένων στα οποία αναφέρεται το αίτημα. Παρακαλείσθε να δώσετε όσο το δυνατόν περισσότερες πληροφορίες, ώστε τα δεδομένα να μπορούν να προσδιοριστούν με σαφήνεια |
| **Λεπτομέριες αιτήματος** | Λεπτομέρειες σχετικά με το αίτημα, δηλαδή τι ζητά να γίνει το υποκείμενο των δεδομένων |
| **Αιτιολογία** | Ο (οι) λόγος (-οι) του αιτήματος και ο λόγος για τον οποίο το υποκείμενο των δεδομένων πιστεύει ότι το αίτημα είναι δικαιολογημένο |
| **Βεβαίωση ταυτότητας** | Έχει επιβεβαιωθεί η ταυτότητα του υποκειμένου των δεδομένων μέσω μιας ή περισσότερων εγκεκριμένων μεθόδων; |
| **Αξιολόγηση της εγκυρότητας** | Αξιολόγηση από κατάλληλο άτομο εντός της οργάνωσης σχετικά με το κατά πόσον η αίτηση είναι νομικά έγκυρη και πρέπει να τηρείται. Πρέπει να αναφέρονται οι λόγοι ισχύος ή μη ισχύος |
| **Χρέωση που εφαρμόστηκε** | Μήπως έγινε χρέωση για τη συμμόρφωση με το αίτημα; Αν ναι, δηλώστε το ποσό της χρέωσης |
| **Επέκταση χρόνου** | Ήταν μια επέκταση στον προεπιλεγμένο χρόνο που ήταν διαθέσιμος για να συμμορφωθεί με το αίτημα που ελήφθη; Αν ναι, δηλώστε τον λόγο (τους λόγους) και τη διάρκεια |
| **Δράση που ελήφθη** | Αναφέρατε τις ενέργειες που έλαβε ο οργανισμός σχετικά με αυτό το αίτημα |
| **Κατάσταση αιτήματος** | Η τρέχουσα κατάσταση του αιτήματος, π.χ. εκκρεμεί, ολοκληρώθηκε |
| **Ημερομηνία Ολοκλήρωσης** | Εάν ολοκληρώθηκε, η ημερομηνία ολοκλήρωσης του αιτήματος |

**ΦΟΡΜΑ ΥΠΟΒΟΛΗΣ ΑΙΤΗΜΑΤΟΣ ΑΠΟ ΤΟ ΥΠΟΚΕΙΜΕΝΟ ΤΩΝ ΔΕΔΟΜΕΝΩΝ**

Το παρόν έντυπο πρέπει να χρησιμοποιείται για την υποβολή αίτησης από το υποκείμενο των δεδομένων σύμφωνα με τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (ΓΚΠΔ).

**Λεπτομέρειες του Υποβάλλοντα του Αιτήματος**

| | |
|---|---|
| **Τίτλος:** | |
| **Όνομα:** | |
| **Διεύθυνση:** | |
| **Αριθμός Μητρώου :** | |

**Είδος Αιτήματος**

Παρακαλώ επιλέξτε τον τύπο του αιτήματος, που υποβάλλετε:

☐ *Άρση Συναίνεσης*

☐ *Αίτημα Πρόσβασης*

☐ *Διόρθωση Προσωπικών Δεδομένων*

☐ *Διαγραφή Προσωπικών Δεδομένων*

☐ *Περιορισμός της Επεξεργασίας των Προσωπικών Δεδομένων*

☐ *Αίτημα Φορητότητας Προσωπικών Δεδομένων*

☐ *Αντίρρηση στην Επεξεργασία Προσωπικών Δεδομένων*

☐ *Αίτημα σχετικά με την αυτοματοποιημένη λήψη αποφάσεων και τη δημιουργία προφίλ*

**Προσωπικά Δεδομένα που εμπλέκονται**

| |
|---|
| |

**Λεπτομέρειες αιτήματος**

| |
|---|
| |

**Λόγος/αιτιολογία αιτήματος**

| |
|---|
| |

| | |
|---|---|
| **Υπογραφή:** | |
| **Όνομα:** | |
| **Ημερομηνία:** | |

Μόλις ολοκληρωθεί, αυτή η φόρμα θα πρέπει να υποβληθεί μέσω e-mail στο

dpo@master-ateith.gr.

**ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΕΚΤΙΜΗΣΗΣ ΕΠΙΠΤΩΣΕΩΝ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ**

Αυτή η φόρμα θα πρέπει να χρησιμοποιηθεί για την καταγραφή των βασικών πληροφοριών σχετικά με μία εκτίμηση επιπτώσεων για την προστασία των δεδομένων (DPIA) η οποία μπορεί να απαιτηθεί ως μέρος των διατάξεων του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) της Ευρωπαϊκής Ένωσης.

**Λεπτομέρειες Έργου**

| | |
|---|---|
| **Όνομα έργου:** | |
| **Αναφορά/παραπομπή έργου:** | |
| **Περιγραφή έργου:** | [Παρακαλούμε περιγράψετε το εσωτερικό και εξωτερικό περιεχόμενο του έργου και τους γενικούς στόχους του] |

**Λόγος για την εκτίμηση των επιπτώσεων για την προστασία των δεδομένων**

Παρακαλώ επιλέξτε το λόγο για τον οποίο είναι απαραίτητη η DPIA:

- ☐ *Πληροφορίες σχετικά με φυσικά πρόσωπα που βρίσκονται εν ζωή θα συλλεχθούν και θα επεξεργαστούν για πρώτη φορά*
- ☐ *Πληροφορίες σχετικά με φυσικά πρόσωπα που βρίσκονται εν ζωή θα κοινοποιηθούν σε ανθρώπους ή οργανισμούς, οι οποίοι δεν είχαν πρόσβαση σε αυτά στο παρελθόν*
- ☐ *Αλλαγή χρήσης των υπαρχόντων προσωπικών δεδομένων*
- ☐ *Η χρήση νέας τεχνολογίας που συλλέγει ή χρησιμοποιεί δεδομένα προσωπικής φύσεως π.χ. βιομετρικά στοιχεία*
- ☐ *Υπάρχοντα προσωπικά δεδομένα θα χρησιμοποιηθούν για τη λήψη αποφάσεων ως μέρος μίας αυτοματοποιημένης διαδικασίας*
- ☐ *Θα ήταν αναμενόμενο ένα φυσικό πρόσωπο να θεωρήσει κάποια πτυχή του έργου ως παραβίαση ή τα δεδομένα που περιλαμβάνονται ιδιωτικά*
- ☐ *Άλλος λόγος (παρακαλώ εξηγήστε)*

## ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΗΣ DPIA

Ορίστε το πεδίο εφαρμογής με όρους:

- γεωγραφικής τοποθεσίας π.χ. χώρες, γραφεία, κέντρα δεδομένων
- οργανωτικές μονάδες π.χ. συγκεκριμένα τμήματα
- διαδικασία(-ες) του Φορέα
- υπηρεσίες Πληροφορικής, συστήματα και δίκτυα
- δημότες ή υπηρεσίες]

### Προσωπικά δεδομένα που περιλαμβάνονται

[Περιγράψτε τα δεδομένα που θα αποθηκευτούν και θα τεθούν υπό επεξεργασία. Μπορείτε επίσης να χρησιμοποιήσετε το Εργαλείο Χαρτογράφησης της Ροής των Προσωπικών Δεδομένων για να συμπληρώσετε την περιγραφή σας]

**Πως θα αποκτηθούν τα δεδομένα;**

[Περιγράψτε εάν τα δεδομένα θα αποκτηθούν απευθείας από το υποκείμενο των δεδομένων ή έμμεσα από ένα τρίτο μέρος]

**Τι επεξεργασία θα γίνει στα δεδομένα;**

[Για τι θα χρησιμοποιηθούν τα δεδομένα; Η επεξεργασία θα γίνει εσωτερικά ή από ένα ή περισσότερα τρίτα μέρη;]

**Ποια είναι τα χρονοδιαγράμματα της διατήρησης των δεδομένων;**

[Για πόσο καιρό θα διατηρηθούν τα δεδομένα και γιατί;]

**Πως θα γίνει η αποθήκευση των δεδομένων;**

[Που θα αποθηκευτούν και σε τι ελέγχους θα υποβληθούν π.χ. κρυπτογράφηση των αποθηκευμένων δεδομένων;]

**Υπάρχει πιθανότητα άλλων μελλοντικών χρήσεων των δεδομένων;**

[Είναι πιθανό τα δεδομένα να χρησιμοποιηθούν για σκοπούς άλλους από εκείνους για τους οποίους συλλέγονται και αν ναι, τι σκοπούς;]

**Που θα μεταφερθούν τα δεδομένα και υπό ποιες συνθήκες;**

Τα δεδομένα θα σταλούν σε άλλες περιοχές ή τρίτα μέρη σε άλλες χώρες; Αν ναι, τι θα αποτελέσει αφορμή για τη μεταφορά και γιατί;]

**Ποιος θα έχει πρόσβαση στα δεδομένα και με ποιο τρόπο;**

Ποιος θα έχει πρόσβαση στα δεδομένα εντός και εκτός του οργανισμού και τι έλεγχοι θα εφαρμοστούν για τη διαχείριση των προσβάσεων;]

| | |
|---|---|
| **Υπογραφή:** | |
| **Όνομα:** | |
| **Ημερομηνία:** | |

Μόλις συμπληρωθεί, αυτή η φόρμα θα πρέπει να υποβληθεί μέσω email στη διεύθυνση dpo@master-ateith.gr.

**ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΑΝΑΛΥΣΗΣ ΑΝΤΙΚΤΥΠΟΥ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ**

| | |
|---|---|
| **Επιχειρησιακή Λειτουργία / Υπηρεσία**<br><br>**(Operational Process):** | |
| **Υπεύθυνος (Owner):** | |
| **Περιγραφή λειτουργίας:** | |
| **Συστήματα (Systems):** | |
| **Δεδομένα (Data):** | |

## ΑΛΛΗΛΕΠΙΔΡΑΣΕΙΣ ΛΕΙΤΟΥΡΓΙΩΝ

**Περιγραφή Υπηρεσίας**

1. **Προσδιορίστε τα είδη των πληροφοριών**

2. **Προσδιορίστε ποιες από τις παραπάνω πληροφορίες αποτελούν προσωπικά δεδομένα και ποιες ευαίσθητα προσωπικά δεδομένα.**

3. **Απειλές/Κίνδυνοι**

## ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ

4. **Συμπληρώστε τους παρακάτω πίνακες επιπτώσεων, με βάση τις ακόλουθες κατηγορίες**:

| ***ΚΑΤΗΓΟΡΙΕΣ ΕΠΙΠΤΩΣΕΩΝ*** | |
|---|---|
| **High** | Σε περίπτωση που ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. |
| **Medium** | Σε περίπτωση που ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει μεσαίου επιπέδου κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. |
| **Low** | Σε περίπτωση ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει χαμηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. |

### 4.1 Διαθεσιμότητα Δεδομένων

| *Απώλεια Διαθεσιμότητας Δεδομένων (μη δυνατότητα ανάκτησης από αντίγραφα ασφαλείας)* | | | | | |
|---|---|---|---|---|---|
| **Πληροφορίες/ Δεδομένα** | Μέχρι 1 ώρα | Από 1 ώρα μέχρι 1 μέρα | Από 1 μέρα μέχρι 1 εβδομάδα | Από 1 εβδομάδα μέχρι 1 μήνα | Από 1 μήνα και πέρα |
| | | | | | |

**Αν η απώλεια διαθεσιμότητας πληροφοριών ανήκει στις κατηγορίες High ή Medium συμπληρώστε τα παρακάτω στοιχεία σχετικά με τη φύση των επιπτώσεων. Όπου είναι εφικτό προσδιορίστε το οικονομικό κόστος.** *(Θεωρήστε την περίπτωση με τη μεγαλύτερη κρισιμότητα και φόρτο εργασίας)*

- Κανονιστική και συμβατική συμμόρφωση:
  - Περιγραφή:
  - Κόστος:
- Επιχειρησιακή Λειτουργία:
  - Περιγραφή:
  - Κόστος:
- Εμπιστοσύνη πολιτών /προμηθευτών/ προσωπικού, Φήμη οργανισμού:
  - Περιγραφή:
  - Κόστος:

### 4.2 Ακεραιότητα Δεδομένων

| *Απώλεια Ακεραιότητας Δεδομένων (εσκεμμένη ή μη)* | | | | |
|---|---|---|---|---|
| **Πληροφορίες/ Δεδομένα** | Low | Medium | High | Σχόλια/Παρατηρήσεις |
| | | | | |

**Αν η απώλεια ακεραιότητας πληροφοριών ανήκει στις κατηγορίες High ή Medium συμπληρώστε τα παρακάτω στοιχεία σχετικά με τη φύση των επιπτώσεων. Όπου είναι εφικτό προσδιορίστε το οικονομικό κόστος.** *(Θεωρήστε την περίπτωση με τη μεγαλύτερη)*

- Κανονιστική και συμβατική συμμόρφωση:
    - Περιγραφή:
    - Κόστος:
- Επιχειρησιακή Λειτουργία:
    - Περιγραφή:
    - Κόστος:
- Εμπιστοσύνη πολιτών /προμηθευτών/ προσωπικού, Φήμη οργανισμού:
    - Περιγραφή:
    - Κόστος:

**Εμπιστευτικότητα Δεδομένων**

| *Απώλεια Εμπιστευτικότητας Δεδομένων (εσκεμμένη ή μη)* | | | | |
|---|---|---|---|---|
| **Πληροφορίες/ Δεδομένα** | Low | Medium | High | Σχόλια/Παρατηρήσεις |
| | | | | |

**Αν η απώλεια εμπιστευτικότητας πληροφοριών ανήκει στις κατηγορίες High ή Medium συμπληρώστε τα παρακάτω στοιχεία σχετικά με τη φύση των επιπτώσεων. Όπου είναι εφικτό προσδιορίστε το οικονομικό κόστος.** *(Θεωρήστε την περίπτωση με τη μεγαλύτερη κρισιμότητα και φόρτο εργασίας)*

- Κανονιστική και συμβατική συμμόρφωση:
    - Περιγραφή:
    - Κόστος:
- Επιχειρησιακή Λειτουργία:
    - Περιγραφή:
    - Κόστος:
- Εμπιστοσύνη πολιτών /προμηθευτών/ προσωπικού, Φήμη οργανισμού:
    - Περιγραφή:
    - Κόστος:

## ΔΕΔΟΜΕΝΑ

1. Από πού προήλθαν τα δεδομένα;
2. Σε ποιον μοιράζονται;
3. Ποιος είναι ο σκοπός της επεξεργασίας;
4. Περιγράψτε την επεξεργασία των δεδομένων.
5. Για πόσο διάστημα κρατούνται τα δεδομένα;
6. Σε περίπτωση που ο οργανισμός δε χρειάζεται πλέον τα δεδομένα, με ποιον τρόπο γίνεται η διαγραφή;
7. Υπάρχει καταγεγραμμένη η διαδικασία που ακολουθήθηκε κατά τη διαγραφή;
8. Τα εν λόγω δεδομένα υπάρχουν και σε άλλη τοποθεσία; Εάν ναι, με ποιον τρόπο καλύπτονται τα 6 και 7.

**Επιμέρους σχόλια:**

## ΥΠΟΚΕΙΜΕΝΟ ΔΕΔΟΜΕΝΩΝ

1. Γνωστοποιείται ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία στο υποκείμενο των δεδομένων;
2. Το υποκείμενο των δεδομένων ενημερώνεται για τους σκοπούς της επεξεργασίας;
3. Με ποιον τρόπο παρέχεται η συγκατάθεση του υποκειμένου του δεδομένων υπέρ της επεξεργασίας των δεδομένων που το αφορούν;
4. Με ποιον τρόπο αποδεικνύεται ότι το υποκείμενο των δεδομένων συγκατατέθηκε στην πράξη επεξεργασίας;

# Αρχείο παραβιάσεων προσωπικών δεδομένων

*Τα ακόλουθα άρθρα του ΓΚΠΔ καλύπτονται από το παρόν έγγραφο: Άρθρο 33 - Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή*
*Εδώ πρέπει να καταγράφονται οι λεπτομέρειες των παραβιάσεων των προσωπικών δεδομένων.*

| | |
|---|---|
| **Τελευταία ενημέρωση:** | dd/mm/yy |
| **Από:** | [Name] |

**Αρχείο παραβιάσεων προσωπικών δεδομένων**

| Ημερομηνία Προσδιορισμού Παραβίασης | Ώρα Προσδιορισμού Παραβίασης | Περιγραφή Παραβίασης | Ημερομηνία Κοινοποίησης της Παραβίασης στην Εποπτική Αρχή |
|---|---|---|---|
| | | | |
| | | | |
| **Ώρα Κοινοποίησης της Παραβίασης στην Εποπτική Αρχή** | **Χρόνος που πέρασε μέχρι την Ειδοποίηση (Ώρες)** | **Πιθανές Συνέπειες για τα Υποκείμενα των Δεδομένων** | **Εφαρμογή Διορθωτικής Ενέργειας (συμπεριλαμβανομένης οποιασδήποτε επικοινωνίας με τα υποκείμενα των δεδομένων)** |

