ΠΟΛΙΤΙΚΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Πίνακας Περιεχομένων

1. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΚΑΙ ΧΡΗΣΤΕΣ

ΠΟΛΥΤΙΜΗ ΚΑΡΑΝΙΚΑ & ΣΙΑ Ο.Ε., Καλλιρρόης 85, 116423801000, εφεξής η 'Επιχείρηση', επιδιώκει τη συμμόρφωσή της με την νομοθεσία αναφορικά με την προστασία των προσωπικών δεδομένων που εφαρμόζεται οπουδήποτε αναπτύσσει επιχειρηματική δραστηριότητα. Η παρούσα Πολιτική καθορίζει τις θεμελιώδεις αρχές με βάση τις οποίες η Επιχείρηση, υπό την ιδιότητά της ως Υπεύθυνος Επεξεργασίας και κατά περίπτωση ως Εκτελών την Επεξεργασία επεξεργάζεται τα προσωπικά δεδομένα των καταναλωτών, πελατών, προμηθευτών, επιχειρηματικών συνεργατών, υπαλλήλων της καθώς και οποιουδήποτε φυσικού προσώπου που αποτελεί κατά περίπτωση Υποκείμενο Δεδομένων και περιλαμβάνει τις αρμοδιότητες και την ευθύνη των τμημάτων της επιχείρησής του καθώς και των εργαζομένων του στο πλαίσιο των δράσεων επεξεργασίας προσωπικών δεδομένων που εκτελούν ή συμμετέχουν.

2. ΕΓΓΡΑΦΑ ΑΝΑΦΟΡΑΣ

- Ο ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕC, στο εξής 'ΓΚΠΔ'
- Ελληνική νομοθεσία περί προστασίας προσωπικών δεδομένων
- Πολιτική Προστασίας Προσωπικών Δεδομένων Εργαζομένων
- Πολιτική Τήρησης Δεδομένων
- Περιγραφή Θέσης του Υπευθύνου Προστασίας Δεδομένων (DPO)
- Κατευθυντήριες Γραμμές για το Μητρώο Δεδομένων και Δράσεων Επεξεργασίας
- Διαδικασία αίτησης πρόσβασης του υποκειμένου των δεδομένων
- Κατευθυντήριες Γραμμές σχετικά με την διενέργεια εκτίμησης αντικτύπου
- Διαδικασία Διασυνοριακής Ροής Δεδομένων
- Πολιτικές Ασφαλείας Πληροφοριών
- Διαδικασία Γνωστοποίησης Περιστατικού Παραβίασης

3. ΟΡΙΣΜΟΙ

Οι ακόλουθοι ορισμοί που χρησιμοποιούνται στην παρούσα περιλαμβάνονται στο άρθρο 4 του ΓΚΠΔ:

Δεδομένα Προσωπικού Χαρακτήρα: 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 (online) 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.

Ευαίσθητα Προσωπικά Δεδομένα: Τα προσωπικά δεδομένα, τα οποία λόγω της φύσης τους είναι ιδιαιτέρως ευαίσθητα σε σχέση με τα θεμελιώδη δικαιώματα και τις ελευθερίες, αξιώνουν ιδιαίτερη προστασία, καθώς το πλαίσιο της επεξεργασίας τους μπορεί να δημιουργήσει σημαντικούς κινδύνους για τα θεμελιώδη δικαιώματα και τις ελευθερίες. Αυτά τα προσωπικά δεδομένα περιλαμβάνουν πληροφορίες που αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικές απόψεις, θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή συμμετοχή σε συνδικαλιστικές οργανώσεις, γενετικά δεδομένα, βιομετρικά δεδομένα με μόνο σκοπό τον εντοπισμό φυσικού προσώπου, δεδομένα σχετικά με την υγεία ή δεδομένα σχετικά με το φύλο ενός φυσικού προσώπου ζωής ή γενετήσιου προσανατολισμού.

Υπεύθυνος Επεξεργασίας: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας τα οποία, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Εκτελών την Επεξεργασία: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας.

Επεξεργασία: 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.

Ανωνυμοποίηση: Μη αναστρέψιμη εξακρίβωση των προσωπικών δεδομένων, κατά τρόπον ώστε το πρόσωπο να μην μπορεί να αναγνωριστεί χρησιμοποιώντας εύλογο χρόνο, κόστος και τεχνολογία είτε από τον υπεύθυνο επεξεργασίας είτε από οποιοδήποτε άλλο πρόσωπο για να προσδιορίσει το συγκεκριμένο άτομο. Οι αρχές επεξεργασίας δεδομένων προσωπικού χαρακτήρα δεν ισχύουν για ανώνυμα δεδομένα, δεδομένου ότι δεν είναι πλέον δεδομένα προσωπικού χαρακτήρα.

