



**ΣΩΜΑΤΕΙΟ ΕΡΓΑΖΟΜΕΝΩΝ
MOTOR OIL (Σ.Ε.Μ.Ο)
MOTOR OIL WORKERS
UNION (M.O.W.U.)**

ΓΕΝΙΚΗ ΠΟΛΙΤΙΚΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

1^η ΕΚΔΟΣΗ

Αθήνα 2019

ΠΕΡΙΕΧΟΜΕΝΑ

1.Εισαγωγή.....	2
2. Ορισμοί.....	3
3. Δήλωση Γενικής Πολιτικής Προστασίας Δεδομένων.....	3
4. Συλλογή Δεδομένων από το Σωματείο.....	4
5. Αρχές που διέπουν την επεξεργασία.....	5
6. Δικαιώματα του Υποκειμένου των Δεδομένων.....	7
7. Ευθύνη του Σωματείου.....	9
8. Τεχνικά και Οργανωτικά Μέτρα.....	9
9. Εκτελών την επεξεργασία.....	10
10. Υπεύθυνος Προστασίας Δεδομένων.....	10
11. Προστασία των δεδομένων ήδη από το σχεδιασμό.....	11
12. Εκτίμηση αντικτύπου.....	11
13. Ασφαλής αρχειοθέτηση δεδομένων.....	11
14. Φάκελος προστασίας δεδομένων προσωπικού χαρακτήρα.....	12
15. Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα.....	12
16. Δέσμευση Διοικητικού Συμβουλίου.....	13

1. Εισαγωγή

Το παρόν εγχειρίδιο, παρέχει το γενικό πλαίσιο για τις πολιτικές και τις διαδικασίες που έχει θεσπίσει το ΔΣ του Σωματείου Εργαζομένων της MOTOR OIL για την προστασία των προσωπικών δεδομένων, σύμφωνα με τις απαιτήσεις Γενικού Κανονισμού 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και του Ν. 4624/2019.

Το εγχειρίδιο περιγράφει με λεπτομέρειες την προσέγγιση του Σωματείου για τη διαχείριση της προστασίας των δεδομένων του και περιλαμβάνει τη γενική στρατηγική για το σχεδιασμό, την υποστήριξη, την λειτουργία, την αξιολόγηση και την συνεχή βελτίωση της παρεχόμενης προστασίας.

Η προσέγγιση αυτή εφαρμόζεται σε όλες τις διαδικασίες και τους ανθρώπους του Σωματείου, συμπεριλαμβανομένων και των μελών του ΔΣ.

2. Ορισμοί

Στον 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».

Ως **υπεύθυνος επεξεργασίας** ορίζεται «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».

Ως **εκτελών την επεξεργασία** ορίζεται «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας».

3. Δήλωση Γενικής Πολιτικής Προστασίας Δεδομένων

Στόχος της Γενικής Πολιτικής Προστασίας Δεδομένων είναι η προστασία των δεδομένων προσωπικού χαρακτήρα έναντι όλων των εσωτερικών, εξωτερικών, εκούσιων ή ακούσιων απειλών. Το Σωματείο έχει εγκρίνει την Γενική Πολιτική Προστασίας Δεδομένων και προσυπογράφει, δια του παρόντος, την πλήρη δέσμευσή του για την αποτελεσματική εφαρμογή της.

Η Γενική Πολιτική Προστασίας Δεδομένων αποσκοπεί στο να διασφαλιστούν τα εξής:

- Συνεχής προστασία των δεδομένων από τυχόν μη εξουσιοδοτημένη πρόσβαση.
- Διασφάλιση της Εμπιστευτικότητας των δεδομένων του Σωματείου.
- Διατήρηση της Ακεραιότητας των δεδομένων του Σωματείου.
- Συνεχής διασφάλιση της Διαθεσιμότητας των δεδομένων.
- Διαρκής παρακολούθηση και τήρηση των Νομοθετικών και Κανονιστικών Απαιτήσεων του Σωματείου.
- Συνεχής εκπαίδευση σε θέματα Προστασίας Δεδομένων για όλους τους εμπλεκόμενους στις διαδικασίες του Σωματείου.
- Ανάπτυξη και εφαρμογή κατάλληλων διαδικασιών και επιμέρους πολιτικών προστασίας δεδομένων για την υποστήριξη της εν λόγω πολιτικής, περιλαμβανομένων τεχνικών και οργανωτικών μέτρων προστασίας.
- Η συμμόρφωση με τη Γενική Πολιτική Προστασίας Δεδομένων είναι υποχρεωτική για όλους όσους εμπλέκονται με τις διαδικασίες του Σωματείου.
- Τυχόν παραβιάσεις της Γενικής Πολιτικής Προστασίας Δεδομένων, υπόκεινται σε πειθαρχικές κυρώσεις. Κάθε κύρωση εξαρτάται από τη φύση και την επίπτωση της παράβασης.

4. Συλλογή Δεδομένων από το Σωματείο

Σύμφωνα με το τρέχον σχετικό θεσμικό πλαίσιο, σκοπός του Σωματείου είναι η ηθική και υλική εξύψωση των μελών, η ανάπτυξη του πνεύματος της συναδελφώσεως και αλληλεγγύης μεταξύ αυτών η μελέτη, η προστασία, η υποστήριξη και η προαγωγή των επαγγελματικών συμφερόντων των μελών, η αναγνώριση και κατοχύρωση των δικαιωμάτων και υποχρεώσεων των μελών αυτού στην κοινωνία και την πολιτεία.

Το Σωματείο συλλέγει προσωπικά δεδομένα που παρέχετε εσείς άμεσα με την εγγραφή σας. Η παροχή των προσωπικών σας αυτών δεδομένων γίνεται μέσω συμπλήρωσης και υποβολής της σχετικής αίτησης.

Για την εγγραφή σας στο Σωματείο σας ζητούνται τα εξής προσωπικά δεδομένα: ονοματεπώνυμο, όνομα πατρός, έτος γέννησης, τόπος διαμονής (οδός, αριθμό ΤΚ), οικογενειακή κατάσταση, ειδικότητα, τμήμα, βάρδια, ημερομηνία πρόσληψης, ημερομηνία εγγραφής, ΑΦΜ, ΑΔΤ και αριθμός τηλεφώνου (**στοιχεία αίτησης**).

Στο πλαίσιο του παραπάνω σκοπού, η συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι σύννομη, ακόμη και χωρίς τη ρητή συγκατάθεση των υποκειμένων, στο βαθμό που η συλλογή προσωπικών δεδομένων πηγάζει από το νόμο και το καταστατικό του Σωματείου (αρ. 4 του Καταστατικού).

Τα δεδομένα αυτά είναι ακριβή, κατάλληλα και συναφή προς το σκοπό συλλογής τους, επικαιροποιούνται όταν είναι αναγκαίο και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με τον προαναφερθέντα σκοπό.

Σε περίπτωση που η επεξεργασία αφορά παιδιά κάτω των 16 ετών, λαμβάνεται συγκατάθεση του γονέα / κηδεμόνα.

Απαγορεύεται η επεξεργασία προσωπικών δεδομένων **ειδικών κατηγοριών**, όπως φυλετική προέλευση, εθνική καταγωγή, πολιτικά φρονήματα, θρησκευτικές πεποιθήσεις, φιλοσοφικές πεποιθήσεις, συμμετοχή σε ένωση, σωματείο, γενετικά δεδομένα, βιομετρικά δεδομένα, δεδομένα υγείας, στοιχεία σχετικά με τη σεξουαλική ζωή ενός φυσικού προσώπου, σεξουαλικός προσανατολισμός, ιατρικό ιστορικό, ιατρικοί ισχυρισμοί, διαγνώσεις, θεραπείες, αντίγραφο ποινικού μητρώου.