**Φόρμα Γνωστοποίησης Παραβίασης Προσωπικών Δεδομένων**

**Λεπτομέρειες Γνωστοποίησης**

| | |
|---|---|
| **Όνομα**: | |
| **Τίτλος:** | |
| **Όνομα Οργανισμού**: | |
| **Διεύθυνση Οργανισμού:** | |
| **Τηλέφωνο**: | |
| **Διεύθυνση Email:** | |
| **Ημερομηνία και Ώρα** | |

| | |
|---|---|
| **Υποβολής Γνωστοποίησης:** | |
| **Ημερομηνία και Ώρα Ανίχνευσης της Παραβίασης:** | |
| **Χρόνος που έχει παρέλθει μεταξύ της ανίχνευσης και της ειδοποίησης:** | |

**Περιγραφή της Φύσης της Παραβίασης Προσωπικών Δεδομένων**

**Πιθανές Συνέπειες της Παραβίασης των Δεδομένων**

**Μέτρα που έχουν ήδη ληφθεί για την αντιμετώπιση της παραβίασης**

**Προτεινόμενα μέτρα που πρέπει να ληφθούν για την περαιτέρω αντιμετώπιση της παραβίασης**

**Λόγοι καθυστέρησης της γνωστοποίησης, εάν ισχύει**

## ΟΔΗΓΙΕΣ ΧΡΗΣΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ & ΔΙΑΔΙΚΤΥΟΥ

### Υπηρεσία Ηλεκτρονικού Ταχυδρομείου (e-mail)

- ✓ Το σύστημα ηλεκτρονικού ταχυδρομείου της εταιρίας προορίζεται για επαγγελματικούς σκοπούς. Ωστόσο, η εταιρία κατανοεί την ανάγκη για περιορισμένη και περιστασιακή χρήση του για προσωπικούς σκοπούς μόνο εφόσον υπάρχει η κατάλληλη διαβάθμιση και δεν αποστέλλεται παράνομο ή υβριστικό περιεχόμενο.
- ✓ Απαγορεύεται η αποστολή εσωτερικών επικοινωνιών ή υλικών εμπιστευτικού περιεχομένου εκτός της εταιρίας, εκτός εάν υπάρχει ρητή εξουσιοδότηση γι' αυτόν το σκοπό.
- ✓ Αναγνωριστικά, λογαριασμοί πρόσβασης και κωδικοί ασφαλείας δεν πρέπει να συμπεριλαμβάνονται σε e-mails.
- ✓ Δεν επιτρέπεται η χρήση του ηλεκτρονικού ταχυδρομείου για διαβίβαση οποιουδήποτε υλικού το οποίο καταγγέλλεται ότι παραβιάζει δικαιώματα πνευματικής ιδιοκτησίας άλλων.
- ✓ Το spam αποτελεί μη αποδεκτή χρήση του δικτύου της εταιρίας. Ως spam ορίζεται η μαζική αποστολή ηλεκτρονικών μηνυμάτων σε μια προσπάθεια προώθησης προϊόντων ή ιδεών.
- ✓ Απαγορεύεται η αποστολή μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου ιών Διαδικτύου, worms, trojan, καθώς επίσης και η διανομή πληροφοριών σχετικών με τη δημιουργία και την αποστολή αυτών.
- ✓ Εάν έχετε έγκριση για χρήση μιας προσωπικής συσκευής με σκοπό την αποθήκευση ή την προσπέλαση εταιρικών e-mail ή άλλων δεδομένων, η συσκευή σας θα υπόκειται στις ίδιες πρακτικές ασφάλειας και διαχείρισης δεδομένων που ισχύουν για τις εταιρικές συσκευές. Σε αυτές ενδέχεται να περιλαμβάνονται, μεταξύ άλλων, η υποχρεωτική χρήση κωδικού κλειδώματος όταν η συσκευή βρίσκεται σε αδράνεια και η κρυπτογράφηση δεδομένων. Η εταιρία θα έχει το δικαίωμα να ανακτά ή να διαγράφει εταιρικά δεδομένα από τη συσκευή, σύμφωνα με τους ισχύοντες νόμους και τις Πολιτικές Ασφάλειας Πληροφοριών.
- ✓ Σε περίπτωση που λαμβάνουμε ανεπιθύμητα μηνύματα, δεν ανοίγουμε τα συνημμένα των μηνυμάτων.
- ✓ Μην ανοίγετε e-mail από άγνωστους αποστολείς με περίεργα θέματα ή χωρίς θέμα.