Ψευδωνυμοποίηση: Η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μη 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 οργανικά μέτρα προκειμένου να διασφαλιστεί ότι δε μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Η ψευδωνυμοποίηση μειώνει, αλλά δεν εξαλείφει εντελώς, τη δυνατότητα σύνδεσης προσωπικών δεδομένων με ένα υποκείμενο των δεδομένων. Επειδή τα ψευδωνυμοποιημένα δεδομένα εξακολουθούν να είναι δεδομένα προσωπικού χαρακτήρα, η επεξεργασία των ψευδωνυμοποιημένων δεδομένων πρέπει να συμμορφώνεται με τις αρχές επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Διασυνοριακή επεξεργασία : η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο των δραστηριοτήτων διαφόρων εγκαταστάσεων σε περισσότερα του ενός κράτη μέλη υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση όπου ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι εγκατεστημένος σε περισσότερα του ενός κράτη μέλη ή η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο δραστηριοτήτων μίας μόνης εγκατάστασης υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση αλλά που επηρεάζει ή ενδέχεται να επηρεάσει ουσιωδώς υποκείμενα των δεδομένων σε περισσότερα του ενός κράτη μέλη.

Εποπτική Αρχή: Η Ελληνική Αρχή Προστασίας Προσωπικών Δεδομένων.

Επικεφαλής Εποπτική Αρχή: Η εποπτική αρχή με πρωταρχική ευθύνη για τη διεκπεραίωση μιας δραστηριότητας διασυνοριακής επεξεργασίας δεδομένων, για παράδειγμα όταν ένα υποκείμενο δεδομένων υποβάλλει καταγγελία σχετικά με την επεξεργασία των προσωπικών του δεδομένων. Είναι υπεύθυνη, μεταξύ άλλων, για τη λήψη των κοινοποιήσεων παραβίασης των δεδομένων, για να ενημερώνεται σχετικά με την επικίνδυνη δραστηριότητα επεξεργασίας και θα έχει πλήρη εξουσία όσον αφορά τα καθήκοντά της για την εξασφάλιση της συμμόρφωσης με τις προβλέψεις του ΓΚΠΔ.

Κάθε «τοπική εποπτική αρχή» θα εξακολουθήσει να διατηρεί στην επικράτειά της και θα παρακολουθεί κάθε τοπική επεξεργασία δεδομένων που επηρεάζει τα πρόσωπα στα οποία αναφέρονται τα δεδομένα ή που πραγματοποιείται από ευρωπαίο ή μη υπεύθυνο επεξεργασίας ή τρίτης χώρας, όταν η επεξεργασία στοχεύει σε υποκείμενα δεδομένων που κατοικούν στην επικράτειά του . Τα καθήκοντα και οι αρμοδιότητές της περιλαμβάνουν τη διεξαγωγή ερευνών και την εφαρμογή διοικητικών μέτρων και προστίμων, την ευαισθητοποίηση του κοινού σχετικά με τους κινδύνους, τους κανόνες, την ασφάλεια και τα δικαιώματα σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την πρόσβαση σε όλες τις εγκαταστάσεις του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία, συμπεριλαμβανομένου οποιουδήποτε εξοπλισμού και μέσων επεξεργασίας δεδομένων.

"Κύρια εγκατάσταση του υπευθύνου επεξεργασίας" με εγκατάσταση σε περισσότερα του ενός κράτη μέλη, νοείται ο τόπος της κεντρικής διοικήσεως του εντός της Ένωσης, εκτός αν οι αποφάσεις περί τους σκοπούς και τους τρόπους επεξεργασίας λαμβάνονται σε διαφορετική εγκατάσταση του υπευθύνου εντός της Ένωσης και η τελευταία αυτή εγκατάσταση έχει τέτοιου είδους εξουσία στην επιβολή αποφάσεων ώστε να θεωρείται αυτή η κύρια εγκατάστασή του.

"Κύρια εγκατάσταση του εκτελούντος την επεξεργασία" με εγκατάσταση σε περισσότερα του ενός κράτη μέλη, νοείται ο τόπος της κεντρικής διοικήσεως του εντός της Ένωσης, ή, σε περίπτωση που ο εκτελών δεν έχει κεντρική διοίκηση εντός της Ένωσης, νοείται η εγκατάσταση του εκτελούντος στην Ένωση όπου λαμβάνουν χώρα οι κύριες δραστηριότητες επεξεργασίας στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης εκτελούντος, στο βαθμό που ο εκτελών την επεξεργασία υπόκειται σε συγκεκριμένες υποχρεώσεις υπό το πρίσμα του Κανονισμού.

4. ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η Επιχείρηση υπό την ιδιότητά του ως Υπεύθυνος Επεξεργασίας ή Εκτελών την Επεξεργασία κατά περίπτωση εκτελεί τις δράσεις επεξεργασίας προσωπικών δεδομένων - με βάσει τις κατωτέρω αρχές που πρέπει να διέπουν τις δράσεις επεξεργασίας προσωπικών δεδομένων.

4.1. ΝΟΜΙΜΟΤΗΤΑ, ΑΝΤΙΚΕΙΜΕΝΙΚΟΤΗΤΑ, ΔΙΑΦΑΝΕΙΑ

Τα προσωπικά δεδομένα υποβάλλονται σε σύννομη, θεμιτή και διαφανή επεξεργασία σε σχέση με το υποκείμενο των δεδομένων.

4.2. ΠΕΡΙΟΡΙΣΜΟΣ ΤΟΥΣ ΣΚΟΠΟΥ

Τα προσωπικά δεδομένα συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς.

4.3. ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Τα προσωπικά δεδομένα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στο μέτρο του αναγκαίου σε συνάρτηση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία. Η Επιχείρηση εφαρμόζει μεθόδους ανωνυμοποίησης και ψευδωνυμοποίησης στα προσωπικά δεδομένα που επεξεργάζεται στο μέτρο του εφικτού προκειμένου να μειώνει τους κινδύνους που αφορούν τα υποκείμενα των δεδομένων λόγω της επεξεργασίας.

4.4. ΑΚΡΙΒΕΙΑ

Τα προσωπικά δεδομένα πρέπει να είναι και να διατηρούνται ακριβή και εφόσον είναι αναγκαίο να επικαιροποιούνται. Η Επιχείρηση λαμβάνει όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα που είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας.

4.5. ΠΕΡΙΟΡΙΣΜΟΣ ΤΗΣ ΠΕΡΙΟΔΟΥ ΑΠΟΘΗΚΕΥΣΗΣ

Τα προσωπικά δεδομένα διατηρούνται μόνο για το χρονικό διάστημα που είναι αναγκαίο για τους σκοπούς της επεξεργασίας τους.

4.6. ΑΚΕΡΑΙΟΤΗΤΑ ΚΑΙ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Λαμβάνοντας υπόψη τα μέτρα ασφαλείας που παρέχει η τεχνολογία καθώς και τα λοιπά διαθέσιμα μέτρα ασφαλείας, το κόστος εφαρμογής τους καθώς και την πιθανότητα επέλευσης αλλά και την σοβαρότητα των κινδύνων για τα προσωπικά δεδομένα, η Επιχείρηση χρησιμοποιεί κατάλληλα τεχνικά και οργανωτικά μέτρα κατά την επεξεργασία των Προσωπικών Δεδομένων ώστε να είναι σε θέση να εγγυηθεί την ενδεδειγμένη ασφάλεια τους, συμπεριλαμβανομένης της προστασίας τους από τυχαία ή παράνομη καταστροφή, απώλεια, μετατροπή, μη εξουσιοδοτημένη πρόσβαση ή κοινοποίηση.

4.7. ΛΟΓΟΔΟΣΙΑ

Η Επιχείρηση είναι υπεύθυνη για την τεκμηρίωση και την απόδειξη της συμμόρφωσή του με τις ανωτέρω αρχές επεξεργασίας.

5. ΕΦΑΡΜΟΓΗ ΜΕΤΡΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ ΕΠΙΧΕΙΡΗΜΑΤΙΚΗΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ

Η Επιχείρηση εφαρμόζει πολιτικές, διαδικασίες και μέτρα για την προστασία των προσωπικών δεδομένων κατά την επεξεργασία στο πλαίσιο της επιχειρηματικής του δραστηριότητας.