Εξάιρεση αποτελούν οι κάτωθι περιπτώσεις, όπου:

- Το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς.
- Η επεξεργασία είναι απαραίτητη για:
 - (1) την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του Σωματείου ή του υποκειμένου των δεδομένων.
 - (2) την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί.
 - (3) τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.
 - (4) λόγους ουσιαστικού δημοσίου συμφέροντος.
 - (5) σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής, ιστορικής ή στατιστικής έρευνας.
- Η επεξεργασία αφορά σε δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων.

5. Αρχές που διέπουν την επεξεργασία

Τα δεδομένα προσωπικού χαρακτήρα υπόκεινται σε επεξεργασία, η οποία διενεργείται σύμφωνα με τις αρχές της νομιμότητας, της αντικειμενικότητας και της διαφάνειας, λαμβάνοντας υπόψη τυχόν επιπλέον περιορισμούς που επιβάλλει ο σκοπός της επεξεργασίας. Παρακάτω παρουσιάζονται συνοπτικά οι βασικές αρχές, όπως προκύπτουν από το Γενικό Κανονισμό Προστασίας Δεδομένων:

(1) Αρχή της Νομιμότητας, Αντικειμενικότητας και Διαφάνεια

Τα δεδομένα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς και η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων

που επιδιώκει το Σωματείο 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. Η διαφάνεια απαιτεί η ενημέρωση του υποκειμένου να είναι συνοπτική, εύκολα προσβάσιμη, κατανοητή, με σαφή και απλή διατύπωση.

(2) Αρχή του Σκοπού

Ο σκοπός είναι βασικό στοιχείο του δικαιώματος και αποτελεί γνώμονα αξιολόγησης και των υπολοίπων αρχών. Τα δεδομένα υπόκεινται σε επεξεργασία για καθορισμένους, ρητούς και νόμιμους σκοπούς, ενώ δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Εν προκειμένου, τα δεδομένα υποβάλλονται σε επεξεργασία για τους σκοπούς της συνδικαλιστικής δράσης, όπως προσδιορίζονται στο καταστατικό του Σωματείου και στους οικείους νόμους. Επίσης, υποβάλλονται σε επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, σκοπούς επιστημονικής, ιστορικής ή στατιστικής έρευνας.

(3) Αρχή της Αναλογικότητας

Τα δεδομένα είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς τους οποίους υποβάλλονται σε επεξεργασία. Η αρχή της «ελαχιστοποίησης των δεδομένων»(dataminimisation) αναδεικνύεται σε βασικό γνώμονα επεξεργασίας και αξιολόγησης της συμμόρφωσης.

(4) Αρχή της Ακρίβειας – Επικαιροποίησης

Τα δεδομένα είναι ακριβή και επικαιροποιούνται εφόσον απαιτείται. Επιπλέον, εύλογα μέτρα τηρούνται για την άμεση διαγραφή ή διόρθωση των δεδομένων. Επιπλέον, δίνεται η δυνατότητα στα υποκείμενα να διορθώνουν τα δεδομένα τους.

(5) Αρχή της Περιορισμένης Διάρκειας Τήρησης

Τα δεδομένα τηρούνται μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας. Εξαιρεση αποτελούν τα δεδομένα που τηρούνται για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής, ιστορικής ή στατιστικής έρευνας.

(6) Αρχή της Ενδεδειγμένης Ασφάλειας

Τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια τους, την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία, τυχαία απώλεια, καταστροφή ή φθορά, με τη χρήση κατάλληλων τεχνικών και οργανωτικών μέτρων.

(7) Αρχή της Λογοδοσίας

Το Σωματείο φέρει την ευθύνη και βρίσκεται πάντα σε θέση να αποδείξει τη συμμόρφωση με τις αρχές που διέπουν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

6. Δικαιώματα του Υποκειμένου των Δεδομένων

Το Σωματείο λαμβάνει τα κατάλληλα μέτρα προκειμένου να διευκολύνει την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων, όπως αυτά απορρέουν από το Γενικό Κανονισμό.