- ✓ Στην περίπτωση που το e-mail έχει έρθει από γνωστό αποστολέα, δεν ανοίγουμε συνημμένα που μας έχουν έρθει ως πιθανώς κακόβουλα. Τα προωθούμε στη Δ/νση IT για να τα ελέγξει και να μας ενημερώσει.
- ✓ Πάντα ελέγχουμε τη διεύθυνση e-mail του αποστολέα, αφήνοντας για λίγο το mouse πάνω της ώστε να τη συγκρίνουμε με αυτή που φαίνεται αρχικά.
- ✓ Σε περίπτωση που ένα e-mail περιέχει κάποιο link ελέγχουμε εάν είναι αξιόπιστο.
- ✓ Σε περίπτωση εμφάνισης αναδυόμενων παραθύρων, θα πρέπει να αποφεύγουμε να εισάγουμε προσωπικά δεδομένα, που μας ζητούνται δήθεν για επιβεβαίωση.
- ✓ Δεν απαντάμε σε e-mail αγνώστων και δεν κάνουμε unsubscribe.
- ✓ Να θυμάστε ότι τα εταιρικά logos μπορούν πολύ εύκολα να αντιγραφούν σε ένα e-mail κάνοντάς το να φαίνεται γνήσιο.
- ✓ Τηρούμε εχεμύθεια και δεν αποκαλύπτουμε εμπιστευτικές πληροφορίες που αφορούν την εταιρία σε τρίτους.
- ✓ Προσοχή στην αποστολή εμπιστευτικών πληροφοριών μέσω e-mail (ελέγξτε προσεκτικά σε ποιους το αποστέλλετε) και προσοχή στις κοινοποιήσεις μηνυμάτων σε πρόσωπα εκτός από τον παραλήπτη (mail chain).

**Πρόσβαση στο Διαδίκτυο (Internet)**

- ✓ Δεν επισκεπτόμαστε ιστοσελίδες για τις οποίες δεν είμαστε σίγουροι ότι είναι νόμιμες και ασφαλείς (legitimate sites).
- ✓ Προσοχή στα links που εμπεριέχονται σε legitimate sites.
- ✓ Όχι άμεση εγκατάσταση από download. Προσέχουμε τι εγκαθιστούμε.
- ✓ Δεν εισάγουμε ευαίσθητα δεδομένα σε φόρμες που υπάρχουν σε ιστοσελίδες αν δεν είναι HTTPS το πρωτόκολλο επικοινωνίας.
- ✓ Η εμφάνιση του εικονιδίου με το πράσινο λουκέτο σε μια διαδικτυακή τοποθεσία είναι σημάδι ασφαλούς ιστοσελίδας. Όμως, το εικονίδιο με το λουκέτο μπορεί να είναι ψεύτικο.
- ✓ Δε συζητάμε ποτέ στα social media για Business Cases και γενικότερα για οτιδήποτε αφορά την εργασία μας.
- ✓ Προστατεύστε το αγαθό της ιδιωτικότητάς σας! Μη δίνετε ποτέ προσωπικά σας στοιχεία και μην αποκαλύπτετε λεπτομέρειες της προσωπικής σας ζωής στο Διαδίκτυο.
- ✓ Μη γνωστοποιείτε μέσω του Διαδικτύου τα στοιχεία επικοινωνίας σας σε αγνώστους.
- ✓ Μην αποκαλύπτετε τους κωδικούς πρόσβασης (password) που χρησιμοποιείτε.

- ✓ Να είστε επιφυλακτικοί ως προς την αποδοχή όσων διαβάζετε στο Διαδίκτυο ή αυτών που σας λένε οι άλλοι χρήστες, πριν το σκεφτείτε και το ελέγξετε.
- ✓ Μη στέλνετε υλικό από τον υπολογιστή σας (φωτογραφίες, μουσική, βίντεο) που προστατεύεται από πνευματικά δικαιώματα.
- ✓ Να έχετε πάντα υπόψη σας ότι τα προϊόντα της πνευματικής δημιουργίας (μουσική, λογοτεχνία, κινηματογράφος, video κ.λπ.) προστατεύονται από τους νόμους και η διανομή τους μέσω του Διαδικτύου είναι παράνομη πράξη.
- ✓ Παράνομη πράξη θεωρείται και η διακίνηση προγραμμάτων υπολογιστών (software) εκτός και αν ανήκουν στην κατηγορία του Ελεύθερου Λογισμικού (Open source software).