5.1. ΕΝΗΜΕΡΩΣΗ ΥΠΟΚΕΙΜΕΝΟΥ

(Βλ. Ενότητα: Κατευθυντήριες Γραμμές Επεξεργασίας)

5.2. ΔΙΚΑΙΩΜΑ ΕΠΙΛΟΓΗΣ ΚΑΙ ΣΥΓΚΑΤΑΘΕΣΗ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ

(Βλ. Ενότητα: Κατευθυντήριες Γραμμές Επεξεργασίας)

5.3. ΣΥΛΛΟΓΗ

Η Επιχείρηση συλλέγει τον ελάχιστο δυνατό όγκο προσωπικών δεδομένων. Στην περίπτωση που τα προσωπικά δεδομένα συλλέγονται από τρίτο, ο *Διαχειριστής ΙΤ* πρέπει να διασφαλίζει τη σύννομή συλλογή των προσωπικών δεδομένων.

5.4. ΧΡΗΣΗ, ΔΙΑΤΗΡΗΣΗ ΚΑΙ ΔΙΑΘΕΣΗ

Οι σκοποί, οι μέθοδοι, ο περιορισμός περιόδου αποθήκευσης και διατήρησης των προσωπικών δεδομένων πρέπει να είναι σε συμμόρφωση με τις πληροφορίες που περιέχονται στην Ενημέρωση περί Απορρήτου. Η Επιχείρηση οφείλει να διατηρεί την ακρίβεια, ακεραιότητα, εμπιστευτικότητα και συνάφεια των προσωπικών δεδομένων με βάση το σκοπό επεξεργασίας. Πρέπει να χρησιμοποιούνται επαρκείς μηχανισμοί ασφάλειας σχεδιασμένοι να προστατεύουν τα προσωπικά δεδομένα ώστε να παρεμποδίζεται η κλοπή, η κακή χρήση, η κατάχρηση των προσωπικών δεδομένων και να εμποδίζονται οι παραβιάσεις τους. Ο *Διαχειριστής ΙΤ* φέρει την ευθύνη συμμόρφωσης με τις υποχρεώσεις που απαριθμούνται σε αυτή την ενότητα.

5.5. ΚΟΙΝΟΠΟΙΗΣΗ ΣΕ ΤΡΙΤΟΥΣ

Κάθε φορά που η Επιχείρηση χρησιμοποιεί τρίτο προμηθευτή ή επιχειρηματικό συνέταιρο για να επεξεργαστεί προσωπικά δεδομένα για λογαριασμό της, ο *Διαχειριστής ΙΤ* οφείλει να διασφαλίζει ότι ο συγκεκριμένος εκτελών την επεξεργασία εφαρμόζει επαρκή μέτρα και πολιτικές για την προστασίας των προσωπικών δεδομένων και παρέχει επαρκείς εγγυήσεις για την συμμόρφωσή του με τον ΓΚΠΔ. Για το σκοπό αυτό συστήνεται η χρήση σχετικού ερωτηματολογίου για τον έλεγχο συμμόρφωσης.

Η Επιχείρηση οφείλει να απαιτεί συμβατικά από τους συνεργάτες της – π.χ. προμηθευτές, επιχειρηματικοί εταίροι – να παρέχουν το ίδιο επίπεδο προστασίας των προσωπικών δεδομένων με αυτό που παρέχει η ίδια στα υποκείμενα. Οι συνεργάτες της Επιχείρησης οφείλουν να επεξεργάζονται τα προσωπικά δεδομένα στο πλαίσιο και σε συμμόρφωση με τις συμβατικές υποχρεώσεις που ανέλαβαν έναντι της Επιχείρησης ή μόνο υπό την καθοδήγησή της και όχι για οποιονδήποτε περαιτέρω σκοπό. Όταν η Επιχείρηση επεξεργάζεται προσωπικά δεδομένα από κοινού με ένα τρίτο μέρος εκτός επιχείρησης, η

Επιχείρηση οφείλει να προσδιορίζει ρητώς τις αρμοδιότητες, τα καθήκοντα, τις υποχρεώσεις και ως εκ τούτου και το πεδίο ευθύνης του τρίτου αυτού προσώπου στην σχετική σύμβαση ή με οποιοδήποτε άλλο δεσμευτικό έγγραφο νομικώς δεσμευτικό έγγραφο.

5.6. ΔΙΑΣΥΝΟΡΙΑΚΗ ΡΟΗ

Η Επιχείρηση αναγνωρίζει ότι η διαβίβαση προσωπικών δεδομένων εκτός της Ευρωπαϊκής Ένωσης και των λοιπών κρατών που υπάγονται στην Ευρωπαϊκή Οικονομική Ζώνη (ΕΟΖ) εμπίπτει σε ειδικούς κανόνες προκειμένου να διασφαλίζεται επαρκές επίπεδο προστασίας των προσωπικών δεδομένων κατά την επεξεργασία τους. Τα μέτρα που θα λαμβάνονται θα αποφασίζονται κατά περίπτωση και θα είναι σε συμμόρφωση με τα προβλεπόμενα στον ΓΚΠΔ και την εφαρμοστέα νομοθεσία.