Σημειώνεται ότι τα δικαιώματα διαγραφής, εναντίωσης και φορητότητας δύναται να ασκηθούν μόνο στην περίπτωση που από την άσκησή τους δεν βλάπτεται άλλο δικαίωμα του υποκειμένου των δεδομένων ή δεν εμποδίζεται η εκπλήρωση της υποχρέωσης που έχει αναλάβει το Σωματείο έναντι των υποκειμένων των δεδομένων.

(1) Δικαίωμα Ενημέρωσης

Το Σωματείο παρέχει στο υποκείμενο πληροφορίες σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν. Η ενημέρωση δύναται να γίνει εγγράφως, ηλεκτρονικά ή προφορικά, κατ' αίτηση, σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή. Στην περίπτωση όπου το υποκείμενο των δεδομένων επιθυμεί την προφορική ενημέρωση, οφείλει να αποδεικνύει την ταυτότητα του με άλλα μέσα.

Σύμφωνα με τον Κανονισμό, η ενημέρωση πραγματοποιείται εντός εύλογης προθεσμίας, το αργότερο δηλαδή, εντός μηνός, από την παραλαβή του αιτήματος. Εάν, λόγω πολυπλοκότητας του αιτήματος και του αριθμού των αιτημάτων απαιτείται μεγαλύτερο χρονικό διάστημα, τότε το Σωματείο δύναται να ικανοποιήσει το αίτημα εντός διμήνου από την παρέλευση του μηνός, έπειτα από πληροφόρηση του υποκειμένου για την παράταση αυτή.

Η ενημέρωση οφείλει να πραγματοποιείται στις ακόλουθες περιπτώσεις:

- i. Κατά την πρώτη επικοινωνία με το υποκείμενο των δεδομένων, αν πρόκειται να χρησιμοποιηθούν τα δεδομένα για επικοινωνία με αυτό.
- ii. Όταν τα δεδομένα γνωστοποιούνται για πρώτη φορά σε άλλον (τρίτο) αποδέκτη.
- iii. Πριν από την περαιτέρω επεξεργασία για σκοπό διάφορο από αυτόν που αρχικώς είχαν συλλεχθεί τα δεδομένα.

(2) Δικαίωμα Πρόσβασης

Το υποκείμενο των δεδομένων δικαιούται να λαμβάνει από το Σωματείο επιβεβαίωση για το κατά πόσον τα δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία, τους σκοπούς επεξεργασίας και τη νομική βάση για την επεξεργασία, τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα των οποίων γίνεται επεξεργασία, τους αποδέκτες (παρόντες και μελλοντικούς) στους οποίους κοινοποιήθηκαν τα

δεδομένα προσωπικού χαρακτήρα και το δικαίωμα υποβολής καταγγελίας στην κατά περίπτωση αρμόδια εποπτική αρχή και τα στοιχεία επικοινωνίας με αυτή.

Εφόσον ζητηθεί, το Σωματείο παράσχει αντίγραφο των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Για επιπλέον αντίγραφα που ενδέχεται να ζητηθούν από το υποκείμενο των δεδομένων, δύναται να επιβληθεί η καταβολή εύλογου τέλους για διοικητικά έξοδα..

(3) Δικαίωμα Διόρθωσης

Το υποκείμενο των δεδομένων δικαιούται να απαιτήσει από το Σωματείο, χωρίς αδικαιολόγητη καθυστέρηση, την διόρθωσή ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Λαμβάνοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο είναι σε θέση να απαιτήσει την συμπλήρωση ελλিপών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων, μέσω συμπληρωματικής δήλωσης. Το Σωματείο δεν στερείται του δικαιώματος να ζητήσει απόδειξη της επικαλούμενης ανακρίβειας ή έλλειψης.