**Υπεύθυνη Δήλωση Αποδοχής Πολιτικής Ασφάλειας Πληροφοριών και Προστασίας Προσωπικών Δεδομένων του Φορέας.**

Με την παρούσα υπεύθυνη δήλωση, ο/η …… , εργαζόμενος /η του Π.Μ.Σ, δηλώνει ενυπόγραφα τη συμμόρφωση του/της με όσα ορίζουν οι Πολιτικές Ασφάλειας Πληροφοριών και Προστασίας Προσωπικών Δεδομένων του Π.Μ.Σ. Ιδιαίτερα, οφείλει να γνωρίζει και να τηρεί όσα προβλέπονται στο Εγχειρίδιο Ασφάλειας Πληροφοριών, στην Πολιτική Αποδεκτής Χρήσης, στις Οδηγίες Χρήσης Ηλεκτρονικού Ταχυδρομείου & Internet, στην Πολιτική Ασφάλειας Πληροφοριών και στην Πολιτική για την Ιδιωτικότητα και την Προστασία των Προσωπικών Δεδομένων του Π.Μ.Σ. Όλα τα παραπάνω, του/της κοινοποιούνται και επεξηγούνται αμέσως μετά την πρόσληψή του/της, από τον Υπεύθυνο Διαχείρισης Ασφάλειας Πληροφοριών (ΥΔΑΠ) του Φορέα. Σκοπός του Εγχειριδίου Ασφάλειας Πληροφοριών είναι να παρουσιάσει το πλαίσιο και την οργάνωση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών που ανέπτυξε και υλοποιεί το φορέα. Σκοπός της Πολιτικής Αποδεκτής Χρήσης είναι να διασφαλίσει ότι οι χρήστες του Π.Μ.Σ δε θα εκμεταλλευτούν την πρόσβαση η οποία τους παρέχεται σύμφωνα με την Πολιτική Πρόσβασης σε υπολογιστές, εφαρμογές και παντός είδους τηλεπικοινωνιακά δίκτυα προκειμένου να προβούν σε ενέργειες οι οποίες παραβιάζουν την Πολιτική Πρόσβασης, νόμους του κράτους, ή γενικότερα βλάπτουν την επιχειρηματική εικόνα του φορέα. Σκοπός των Οδηγιών Χρήσης Ηλεκτρονικού Ταχυδρομείου & Internet είναι να ορίσει τους κανόνες χρήσης του Ηλεκτρονικού Ταχυδρομείου και του Διαδικτύου ως ασφαλή μέσα για τη μετάδοση πληροφοριών του φορέα καθώς και να διασφαλίσει τους χρήστες τους. Σκοπός της Πολιτικής Ασφάλειας Πληροφοριών είναι να ορίσει την αποστολή και τη δέσμευση του φορέα όσον αφορά την εφαρμογή Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών και τη συνεχή προσπάθεια βελτίωσής του. Σκοπός της Πολιτικής για την Ιδιωτικότητα και την Προστασία των Προσωπικών Δεδομένων είναι να περιγράψει τη σχετική νομοθεσία και να παρουσιάσει τα βήματα που ακολουθεί το Π.Μ.Σ για να εξασφαλίσει τη συμμόρφωσή του σε αυτή. Επιπλέον, ο/η εργαζόμενος/η οφείλει να διαχειρίζεται τις πληροφορίες του φορέα, στις οποίες έχει πρόσβαση, σύμφωνα με το βαθμό διαβάθμισής τους, όπως αυτός έχει οριστεί από τον ιδιοκτήτη της πληροφορίας. Ειδικά για τα έγγραφα που έχουν διαβαθμιστεί ως εμπιστευτικά απαγορεύεται ρητά η κοινοποίησή τους σε μη εξουσιοδοτημένα άτομα.Ο/Η εργαζόμενος, με την παρούσα, δηλώνει ενυπόγραφα τη συμμόρφωσή του/της υπέρ της επίτευξης του σκοπού ύπαρξης των προαναφερθεισών πολιτικών και γενικότερα τη συμβολή του/της ώστε να υιοθετείται ομαλά το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών και το Πρόγραμμα Προστασίας Προσωπικών Δεδομένων του Π.Μ.Σ.

Ημερομηνία: __ / __ / ____

Ο/Η εργαζόμενος/η

…….

Ο Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών

Ονοματεπώνυμο

**Β Ι Β Λ Ι Ο  Ε Π Ι Σ Κ Ε Π Τ Ω Ν**

| **Ημερομηνία** | **Χρόνος Εισόδου** | **Χρόνος Εξόδου** | **Ονοματεπώνυμο Επισκέπτη** | **Σκοπός Επίσκεψης** | **Χώρος Επίσκεψης** | **Υπογραφή Συνοδεύοντος** |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |

## ΔΗΛΩΣΗ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ – ΑΝΕΞΑΡΤΗΣΙΑΣ

Ο/Η παρακάτω υπογράφων/ουσα ……..……..