5.7. ΔΙΚΑΙΩΜΑ ΠΡΟΣΒΑΣΗΣ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ

Η Επιχείρηση, όταν ενεργεί ως υπεύθυνος επεξεργασίας οφείλει να εφαρμόζει διαδικασίες και μηχανισμούς προκειμένου να παρέχει στα υποκείμενα των δεδομένων πρόσβαση στα προσωπικά τους δεδομένα, την δυνατότητα να τα επικαιροποιούν, να τα διορθώνουν, να τα διαγράφουν στο βαθμό που δεν αντίκειται σε διάταξη νόμου ή στην συμμόρφωση της Επιχείρησης με νόμιμη υποχρέωσή της. Ο μηχανισμός πρόσβασης αναπτύσσεται λεπτομερώς στη Διαδικασία Αίτησης Πρόσβασης των Υποκειμένων.

5.8. ΦΟΡΗΤΟΤΗΤΑ ΔΕΔΟΜΕΝΩΝ

Τα Υποκείμενα των δεδομένων έχουν δικαίωμα να λαμβάνουν κατόπιν αιτήσεώς τους αντίγραφο των δεδομένων που παρείχαν στην Επιχείρηση σε δομημένο μορφότυπο καθώς και να τα μεταφέρονται τα δεδομένα τους σε άλλο υπεύθυνο επεξεργασίας άνευ ανταλλάγματος. Ο *Διαχειριστής ΙΤ* φέρει την ευθύνη να διασφαλίζει ότι τέτοιου είδους αιτήματα θα διεκπεραιώνονται εντός ενός (1) μήνα και ότι είναι εύλογα π.χ. ότι δεν είναι υπερβολικά ή ότι δεν επηρεάζουν δυσμενώς τα δικαιώματα προστασίας προσωπικών δεδομένων άλλων φυσικών προσώπων.

5.9. ΔΙΚΑΙΩΜΑ ΣΤΗ ΛΗΘΗ

Τα υποκείμενα δεδομένων έχουν το δικαίωμα να ζητήσουν από την Επιχείρηση τη διαγραφή των προσωπικών τους δεδομένων. Όταν η Επιχείρηση ενεργεί ως υπεύθυνος επεξεργασίας, ο *Διαχειριστής ΙΤ* πρέπει να λάβει τα απαραίτητα οργανωτικά και τεχνικά μέτρα για να ενημερώσει ανάλογα τους τρίτους που χρησιμοποιούν ή επεξεργάζονται τα δεδομένα αυτά ώστε να συμμορφωθούν με το αίτημα.

6. ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Τα προσωπικά δεδομένα υφίστανται επεξεργασία κατά την ρητή εξουσιοδότηση του *Διαχειριστής ΙΤ.*

Η Επιχείρηση οφείλει να αποφασίζει αν θα διεξάγει εκτίμηση αντικτύπου σχετικά με την προστασία των προσωπικών δεδομένων για κάθε δραστηριότητα επεξεργασίας σύμφωνα με τις σχετικές κατευθυντήριες γραμμές για την διεξαγωγή εκτίμησης αντικτύπου τις οποίες συμβουλεύεται και εφαρμόζει.

6.1. ΕΝΗΜΕΡΩΣΗ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ

Πριν ή κατά τη διάρκεια της συλλογής προσωπικών δεδομένων αναφορικά με οποιαδήποτε δράση επεξεργασίας, όπως π.χ. πώληση προϊόντων και παροχή υπηρεσιών ή ενεργειών προώθησης, *Διαχειριστής IT* είναι υπεύθυνος για την κατάλληλη ενημέρωση των υποκειμένων των δεδομένων αναφορικά με τα ακόλουθα:

- τις κατηγορίες προσωπικών δεδομένων που συλλέγονται,
- τους σκοπούς της επεξεργασίας,
- τις μεθόδους επεξεργασίας,
- τα δικαιώματα των υποκειμένων σε σχέση με τα προσωπικά τους δεδομένα,
- την περίοδο διατήρησής τους,
- το ενδεχόμενο διεθνούς διαβίβασης των δεδομένων, αν τα δεδομένα κοινοποιούνται και σε τρίτους και
- τα μέτρα που εφαρμόζει η Επιχείρηση την εξασφάλιση της προστασίας των προσωπικών δεδομένων.