(4) Δικαίωμα Διαγραφής («δικαίωμα στη λήθη»)

Το Σωματείο επεξεργάζεται αιτήματα που σχετίζονται με την διαγραφή δεδομένων προσωπικού χαρακτήρα και προέρχονται από το ίδιο το υποκείμενο που αφορούν.

Το αίτημα του υποκειμένου δεν δύναται να ικανοποιηθεί στο βαθμό που η επεξεργασία είναι απαραίτητη για:

- i. την άσκηση του δικαιώματος ελευθερίας της έκφρασης και δικαιώματος στην ενημέρωση,
- ii. λόγους δημόσιου συμφέροντος,
- iii. σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής, ιστορικής ή στατιστικής έρευνας, εφόσον το δικαίωμα της διαγραφής είναι πιθανόν να καταστήσει αδύνατη ή να εμποδίσει σε μεγάλο βαθμό την επίτευξη σκοπών της εν λόγω επεξεργασίας,
- iv. τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

(5) Δικαίωμα περιορισμού της επεξεργασίας

Το Σωματείο εξασφαλίζει στο υποκείμενο των δεδομένων το δικαίωμα περιορισμού της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα σε περίπτωση που:

- i. Το υποκείμενο των δεδομένων αμφισβητεί την ακρίβεια των δεδομένων προσωπικού χαρακτήρα, για χρονικό διάστημα που επιτρέπει στο Σωματείο να επαληθεύσει την ακρίβειά τους.
- ii. Η επεξεργασία είναι παράνομη και το υποκείμενο εγείρει αντιρρήσεις ή αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους.

- iii. Το Σωματείο δεν χρειάζεται τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς επεξεργασίας, αλλά απαιτούνται για την θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Το Σωματείο δεν δύναται να προβεί στην επεξεργασία των δεδομένων για το χρονικό διάστημα που αυτά είναι περιορισμένα. Επίσης, ενημερώνει και τους τρίτους, στους οποίους ενδέχεται να έχουν κοινοποιηθεί τα δεδομένα.

(6) Δικαίωμα φορητότητας των δεδομένων

Το Σωματείο εξυπηρετεί αιτήματα για φορητότητα δεδομένων προσωπικού χαρακτήρα, τα οποία προέρχονται από το ίδιο το υποκείμενο που αφορούν. Τα υποκείμενα δύναται να ζητούν την απευθείας διαβίβαση των δεδομένων αυτών από έναν υπεύθυνο επεξεργασίας σε άλλον, σε περίπτωση που αυτό είναι τεχνικά εφικτό. Το αίτημα ικανοποιείται μόνο στις περιπτώσεις όπου είτε η επεξεργασία βασίζεται σε συγκατάθεση ή σύμβαση, είτε διενεργείται με αυτοματοποιημένα μέσα.

Το εν λόγω δικαίωμα δεν ισχύει για την επεξεργασία που είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στο Σωματείο και δεν επηρεάζει δυσμενώς δικαιώματα και ελευθερίες άλλων.

7. Ευθύνη του Σωματείου

Το Σωματείο εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα, προκειμένου να διασφαλίζει και να αποδεικνύει ότι η επεξεργασία διενεργείται σύννομα, σε συνάρτηση με τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, λαμβάνοντας υπόψη τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

8. Τεχνικά και Οργανωτικά Μέτρα

Στα τεχνικά και οργανωτικά μέτρα που εφαρμόζει το Σωματείο και ο εκτελών την επεξεργασία, περιλαμβάνονται, μεταξύ άλλων, κατά περίπτωση και:

- (1) **Η κρυπτογράφηση και η αποκρυπτογράφηση** των δεδομένων προσωπικού χαρακτήρα, με τα οποία το Σωματείο κατά την διαβίβαση των δεδομένων των μελών του ακολουθεί διαδικασία μετατροπής των δεδομένων σε μια μορφή, στην οποία θα αποκρύπτεται το περιεχόμενό τους.
- (2) **Η ψευδωνυμοποίηση και η ανωνυμοποίηση** των δεδομένων προσωπικού χαρακτήρα, με τα οποία το Σωματείο επεξεργάζεται τα δεδομένα των μελών του κατά τρόπο ώστε τα δεδομένα αυτά να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα.