μέλος του προσωπικού του φορέα δηλώνω ότι κατά την εκτέλεση των καθηκόντων μου στο εργαστήριο :

1. Θα συμμορφώνομαι και θα εκτελώ με ακρίβεια τα καθήκοντα που αναφέρονται στο Εγχειρίδιο Ποιότητας του εργαστηρίου και τα οποία με αφορούν.
2. Θα χειρίζομαι ως εμπιστευτικές όλες τις πληροφορίες που λαμβάνω κατά την εκτέλεση των καθηκόντων μου και δεν θα αποκαλύπτω αυτές σε οποιοδήποτε πρόσωπο ή φορέα, τώρα ή στο μέλλον και δε θα χρησιμοποιώ αυτές για προσωπικό μου όφελος.
3. Θα αποκαλύπτω τα συμπεράσματα που προέρχονται από τις εργασίες που εκτελώ μόνον στα πρόσωπα ή στους φορείς, στα οποία από τις διαδικασίες του εργαστηρίου προβλέπεται να κοινοποιούνται.
4. Θα διατηρώ το υλικό τεκμηρίωσης που λαμβάνω στο φορέα με τρόπο ασφαλή, δεν θα προβώ σε αναπαραγωγή αυτού χωρίς την γραπτή άδεια του φορέα και δεν θα παραδώσω το υλικό αυτό σε τρίτους.
5. Δεν θα έχω οικονομική ή άλλη εξάρτιση από συνεργαζόμενο του φορέα ή από συνδεόμενο με αυτόν φορέα, ούτε θα δεχθώ οποιαδήποτε σχέση ή επιρροή η οποία θα μπορούσε να επηρεάσει την αντικειμενικότητα της κρίσης μου κατά την εκτέλεση των καθηκόντων μου.
6. Σε περίπτωση αθέτησης της παρούσας δήλωσης θα παράσχω στη διοίκηση του φορέα οποιαδήποτε πληροφορία μου ζητηθεί στα πλαίσια της εξέτασης της σχετικής υπόθεσης.

Ημερομηνία : ___ / ___ / _____

Ο/Η ΔΗΛΩΝ/ΟΥΣΑ

(υπογραφή)

## *ΒΙΒΛΙΟΓΡΑΦΙΑ*


British, The, and Assessment Bureau. 2016. “Source: ISO2K7 Forum, 2016.”

Data, New, and Protection Bill. 2018. “Colleges and the General Data Protection Regulations ( GDPR ).” (September 2017).

“Directive 95/46/EC of the European Parliament and of the Council.”

Iso-Iec Standards. 2011. “INTERNATIONAL STANDARD ISO / IEC Techniques — Information Security Risk.” *Iso-Iec Standards* 2011.

Laudon, Kenneth C. 2014. *Πληροφοριακά Συστήματα Διοίκησης*. ATHENS: Κλειδάριθμος.

MANCHESTER METROPOLTAN UNIVERSITY. 2018. *Data Protection Training Module*.

Miroslav Hrubý. 2016. “GENERAL DATA PROTECTION REGULATION (GDPR) AND DISTANCE LEARNING.” http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

Moskal, Patsy, Charles Dziuban, and Joel Hartman. 2013. “Blended Learning: A Dangerous Idea?” *Internet and Higher Education* 18: 15–23. http://dx.doi.org/10.1016/j.iheduc.2012.12.001.

UNIVERSITY OF CAMBRIDGE GDPR DATA PROTECTION WORKING. 2018. *TOOLKIT TO HELP UNIVERSITY INSTITUTIONS PREPARE FOR NEW DATA PROTECTION LEGISLATION (GDPR) NOVEMBER*.

*UNIVERSITY OF CAMBRIDGE UPDATE ON PREPARATIONS FOR THE GDPR*. 2018.

UNIVERSITY OF STIRLING. 2018. *Data Protection Guidance Handbook*.

“Επίσημη Εφημερίδα Τον Ευρωπαϊκών Κοινοτήτων.” 1995. : 31–50.

Ευρωπαϊκή Ένωση. 2016. “ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ Της 27ης Απριλίου 2016.” 2014.

“Ευρωπαϊκή ΣύμβΑση Δικαιωμάτων Του Ανθρώπου Ευρωπαϊκή ΣύμβΑση Δικαιωμάτων Του Ανθρώπου.” 2002.

Κυριακή Σπανού. 1996. *Το ΠρόβΛημα Της Δημόσιας Διοίκησης: Μια Πρώτη Προσέγγιση.* ed. Εκδ. ΙΟΒΕ. ΑΘΗΝΑ.