Η Επιχείρηση ακολουθεί κατάλληλη διαδικασία ενημέρωσης ανάλογα μα τη δραστηριότητα επεξεργασίας και τις κατηγορίες προσωπικών δεδομένων που συλλέγονται και τυγχάνουν επεξεργασίας, η οποία διαφοροποιείται κατά περίπτωση.

Όταν τα προσωπικά δεδομένα κοινοποιούνται και σε τρίτους, ο *Διαχειριστής IT* πρέπει να διασφαλίζει ότι τα υποκείμενα έχουν ενημερωθεί κατάλληλα.

Σε περίπτωση που ενδέχεται να πραγματοποιηθεί διαβίβαση προσωπικών δεδομένων σε τρίτη χώρα η σχετική ενημέρωση πρέπει να περιλαμβάνει την οντότητα στην οποία θα διαβιβαστούν και τον τόπο και δικαιοδοσία που την διέπει.

Όπου συλλέγονται ευαίσθητα δεδομένα προσωπικού χαρακτήρα, ο *Διαχειριστής IT* διασφαλίζει ότι η σχετική ενημέρωση περί Απορρήτου περιλαμβάνει ρητά τους σκοπούς για τους οποίους συλλέγονται.

6.2. ΛΗΨΗ ΣΥΓΚΑΤΑΘΕΣΗΣ

Όταν η επεξεργασία προσωπικών δεδομένων βασίζεται στη συγκατάθεση του υποκειμένου, ο *Διαχειριστής IT* έχει την αρμοδιότητα τήρησης του αρχείου που περιλαμβάνει αυτού του είδους τις συγκαταθέσεις κατά τέτοιο τρόπο ώστε να είναι δυνατή η απόδειξη της σύννομης λήψης της. Ο *Διαχειριστής IT* είναι υπεύθυνος να παρέχει εναλλακτικούς τρόπους χορήγησης της συγκατάθεσης στα υποκείμενα των δεδομένων και να τα ενημερώνει ότι η συγκατάθεση μπορεί οποτεδήποτε να ανακληθεί, διασφαλίζοντας έναν τρόπο ανάκλησης εξίσου εύκολο με τον τρόπο αρχικής λήψης της.

Σε περιπτώσεις που η λήψη της σχετίζεται με παιδί ηλικίας κάτω των 16 ετών, ο *Διαχειριστής IT* οφείλει να διασφαλίζει ότι δόθηκε πριν από τη συλλογή η συγκατάθεση του γονέα χρησιμοποιώντας στη Φόρμα Συγκαταθέσεως του Γονέα. Σε αυτή την περίπτωση, η Επιχείρηση οφείλει να καταβάλλει κάθε εύλογη προσπάθεια προκειμένου να διαπιστώσει ότι η παρεχόμενη συγκατάθεση δίδεται από τον πρόσωπο που έχει την επιμέλεια του παιδιού, αξιοποιώντας τα διαθέσιμα τεχνολογικά μέσα.

Στις περιπτώσεις αιτημάτων διορθώσεως, τροποποίησης ή καταστροφής αρχείων προσωπικών δεδομένων, ο *Διαχειριστής IT* πρέπει να διασφαλίζει ότι τα αιτήματα αυτά διεκπεραιώνονται εντός εύλογου χρονικού διαστήματος που δεν θα ξεπερνά τον ένα μήνα από την παραλαβή του αιτήματος. Η προθεσμία αυτή μπορεί να παραταθεί κατά δύο (2) ακόμη μήνες λαμβάνοντας υπόψιν την πολυπλοκότητα του αιτήματος ή/ και του αριθμού των αιτημάτων υπό την προϋπόθεση ότι το υποκείμενο θα ενημερωθεί ειδικά και τεκμηριωμένα. Ο *Διαχειριστής IT* οφείλει να καταγράφει και να τηρεί σε αρχείο τα αιτήματα αυτά.

Τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία μόνο για τον σκοπό για τον οποίο συλλέχθηκαν αρχικά. Σε περίπτωση που η Επιχείρηση επιθυμεί να επεξεργαστεί τα συλλεχθέντα προσωπικά δεδομένα για άλλο σκοπό, πρέπει να ζητήσει τη συγκατάθεση των υποκειμένων των δεδομένων της με σαφή και συνοπτικό τρόπο. Κάθε τέτοιο αίτημα πρέπει να περιλαμβάνει τον αρχικό σκοπό για τον οποίο συλλέχθηκαν τα δεδομένα, καθώς και τον νέο ή πρόσθετο σκοπό. Η αίτηση πρέπει επίσης να περιλαμβάνει την αιτιολογία για τη μεταβολή του σκοπού. Ο *Διαχειριστής IT* είναι υπεύθυνος για τη συμμόρφωση με τους κανόνες της παρούσας παραγράφου καθώς και την διασφάλιση ότι οι μέθοδοι συλλογής συμμορφώνονται με το σχετικό δίκαιο, τις ορθές πρακτικές και τα πρότυπα του κλάδου.