- (3) Η δυνατότητα **διασφάλισης του απορρήτου** με την ύπαρξη απαραίτητου ελέγχου λογικής πρόσβασης σε όλα τα συστήματα με τον καθορισμό διαφορετικών κατηγοριών.
- (4) Η δυνατότητα της **ακεραιότητας** και της **αξιοπιστίας** του συστήματος επεξεργασίας σε συνεχή βάση, μέσω της χρήσης αποτελεσματικού προγράμματος Antivirus.
- (5) Η δυνατότητα της **διαθεσιμότητας**. Κάθε κρίσιμο στοιχείο είναι τουλάχιστον διπλό, ώστε να μην υπάρχει μοναδικό σημείο ή βλάβη που θα καθιστά το όλο σύστημα μη διαθέσιμο και τα αντίγραφα ασφαλείας θα πρέπει να φυλάσσονται σε ξεχωριστό χώρο από αυτόν που φιλοξενείται και λειτουργεί το κύριο πληροφοριακό σύστημα.
- (6) Η διαδικασία για την **τακτική δοκιμή, εκτίμηση και αξιολόγηση** της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας. Όλες οι αδυναμίες, τα περιστατικά ασφαλείας καταγράφονται, αναλύονται και αξιολογούνται, ώστε να κλείνουν άμεσα και αποτελεσματικά, ώστε να αποφεύγεται η επανεμφάνισή τους στο μέλλον.

Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας πρέπει να λαμβάνονται υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

9. Εκτελών την επεξεργασία

Για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, το Σωματείο δύναται να αναθέτει την επεξεργασία σε εκτελούντες, για τους οποίους μεριμνά ότι τηρούν τις ρυθμίσεις και τις υποχρεώσεις που απορρέουν από το Γενικό Κανονισμό Προστασίας Δεδομένων. Οι εκτελούντες την επεξεργασία οφείλουν να παρέχουν επαρκείς εγγυήσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, ώστε να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων.

Η επεξεργασία από τον εκτελούντα διέπεται από σύμβαση ή άλλη νομική πράξη, που τον συνδέει με το Σωματείο. Σε αυτήν καθορίζεται το αντικείμενο, η διάρκεια, η φύση και ο σκοπός επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα, οι κατηγορίες των υποκειμένων των δεδομένων, καθώς επίσης οι υποχρεώσεις και τα δικαιώματα του Σωματείου.

Ο εκτελών την επεξεργασία δεν δύναται να προσλάβει άλλον εκτελούντα την επεξεργασία, χωρίς να έχει παρασχεθεί ειδική ή γενική γραπτή άδεια από το Σωματείο.

10. Υπεύθυνος Προστασίας Δεδομένων

Το Σωματείο δεν είναι δημόσια αρχή, ούτε εκτελεί επεξεργασίες μεγάλης κλίμακας ή επεξεργασίες ιδιαίτερα ευαίσθητων κατηγοριών δεδομένων. Επομένως, με βάση τον ΓΚΠΔ, το Σωματείο δεν υποχρεούται να αναδείξει Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ).

Ωστόσο, σε περίπτωση που οριστεί Υπεύθυνος Προστασίας Δεδομένων, την θέση αυτή θα την αναλαμβάνει ο Πρόεδρος του Διοικητικού Συμβουλίου.

11. Προστασία των δεδομένων ήδη από το σχεδιασμό

Το Σωματείο έχει υιοθετήσει την αρχή της προστασίας των δεδομένων ήδη από το σχεδιασμό (bydesign) και εξασφαλίζει 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, συμπεριλαμβανομένης και της διενέργειας μίας ή περισσότερων αξιολογήσεων των επιπτώσεων στην προστασία των δεδομένων (Μελέτες Αντικτύπου).