7. ΟΡΓΑΝΩΣΗ ΚΑΙ ΕΥΘΥΝΕΣ

Η ευθύνη για τη διασφάλιση της κατάλληλης επεξεργασίας των προσωπικών δεδομένων ανήκει σε όλους όσους εργάζονται για ή με την Επιχείρηση και έχουν πρόσβαση σε προσωπικά δεδομένα που επεξεργάζεται η Επιχείρηση.

Οι κύριοι τομείς αρμοδιοτήτων για την επεξεργασία προσωπικών δεδομένων έχουν τους ακόλουθους οργανωτικούς ρόλους:

Τα **αρμόδια όργανα για την διοίκηση της Επιχείρησης και οι διευθυντές** [Τένια Καρανίκα, Αντώνιος Δάσκος].

Ο **αρμόδιος για την διαχείριση των δεδομένων ή κάθε άλλος εργαζόμενος που αναλαμβάνει σχετικές αρμοδιότητες,** είναι υπεύθυνος για τη διαχείριση του προγράμματος προστασίας προσωπικών δεδομένων και για την ανάπτυξη και προώθηση ολοκληρωμένων πολιτικών προστασίας, όπως αυτές περιγράφονται στην Περιγραφή θέσης του προσώπου αυτού.

Το Νομικό Τμήμα μαζί με τον Αρμόδιο για την διαχείριση Δεδομένων παρακολουθεί και αναλύει το δίκαιο των προσωπικών δεδομένων και τις αλλαγές στους κανονισμούς και την νομοθεσία, αναπτύσσει τις προϋποθέσεις συμμορφώσεως, και βοηθά τα επιχειρηματικά τμήματα να επιτύχουν τους στόχους σχετικά με την προστασία των προσωπικών δεδομένων.

Ο **διαχειριστής IT,** φέρει την ευθύνη για:

- Την εξασφάλιση ότι όλα τα συστήματα, οι υπηρεσίες και ο εξοπλισμός που χρησιμοποιούνται για την αποθήκευση δεδομένων πληρούν αποδεκτά πρότυπα ασφαλείας.
- Την εκτέλεση τακτικών ελέγχων και σαρώσεων για να διασφαλίζεται ότι το υλικό και το λογισμικό ασφαλείας λειτουργούν σωστά.

Ο **υπεύθυνος Διαφήμισης/ προώθησης**, είναι υπεύθυνος για :

• Την έγκριση των δηλώσεων προστασίας δεδομένων που επισυνάπτονται σε επικοινωνίες, όπως μηνύματα ηλεκτρονικού ταχυδρομείου και επιστολές.

• Την αντιμετώπιση τυχόν ερωτημάτων προστασίας δεδομένων από δημοσιογράφους ή μέσα μαζικής ενημέρωσης, όπως εφημερίδες.

• Όπου είναι απαραίτητο, τη συνεργασία με τον υπεύθυνο προστασίας δεδομένων για να εξασφαλιστεί ότι οι πρωτοβουλίες μάρκετινγκ θα τηρούν τις αρχές προστασίας δεδομένων.

Ο **υπεύθυνος Ανθρώπινου Δυναμικού** είναι υπεύθυνος για:

• τη βελτίωση της ευαισθητοποίησης όλων των εργαζομένων σχετικά με την προστασία των προσωπικών δεδομένων των χρηστών.

• την οργάνωση εμπειρογνωμοσύνης για την προστασία των προσωπικών δεδομένων και κατάρτιση ευαισθητοποίησης των εργαζομένων που εργάζονται με προσωπικά δεδομένα.

• την προστασία προσωπικών δεδομένων των εργαζομένων από άκρο σε άκρο. Πρέπει να εξασφαλίζει ότι τα προσωπικά δεδομένα των εργαζομένων θα υποβάλλονται σε επεξεργασία με βάση τους νόμιμους επιχειρηματικούς σκοπούς και την αναγκαιότητα του εργοδότη.

Ο Διευθυντής Προμηθειών είναι υπεύθυνος για τη μεταβίβαση αρμοδιοτήτων προστασίας των προσωπικών δεδομένων στους προμηθευτές και τη βελτίωση των επιπέδων ευαισθητοποίησης των προμηθευτών σχετικά με την προστασία των προσωπικών δεδομένων, καθώς και τη μείωση των απαιτήσεων προσωπικών δεδομένων προς οποιοδήποτε τρίτο προμηθευτή που χρησιμοποιούν. Το Τμήμα Προμηθειών πρέπει να διασφαλίζει ότι η Εταιρεία διατηρεί το δικαίωμα να ελέγχει τους προμηθευτές.

7.1. ΚΑΤΕΥΘΥΝΤΥΡΙΕΣ ΓΡΑΜΜΕΣ ΓΙΑ ΤΟΝ ΚΑΘΟΡΙΣΜΟ ΤΗΣ ΕΠΙΚΕΦΑΛΗΣ ΑΡΧΗΣ ΕΠΟΠΤΕΙΑ

Ο προσδιορισμός μιας επικεφαλής εποπτικής αρχής είναι σημαντικός μόνο εάν η Επιχείρηση διεξάγει τη διασυνοριακή επεξεργασία προσωπικών δεδομένων.

Η διασυνοριακή διαβίβαση δεδομένων προσωπικού χαρακτήρα πραγματοποιείται εάν:

(α) η επεξεργασία προσωπικών δεδομένων πραγματοποιείται από θυγατρικές της Εταιρείας που εδρεύουν σε άλλα κράτη μέλη, ή

(β) η επεξεργασία προσωπικών δεδομένων πραγματοποιείται σε μια ενιαία εγκατάσταση της Επιχείρησης στην Ευρωπαϊκή Ένωση αλλά επηρεάζει ουσιαστικά ή ενδέχεται να επηρεάσει ουσιωδώς τα υποκείμενα των δεδομένων σε περισσότερα του ενός κράτη μέλη.

Εάν η Επιχείρηση έχει εγκαταστάσεις μόνο σε ένα κράτος μέλος και οι δραστηριότητες επεξεργασίας της αφορούν μόνο τα πρόσωπα που αφορούν τα δεδομένα σε αυτό το κράτος μέλος, δεν υπάρχει λόγος να συσταθεί η κύρια εποπτική αρχή. Η μόνη αρμόδια αρχή θα είναι η Εποπτική Αρχή της χώρας όπου η Εταιρεία είναι νόμιμα εγκατεστημένη.

8. ΑΝΤΑΠΟΚΡΙΣΗΣ ΣΕ ΠΕΡΙΣΤΑΤΙΚΑ ΠΑΡΑΒΙΑΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Εάν η Επιχείρηση ενημερωθεί για περιστατικά ή υποψία παραβίασης προσωπικών δεδομένων, ο *διαχειριστής IT* πρέπει να διενεργήσει εσωτερικό έλεγχο και να λάβει τα κατάλληλα διορθωτικά μέτρα εγκαίρως, σύμφωνα με την Πολιτική Παραβίασης Ασφάλειας Δεδομένων. Εφόσον διαπιστωθεί ότι υφίσταται κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, η Επιχείρηση οφείλει να ενημερώσει τις αρμόδιες αρχές προστασίας δεδομένων χωρίς αδικαιολόγητη καθυστέρηση και, εφόσον είναι δυνατόν, εντός 72 ωρών.

9. ΑΞΙΟΛΟΓΗΣΗ ΚΑΙ ΕΛΕΓΧΟΣ

Την ευθύνη για τον έλεγχο και την αξιολόγηση της τήρησης και εφαρμογής της παρούσας πολιτικής φέρει ο *διαχειριστής IT.*

Πιθανή παραβίαση της παρούσας πολιτικής από εργαζόμενο της Επιχείρησης μπορεί να επιφέρει πειθαρχικές ποινές καθώς και αστικές και ποινικές ευθύνες στο βαθμό που παραβιάζονται και διατάξεις της ισχύουσας νομοθεσίας.

10. ΕΓΚΥΡΟΤΗΤΑ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΕΓΓΡΑΦΩΝ

Το παρόν έγγραφο ισχύει από 20 Ιανουαρίου 2021 και δημοσιεύεται ως εξής:

Το αρμόδιο πρόσωπο για την διαχείριση του εγγράφου αυτού είναι ο *διαχειριστής IT* ο οποίος πρέπει να ελέγχει και, αν είναι απαραίτητο, να επικαιροποιεί το έγγραφο τουλάχιστον μία φορά το χρόνο.