12. Εκτίμηση αντικτύπου

Όταν μια μορφή επεξεργασίας, ιδίως με τη χρήση νέων τεχνολογιών λαμβανομένων υπόψη της φύσης, του πλαισίου, του πεδίου εφαρμογής και των σκοπών της επεξεργασίας, είναι πιθανόν να προκαλέσει μεγάλο κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, το Σωματείο, πριν από την επεξεργασία, προβαίνει σε εκτίμηση επιπτώσεων των προβλεπόμενων πράξεων επεξεργασίας στην προστασία των δεδομένων προσωπικού χαρακτήρα.

Η διενέργεια εκτίμησης επιπτώσεων της επεξεργασίας στο δικαίωμα προστασίας δεδομένων προσωπικού χαρακτήρα είναι αναγκαία στην περίπτωση που πρόκειται να πραγματοποιηθεί επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων ή αυτοματοποιημένη ατομική λήψη αποφάσεων.

Όπου ενδείκνυται, το Σωματείο ζητεί τη γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους για τη σχεδιαζόμενη επεξεργασία, με την επιφύλαξη της προστασίας εμπορικών ή δημόσιων συμφερόντων ή της ασφάλειας των πράξεων επεξεργασίας.

Όταν η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο, ελλείψει μέτρων μετριασμού του κινδύνου, από τον υπεύθυνο επεξεργασίας, το Σωματείο ζητεί τη γνώμη της Εποπτικής Αρχής Προστασίας Δεδομένων, πριν από την επεξεργασία.

13. Ασφαλής αρχειοθέτηση δεδομένων

Πρέπει να διασφαλίζεται ότι σε περίπτωση που το Σωματείο διατηρεί αρχεία δεδομένων που δεν χρησιμοποιούνται σε καθημερινή βάση, αλλά δεν έχει επέλθει η λήξη της περιόδου τήρησης τους, τότε τα αρχεία αυτά παραμένουν ασφαλή, και ειδικά στην περίπτωση που τα δεδομένα αυτά είναι δεδομένα προσωπικού χαρακτήρα ή ειδικών κατηγοριών.

- Το Σωματείο μπορεί να δημιουργήσει διαδικασία διαχείρισης αρχείων, στην οποία θα καθορίζονται τα δεδομένα τα οποία πρέπει να αρχειοθετούνται, ο τρόπος και η τοποθεσία αποθήκευσής τους, καθώς και ο τρόπος διαχείρισης των περιγραφικών δεδομένων.
- Το Σωματείο εφαρμόζει συγκεκριμένες μεθόδους πρόσβασης σε αρχειοθετημένα δεδομένα, καθώς η χρήση τέτοιων δεδομένων υποχρεούται να ακολουθεί ειδικό χειρισμό.
- Για την καταστροφή ενός αρχείου δεδομένων, το Σωματείο εφαρμόζει διαδικασία που να εγγυάται την πλήρη καταστροφή του.

Το Σωματείο οφείλει να αποφεύγει την χρήση μέσων τα οποία δεν έχουν επαρκή εγγύηση ως προς την διάρκεια λειτουργίας τους.

Τέλος, σε περίπτωση που το Σωματείο τηρεί δεδομένα σε ενεργές βάσεις δεδομένων, τις δηλώνει ως αρχειοθετημένες.

14. Φάκελος προστασίας δεδομένων προσωπικού χαρακτήρα

Η τήρηση των κανόνων και, εν γένει, η συμμόρφωση προς τις κανονιστικές απαιτήσεις υποστηρίζεται σημαντικά από την τήρηση φακέλου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Για τον λόγο αυτό, το Σωματείο μπορεί να δημιουργήσει αρχείο, όπου θα τηρούνται όλα τα έγγραφα και οι αποφάσεις που αφορούν στην προστασία δεδομένων προσωπικού χαρακτήρα, η σχετική τεκμηρίωση (π.χ. κώδικας δεοντολογίας) και το σύνολο της αλληλογραφίας με την ΑΠΔΠΧ.

15. Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα

Κάθε παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία, γνωστοποιείται στην Εποπτική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και το υποκείμενο των δεδομένων. Ο εκτελών την επεξεργασία ενημερώνει το Σωματείο αμέσως μόλις αντιληφθεί παραβίαση δεδομένων προσωπικού χαρακτήρα.

Το Σωματείο κοινοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος κατ' ελάχιστον στην **Εποπτική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα** τη φύση και τις κατηγορίες της παραβίασης, τον κατά προσέγγιση αριθμό και τις κατηγορίες των θιγομένων, τον κατά προσέγγιση αριθμό των επηρεαζόμενων αρχείων, τις ενδεχόμενες συνέπειες της παραβίασης και τα ληφθέντα ή προτεινόμενα μέτρα για αντιμετώπιση της παραβίασης, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών επιπτώσεών της.

Εξαιρούνται περιπτώσεις παραβιάσεων δεδομένων προσωπικού χαρακτήρα που δεν ενδέχεται να προκαλέσουν κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Σε περίπτωση που δεν είναι δυνατόν να παρασχεθούν οι πληροφορίες ταυτόχρονα, οφείλουν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση.

Τέλος, ο υπεύθυνος επεξεργασίας τεκμηριώνει κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα, που συνίστανται στα πραγματικά περιστατικά που αφορούν την παραβίαση αυτή, τις συνέπειες και τα ληφθέντα διορθωτικά μέτρα. Η εν λόγω τεκμηρίωση επιτρέπει στην Εποπτική Αρχή Προστασίας Δεδομένων να επαληθεύει τη συμμόρφωση με το άρθρο 33 του ΓΚΠΔ.

Υπό το ΓΚΠΔ, η Εποπτική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει την εξουσιοδότηση να επιβάλει είτε πρόστιμο είκοσι (20) εκατομμυρίων ευρώ, είτε πρόστιμο που να ανέρχεται έως το 4 τοις εκατό του ετήσιου παγκόσμιου κύκλου εργασιών, αναλόγως του ποιο από τα δύο είναι υψηλότερο, σε περίπτωση παραβίασης του Γενικού Κανονισμού.

Το Σωματείο ανακοινώνει αμελλητί τις παραβιάσεις των προσωπικών δεδομένων στα **υποκείμενα**, όταν ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Εξαιρούνται περιπτώσεις στις οποίες ο υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, έλαβε μέτρα που διασφαλίζουν ότι δεν θα επέλθει ο κίνδυνος, είτε απαιτούνται δυσανάλογες προσπάθειες για την ενημέρωση. Ειδικότερα για την τελευταία περίπτωση, αντί της γνωστοποίησης, γίνεται δημόσια ανακοίνωση ή αναζητείται παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων θα ενημερωθούν με εξίσου αποτελεσματικό τρόπο.

16. Δέσμευση Διοικητικού Συμβουλίου

Το ΔΣ του Σωματείου δεσμεύεται για την αποτελεσματική διαχείριση προστασίας των δεδομένων, μέσω της επιβολής των πολιτικών.

Σε ετήσια βάση, καθορίζονται οι στόχοι για την προστασία των δεδομένων, σε συνδυασμό με το σχεδιασμό του προϋπολογισμού. Αυτό εξασφαλίζει ότι επιτυγχάνεται επαρκής χρηματοδότηση για τη βελτίωση των δραστηριοτήτων που εντοπίζονται.

Σύμφωνα με το Γενικό Κανονισμό Προστασίας Δεδομένων, οι στόχοι των μέτρων προστασίας, οι πολιτικές, οι διαδικασίες και τα τεχνικά μέτρα προστασίας επανεξετάζονται σε τακτά χρονικά διαστήματα και ανάλογα με τα αποτελέσματα της Μελέτης Αποτίμησης Επικινδυνότητας και του Σχεδίου Διαχείρισης Επικινδυνότητας.